Configuring the Wireless Array

The following topics include procedures for configuring the Array using the product's embedded Web Management Interface (WMI). Procedures have been organized into functional areas that reflect the flow and content of the WMI.

The following WMI windows allow you to establish configuration parameters for your Array, and include:

- **"Express Setup" on page 159**
- **"Network" on page 165**
- **"Services" on page 179**
- **"VLANs" on page 204**
- **"Tunnels" on page 209**
- **"Security" on page 213**
- **"SSIDs" on page 254**
- **"Groups" on page 280**
- **"IAPs" on page 287**
- **"WDS" on page 358**
- **"Filters" on page 365**
- **"Clusters" on page 374**
- **"Mobile" on page 380**

After making changes to the configuration settings of an Array you must click the **Save** button at the top of the configuration window, otherwise the changes you make will not be applied the next time the Array is rebooted.

Some settings are only available if the Array's license includes appropriate features. If a setting is unavailable (grayed out), then your license does not support the feature. See ***"About Licensing and Upgrades" on page 387****.*

Note that the **Configuration** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See Figure 39 on page 86.)

This chapter only discusses using the configuration windows on the Array. To view status or use system tools on the Array, please see:

- **"Viewing Status on the Wireless Array" on page 91**
- **"Using Tools on the Wireless Array" on page 385**

Express Setup

Initial Array configuration via XMS sets items such as SSIDs and security, as described in "Zero-Touch Provisioning and Ongoing Management" on page 69. This page allows you to see many of these values, or change them locally.

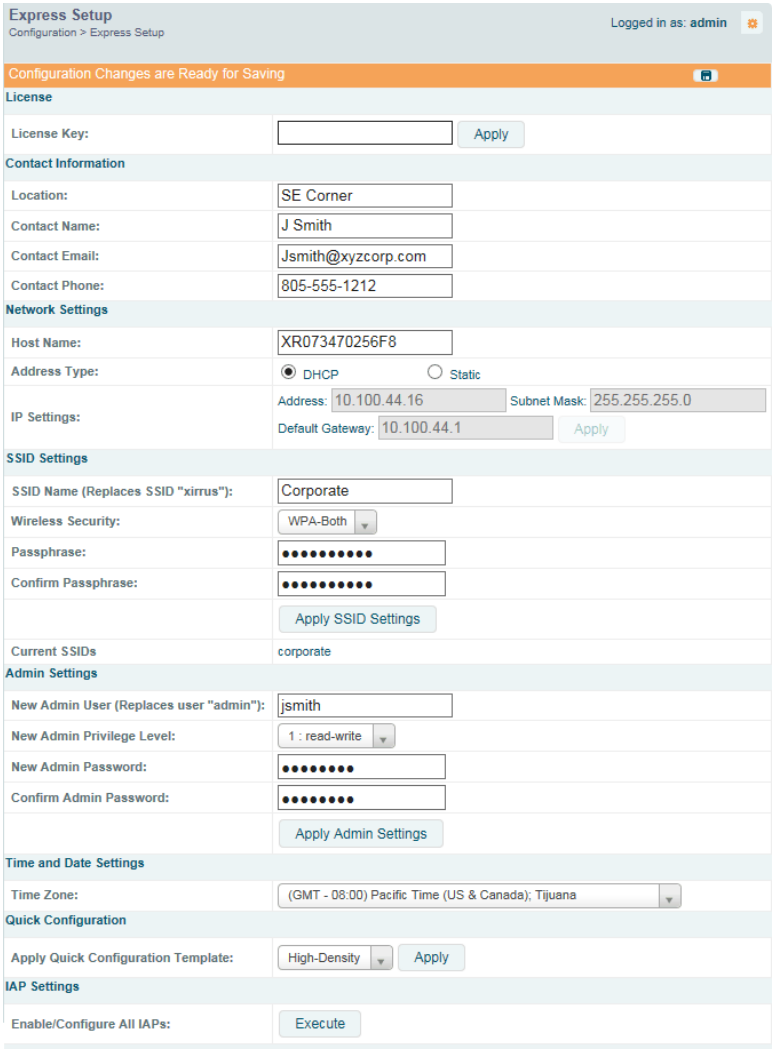


Figure 95. WMI: Express Setup

When finished, click the **Save** button if you wish to make your changes permanent.

Procedure for Performing an Express Setup

1. **License Key**: An unlicensed Array will automatically contact Xirrus to obtain its license, if it has Internet connectivity. If you need to enter a license manually, enter it here. See "Licensing" on page 74.
2. Configure the **Contact Information** settings.
   a. **Location**: Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
   b. **Contact Name**: Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
   c. **Contact Email**: Enter the email address of the admin contact you entered in Step 3.
   d. **Contact Phone**: Enter the telephone number of the admin contact you entered in Step 3.
3. Configure the **Network** settings. Please see "Network Interfaces" on page 166 for more information.
   a. **Host Name**: Specify a unique host name for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is the Array's serial number.
   b. **Address Type**: Choose **DHCP** to instruct the Array to use DHCP to assign IP addresses to the Array's Ethernet interfaces, or choose **Static** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following **IP Settings**:
   c. **IP Settings**: If you choose the **Static** IP addressing option, enter the following:

- **Address**: Enter a valid IP address for this Array. To use a remote connection (Web, SNMP, or SSH), a valid IP address must be used.
- **Subnet Mask**: Enter a valid IP address for the subnet mask (the default is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
- **Default Gateway**: Enter a valid IP address for the default gateway. This is the IP address of the router that the Array uses to forward data to other networks.
- Click the **Apply** button for this interface when done making IP changes.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the Array" on page 76.

4. **SSID Settings**: This section specifies the wireless network name and security settings.
   a. **SSID Name** is a unique name that identifies a wireless network. The default SSID is **xirrus**. Entering a value in this field will replace the this default SSID with the new name.

      For additional information about SSIDs, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 492.

   b. **Wireless Security**: Select the desired wireless security scheme (Open, WEP or WPA). Make your selection from the choices available in the pull-down list.

      - **Open**—This option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
      - **WEP** (Wired Equivalent Privacy)—An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both

source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

- **WPA** (Wi-Fi Protected Access)—A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1x for authentication. WPA is the stronger of the two wireless security schemes.
- **WPA2** (Wi-Fi Protected Access 2)—WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.
- **WPA-Both** (WPA and WPA2)—This option makes use of both WPA and WPA2.

For more information about security, including a full review of all security options and settings, go to "Understanding Security" on page 214.

c. **WEP Encryption Key/WPA Passphrase**: Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase. This field and the one below only appear if you select a **Wireless Security** option other than **Open**.

d. **Confirm Encryption Key/Passphrase**: If you entered a WEP key or WPA passphrase, confirm it here.

e. Click **Apply SSID Settings** when done.

f. **Current SSIDs**: This lists all of the currently defined SSIDs for you (regardless of whether they are enabled or not).

5. **Admin Settings:** This section allows you to change the default admin username, password, and privileges for the Array. You may change the password and leave the user name as is, but we suggest that you change both to improve Array security.

   a. **New Admin User (Replaces user "admin")**: Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the Array also offers the option of authenticating administrators using a RADIUS server (see "Admin Management" on page 219)).

   b. **New Admin Privilege Level**: By default, the new administrator will have read/write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see "Admin Privileges" on page 221. Take care to make sure to leave yourself enough read/write privileges on at least one account to be able to administer the Array.

   c. **New Admin Password**: Enter a new administration password for managing this Array. If you forget this password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).

   d. **Confirm Admin Password**: If you entered a new administration password, confirm the new password here.

   e. Click **Apply Admin Settings** when done.

6. **Time and Date Settings:** System time is synchronized using NTP (Network Time Protocol) by default. Use the pull-down menu to select the **Time Zone**.

7. **Quick Configuration:** This offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate

to your deployment, select it and click **Apply**. For example, the **High-Density** option uses best practices to configure the Array for high density settings such as lecture halls, convention centers, stadiums, etc.

8. **IAP Settings:**

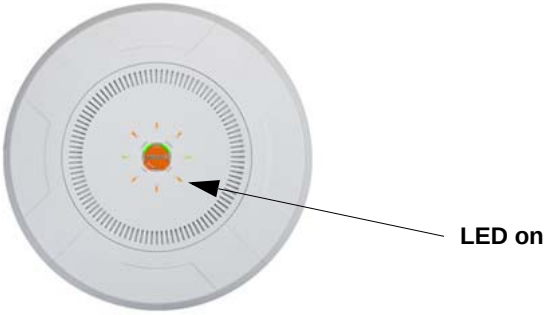


Figure 96. LEDs are Switched On

Enable/Configure All IAPs: Click on the **Execute** button to enable and auto configure all IAPs (a message displays the countdown time—in seconds—to complete the auto-configuration task). When an IAP is enabled, its LED is switched on.

9. Click the **Save** button at the upper right to make your changes permanent, i.e., these settings will still be in effect after a reboot.

Network

This is a status-only window that provides a snapshot of the configuration settings currently established for the Ethernet interfaces. DNS Settings and CDP Settings (Cisco Discovery Protocol) are summarized as well. You must go to the appropriate configuration window to make changes to any of the settings displayed here (configuration changes cannot be made from this window). You can click on any item in the **Interface** column to "jump" to the associated configuration window.

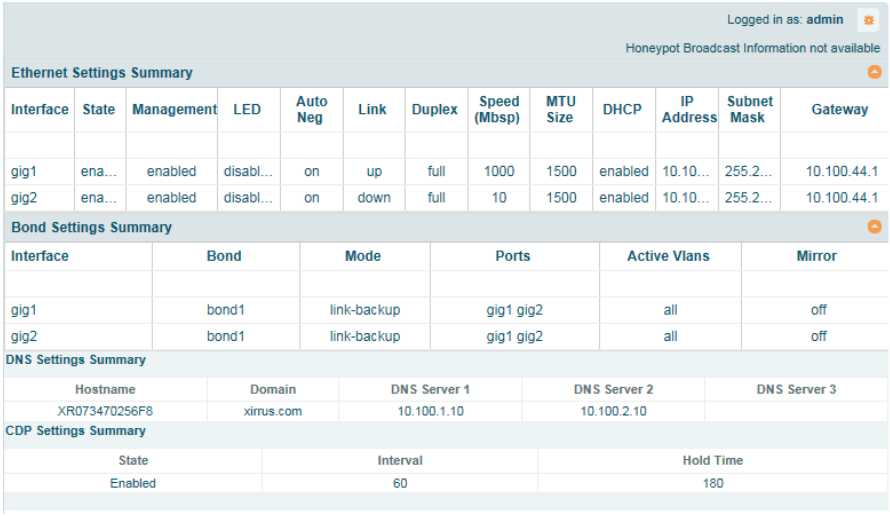


Figure 97. Network Interfaces

WMI windows that allow you to change or view configuration settings associated with the network interfaces include:

- "Network Interfaces" on page 166
- "Bonds and Bridging" on page 169
- "DNS Settings" on page 176
- "CDP Settings" on page 177

See Also

DNS Settings
Network Interfaces
Network Status Windows
Spanning Tree Status
Network Statistics

Network Interfaces

XR-500, XR-1000, and some XR-2000 Series Arrays have one Gigabit Ethernet interface, while XR- 600, XR-4000 and some XR-2000 Series Arrays have two, and XR-6000 Series models have four. This window allows you to establish configuration settings for these interfaces.

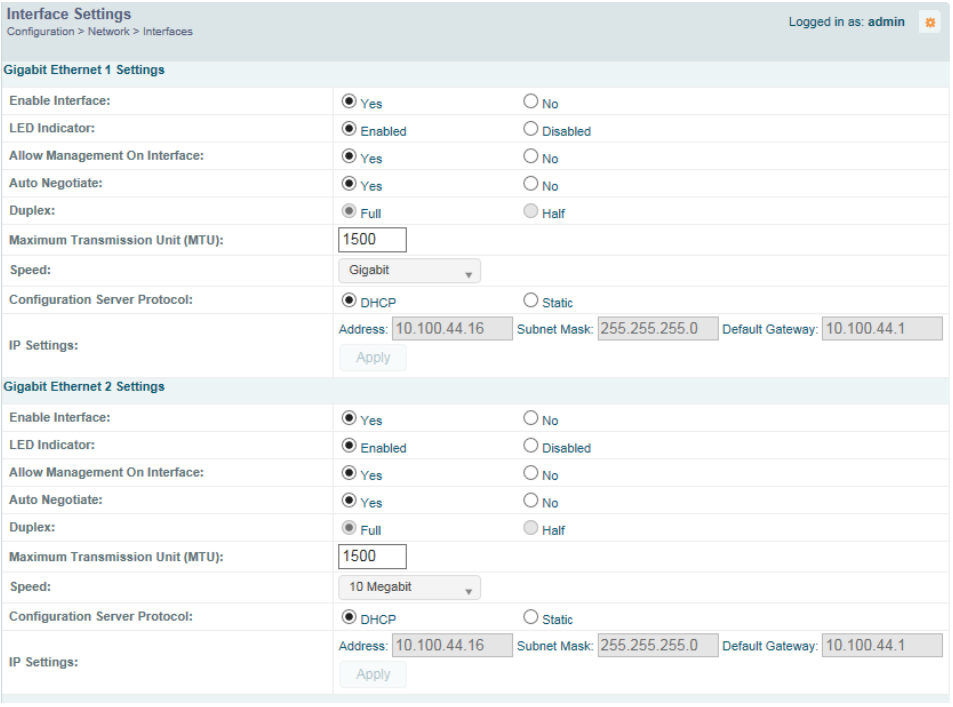


Figure 98. Network Settings

When finished making changes, click the **Save** button if you wish to make your changes permanent. When the status of a port changes, a Syslog entry is created describing the change.

Network Interface Ports

For the location of network interface ports on the underside of an XR Series Array, see the illustrations starting with Figure 32 on page 71.

Procedure for Configuring the Network Interfaces

Configure the **Gigabit** network interfaces. The fields for each of these interfaces are the same, and include:

1. **Enable Interface:** Choose **Yes** to enable this network interface, or choose No to disable the interface.
2. **LED Indicator**: Choose **Enabled** to allow the LED for this interface to blink with traffic on the port, or choose **Disabled** to turn the LED off. The LED will still light during the boot sequence, then turn off. This option is only available for the Gigabit interfaces.
3. **Allow Management on Interface**: Choose **Yes** to allow management of this Array via the selected network interface, or choose **No** to deny all management privileges for this interface.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the Array" on page 76.

4. **Auto Negotiate**: This feature allows the Array to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available). Both sides of the link **must** have the same values for the following settings, or the connection will have errors.
    a. **Duplex**: Full-duplex mode transmits data in two directions simultaneously (for example, a telephone is a full-duplex device

because both parties can talk and be heard at the same time). Half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.

b. **MTU**: the Maximum Transmission Unit size. This is the largest packet size (in bytes) that the interface can pass along.

c. **Speed**: If the Auto-Negotiate feature is disabled, you must manually choose the data transmission speed from the pull-down list. For the Gigabit interfaces the options are **10 Megabit** or **100 Megabit**. (Note that 1000 Megabit speed can only be set by Auto-Negotiation.)

5. **Configuration Server Protocol / IP Settings**: Choose **DHCP** to instruct the Array to use DHCP when assigning IP addresses to the Array, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.

   a. **Address**: If you selected the Static IP option, enter a valid IP address for the Array. To use any of the remote connections (Web, SNMP, or SSH), a valid IP address must be established.

   b. **Subnet Mask**: If you selected the Static IP option, enter a valid IP address for the subnet mask (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.

   c. **Default Gateway**: If you selected the Static IP option, enter a valid IP address for the default gateway. This is the IP address of the router that the Array uses to send data to other networks. (You don't need to enter the gateway if it is on the same subnet as the Array.)

   d. Click the **Apply** button for this interface when done making IP changes.

6. When done configuring all interfaces as desired, click the **Save** button if you wish to make your changes permanent.

See Also

Bonds and Bridging
DNS Settings
Network
Network Statistics
Spanning Tree Status

Bonds and Bridging

On models with more than one Gigabit port these ports may be bonded, i.e. configured to work together in sets. For example, one port may provide active backup or load balancing for another, or other options as described in this section. XR-6000 Series Arrays have four Gigabit ports, and you may specify which ports are bonded to work together as a pair. You may also select more than two ports to work together in one group.

A special option lets you configure bridging between the gigabit ports on an Array that has two of these ports.

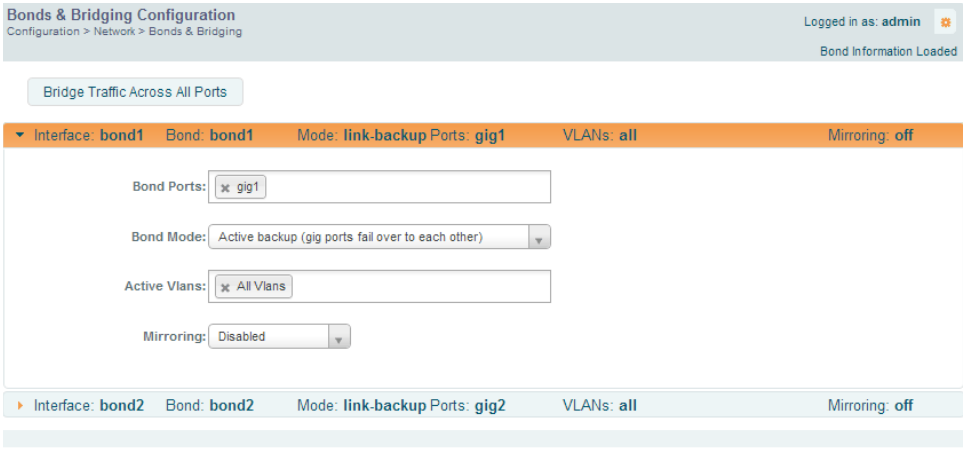


Figure 99. Network Bonds and Bridging

You may use the mirror option to have all the traffic that is ingressing and egressing one bond be transmitted by the bond you are configuring. For example, if you configure Bond2 to mirror Bond1, then all traffic going in and out of

Bond1's Gigabit ports will be transmitted out of Bond2's Gigabit ports. This way of duplicating one bond's traffic to another bond is very useful for troubleshooting with a network analyzer.

If a set of Gigabit ports have been bonded, the IP address, IP mask, IP gateway, IP DHCP, and Management settings are shared between bonded ports. Any changes you make to these settings on one member will be reflected in the settings of the other members. Other settings may be configured individually.

Procedure for Configuring Network Bonds

Configure the bonding behavior of the **Gigabit** network interfaces. The fields for each of these bonds are the same, and include:

1. **Bridge Traffic Across All Ports:** Click this for Layer 2 bridging between *all* Gigabit ports. (Figure 100)

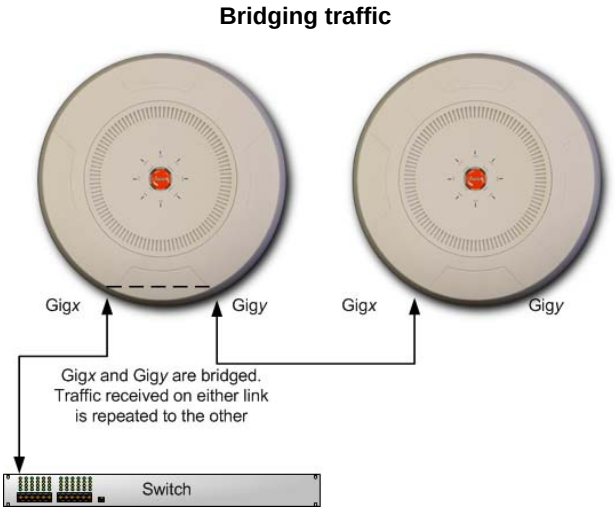


Figure 100. Bridging Traffic

Traffic received on Gig*x* is transmitted by Gig*y*; similarly, traffic received on Gig*y* is transmitted by Gig*x*. The Array acts as a wired bridge—this allows Arrays to be chained and still maintain wired connectivity.

Each Array in a chain must have power supplied to its PoE port from a compatible power injector or powered switch port. ***An Array does not supply power to another Array.***

When bridging is enabled, it configures the following bond settings for each bond. Do not make any manual changes to these settings afterwards if you wish to continue bridging.

- **Bond Mode is** set to **Active Backup** (the default value).
- Each port is in its own bond, by itself.
- **Bond Mirror** is **Off**.
- You will typically need to enable use of Spanning Tree manually, to prevent network loops.
- **Active VLANs** is set to **All**.

A bridge between ports **Gig1** and **Gig2** sets **Bond1** to contain only **Gig1**. **Bond2** contains only **Gig2**.

If you are bridging a chain of more than two Arrays, the endpoint Array is not actually bridging. It can be left with the default settings—**Bond1** is set to **Active Backup**, and will contain **Gig1** and **Gig2**.

Skip to Step 7 on page 175.

2. If you are not enabling bridging, configure the bonding behavior of the **Gigabit** network interfaces as described in the following steps. The fields for each of these bonds are the same.

3. **Bond Mode**: Select the desired behavior for a set of bonded Gigabit Ethernet ports from the following options.

   The modes below describe the relationship between a set of Gigabit ports—for example, load balancing or active backup. Use the **Bond Ports** field to select the ports that are bonded (set in Step 4). Two or more ports

may be bonded. You may also include just one single port in a bond—this is useful for mirroring one Gigabit port to another port (Step c on page 174). In Arrays that have four Gigabit ports, you have the option of bonding three or four ports together. In this discussion, we call two ports that are bonded **Gig*x*** and **Gig*y***.

a. **Active Backup (gig ports fail over to each other)**—This mode provides fault tolerance and is the default mode. Gig*x* acts as the primary link. Gig*y* is the backup link and is passive. Gig*y* assumes the IP properties of Gig*x*. If Gig*x* fails, the Array automatically fails over to Gig*y*. When a failover occurs in this mode, Gig*y* issues gratuitous ARPs to allow it to substitute for Gig*x* at Layer 3 as well as Layer 2. See Figure 101 (a). You may include more than two ports in the bond with Active Backup to provide additional fault tolerance. For example, if you have three Gigabit ports configured in a bond, if the first two ports in the bond were to go down, the Array would fail over traffic to the third Gigabit port.

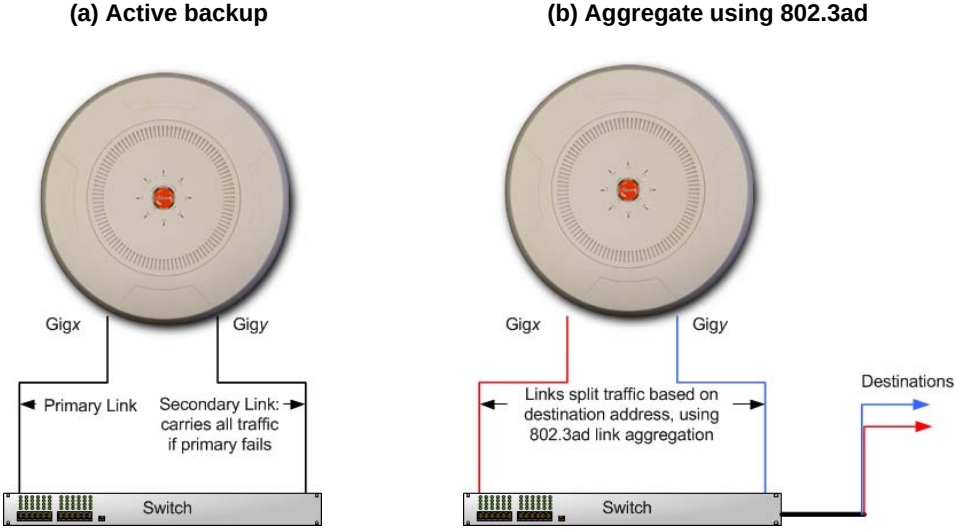


Figure 101. Port Modes (a, b)

b. **Aggregate Traffic from gig ports using 802.3ad**—The Array sends network traffic across all member Gigabit ports to increase link speed to the network. These ports act as a single logical interface, using a load balancing algorithm to balance traffic across the ports. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. If the packet is a fragment or not TCP or UDP, the source and destination IP addresses are used to do the calculation. If the packet is TCP or UDP over IP then the source IP address, destination IP address, source port number and destination port number are all used to do the calculation. The network switch must also support 802.3ad. If a port fails, the connection degrades gracefully—the other port still transmits. See Figure 101 (b).

c. **Transmit Traffic on all gig ports**—Transmits incoming traffic on all Gigabit ports. Any traffic received on Gigabit ports is sent to the onboard processor. This mode provides fault tolerance. See Figure 102 (c).

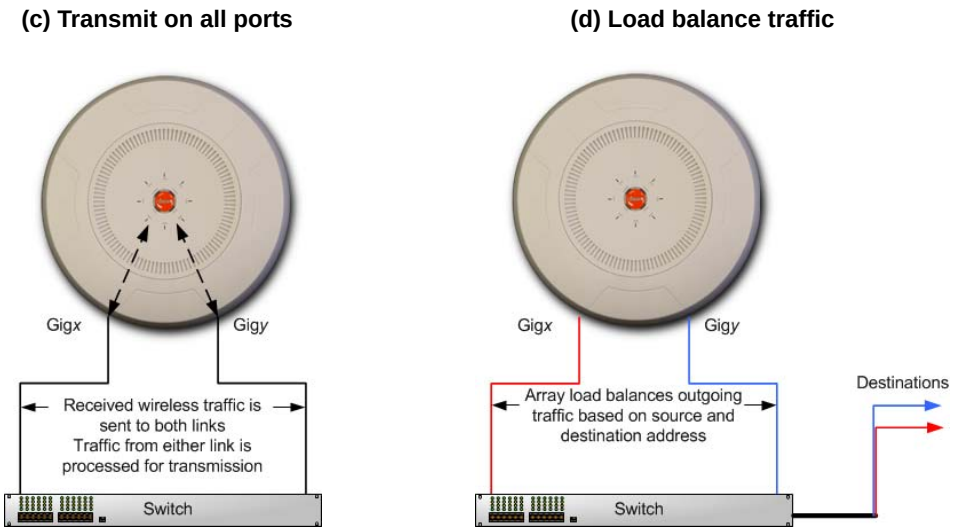


Figure 102. Port Modes (c, d)

d. **Load balance traffic between gig ports**—This option provides trunking, similar to option (b)—**Aggregate Traffic from gig1 & gig2 using 802.3ad**, but it does not use 802.3ad and it uses a different load balancing algorithm to determine the outgoing Gigabit port. The outgoing port used is based on an exclusive OR of the source and destination MAC address. Like option (b), this mode also provides load balancing and fault tolerance. See Figure 102 (d).

4. **Bond Ports**: Select the ports to be members of this bond for the behavior specified by **Bond Mode**. By default, Bond1 contains Gig1 and Gig2. You may also set up a bond with a single port, for example, if you wish to mirror one Gigabit port to another. In Arrays that have four Gigabit ports, you also have the option of bonding three or four ports together.

   When you check off a port to be a member of a bond, that port is automatically removed from any other bonds that contain it.

5. **Active VLANs**: **Active VLANs** shows the VLANs that you have selected to be passed through this port. Create and manage the list of VLANs that are allowed to be passed through this port. Traffic will be dropped for VLANs that are not in this list. The default setting is to pass All VLANs.

   a. To add a VLAN to the list of allowed VLANs, click this field and select the desired VLAN from the drop-down list. To allow all VLANs (current or future) to be passed, select **All VLANs**.

   b. To allow only the set of currently defined VLANs (see "VLANs" on page 204) to be passed, select **All Current VLANs**. Essentially, this "fixes" the Active VLANs list to contain the currently defined VLANs, and only this set, until you make explicit changes to the Active VLANs list. If you create new VLANs, they will not be passed unless you take action to add them to the list.

   c. To remove a VLAN from the list of allowed VLANs, click the **X** before its name.

6. **Mirroring**—Specify one of the active bonds (Bond*x*) that is to be mirrored by this bond (Bond*y*). (Figure 103) All wireless traffic received on the Array is transmitted out both Bond*x* and Bond*y*. All traffic

received on Bond*x* is passed on to the onboard processor as well as out Bond*y*. All traffic received on Bond*y* is passed on to the onboard processor as well as out Bond*x*. This allows a network analyzer to be plugged into Bond*y* to capture traffic for troubleshooting, while the bonded ports provide network connectivity for data traffic.

If each bond contains just one port, then you have the simple case of one port mirroring another.

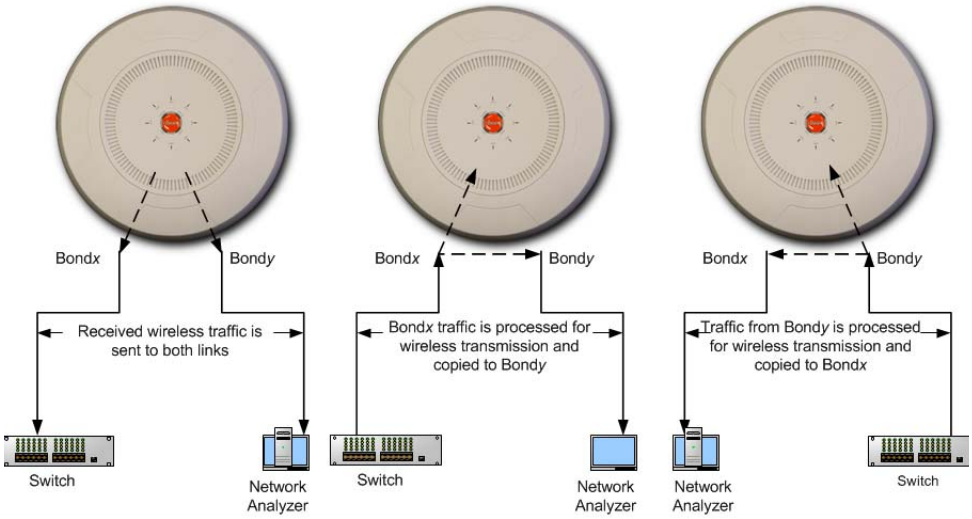


Figure 103. Mirroring Traffic

7. When done configuring bonds and bridging as desired, click the **Save** button if you wish to make your changes permanent.

See Also

Network Interfaces
DNS Settings
Network
Network Statistics
Spanning Tree Status

DNS Settings

This window allows you to establish your DNS (Domain Name System) settings. The Array uses these DNS servers to resolve host names into IP addresses. The Array also registers its own Host Name with these DNS servers, so that others may address the Array using its name rather than its IP address. An option allows you to specify that the Array's DNS servers will be assigned via a DHCP server on the wired network.

Note that the DNS servers defined here are not used by wireless clients—servers for stations associated to the Array are defined along with DHCP pools. See "DHCP Server" on page 194. At least one DNS server must be set up if you want to offer clients associating with the Array the ability to use meaningful host names instead of numerical IP addresses. When finished, click the **Save** button if you wish to make your changes permanent.

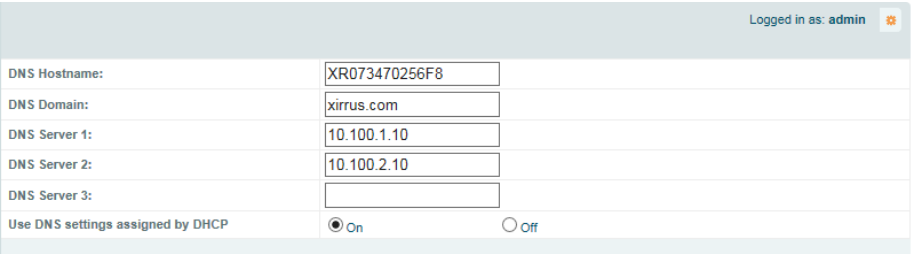


Figure 104. DNS Settings

Procedure for Configuring DNS Servers

1. **DNS Host Name:** Enter a valid DNS host name.
2. **DNS Domain**: Enter the DNS domain name.
3. **DNS Server 1**: Enter the IP address of the primary DNS server.
4. **DNS Server 2** and **DNS Server 3**: Enter the IP address of the secondary and tertiary DNS servers (if required).
5. **Use DNS settings assigned by DHCP**: If you are using DHCP to assign the Array's IP address, you may turn this option **On**. The Array will then obtain its DNS domain and server settings from the network DHCP

server that assigns an IP address to the Array, rather than using the DNS Server fields above. You may also configure that DHCP server to assign a host name to the Array.

6. Click the **Save** button if you wish to make your changes permanent.

See Also

DHCP Server
Network
Network Interfaces
Network Statistics
Spanning Tree Status

CDP Settings

CDP (Cisco Discovery Protocol) is a layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Wireless Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors (see "CDP Neighbors" on page 108).

This window allows you to establish your CDP settings. When finished, the **Save** button if you wish to make your changes permanent.

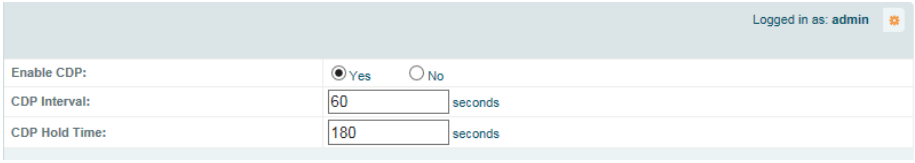


Figure 105. CDP Settings

Procedure for Configuring CDP Settings

1. **Enable CDP:** When CDP is enabled, the Array sends out CDP announcements of the Array's presence, and gathers CDP data sent by neighbors. When disabled, it does neither. CDP is enabled by default.

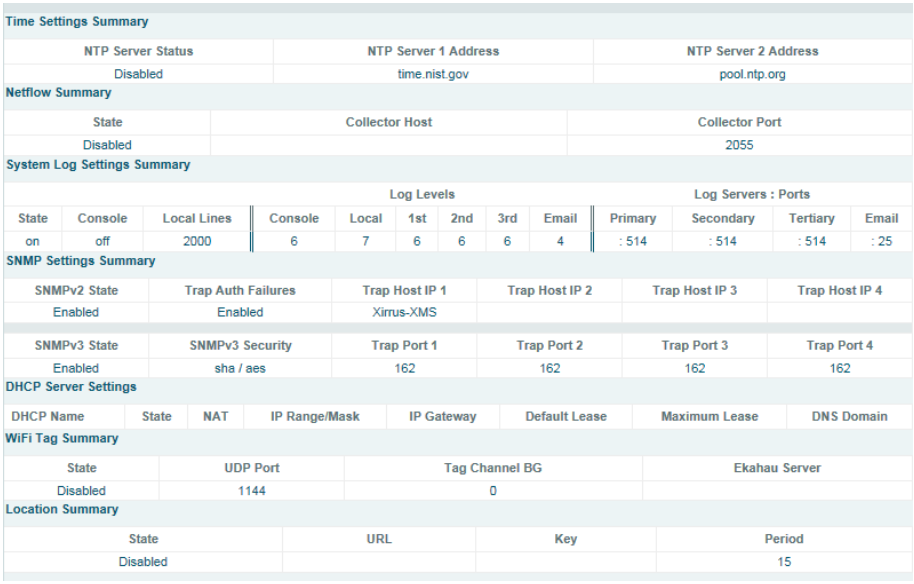
2. **CDP Interval**: The Array sends out CDP announcements advertising its presence at this interval. The default is 60 seconds.
3. **CDP Hold Time**: CDP information received from neighbors is retained for this period of time before aging out of the Array's neighbor list. Thus, if a neighbor stops sending announcements, it will no longer appear on the CDP Neighbors window after CDP Hold Time seconds from its last announcement. The default is 180 seconds.

See Also

CDP Neighbors
Network
Network Interfaces
Network Statistics

Services

This is a status-only window that allows you to review the current settings and status for services on the Array, including DHCP, SNMP, Syslog, and Network Time Protocol (NTP) services. For example, for the DHCP server, it shows each DHCP pool name, whether the pool is enabled, the IP address range, the gateway address, lease times, and the DNS domain being used. There are no configuration options available in this window, but if you are experiencing issues with network services, you may want to print this window for your records.



Time Settings Summary

NTP Server Status	NTP Server 1 Address	NTP Server 2 Address
Disabled	time.nist.gov	pool.ntp.org

Netflow Summary

State	Collector Host	Collector Port
Disabled		2055

System Log Settings Summary

			Log Levels						Log Servers : Ports			
State	Console	Local Lines	Console	Local	1st	2nd	3rd	Email	Primary	Secondary	Tertiary	Email
on	off	2000	6	7	6	6	6	4	: 514	: 514	: 514	: 25

SNMP Settings Summary

SNMPv2 State	Trap Auth Failures	Trap Host IP 1	Trap Host IP 2	Trap Host IP 3	Trap Host IP 4
Enabled	Enabled	Xirrus-XMS			

SNMPv3 State	SNMPv3 Security	Trap Port 1	Trap Port 2	Trap Port 3	Trap Port 4
Enabled	sha / aes	162	162	162	162

DHCP Server Settings

DHCP Name	State	NAT	IP Range/Mask	IP Gateway	Default Lease	Maximum Lease	DNS Domain

WiFi Tag Summary

State	UDP Port	Tag Channel BG	Ekahau Server
Disabled	1144	0	

Location Summary

State	URL	Key	Period
Disabled			15

Figure 106. Services

The following sections discuss configuring services on the Array:

- **“Time Settings (NTP)” on page 180**
- **“NetFlow” on page 182**
- **“Wi-Fi Tag” on page 183**
- **“Location” on page 184**
- **“System Log” on page 186**
- **“SNMP” on page 191**

- "DHCP Server" on page 194
- "Proxy Forwarding" on page 196

Time Settings (NTP)

This window allows you to manage the Array's time settings, including synchronizing the Array's clock with a universal clock from an NTP (Network Time Protocol) server. We recommend that you use NTP for proper operation of SNMP in XMS (the Xirrus Management System), since a lack of synchronization will cause errors to be detected. Synchronizing the Array's clock with an NTP server also ensures that Syslog time-stamping is maintained across all units.

It is possible to use authentication with NTP to ensure that you are receiving synchronization from a known source. For example, the instructions for requesting a key for the NIST Authenticated NTP server are available at http://www.nist.gov/pml/div688/grp00/upload/ntp_instructions.pdf. The Array allows you to enter optional authentication information.

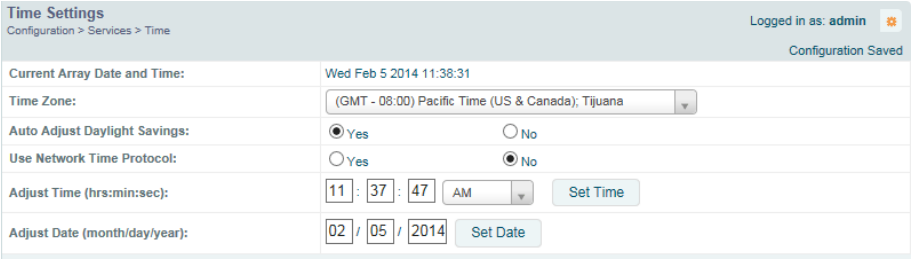


Figure 107. Time Settings (Manual Time)

Procedure for Managing the Time Settings

1. **Current Array Date and Time:** Shows the current time.
2. **Time Zone**: Select the time zone you want to use (normally your local time zone) from the pull-down list.
3. **Auto Adjust Daylight Savings**: Check this box to have the system adjust for daylight savings automatically, else leave it unchecked (default).
4. **Use Network Time Protocol:** select whether to set time manually or use NTP to manage system time.

5. **Setting Time Manually**

   a. **Adjust Time (hrs:min:sec)**: If you are not using NTP, use this field if you want to adjust the current system time. Enter a revised time (hours, minutes, seconds, am/pm) in the corresponding fields. Click **Set Time** to apply the changes.

   b. **Adjust Date (month/day/year)**: If you are not using NTP, use this field if you want to adjust the current system date. Enter a revised date (month, day and year) in the corresponding fields. Click **Set Date** to apply the changes.

6. **Using an NTP Server**

   a. **NTP Primary Server**: If you are using NTP, enter the IP address or domain name of the NTP server.

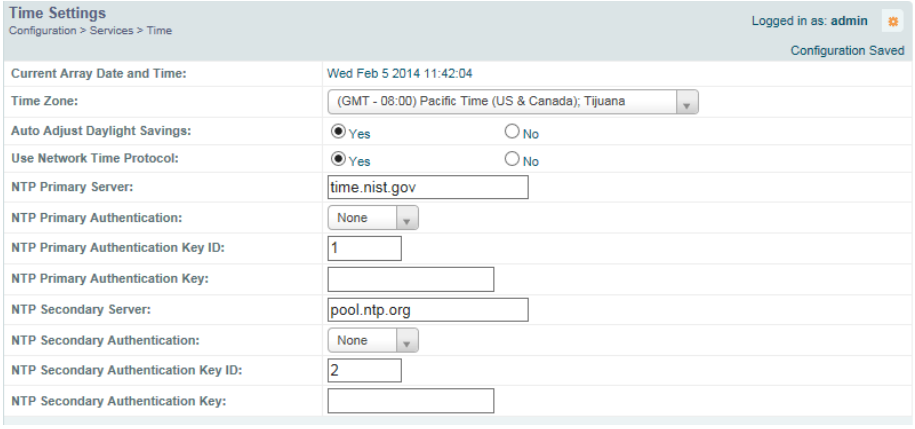


Figure 108. Time Settings (NTP Time Enabled)

   b. **NTP Primary Authentication**: (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default).

   c. **NTP Primary Authentication Key ID**: Enter the key ID, which is a decimal integer.

d. **NTP Primary Authentication Key**: Enter your key, which is a string of characters.

e. **NTP Secondary Server**: Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

See Also

Express Setup
Services
SNMP
System Log

NetFlow

This window allows you to enable or disable the sending of NetFlow information to a designated collector. NetFlow is a proprietary but open network protocol developed by Cisco Systems for collecting IP traffic information. When NetFlow is enabled, the Array will send IP flow information (traffic statistics) to the designated collector.

Figure 109. NetFlow

NetFlow sends per-flow network traffic information from the Array. Network managers can use a NetFlow collector to view the statistics on a per-flow basis and use this information to make key decisions. Knowing how many packets and bytes are sent to and from certain IP addresses or across specific network interfaces allows administrators to track usage by various areas. Traffic flow information may be used to engineer networks for better performance.

Procedure for Configuring NetFlow

1. **Enable NetFlow:** Select one of the Netflow versions to enable NetFlow functionality: **v5**, **v9**, or **IPFIX**. Internet Protocol Flow Information Export (IPFIX) is an IETF protocol (www.ietf.org**)** performing many of the same functions as Netflow. Choose **Disable** if you wish to disable this feature.
2. **NetFlow Collector Host (Domain or IP)**: If you enabled NetFlow, enter the domain name or IP address of the collector.
3. **NetFlow Collector Port**: If you enabled NetFlow, enter the port on the collector host to which to send data.

Wi-Fi Tag

This window enables or disables Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channel. These tags are transmitted by specialized tag devices (for example, AeroScout or Ekahau tags). A Wi-Fi tagging server then queries the Array for a report on the tags that it has received. The Wi-Fi tagging server uses proprietary algorithms to determine locations for devices sending tag signals.

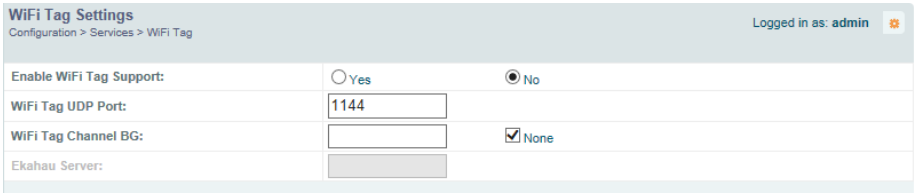


Figure 110. Wi-Fi Tag

Procedure for Configuring Wi-Fi Tag

1. **Enable Wi-Fi Tag:** Choose **Yes** to enable Wi-Fi tag functionality, or choose **No** to disable this feature.

2. **Wi-Fi Tag UDP Port**: If Wi-Fi tagging is enabled, enter the UDP port that the Wi-Fi tagging server will use to query the Array for data. When queried, the Array will send back information on tags it has observed. For each, the Array sends information such as the MAC address of the tag transmitting device, and the RSSI and noise floor observed.
3. **Wi-Fi Tag Channel BG**: If you enabled Wi-Fi tagging, enter the 802.11 channel on which the Array will listen for tags. The tag devices must be set up to transmit on this channel. Only one channel may be configured, and it must be an 802.11b/g channel in the range of Channel 1 to 11.
4. **Ekahau Server**: If you enabled Wi-Fi tagging and you are using an Ekahau server, enter its IP address or hostname. Ekahau Wi-Fi Tag packets received by the Array will be encapsulated as expected by Ekahau, and forwarded to the server.

Location

The Array offers an integrated capability for capturing and uploading visitor analytics data, eliminating the need to install a standalone sensor network. This data can be used to characterize information such as guest or customer traffic and location, visit duration, and frequency. Use this Location window to configure the Array to send collected data to an analytics server, such as Euclid.

When Location Support is enabled, the Array collects information about stations, including the station ID and manufacturer, time and length of the visit and related time interval statistics, and signal strength and its related statistics. Data collected from stations comprises only basic device information that is broadcast by Wi-Fi enabled devices. Devices that are only detected are included, as well as those that actually connect to the Array. The Array sending the data also sends its own ID so that the server knows where the visitors were detected. Data messages are uploaded via HTTPS, and they are encrypted if a **Location Customer Key** has been entered. Data is sent as JSON (JavaScript Object Notation) objects, as described in "Location Service Data Formats" on page 504.

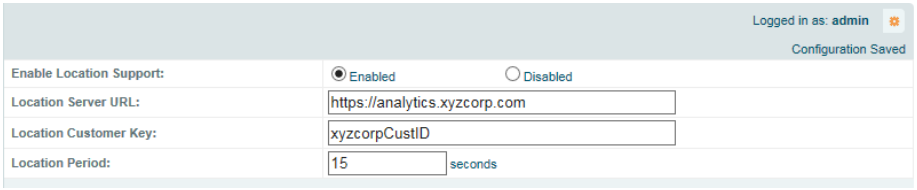


Figure 111. Location

Procedure for Configuring Location

1. **Enable Location Support:** Choose **Yes** to enable the collection and upload of visitor analytic data, or choose **No** to disable this feature.

2. **Location URL**: If Location Support is enabled, enter the IP address or hostname of the location/analytics server. If this URL contains the string **euclid**, then the Array knows that data is destined for a Euclid location server.

   For a Euclid analytics server, use the URL that was assigned to you as a customer by Euclid. The Array will send JSON-formatted messages in the form required by Euclid via HTTPS.

   For any other location analytics server, enter its URL. The Array will send JSON-formatted messages in the form described in "Location Service Data Formats" on page 504.

3. **Location Customer Key**: (optional) If a **Location Customer Key** has been entered, data is sent encrypted using AES with that key.

4. **Location Period**: If you enabled Location Support, specify how often data is to be sent to the server, in seconds.

System Log

This window allows you to enable or disable the Syslog server, define primary, secondary, and tertiary servers, set up email notification, and set the level for Syslog reporting for each server and for email notification—the Syslog service will send Syslog messages at the selected severity or above to the defined Syslog servers and email address. An option allows you to use a Splunk application to analyze Array events by sending data in key:value pairs, as described in "About Using the Splunk Application for Xirrus Arrays" on page 189.

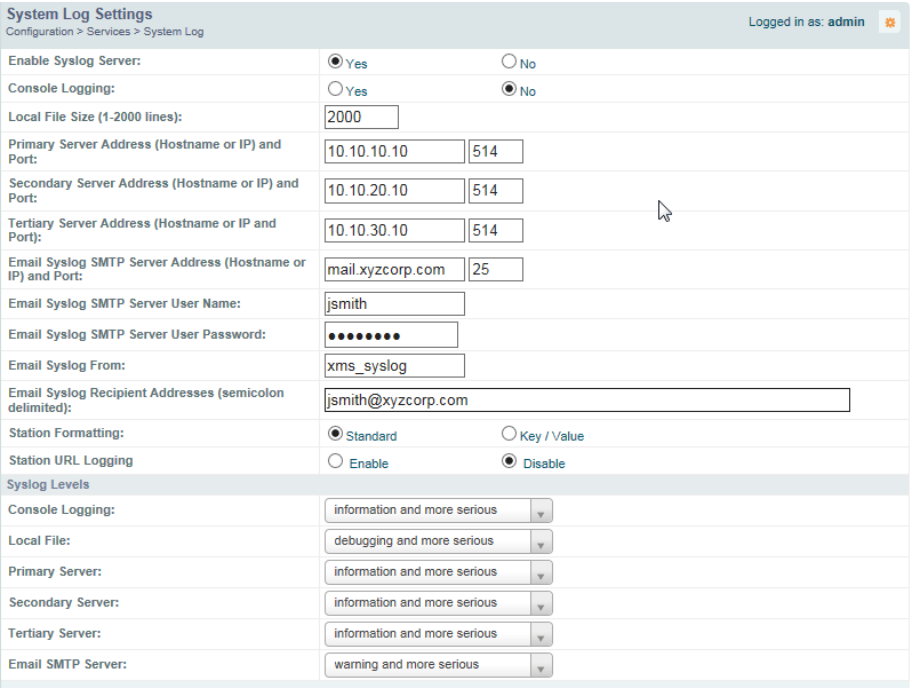


Figure 112. System Log

Procedure for Configuring Syslog

1. **Enable Syslog Server:** Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.

2. **Console Logging**: If you enabled Syslog, select whether or not to echo Syslog messages to the console as they occur. If you enable console logging, be sure to set the Console Logging level (see Step 9 below).

3. **Local File Size** (1-2000 lines): Enter a value in this field to define how many Syslog records are retained locally on the Array's internal Syslog file. The default is 2000.

4. **Primary Server Address (Hostname or IP) and Port**: If you enabled Syslog, enter the hostname or IP address of the primary Syslog server. You may also change the port used on the server if you do not wish to use 514, the default port.

5. **Secondary/Tertiary Server Address (Hostname or IP) and Port**: (Optional) If you enabled Syslog, you may enter the hostname or IP address of one or two additional Syslog servers to which messages will also be sent. You may also change the port used on each server if you do not wish to use 514, the default port. You may set one of the server addresses to the address of a server for Splunk (see "About Using the Splunk Application for Xirrus Arrays" on page 189).

6. **Email Notification**: (Optional) The following parameters allow you to send an email to a designated address each time a Syslog message is generated. The email will include the text of the Syslog message.

    a. **Email Syslog SMTP Server Address (Hostname or IP) and Port**: The hostname or the IP address of the SMTP server to be used for sending the email. Note that this specifies the mail server, **not** the email recipient. You may also change the port used on the server if you do not wish to use 25, the default SMTP port.

    b. **Email Syslog SMTP User Name**: Specify a user name for logging in to an account on the mail server designated in Step a.

    c. **Email Syslog SMTP User Password**: Specify a password for logging in to an account on the mail server designated in Step a.

    d. **Email Syslog SMTP From**: Specify the "From" email address to be displayed in the email.

e. **Email Syslog SMTP Recipient Addresses**: Specify the entire email address of the recipient of the email notification. You may specify additional recipients by separating the email addresses with semicolons (;).

7. **Station Formatting**: If you are sending event information to a Splunk server, select **Key/Value** to send data in Splunk's expected format, otherwise leave this at the default value of **Standard**. See "About Using the Splunk Application for Xirrus Arrays" on page 189.

8. **Station URL Logging**: When enabled, Syslog messages are sent for each URL that each station visits. Only HTTP destinations (port 80) are logged; HTTPS destinations (port 443) are not logged. All URLs in a domain are logged, so for example, if an HTTP request to yahoo.com generates requests to 57 other URLs, all are logged. Furthermore, each visit to the same URL generates an additional log message. No deep packet inspection is performed by the URL logging, so no Application Control information is included in the Syslog message.

   The following information is included in the syslog message:

   - Date / Time
   - Source Device MAC and IP address
   - Destination Port
   - Destination Site address (e.g., 20.20.20.1)
   - The specific URL (e.g., http://20.20.20.1.24/online/images/img2.jpg)

   Station URL Logging is disabled by default.

9. **Syslog Levels**: For each of the Syslog destinations, choose your preferred level of Syslog reporting from the pull-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.

   a. **Console Logging**: For messages to be echoed to the console, the default level is **Critical and more serious**. This prevents large numbers of non-critical messages from being displayed on the

console. If you set this level too low, the volume of messages may make it very difficult to work with the CLI or view other output on the console.

b. **Local File**: For records to be stored on the Array's internal Syslog file, choose your preferred level of Syslog reporting from the pull-down list. The default level is **Debugging and more serious**.

c. **Primary Server**: Choose the preferred level of Syslog reporting for the primary server. The default level is **Debugging and more serious**.

d. **Secondary/Tertiary Server**: Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Information and more serious**. (Optional)

e. **Email SMTP Server**: Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.

10. Click the **Save** button if you wish to make your changes permanent.

About Using the Splunk Application for Xirrus Arrays

Splunk may be used to provide visibility into client experience and analyze usage on XR Series Wireless Arrays. A Splunk application (Splunk for Xirrus XR Wireless Arrays) has been developed to present this operational intelligence at a glance. The app includes field extractions, event types, searches and dashboards to help shine a light on station status and activity.

To use Splunk, set up your Splunk server with the Splunk application—available from www.splunk.com at **Splunk for Xirrus XR Wireless Arrays**. Configure the Array to send data to Splunk by setting a **Primary**, **Secondary**, or **Tertiary Server Address** to the IP address or hostname of your Splunk server. Then set **Station Formatting** to **Key/Value** to send data in Splunk's expected format.

You may specify Server Addresses for Syslog servers and a Splunk server on the same Array. Selecting the **Key/Value** option will not cause any problems with Syslog.

See Also

System Log Window
Services
SNMP
Time Settings (NTP)

SNMP

This window allows you to enable or disable SNMP v2 and SNMP v3 and define the SNMP parameters. SNMP allows remote management of the Array by the Xirrus Management System (XMS) and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, neither, or both.

Complete SNMP details for the Array, including trap descriptions, are found in the Xirrus MIB, available at support.xirrus.com, in the **Downloads** section (login is required to download the MIB).

NOTE: If you are managing your Arrays with XMS (the Xirrus Management System), it is very important to make sure that your SNMP settings match those that you have configured for XMS. XMS uses both SNMP v2 and v3, with v3 given preference.

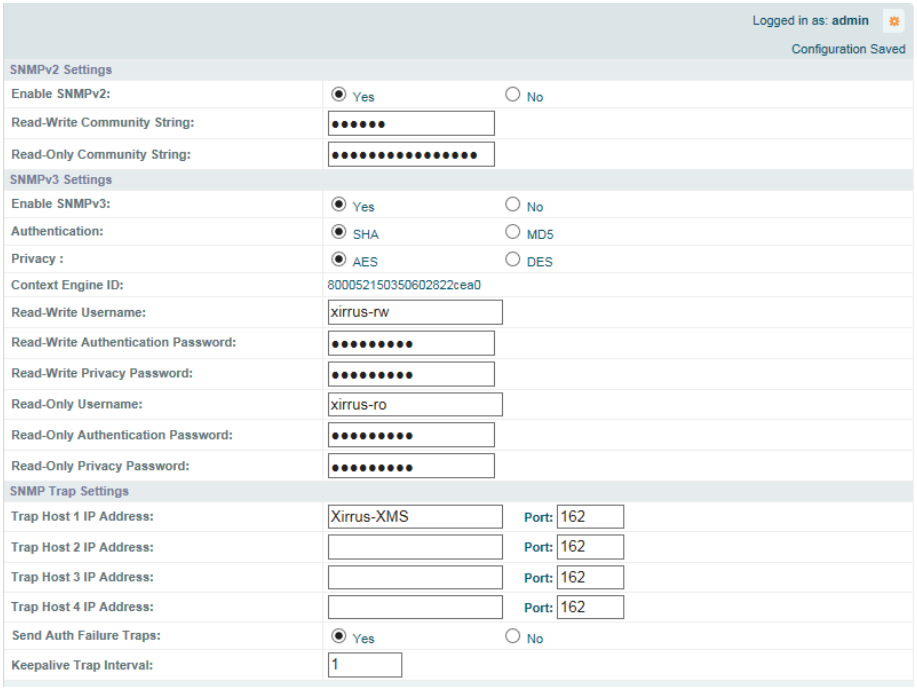


Figure 113. SNMP

Procedure for Configuring SNMP

SNMPv2 Settings

1. **Enable SNMPv2:** Choose **Yes** to enable SNMP v2 functionality, or choose No to disable this feature. When used in conjunction with the Xirrus Management System, SNMP v2 (**not** SNMP v3) must be enabled on each Array to be managed with XMS. The default for this feature is Yes (enabled).
2. **SNMP Read-Write Community String**: Enter the read-write community string. The default is **xirrus**.
3. **SNMP Read-Only Community String**: Enter the read-only community string. The default is **xirrus_read_only**.

SNMPv3 Settings

4. **Enable SNMPv3**: Choose **Yes** to enable SNMP v3 functionality, or choose No to disable this feature. The default for this feature is Yes (enabled).
5. **Authentication**: Select the desired method for authenticating SNMPv3 packets: **SHA** (Secure Hash Algorithm) or **MD5** (Message Digest Algorithm 5).
6. **Privacy**: Select the desired method for encrypting data: **DES** (Data Encryption Standard) or the stronger **AES** (Advanced Encryption Standard).
7. **Context Engine ID**: The unique identifier for this SNMP server. We recommend that you do not change this value. The Context Engine ID must be set if data collection is to be done via a proxy agent. This ID helps the proxy agent to identify the target agent from which data is to be collected.
8. **SNMP Read-Write Username**: Enter the read-write user name. This username and password allow configuration changes to be made on the Array. The default is **xirrus-rw**.
9. **SNMP Read-Write Authentication Password**: Enter the read-write password for authentication (i.e., logging in). The default is **xirrus-rw**.

10. **SNMP Read-Write Privacy Password**: Enter the read-write password for privacy (i.e., a key for encryption). The default is **xirrus-rw**.
11. **SNMP Read-Only Username**: Enter the read-only user name. This username and password do not allow configuration changes to be made on the Array. The default is **xirrus-ro**.
12. **SNMP Read-Only Authentication Password**: Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.
13. **SNMP Read-Only Privacy Password**: Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.

SNMP Trap Settings

14. **SNMP Trap Host IP Address**: Enter the **IP Address** or hostname, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. Note that by default, **Trap Host 1** sends traps to Xirrus-**XMS**. Thus, the Array will automatically communicate its presence to XMS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

    For a definition of the traps sent by Xirrus Wireless Arrays, you may download the Xirrus MIB from support.xirrus.com (login required). Search for the string **TRAP** in the MIB file.

15. **Send Auth Failure Traps**: Choose **Yes** to log authentication failure traps or **No** to disable this feature.
16. **Keepalive Trap Interval** (minutes): Traps are sent out at this interval to indicate the presence of the Array on the network. Keepalive traps are required for proper operation with XMS. To disable keepalive traps, set the value to **0**.
17. Click the **Save** button if you wish to make your changes permanent.

See Also

Services

System Log
Time Settings (NTP)

DHCP Server

This window allows you to create, enable, modify and delete DHCP (Dynamic Host Configuration Protocol) address pools. DHCP allows the Array to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network. If you do not use the DHCP server on the Array, then your wired network must be configured to supply DHCP addresses and gateway and DNS server addresses to wireless clients.

When you create a DHCP pool, you must define the DHCP lease time (default and maximum), the IP address ranges (pools) that the DHCP server can assign, and the gateway address and DNS servers to be used by clients.

Figure 114. DHCP Management

DHCP usage is determined in several windows—see SSID Management, Group Management, and VLAN Management.

Procedure for Configuring the DHCP Server

1. **New Internal DHCP Pool**: Enter a name for the new DHCP pool, then click on the **Create** button. The new pool ID is added to the list of available DHCP pools. You may create up to 16 DHCP pools (up to 8 on the XR-500 Series and on the XR-620).
2. **On**: Click this checkbox to make this pool of addresses available, or clear it to disable the pool.

3. **Lease Time—Default**: This field defines the default DHCP lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
4. **Lease Time—Max**: Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.
5. **Network Address Translation (NAT)**: Check this box to enable the Network Address Translation feature.
6. **Lease IP Range—Start**: Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End**: Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask**: Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway**: If necessary, enter the IP address of the gateway.
10. **Domain**: Enter the DNS domain name. See "DNS Settings" on page 176.
11. **DNS Servers** (1 to 3): Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the assigned IP address. Note that if you leave these blank, no DNS information is sent to the stations. DHCP will **not** default to sending the DNS servers that are configured in DNS Settings. See also, "DNS Settings" on page 176.
12. Click the **Save** button if you wish to make your changes permanent.

See Also

DHCP Leases
DNS Settings
Network Map

Proxy Forwarding

Some smaller Arrays/APs have less memory (XR-500/1000 Series and XR-620) and are not able to run all ArrayOS features at the same time. You will receive an error message if you attempt to configure a feature when there is not enough memory left.

If your organization uses a proxy server such as Blue Coat or Netbox Blue to control Internet access, use this page to configure proxy forwarding on the Array.

About Proxy Forwarding

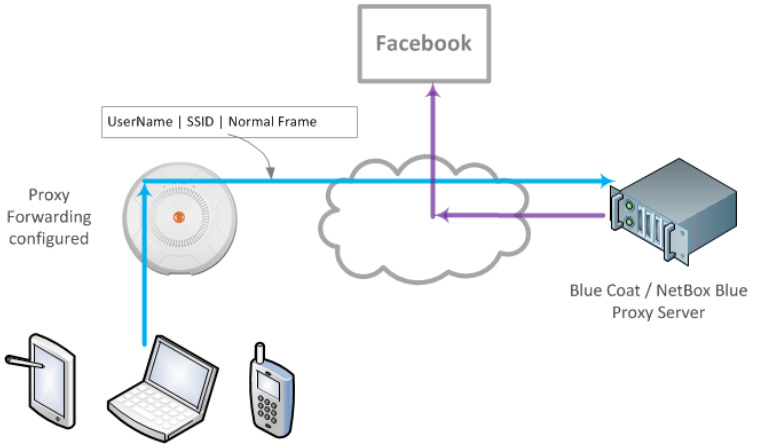


Figure 115. Proxy Forwarding Example

When you configure proxy forwarding settings on the Array, it forwards each HTTP request to the proxy server (for example, Blue Coat) at the specified URL, which checks if the policies that you have set up on the server are satisfied. If so, the proxy server sends the request on to the desired web site. An example is shown in Figure 115. The user of the laptop tries to open Facebook on a browser. The Array forwards this request to the proxy server that you have specified, after adding a prefix with the **user's ID** and the **SSID** (the SSID serves as a user group; for unauthenticated clients, the MAC address serves as the user name). The proxy server checks whether its configured policies permit this access for this user and SSID. If so, the frame is forwarded to the desired web site.

SSID and client User Name restrictions permit the following characters.
— Blue Coat permits only alphanumerics and + and /.
— Netbox Blue permits only alphanumerics and dot, hyphen, underscore, and space characters.

Proxy forwarding on the Array is designed for proxy servers such as Blue Coat and Netbox Blue whose purpose is restricting Internet access to sites, applications and content, and the monitoring and reporting of this activity. It is not used for enhanced performance utilizing content caching.

Blue Coat policy configuration:
The AuthConnector utility is not used with the Xirrus implementation. Traffic must first be passed through the portal to dynamically add the User to Blue Coat's list of recognized Users, based on the User header inserted in the packets. When configuring Blue Coat Content Filtering policy, you may select "Users from Reporting". Only the User value can be used in this manner. The Group header value is not dynamically added to Blue Coat's Group list, and it can't be added manually.

Netbox Blue policy configuration:
Users and Groups are manually configured on the server. Users are manually assigned to Groups, and policy is applied on a per-Group basis.

Proxy forwarding on the Array is configured as described in "Procedure for Configuring Proxy Forwarding on the Array" on page 203. This proxies all HTTP traffic to the specified server. If you wish to proxy HTTPS traffic as well, you must take the additional steps described below.

Proxy Forwarding for HTTPS

There are two usage scenarios for proxy forwarding:

- Use proxy forwarding for HTTP traffic only: set up the Array per "Procedure for Configuring Proxy Forwarding on the Array" on page 203. HTTPS traffic is unaffected and proceeds in the usual way.
- Use proxy forwarding for both HTTP and HTTPS traffic: set up the Array per "Procedure for Configuring Proxy Forwarding on the Array" on

page 203. Then you must set up browsers on client stations (laptops, smart phones, tablets, ...) to proxy both HTTP and HTTPS traffic to the Array. Each client must also download and install the SSL certificate from the Blue Coat or Netbox Blue proxy server. Follow the procedure below to perform these steps on each client. Note that when a proxy is set up and used for HTTPS, HTTP traffic will also use the proxy server, so configure both as instructed in "Configuring Proxy Forwarding on Clients for HTTPS" on page 199.

Summary of Proxy Forwarding Behavior on the Array

If proxy forwarding is **not** enabled in the Array and the client browser is **not** configured to use a proxy:

- HTTP traffic (port 80) and HTTPS traffic (port 443) pass transparently through the Array in the usual way.

If proxy forwarding **is** enabled for Blue Coat or Netbox Blue and the client browser is **not** configured to use a proxy (i.e., you do not wish to proxy secure traffic):

- The browser still uses HTTP (port 80) and this traffic is captured and proxied by the Array.
- The browser still uses HTTPS (port 443) and this traffic is passed transparently through the Array.
- If proxy forwarding is not working correctly, HTTP traffic (port 80) is blocked.

If proxy forwarding **is** enabled for Blue Coat or Netbox Blue and the client browser **is** configured to use a proxy:

- The browser is configured to proxy HTTPS to www.xirrus.com port 4388.
- The browser automatically proxies HTTP traffic to the **same** port that is used for HTTPS traffic—port 4388.
- All HTTP/HTTPS traffic is captured by the Array and proxied to Blue Coat or Netbox Blue per your settings.
- If Array proxy forwarding is not working correctly (for example, if the configuration is incorrect), all HTTP/HTTPS/4388 traffic is blocked.

Configuring Proxy Forwarding on Clients for HTTPS

To set the proxy server on an Apple laptop, skip to Step 3.

1. For Windows laptops, click the desktop **Start** button. In the **Search programs and files** field, enter **Configure proxy server**. The Internet Properties dialog is displayed. (Figure 116) Click the **LAN Settings** button. The Local Area Network dialog displays.

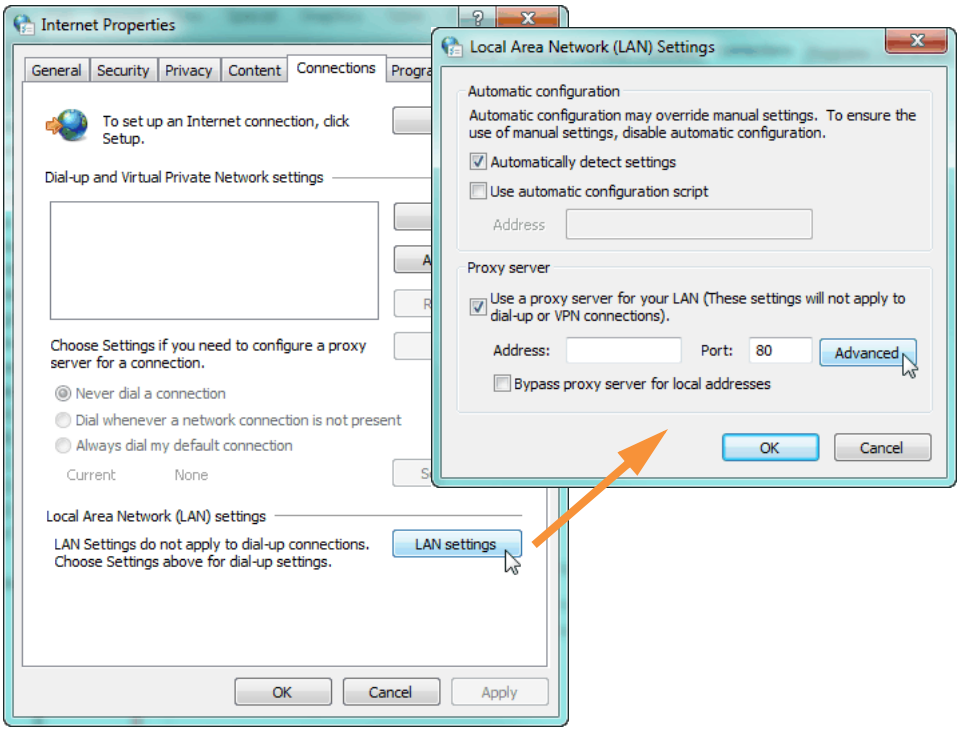


Figure 116. Set up a Proxy Server on each Client (Windows)

2. In the Proxy Server section, click the **Advanced** button. The Proxy Settings dialog displays. (Figure 117)

   For **HTTPS:** Enter any valid address, such as **www.xirrus.com**, in the **Proxy address to use** field. We suggest that you enter **www.xirrus.com**. (This field is not actually used, but Windows needs it to be a valid

address or domain name). You **must** set the **Port** to **4388**. This is **very important**! This is the Array port that should receive all HTTPS traffic if you are using a proxy server.

For **HTTP:** HTTP traffic will automatically use the same port that you have configured for HTTPS: 4388. We suggest that you enter **www.xirrus.com**, **Port 4388** here to make it obvious that HTTP traffic is being proxied in this way.

Continue to Step 5.

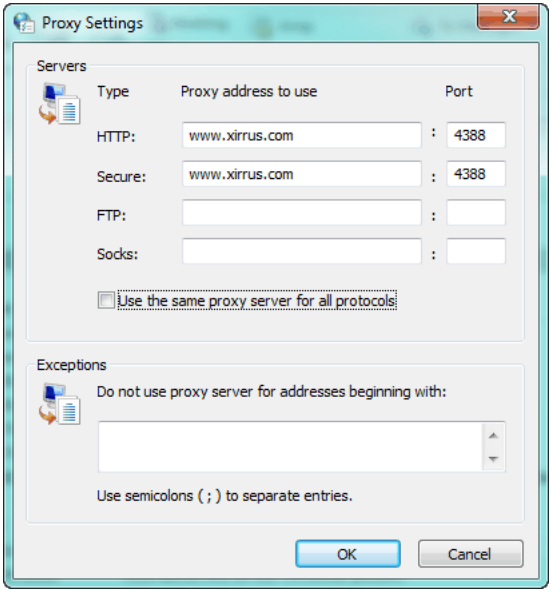


Figure 117. Specify Proxy Servers (Windows)

3. For Apple laptops, open **System Preferences** and select **Network**. The Network dialog is displayed. (Figure 118) Click the **Advanced** button.

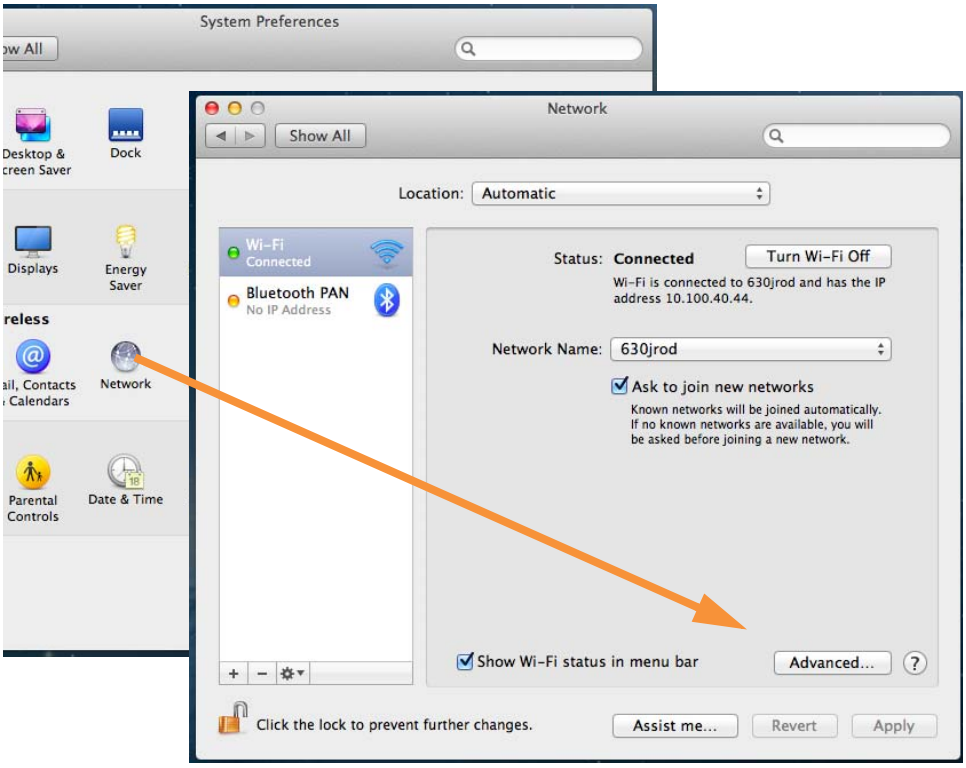


Figure 118. Set up a Proxy Server on each Client (Apple)

4. Select the **Proxies** tab. (Figure 119)

   Check **Secure Web Proxy (HTTPS):** Under **Secure Web Proxy Server**, you can enter any valid address. We suggest that you enter **www.xirrus.com**. (This field is not actually used, but it must be a valid address or domain name). You **must** set the **Port** to **4388**. This is **very** important! This is the Array port that must receive all HTTPS traffic if you are using a proxy server for HTTPS.

Check **Web Proxy (HTTP):** Under **Web Proxy Server**, we suggest that you enter **www.xirrus.com Port 4388** to make it obvious that HTTP traffic is being proxied in this way.

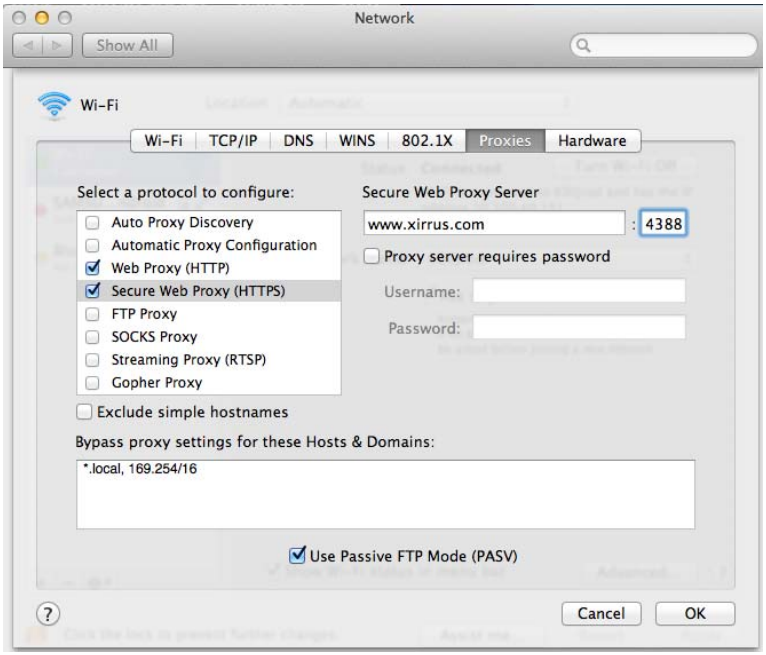


Figure 119. Specify Proxy Servers (Apple)

5. **SSL Certificate**: you must download and install the security certificate from your proxy server—Blue Coat or Netbox Blue. It must be installed on each of your client devices.

Procedure for Configuring Proxy Forwarding on the Array

1. **Enable:** If you wish to use proxy forwarding, select the proxy server type—**Blue Coat** or **Netbox Blue**.

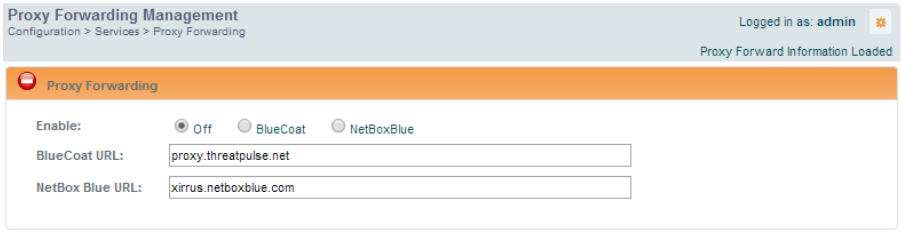


Figure 120. Proxy Forwarding

2. **BlueCoat URL**: If you selected **Blue Coat** above, enter the URL of the proxy server, for example, **http://proxy.threatpulse.net**.
3. **Netbox Blue URL**: If you selected **Netbox Blue** above, enter the actual URL of the proxy server, for example, **xirrus.netboxblue.com**. Note that this default URL is not an actual proxy server—this prevents you from unintentionally forwarding traffic.

VLANs

This is a status-only window that allows you to review the current status of configured VLANs. VLANs are virtual LANs used to create broadcast domains.

You should create VLAN entries on the Array for all of the VLANs in your wired network if you wish to make traffic from those VLANs available on the wireless network. Each tagged VLAN should be associated with a wireless SSID (see "VLAN Management" on page 206). The Array will discard any VLAN-tagged packets arriving on its wired ports, unless the same VLAN has been defined on the Array. See "Undefined VLANs" on page 110.

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN (Step 1 page 207).

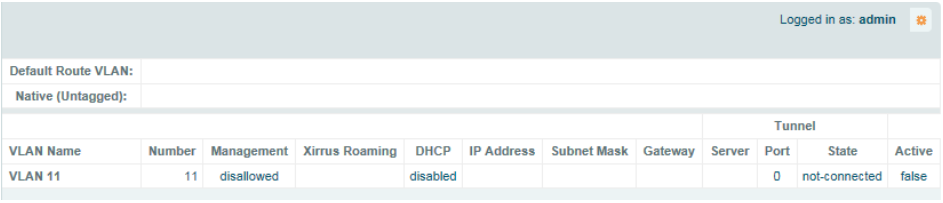


Figure 121. VLANs

For a discussion of implementing Voice over Wi-Fi on the Array, see the ***Xirrus Voice over Wireless Application Note*** *in the Xirrus* ***Resource Center****.*

Understanding Virtual Tunnels

Xirrus Arrays support Layer 2 tunneling. This allows an Array to use tunnels to transport traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 core network. Tunnels may be implemented with:

- The Xirrus Tunnel Server (XTS)—see the Xirrus *Tunnel Server User's Guide*.
- Virtual Tunnel Server (VTS)—see below.

The Array has low overhead and latency for virtual tunnel connections, with high resilience. The Array performs all encryption and decryption in hardware, maintaining wire-rate encryption performance on the tunnel.

Virtual Tunnel Server (VTS)

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from vtun.sourceforge.net. To enable the Array to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in Step 11 on page 208.

VTun may be configured for a number of different tunnel types, protocols, and encryption types. For use with Arrays, we recommend the following configuration choices:

- Tunnel Type: Ether (Ethernet tunnel)
- Protocol: UDP
- Encryption Type: select one of the encryption types supported by VTun (AES and Blowfish options are available)
- Keepalive: yes

VTS Client-Server Interaction

The Array is a client of the Virtual Tunnel Server. When you specify a VTS for an active VLAN-SSID pair, the Array contacts the VTS. The server then creates a tunnel session to the Array. VTun encapsulated packets will cross the Layer 3 network from the Array to the VTS. When packets arrive at the VTS, they will be de-encapsulated and the resultant packets will be passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction.

We recommend that you enable the VTun keep-alive option. This will send a keep-alive packet once per second to ensure that the tunnel remains active. Tunnels can be configured to come up on demand but this is a poor choice for wireless, since tunnel setup can take roughly 5-20 seconds and present a problem for authentication.

VLAN Management

This window allows you to assign and configure VLANs. After creating a new VLAN (added to the list of VLANs), you can modify the configuration parameters of an existing VLAN or delete a selected VLAN. For ArrayOS 6.6 and later releases, you may create up to 64 VLANs (up to 32 on the XR-500 Series and on the XR-620).

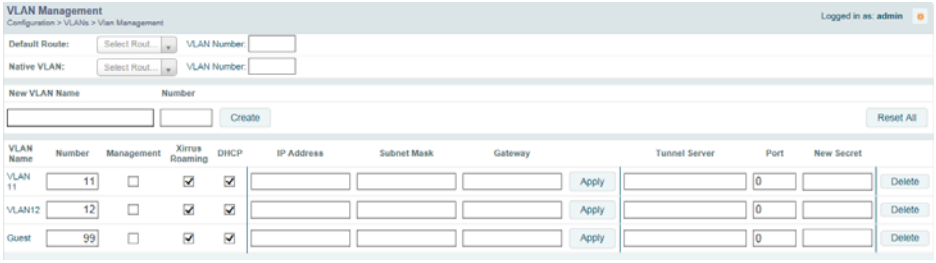


Figure 122. VLAN Management

*The Wireless Array supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Array dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Array (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (**Figure 68 on page 123**)*

It is critical to configure all VLANs to be used on the Array, even those that will be dynamically assigned.

Procedure for Managing VLANs

1. **Default Route:** This option sets a default route from the Array. The Array supports a default route on native and tagged interfaces. Once the default route is configured the Array will attempt to use Address Resolution Protocol (ARP) to find the default router. ARP finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. This option allows you to choose a default VLAN route from the pull-down list. The IP Gateway must be established for this function to work. After changing the **Default Route**, you *must* click the **Save** button *and then reboot*.

2. **Native VLAN**: This option sets whether the Array management is tagged or untagged. If you select a Native VLAN, then that VLAN will use an untagged (Native) link. Otherwise, the Array will use 802.1Q tagging and a specific VLAN ID with management enabled for management of the Array.

3. **New VLAN Name/Number**: Enter a name and number for the new VLAN in this field, then click on the **Create** button. The new VLAN is added to the list.

4. **VLAN Number**: Enter a number for this VLAN (1-4094).

5. **Management**: Check this box to allow management over this VLAN.

6. **Xirrus Roaming**: Check this box to allow roaming over this VLAN.

7. **DHCP**: Check this box if you want the DHCP server to assign the IP address, subnet mask and gateway address to the VLAN automatically, otherwise you must go to the next step and assign these parameters manually.

8. **IP Address**: If the DHCP option is disabled, enter a valid IP address for this VLAN association.

9. **Subnet Mask**: If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.

10. **Gateway**: If the DHCP option is disabled, enter the IP gateway address for this VLAN association.
11. **Tunnel Server**: If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see "Understanding Virtual Tunnels" on page 204.
12. **Port**: If this VLAN is to be tunneled, enter the port number of the tunnel server.
13. **New Secret**: Enter the password expected by the tunnel server.
14. **Delete**: To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.
15. Click the **Save** button if you wish to make your changes permanent.

See Also

VLAN Statistics
VLANs
Tunnels

Tunnels

This read-only window allows you to review the tunnels that have been defined on the Array. It lists all tunnels and their settings, including the type of authentication and the local and remote endpoints for each tunnel.

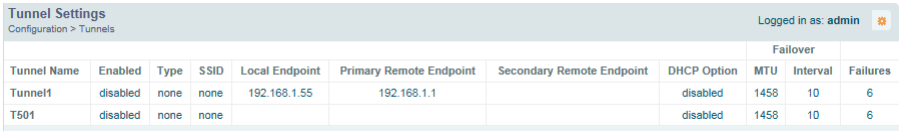


Figure 123. Tunnel Summary

About Xirrus Tunnels

Xirrus Arrays offer GRE (Generic Routing Encapsulation) tunneling with VLAN support. This allows an Array to use tunnels to bridge Layer 2 traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 network. GRE tunneling is quite flexible, and can encapsulate many network layer protocols. As a result, it can support a variety of applications. For example, a Wi-Fi hotspot can allow guest logins and use the tunnel to give guests direct access to the Internet, without allowing access to the local network. In a small office, you may define a tunnel to connect users to the corporate office network. Tunnels may also used when providing cellular offload capability.

Tunnels may be implemented with:

- The Xirrus Tunnel Server (XTS)—see the Xirrus *Tunnel Server User's Guide*. For an additional discussion, see the Xirrus *Tunnel Solutions Application Note* in the Xirrus ***Resource Center***.
- VTS —see "Virtual Tunnel Server (VTS)" on page 205.

To create a tunnel, you specify the **Local Endpoint**, which should be one of the Array's wired ports, and the **Primary Remote Endpoint**. A **Secondary Remote Endpoint** may also be specified in case of a failure at the first endpoint. Traffic for a VLAN-SSID pair is sent in GRE encapsulated packets across the Layer 3 network from the Array to the remote endpoint. When packets arrive, the encapsulation is stripped and the resultant packets are passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for

packets traveling in the other direction. One tunnel is able to transport up to 16 VLANs.

Tunnel Management

This window allows you to create tunnels.

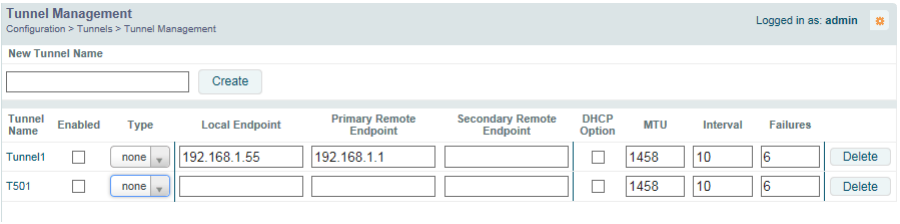


Figure 124. Tunnel Management

Procedure for Managing Tunnels

1. **New Tunnel Name**: Enter a name for the new tunnel in this field, then click on the **Create** button. The new tunnel is added to the list. You may crate up to 250 Layer 3 tunnels.
2. **Enabled**: The new tunnel is created in the disabled state. Click this checkbox to enable it.
3. **Type**: Enter the type of tunnel, **none** or **gre**.
4. **Local Endpoint**: Enter the IP address of the Array Gigabit or 10 Gigabit port where the tunnel is to begin.
5. **Primary Remote Endpoint**: Enter the IP address of the remote endpoint of the tunnel.
6. **Secondary Remote Endpoint**: This provides a failover capability. If the primary tunnel fails, traffic is switched over to the secondary tunnel. Enter the IP address of the remote endpoint of the secondary tunnel.
7. **DHCP Option**: When this option is enabled, the Array snoops station DHCP requests and inserts relay agent information (option 82, in the circuit-ID sub-option) into these DHCP packets. Information inserted includes Array BSSID, SSID name, and SSID encryption type.

8. **MTU**: Set maximum transmission unit (MTU) size.
9. **Interval**: The tunnel mechanism will ping the current remote endpoint periodically to ensure that it is still reachable. Enter the ping interval (in seconds).
10. **Failures**: Enter the number of consecutive ping failures that will cause the Array to consider the tunnel to be down. tunnel to failover to the other remote endpoint.
11. Click the **Save** button if you wish to make your changes permanent.
12. Proceed to SSID Assignments to define the SSIDs (and associated VLANs) for which each tunnel will bridge data. You may create up to 16 tunnels. Each will need an SSID/VLAN pair assigned to it so that it can function properly.

SSID Assignments

This window allows you to select the SSIDs to be bridged by each tunnel. Station traffic for SSIDs assigned will be bridged through a tunnel regardless of whether these SSIDs have VLANs defined for them. If there is a VLAN defined for an SSID that is assigned to a tunnel, then station traffic bridged through that tunnel will be tagged accordingly.

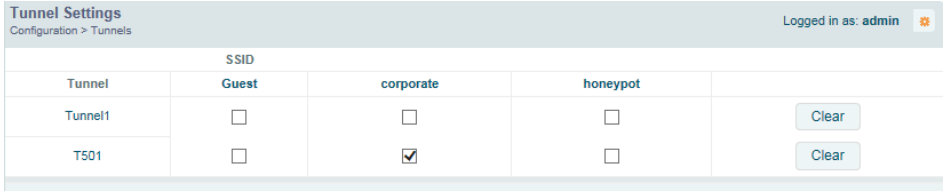


Figure 125. Tunnel SSID Assignments

Procedure for Assigning SSIDs

This window lists the tunnels and SSIDs that you have defined. SSIDs to be tunneled do not need to be associated with a VLAN (see "SSID Management" on page 262).

1. For each tunnel, select the SSIDs that are to be bridged to the remote endpoint. Clear the checkbox for any SSID that you no longer wish to include in the tunnel.
2. Click the **Save** button if you wish to make your changes permanent.

See Also

Tunnels
VLANs
SSIDs

Security

This status- only window allows you to review the Array's security parameters. It includes the assigned network administration accounts, Access Control List (ACL) values, management settings, encryption and authentication protocol settings, and RADIUS configuration settings. There are no configuration options available in this window, but if you are experiencing issues with security, you may want to print this window for your records.

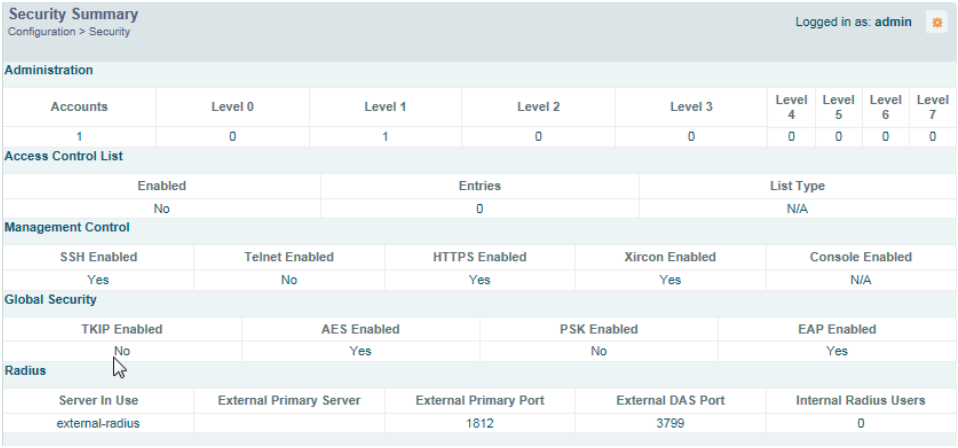


Figure 126. Security

For additional information about wireless network security, refer to:

- **"Security Planning" on page 50**
- **"Understanding Security" on page 214**
- **The Security section of "Frequently Asked Questions" on page 492**

For information about secure use of the WMI, refer to:

- **"Certificates and Connecting Securely to the WMI" on page 217**
- **"Using the Array's Default Certificate" on page 217**
- **"Using an External Certificate Authority" on page 218**
- **"About Creating Admin Accounts on the RADIUS Server" on page 223**
- **"About Creating User Accounts on the RADIUS Server" on page 241**

Security settings are configured with the following windows:

- **"Admin Management" on page 219**
- **"Admin Privileges" on page 221**
- **"Admin RADIUS" on page 223**
- **"Management Control" on page 226**
- **"Access Control List" on page 234**
- **"Global Settings" on page 236**
- **"External Radius" on page 240**
- **"Internal Radius" on page 244**
- **"Active Directory" on page 246**
- **"Rogue Control List" on page 250**
- **"OAuth 2.0 Management" on page 251**

Understanding Security

The Xirrus Wireless Array incorporates many configurable security features. After initially installing an Array, always change the default administrator password (the default is admin), and choose a strong replacement password (containing letters, numbers and special characters). When appropriate, issue read-only administrator accounts.

Other security considerations include:

- **SSH versus Telnet**: Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. SSH-2 provides stronger security than SSH-1. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing**: The optional Xirrus Management System (XMS) offers powerful management features for small or large Xirrus wireless deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.

- **Choosing an encryption method**: Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The Array allows you to establish the following data encryption configuration options:
  - **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
  - **WEP (Wired Equivalent Privacy)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
  - **WPA (Wi-Fi Protected Access) and WPA2**—these are much stronger encryption modes than WEP, using TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) to encrypt data.

    WPA solves security issues with WEP. It also allows you to establish encryption keys on a per-user-basis, with key rotation for added security. In addition, TKIP provides Message Integrity Check (MIC) functionality and prevents active attacks on the wireless network.

    AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, WPA2 with AES is highly recommended for Enterprise networks.

  Any of the above encryption methods can be used and an Array can support multiple encryption methods simultaneously, but only one method may be selected per SSID (except that selecting **WPA-Both** allows WPA and WPA2 to be used at the same time on the same SSID).

Otherwise, if multiple security methods are needed, you must define multiple SSIDs.

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see "SSID Management" on page 262). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security>Global Settings** window under **WPA Settings** (see "Global Settings" on page 236).

- **Choosing an authentication method**: User authentication ensures that users are who they say they are. For this purpose, the Array allows you to choose between the following user authentication methods:
  - **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the Array.

    This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.
  - **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the Wireless Array) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.
  - **MAC Address ACLs (Access Control Lists)**—MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC address of each user in the Allow list. In

the event of a lost or stolen MAC adapter, enter the affected MAC address in the Deny list. The Wireless Array will accept up to 1,000 ACL entries.

Certificates and Connecting Securely to the WMI

When you point your browser to the Array to connect to the WMI, the Array presents an X.509 security certificate to the browser to establish a secure channel. One significant piece of information in the certificate is the Array's host name. This ties the certificate to a particular Array and ensures the client that it is connecting to that host.

Certificate Authorities (CAs) are entities that digitally sign certificates, using their own certificates (for example, VeriSign is a well-known CA). When the Array presents its certificate to the client's browser, the browser looks up the CA that signed the certificate to decide whether to trust it. Browsers ship with a small set of trusted CAs already installed. If the browser trusts the certificate's CA, it checks to ensure the host name (and IP address) match those on the certificate. If any of these checks fail, you get a security warning when connecting to the WMI.

The Array ships with a default certificate that is signed by the Xirrus CA. You may choose to use this certificate, or to use a certificate issued by the CA of your choice, as described in the following sections:

- Using the Array's Default Certificate
- Using an External Certificate Authority

Using the Array's Default Certificate

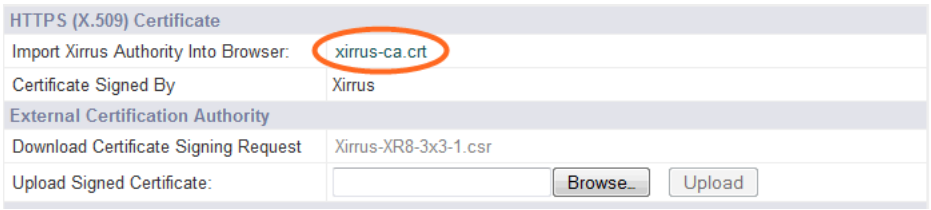


Figure 127. Import Xirrus Certificate Authority

The Array's certificate is signed by a Xirrus CA that is customized for your Array and its current host name. By default, browsers will not trust the Array's certificate. You may import the Xirrus certificate to instruct the browser to trust the Xirrus CA on all future connections to Arrays. The certificate for the Xirrus CA is available on the Array, so that you can import it into your browser's cache of trusted CAs (right alongside VeriSign, for example). On the Management Control window of the WMI you will see the **xirrus-ca.crt** file. (Figure 127)

By clicking and opening this file, you can follow your browser's instructions and import the Xirrus CA into your CA cache (see "Spanning Tree Protocol: this protocol is used in Layer 2 networks to turn off ports when necessary to prevent network loops. It is Off by default, and is turned on automatically if you are using WDS to interconnect Arrays using wireless links. Use the On button to enable spanning tree if your network topology requires it. See "Spanning Tree Status" on page 105." on page 231 for more information). This instructs your browser to trust any of the certificates signed by the Xirrus CA, so that when you connect to any of our Arrays you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the Array. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for 'hostname'.

Since an Array's certificate is based on the Array's host name, any time you change the host name the Array's CA will regenerate and sign a new certificate. This happens automatically the next time you reboot after changing the host name. If you have already installed the Xirrus CA on a browser, this new Array certificate should automatically be trusted.

When you install the Xirrus CA in your browser, it will trust a certificate signed by any Xirrus Array, as long as you connect using the Array's host name.

Using an External Certificate Authority

If you prefer, you may install a certificate on your Array signed by an outside CA.

Why use a certificate from an external CA? The Array's certificate is used for security when stations attempt to associate to an SSID that has Web Page Redirect (captive portal) enabled. In this case, it is preferable for the Array to present a certificate from an external CA that is likely to be trusted by most browsers. When

a WPR login page is presented, the user will not see a security error if the Array's certificate was obtained from an external CA that is already trusted by the user's browser.

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the Array after you obtain it from the CA. This certificate will be tied to the Array's host name and private key. See "External Certification Authority" on page 232 for more details.

Admin Management

This window allows you to manage network administrator accounts (create, modify and delete). It also allows you to limit account access to a read only status. When finished, click the **Save** button if you wish to make your changes permanent.

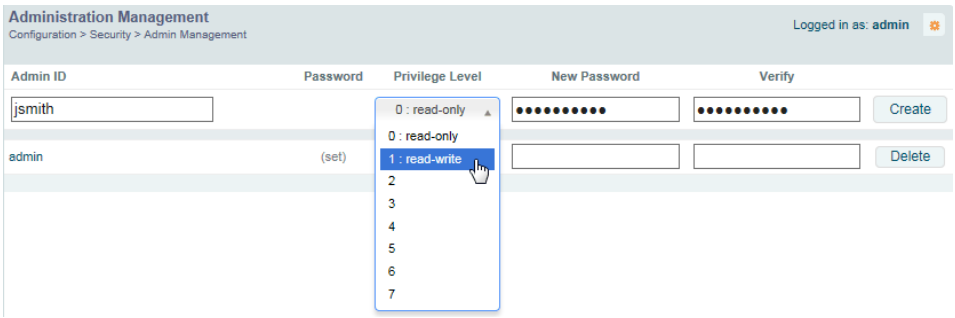


Figure 128. Admin Management

Procedure for Creating or Modifying Network Administrator Accounts

1. **Admin ID:** Enter the login name for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive.
2. **Read/Write**: Choose **1:read-write** if you want to give this administrator ID full read/write privileges, or choose **0:read-only** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations. Or you may select one of your custom-defined privilege levels (see "Admin Privileges" on page 221).

3. **New Password**: Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive.
4. **Verify**: Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).
5. Click on the **Create** button to add this administrator ID to the list.
6. Click the **Save** button if you wish to make your changes permanent.

See Also

Admin Privileges
External Radius
Global Settings (IAP)
Internal Radius
Management Control

Admin Privileges

This window provides a detailed level of control over the privileges of Array administrators. Administrators may be assigned one of eight **Privilege Levels**. You may define the privilege level of each major feature (**Configuration Section**) that may be configured on the Array. For example, say that you set the privilege level to 4 for Reboot Array, Security, Radius Server, and SNMP, and you leave all other configuration sections at the default privilege level of 1. In this case, any administrator with a privilege level of 4 or higher may perform any operation on the Array, while an administrator with a privilege level lower than 4 but at least 1 may perform any operation except those whose level was set to 4. An error message will be displayed if an operation is attempted without a sufficient privilege level.

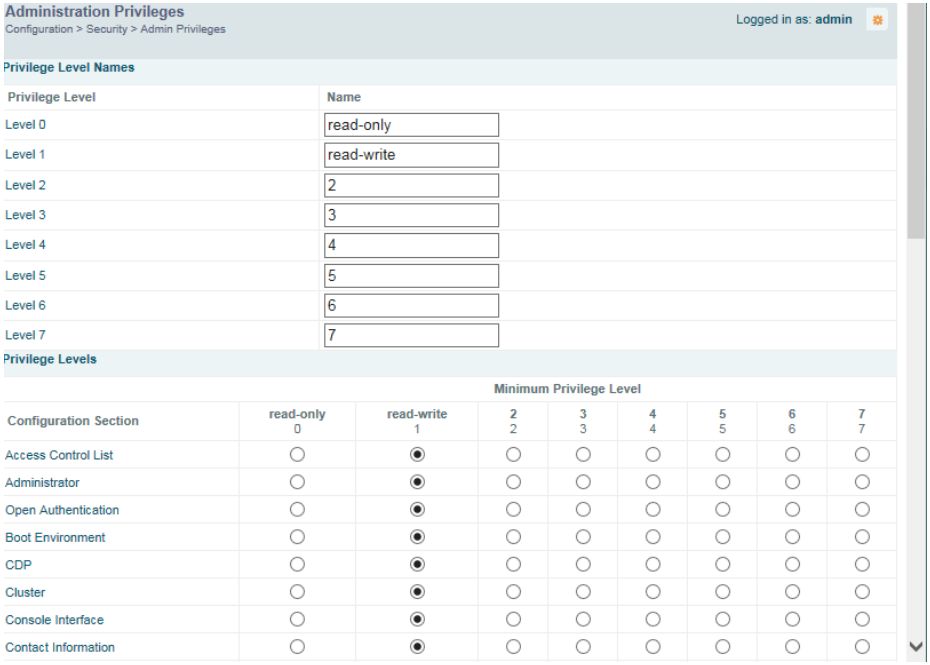


Figure 129. Admin Privileges

Privilege level 0 is **read-only**. As a minimum, all administrators have permission for read access to all areas of Array configuration. Higher privilege levels may be used to define additional privileges for specific configuration sections.

If you are using an Admin RADIUS server to define administrator accounts, please see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" on page 503 to set the privilege level for each administrator.

Procedure for Configuring Admin Privileges

1. **Privilege Level Names** (optional): You may assign a **Name** to each Privilege Level. The name may be used to describe the access granted by this level. By default, levels **0** and **1** are named **read-only** and **read-write**, respectively, and levels **2** through **7** have the same name as their level number.
2. **Privilege Levels**: Use this section to assign a **Minimum Privilege Level** to selected **Configuration Sections** as desired. By default, all sections are assigned level 1. When you select a higher privilege level for a configuration section, then only administrators who have at least that privilege level will be able to make configuration changes to that section.
3. You may click **^** at the bottom of any row to toggle the values in the entire column to either on or off.
4. Click the **Save** button if you wish to make your changes permanent.

See Also

External Radius
Groups
Admin Management
Admin RADIUS
Security

Admin RADIUS

This window allows you to set up authentication of network administrators via RADIUS. Using RADIUS to control administrator accounts for logging in to Arrays has these benefits:

- Centralized control of administrator accounts.
- Less effort—you don't have to set up user names and passwords on each Array; just enter them once on the RADIUS server and then all of the Arrays can pull from the RADIUS server.
- Enforced policies—you may set password rules (e.g., passwords must contain at least one number and be at least 12 characters in length), and you may set expiration times for passwords.

Admin RADIUS settings override any local administrator accounts configured on the Admin Management window. If you have Admin RADIUS enabled, all administrator authentication is done via the configured RADIUS servers. The only exception to this is when you are connected via the Console port (using CLI). If you are using the Console port, the Array will authenticate administrators using accounts configured on the Admin Management window first, and then use the RADIUS servers. This provides a safety net to be ensure that you are not completely locked out of an Array if the RADIUS server is down.

About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Xirrus-Admin-Role** attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its Xirrus-Admin-Role attribute to the desired **Privilege Level Name** string, as defined in "Admin Privileges" on page 221. For more information about the RADIUS VSAs used by Xirrus, see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" on page 503.

When configuring administrator accounts on the RADIUS server, you must observe the same restrictions for length and legal characters as when creating these accounts on the Array using the Admin Management window: the user name and password must be between 5 and 50 characters, inclusive.

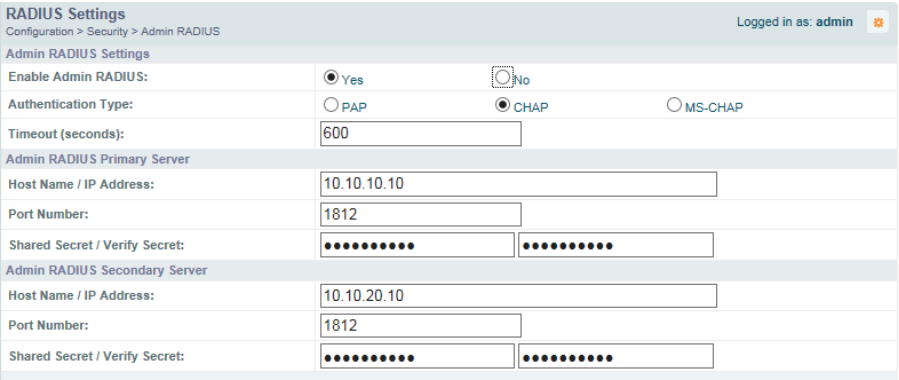


Figure 130. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable administrator authentication via RADIUS, and to set up primary and secondary servers to use for authentication of administrators attempting to log in to the Array.

1. **Admin RADIUS Settings:**

   a. **Enable Admin RADIUS**: Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.

   b. **Authentication Type**: Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).

      - PAP (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
      - CHAP (Challenge-Handshake Authentication Protocol) is a more secure protocol. The login request is sent using a one-way hash function.

   c. **Timeout (seconds)**: Define the maximum idle time (in seconds) before the RADIUS server's session times out. The default is 600 seconds.

2. **Admin RADIUS Primary Server**: This is the RADIUS server that you intend to use as your primary server.
   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.
   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.
   c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

   The shared secret that you define must match the secret used by the RADIUS server.

3. **Admin RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will "failover" to the secondary RADIUS server (defined here).
   a. **Host Name / IP Address**: Enter the IP address or domain name of this RADIUS server.
   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.
   c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

Management Control

This window allows you to enable or disable the Array management interfaces and set their inactivity time-outs. The range is 300 (default) to 100,000 seconds.

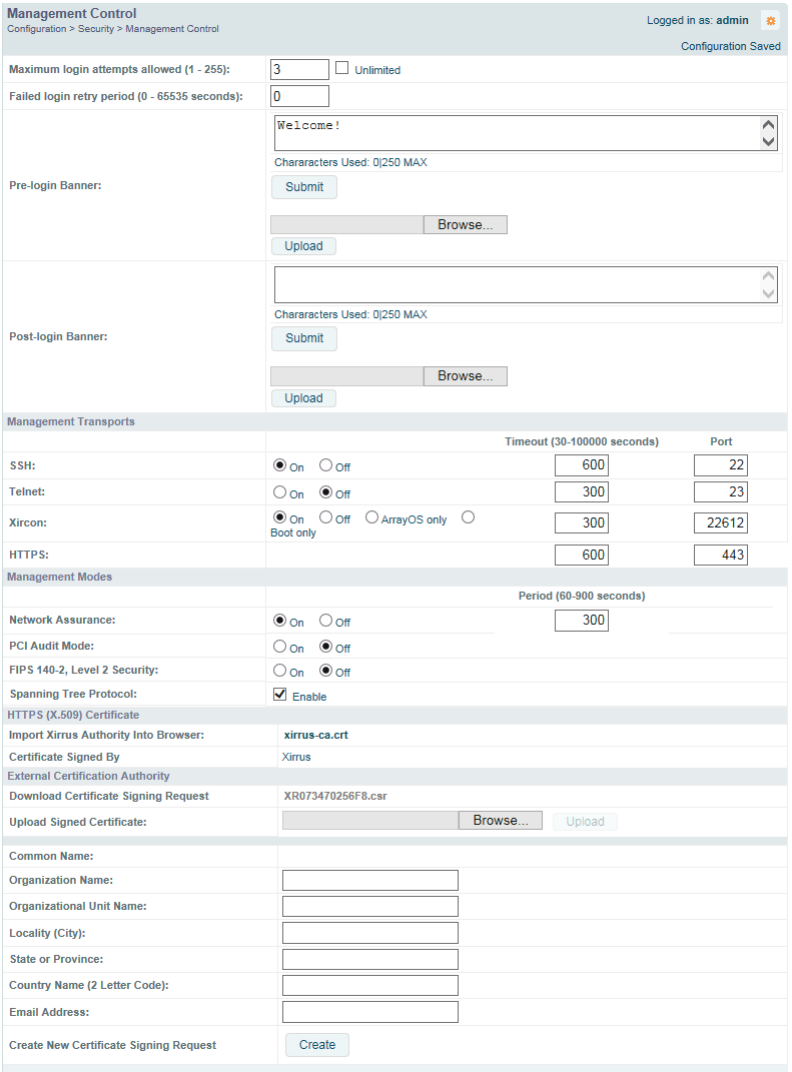


Figure 131. Management Control

Procedure for Configuring Management Control

1. **Management Settings:**

   a. **Maximum login attempts allowed (1-255)**: After this number of consecutive failing administrator login attempts via ssh or telnet, the **Failed login retry period** is enforced. The default is 3.

   b. **Failed login retry period (0-65535 seconds)**: After the maximum number (defined above) of consecutive failing administrator login attempts via ssh or telnet, the administrator's IP address is denied access to the Array for the specified period of time (in seconds). The default is 0.

   c. **Pre-login Banner**: Text that you enter here will be displayed below the WMI login prompt. (Figure 132) Click the **Submit** button when done typing.

      If you wish to display more than 256 characters of text (for instance, to display usage restrictions for the wireless network), you may upload a text file. Click **Choose File** and browse to the file. Click **Upload** when done.

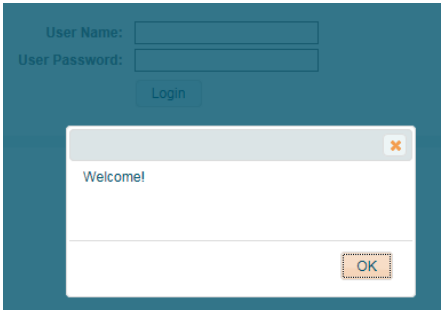


Figure 132. Pre-login Banner

   d. **Post-login Banner**: Text that you enter here will be displayed in a message box after a user logs in to the WMI.

      If you wish to display more than 256 characters of text, upload a text file. Click **Choose File** and browse to the file, then click **Upload**.

2. **SSH**

   a. **On/Off**: Choose **On** to enable management of the Array over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the Array. SSH clients used for connecting to the Array must be configured to use SSH-2.

   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

   c. **Port**: Enter a value in this field to define the port used by SSH. The default port is 22.

3. **Telnet:**

   a. **On/Off**: Choose **On** to enable Array management over a Telnet connection, or **Off** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.

   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

   c. **Port**: Enter a value in this field to define the port used by Telnet. The default port is 23.

4. **Xircon**

   The Xircon utility connects to Xirrus Arrays that do not have a physical console port, or whose console port is not accessible. Please see "Securing Low Level Access to the Array" on page 76 for more information about Xircon. You can enable or disable Xircon access to the Array as instructed below.

! *Warning: If you disable Xircon access completely on models that have no console port, you **must** ensure that you do not lose track of the username and password to log in to CLI/WMI! There is no way to recover from a lost password, other than returning the Array to Xirrus.*

a. **On/Off**: Choose **On** to enable Xircon access to the Array at the ArrayOS (CLI) and Xirrus Boot Loader (XBL) levels, or **Off** to disable access at both levels. On models that have no console port, Xircon access is **On** by default. On all other Array models, Xircon access is **Off** by default.

b. **ArrayOS only**: Choose this radio button to enable Xircon access at the ArrayOS level only (i.e., Xircon can access CLI only). Access to the Array at the Xirrus Boot Loader (XBL) level is disabled.

c. **Boot only**: Choose this radio button to enable Xircon access at the Xirrus Boot Loader (XBL) level only. ArrayOS level (CLI) access to the Array is disabled.

d. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Xircon connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

e. **Port**: Enter a value in this field to define the port used by Xircon. The default port is 22612.

5. **Console**

a. **On/Off**: Choose **On** to enable management of the Array via a serial connection, or choose **Off** to disable this feature.

b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

6. **HTTPS**
   a. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.
   b. **Port**: Enter a value in this field to define the port used by SSH. The default port is 443.
7. **Management Modes**
   a. **Network Assurance**: Click the **On** button to enable this mode. Network assurance checks network connectivity to each server that you configure, such as the NTP server, RADIUS servers, SNMP trap hosts, etc. By proactively identifying network resources that are unavailable, the network manager can be alerted of problems potentially before end-users notice an issue. The distributed intelligence of Arrays provides this monitoring at multiple points across the network, adding to the ability to isolate the problem and expedite the resolution

      Connectivity is checked when you configure a server. If a newly configured server is unreachable, you will be notified directly and a Syslog entry is created. Configured servers are checked once per **Period** which by default is 300 seconds (five minutes). Servers are checked regardless of whether they are configured as IP addresses or host names.

      If a server becomes unreachable, a Syslog message is generated. When the server again becomes reachable, another Syslog message is generated.

      To view the status of all configured servers checked by this feature, please see "Network Assurance" on page 109.

b. **Spanning Tree Protocol**: this protocol is used in Layer 2 networks to turn off ports when necessary to prevent network loops. It is **Off** by default, and is turned on automatically if you are using WDS to interconnect Arrays using wireless links. Use the **On** button to enable spanning tree if your network topology requires it. See "Spanning Tree Status" on page 105.

8. **HTTPS (X.509) Certificate**

ArrayOS releases 6.5 and above only support 2048-bit certificates, while previous releases only support 1024-bit certificates. The Array saves data related to previous 1024-bit and current 2048-bit certificates separately, thus ArrayOS can be upgraded or downgraded without losing any of this data. When ArrayOS is upgraded to 6.5, a new self-signed certificate will be automatically generated.

If you have imported a previous (pre-Release 6.5 version) Xirrus CA-signed certificate into your browser, the trusted Xirrus CA needs to be updated. Delete the current Xirrus CA in the browser. Upgrade the Array to release 6.5 or above and then download the new **xirrus-ca.crt** *file and import it into the browser as a trusted CA, as explained below.*

Similarly, if you are using a certificate signed by an external CA, you will need to update and replace that certificate on the Array.

a. **Import Xirrus Authority into Browser**: This feature imports the Xirrus Certificate Authority (CA) into your browser (for a discussion, please see "Certificates and Connecting Securely to the WMI" on page 217). Click the link (**xirrus-ca.crt**), and then click **Open** to view or install the current Xirrus CA certificate. Click **Install Certificate** to start your browser's Certificate Install Wizard. We recommend that you use this process to install Xirrus as a root authority in your browser.

When you assign a **Host Name** to your Array using the Express Setup window, then the next time you reboot the Array it automatically creates a security certificate for that host name. That

certificate uses Xirrus as the signing authority. Thus, in order to avoid having certificate errors on your browser when using WMI:

- You must have assigned a host name to the Array and rebooted at some time after that.
- Use **Import Xirrus Authority into Browser**
- Access WMI by using the host name of the Array rather than its IP address.

b. **HTTPS (X.509) Certificate Signed By**: This read-only field shows the signing authority for the current certificate.

9. **External Certification Authority**

This step and Step 10 allow you to obtain a certificate from an external authority and install it on an Array. "Using an External Certificate Authority" on page 218 discusses reasons for using an external CA.

For example, to obtain and install a certificate from VeriSign on the Array, follow these steps:

- If you don't already have the certificate from the external (non-Xirrus) Certificate Authority, see Step 10 to create a request for a certificate.
- Use Step 9a to review the request and copy its text to send to VeriSign.
- When you receive the new certificate from VeriSign, upload it to the Array using Step 9b.

External Certification Authority has the following fields:

a. **Download Certificate Signing Request**: After creating a certificate signing request (.csr file—Step 10), click the **View** button to review it. If it is satisfactory, click the name of the .csr file to display the text of the request. You can then copy this text and use it as required by the CA. You may also click on the filename of the .csr file to download it to your local computer.

b. **Upload Signed Certificate**: To use a custom certificate signed by an authority other than Xirrus, use the **Browse** button to locate the certificate file, then click **Upload** to copy it to the Array. The Array's web server will be restarted and will pick up the new certificate. This will terminate any current web sessions, and you will need to reconnect and re-login to the Array.

10. **To create a Certificate Signing Request**

    a. Fill in the fields in this section: **Common Name, Organization Name, Organizational Unit Name, Locality (City), State or Province, Country Name,** and **Email Address**. Spaces may be used in any of the fields, except for Common Name, Country Name, or Email Address. Click the **Create** button to create the certificate signing request. See Step 9 above to use this request.

11. Click the **Save** button if you wish to make your changes permanent.

See Also

Network Interfaces - to enable/disable management over an Ethernet interface
Global Settings (IAP) - to enable/disable management over IAPs
Admin Management
External Radius
Global Settings (IAP)
Internal Radius
Access Control List
Security

Access Control List

This window allows you to enable or disable the use of the global Access Control List (ACL), which controls whether a station with a particular MAC address may associate to the Array. You may create station access control list entries and delete existing entries, and control the type of list.

There is only one global ACL, and you may select whether its type is an Allow List or a Deny List, or whether use of the list is disabled.

There is also a per-SSID ACL (see "Per-SSID Access Control List" on page 276). If the same MAC address is listed in both the global ACL and in an SSID's ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

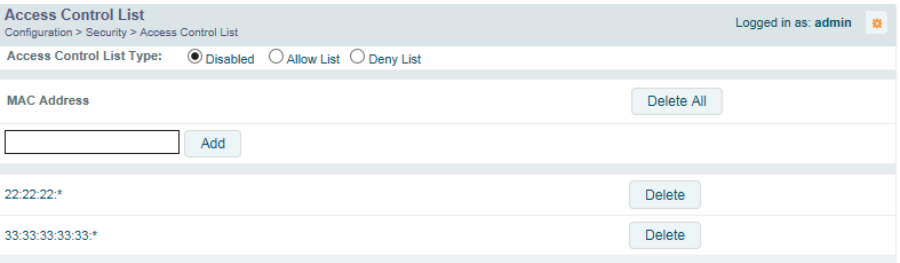


Figure 133. Access Control List

Procedure for Configuring Access Control Lists

1. **Access Control List Type:** Select **Disabled** to disable use of the Access Control List, or select the ACL type—either **Allow List** or **Deny List**.
    - **Allow List**: Only allows the listed MAC addresses to associate to the Array. All others are denied.
    - **Deny List**: Denies the listed MAC addresses permission to associate to the Array. All others are allowed.

    In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

2. **MAC Address**: If you want to add a MAC address to the ACL, enter the new MAC address here, then click on the **Add** button. The MAC address is added to the ACL. You may use a wildcard (*) for one or more digits to match a range of addresses. You may create up to 1000 entries.
3. **Delete**: You can delete selected MAC addresses from this list by clicking their **Delete** buttons.
4. Click the **Save** button if you wish to make your changes permanent.

See Also

External Radius
Global Settings (IAP)
Internal Radius
Management Control
Security
Station Status Windows (list of stations that have been detected by the Array)

Global Settings

This window allows you to establish the security parameters for your wireless network, including WEP, WPA, WPA2 and RADIUS authentication. When finished, click the **Save** button if you wish to make your changes permanent.

For additional information about wireless network security, refer to "Security Planning" on page 50 and "Understanding Security" on page 214.

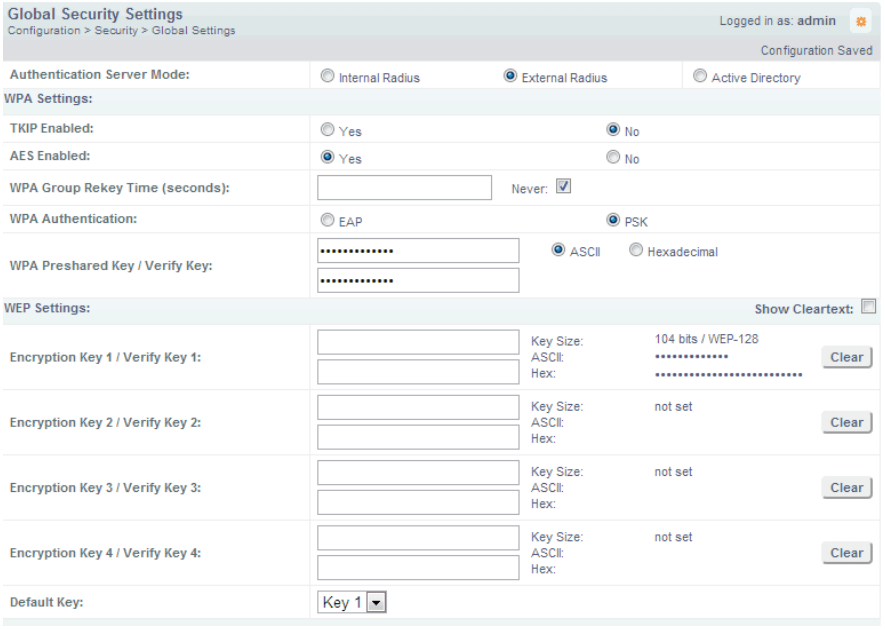


Figure 134. Global Settings (Security)

Procedure for Configuring Network Security

1. **Authentication Server Mode**: Choose the type of Authentication Server that you will use for authenticating wireless users:
   - **Internal RADIUS** defines wireless user accounts locally on the Array. See "Internal Radius" on page 244.
   - **External RADIUS** defines wireless user accounts on a RADIUS server external to the Array. See "External Radius" on page 240.

- **Active Directory** defines wireless user accounts on an Active Directory server external to the Array. See "Active Directory" on page 246.

WPA Settings

These settings are used if the **WPA** or **WPA2** encryption type is selected on the **SSIDs >SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

2. **TKIP Enabled**: Choose **Yes** to enable TKIP (Temporal Key Integrity Protocol), or choose **No** to disable TKIP.

TKIP encryption does not support high throughput rates for 802.11n, per the IEEE 802.11n specification.

*TKIP should never be used for **WDS** links on XR Arrays.*

3. **AES Enabled**: Choose **Yes** to enable AES (Advanced Encryption Standard), or choose **No** to disable AES. If both AES and TKIP are enabled, the station determines which will be used.
4. **WPA Group Rekey Time (seconds)**: Enter a value to specify the group rekey time (in seconds). The default is **Never**.
5. **WPA Preshared Key / Verify Key**: If you enabled PSK, enter a passphrase here, then re-enter the passphrase to verify that you typed it correctly.

WEP Settings

These settings are used if the **WEP** encryption type is selected on the **SSIDs > SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

Click the **Show Cleartext** button to make the text that you type in to the Key fields visible.

WEP encryption does not support high throughput rates or features like frame aggregation or block acknowledgments for 802.11n, per the IEEE 802.11n specification.

WEP should never be used for WDS links on Arrays.

6. **Encryption Key 1 / Verify Key 1:**

   Key Size: Key length is automatically computed based on the Encryption Key that you enter

   - 5 ASCII characters (10 hex) for 40 bits (WEP-64)
   - 13 ASCII characters for (26 hex) 104 bits (WEP-128)

   Encryption Key 1 / Verify Key 1: Enter an encryption key in ASCII or hexadecimal. The ASCII and translated hexadecimal values will appear to the right if you selected the **Show Cleartext** button.

   Re-enter the key to verify that you typed it correctly. You may include special ASCII characters, except for the double quote symbol (“).

7. **Encryption Key 2 to 4/ Verify Key 2 to 4/ Key Mode/Length** (optional): If desired, enter up to four encryption keys, in the same way that you entered the first key.

8. **Default Key**: Choose which key you want to assign as the default key. Make your selection from the pull-down list.

9. Click the **Save** button if you wish to make your changes permanent.

After configuring network security, the configuration must be applied to an SSID for the new functionality to take effect.

See Also

Admin Management
External Radius
Internal Radius
Access Control List
Management Control
Security
Security Planning
SSID Management

External Radius

This window allows you to define the parameters of an external RADIUS server for user authentication. To set up an external RADIUS server, you must choose **External Radius** as the **Authentication Server Mode** in "Global Settings" on page 236.

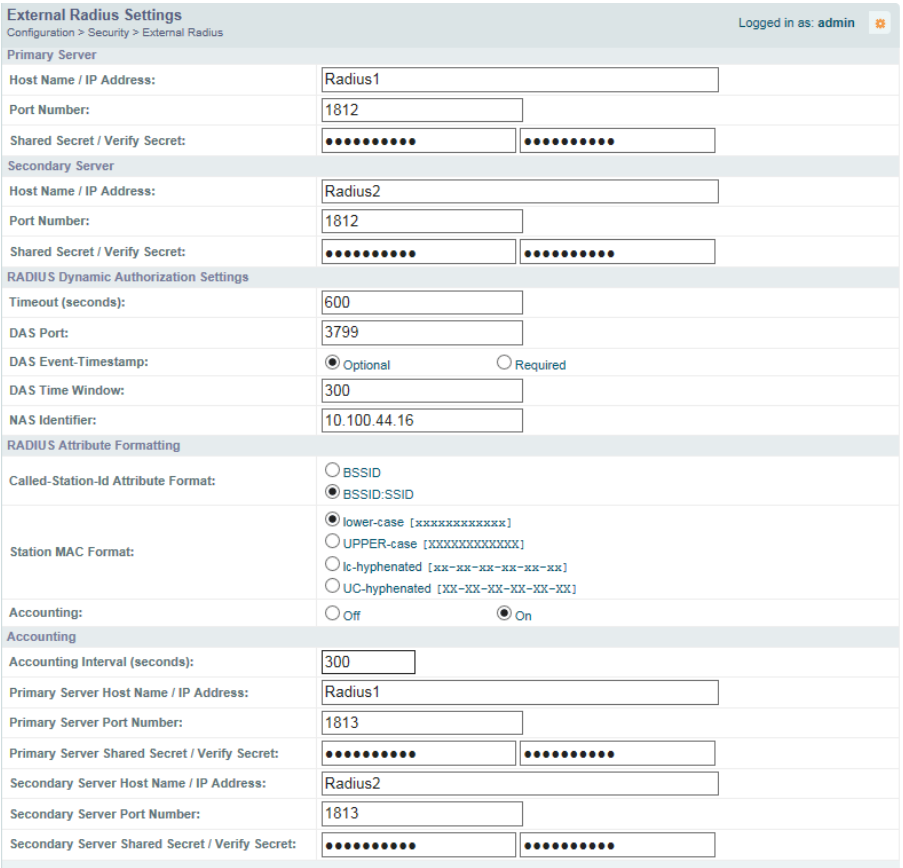


Figure 135. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see "Understanding Groups" on page 280. User groups allow you to easily apply a uniform configuration to a user on the Array.

About Creating User Accounts on the RADIUS Server

A number of attributes of user (wireless client) accounts are controlled by RADIUS Vendor Specific Attributes (VSAs) defined by Xirrus. For example, you would use the VSA named Xirrus**-User-VLAN** if you wish to set the VLAN for a user account in RADIUS. For more information about the RADIUS VSAs used by Xirrus, see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" on page 503.

Procedure for Configuring an External RADIUS Server

1. **Primary Server:** This is the external RADIUS server that you intend to use as your primary server.
   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.
   b. **Port Number**: Enter the port number of this external RADIUS server. The default is 1812.
   c. **Shared Secret / Verify Secret**: Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

   The shared secret that you define must match the secret used by the external RADIUS server.

2. **Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will "failover" to the secondary RADIUS server (defined here).
   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.
   b. **Port Number**: Enter the port number of this external RADIUS server. The default is 1812.
   c. **Shared Secret / Verify Secret**: Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

3. **Settings (RADIUS Dynamic Authorization)**: Some RADIUS servers have the ability to contact the Array (referred to as an NAS, see below) to terminate a user with a Disconnect Message (DM). Or RADIUS may send a Change-of-Authorization (CoA) Message to the Array to change a user's privileges due to changing session authorizations. This implements RFC 5176—Dynamic Authorization Extensions to RADIUS.

   a. **Timeout (seconds)**: Define the maximum idle time before the RADIUS server's session times out. The default is 600 seconds.

   b. **DAS Port**: RADIUS will use the DAS port on the Array for Dynamic Authorization Extensions to RADIUS. The default port is **3799**.

   c. **DAS Event-Timestamp**: The Event-Timestamp Attribute provides a form of protection against replay attacks. If you select **Required**, both the RADIUS server and the Array will use the Event-Timestamp Attribute and check that it is current within the **DAS Time Window**. If the Event-Timestamp is not current, then the DM or CoA Message will be silently discarded.

   d. **DAS Time Window**: This is the time window used with the **DAS Event-Timestamp**, above.

   e. **NAS Identifier**: From the point of view of a RADIUS server, the Array is a client, also called a Network Access Server (NAS). Enter the NAS Identifier (IP address) that the RADIUS servers expect the Array to use—normally the IP address of the Array's Gigabit1 port.

4. **RADIUS Attribute Formatting Settings**: Some RADIUS servers, especially older versions, expect information to be sent to them in a legacy format. These settings are provided for the unusual situation that requires special formatting of specific types of information sent to the RADIUS server. Most users will not need to change these settings.

   a. **Called-Station-Id Attribute Format**: Define the format of the **Called-Station-Id** RADIUS attribute sent from the Array—**BSSID:SSID** (default) or **BSSID**.

b. **Station MAC Format**: Define the format of the **Station MAC** RADIUS attribute sent from the Array—lower-case or upper-case, hyphenated or not. The default is lower-case, not hyphenated.

5. **Accounting Settings**:

   Note that RADIUS accounting start packets sent by the Array will include the client station's Framed-IP-Address attribute.

   a. **Accounting Interval (seconds)**: Specify how often Interim records are to be sent to the server. The default is 300 seconds.

   b. **Primary Server Host Name / IP Address**: Enter the IP address or domain name of the primary RADIUS accounting server that you intend to use.

   c. **Primary Port Number**: Enter the port number of the primary RADIUS accounting server. The default is 1813.

   d. **Primary Shared Secret / Verify Secret**: Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.

   e. **Secondary Server Host Name / IP Address** (optional): If desired, enter an IP address or domain name for an alternative RADIUS accounting server. If the primary server becomes unreachable, the Array will "failover" to this secondary server (defined here).

   f. **Secondary Port Number**: If using a secondary accounting server, enter its port number. The default is 1813.

   g. **Secondary Shared Secret / Verify Secret**: If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.

6. Click the **Save** button if you wish to make your changes permanent.

See Also

Admin Management
Global Settings (IAP)

Internal Radius
Access Control List
Management Control
Security
Understanding Groups

Internal Radius

This window allows you to define the parameters for the Array's internal RADIUS server for user authentication. However, the internal RADIUS server will only authenticate wireless clients that want to associate to the Array. This can be useful if an external RADIUS server is not available. To set up the internal RADIUS server, you must choose **Internal Radius** as the **Authentication Server Mode** in "Global Settings" on page 236.

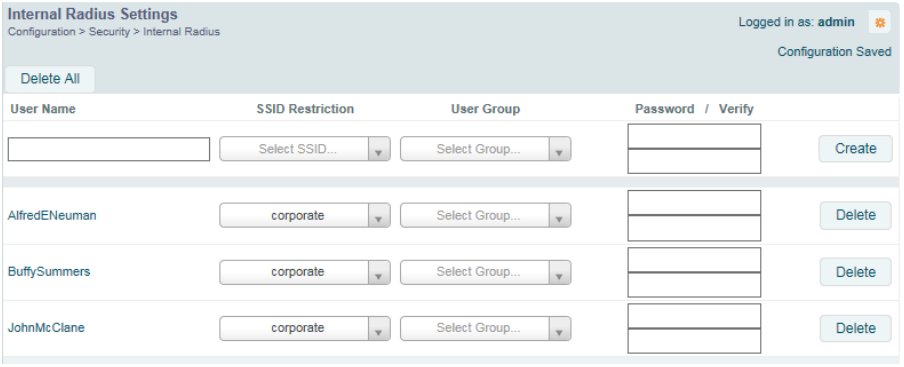


Figure 136. Internal RADIUS Server

Clients using PEAP may have difficulty authenticating to the Array using the Internal RADIUS server due to invalid security certificate errors. To prevent this problem, the user may disable the ***Validate Server Certificate*** *option on the station. Do this by displaying the station's wireless devices and then displaying the properties of the desired wireless interface. In the security properties, disable* ***Validate server certificate****. In some systems, this may be found by setting the authentication method to PEAP and changing the associated settings.*

Procedure for Creating a New User

1. **User Name:** Enter the name of the user that you want to authenticate to the internal RADIUS server. You may enter up to 1000 users (up to 256 on the XR-500 Series and on the XR-620, or up to 480 on the XR-630 and on the XR-1000 Series).
2. **SSID Restriction**: (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the pull-down list.
3. **User Group**: (Optional) If you want to make this user a member of a previously defined user group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 280.
4. **Password**: (Optional) Enter a password for the user.
5. **Verify**: (Optional) Retype the user password to verify that you typed it correctly.
6. Click on the **Create** button to add the new user to the list.

Procedure for Managing Existing Users

1. **SSID Restriction:** (Optional) If you want to restrict a user to associating to a particular SSID, choose an SSID from its pull-down list.
2. **User Group**: (Optional) If you want to change the user's group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 280.
3. **Password**: (Optional) Enter a new password for the selected user.
4. **Verify Password**: (Optional) Retype the user password to verify that you typed it correctly.
5. If you want to delete one or more users, click their **Delete** buttons.
6. Click the **Save** button if you wish to make your changes permanent.

See Also

Admin Management
External Radius

Global Settings (IAP)
Access Control List
Management Control
Security
Understanding Groups

Active Directory

Some smaller Arrays/APs have less memory (XR-500/1000 Series and XR-620) and are not able to run all ArrayOS features at the same time. You will receive an error message if you attempt to configure a feature when there is not enough memory left.

This window allows you to configure 802.1x user authentication without needing to set up and use an External Radius server. The Array performs authentication by utilizing an Active Directory server that you have deployed within your network domain.

This window configures the settings required to connect to the Active Directory server. Additionally, Active Directory Test Tools are provided to ease the process of validating proper communication between the Active Directory server and the Array.

To use the Active Directory settings on this page you must choose **Active Directory** as the **Authentication Server Mode** in "Global Settings" on page 236.

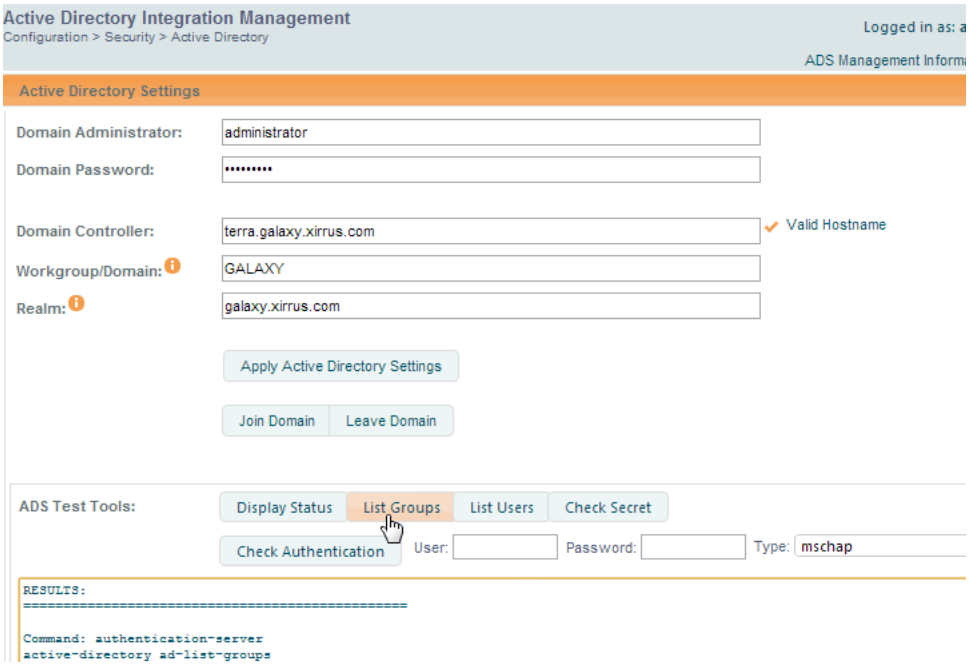


Figure 137. Active Directory Server

Procedure for Use of an Active Directory Server

1. Choose **Active Directory** as the **Authentication Server Mode** in "Global Settings" on page 236.
2. **Domain Administrator**: Enter the administrator account name for access to the domain controller. The Array will use this (together with the password) to create a machine account on the domain for the Array. This can be the name of any account that can join a machine to the domain.
3. **Domain Password**: The password for the **Domain Administrator** entered above.
4. **Domain Controller**: Enter the hostname to access the domain controller. This cannot be entered as an IP address. The Array will check that it is able to access the controller and place a checkmark to the right of the entry to indicate that it has been validated. Note that the checkmark only

appears after you have made a change requiring validation (i.e., entering a new hostname or changing an existing entry to a different hostname). If you return to this page at a later time, the checkmark will not be present.

5. **Workgroup/Domain**: Enter the Pre-Windows 2000 Domain name. This can be found by opening the Active Directory **Users and Computers**. Right click the domain in the left hand window and select **Properties**. This will display the **Domain name** that should be entered.

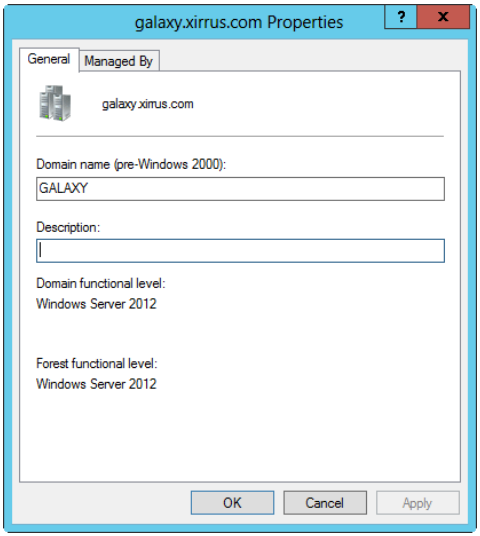


Figure 138. Finding the Domain Name from Active Directory

6. **Realm**: Realm name (may be the same as the domain name). **Workgroup** and **Realm** are both required. To find the Realm, open a command window on the server and type

   echo %userdnsdomain%

   This will display the Realm.

7. Click **Apply Active Directory Settings** to use these settings.

8. You must click **Join Domain** to ask the domain controller to join the Array to the domain. The Array is added to the list of computers in the workgroup. The status of the request will be displayed in the area below

the Test Tools. The domain controller will give the Array a secret that may be used as a key to fetch information. The secret may be checked with the **Check Secret** test tool, below. You may click **Leave Domain** to ask the domain controller to remove the Array from the domain and revoke its secret.

9. You may use the tools below to check that the Array is able to access and use the Active Directory successfully, or to troubleshoot any problems.

Active Directory Test Tools

10. **Display Status**: Displays detailed status information for the Active Directory.
11. **List Groups**: Shows the groups defined in the Active Directory for this **Workgroup**.
12. **List Users**: Shows the users defined in the Active Directory for this **Workgroup**.
13. **Check Secret**: The continued validity of the secret granted by **Join Domain** may be checked with this test tool.
14. **Check Authentication**: Enter a **User** name and **Password**. Select the **Type** of encryption to be used (**MSCHAP**, **NTLM**, **PAP**, or **PEAP-MSCHAPv2**), to check that it will work with the Active Directory server. Then click **Check Authentication** to validate that the Array can authenticate the user with the selected type of encryption.

See Also

Admin Management
External Radius
Internal Radius
Security
Understanding Groups

Rogue Control List

This window allows you to set up a control list for rogue APs, based on a type that you define. You may classify rogue APs as blocked, so that the Array will take steps to prevent stations from associating with the blocked AP. See "About Blocking Rogue APs" on page 351. The Array can keep up to 5000 list entries.

*The **RF Monitor > Intrusion Detection** window provides an alternate method for classifying rogues. You can list all Unknown stations and select all the rogues that you'd like to set to Known or Approved, rather than entering the SSID/BSSID as described below. See **"Intrusion Detection" on page 116**.*

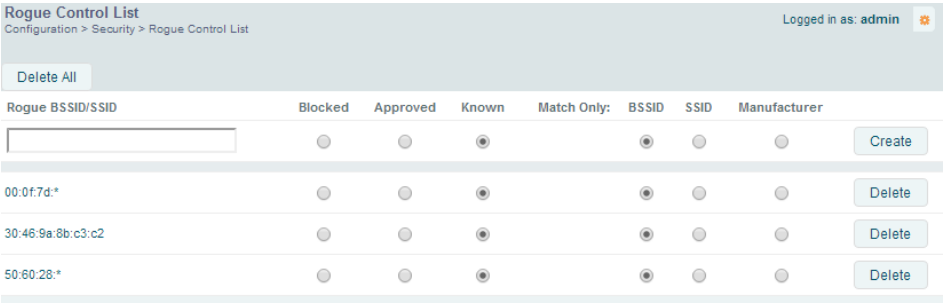


Figure 139. Rogue Control List

Procedure for Establishing Rogue AP Control

1. **Rogue BSSID/SSID:** Enter the BSSID, SSID, or manufacturer string to match for the new rogue control entry. The **Match Only** radio buttons specify what to match (e.g., the MAC address, SSID, or manufacturer).

   You may use the "*" character as a wildcard to match any string at this position. For example, 00:0f:7d:* matches any string that starts with 00:0f:7d:. Xirrus Arrays start with 00:0f:7d: or 50:60:28:. By default, the Rogue Control List contains two entries that match **00:0f:7d:*** and **50:60:28:*** and apply the classification **Known** to all Xirrus Arrays.

2. **Rogue Control Classification**: Enter the classification for the specified rogue AP(s), either **Blocked**, **Known** or **Approved**.

3. **Match Only**: Select the match criterion to compare the **Rogue BSSID/SSID** string against: **BSSID**, **Manufacturer**, or **SSID**. The BSSID field contains the MAC address.
4. Click **Create** to add this rogue AP to the Rogue Control List.
5. **Rogue Control List**: If you want to edit the control type for a rogue AP, just click the radio button for the new type for the entry: **Blocked**, **Known** or **Approved**.
6. To delete rogue APs from the list, click their **Delete** buttons.
7. Click the **Save** button if you wish to make your changes permanent.

See Also

Network Map
Intrusion Detection
SSIDs
SSID Management

OAuth 2.0 Management

This window displays a list of tokens granted by the Array for access to its RESTful API (see "API Documentation" on page 401 for a description of the features available in the API). OAuth 2.0 is used to provide the tokens. The list will be blank until tokens have been issued as described below. You may revoke (delete) existing tokens from the list, if desired.

Xirrus Arrays use the OAuth 2.0 standard's client credential grant model. This allows you to use administrator account credentials to obtain a token to access RESTful API on an individual Array. ArrayPlease note that the Array will issue only **one** token on behalf on of any administrator account at any given time. If you have a need for multiple tokens, then the Array will need multiple administrator accounts.

Follow the steps below to obtain a token and use the RESTful API.

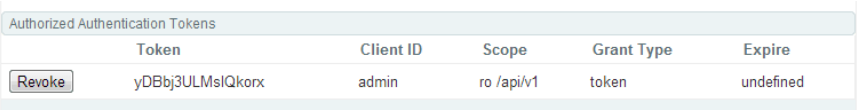


Figure 140. OAuth 2.0 Management - Token List

Procedure for Obtaining a Token and Accessing RESTful API on the Array

1. **Present User Credentials for a Permanent Token**

   A user-developed application must register by presenting the following information to the URL below:

   ```
   https://[Array hostname or IP address]/oauth/authorize
   ```

   - **grant_type**: password
   - **username**: username of an administrator account on the Array.
   - **client_id**: username of an administrator account on the Array (username and client_id must match).
   - **password**: password for the same administrator account on the Array

   The OAuth Authorization API provides a permanent token that the application may use to access the RESTful API. This token remains valid until the administrator revokes the token on the **OAuth 2.0 Management** page, unless the token file somehow becomes corrupted or is removed from the Array's file system.

   The token will be removed if the original account associated with it is deleted.

2. **Access the RESTful API**

   Once registration is completed and a permanent token has been provided, your application may access the API using the **client_id** and the token at the following URL:

   ```
   https://[Array hostname or IP address]/api/v1/[api-name]
   ```

Please see "API Documentation" on page 401 for a description of the features available in the API.

SSIDs

This status-only window allows you to review SSID (Service Set IDentifier) assignments. It includes the SSID name, whether or not an SSID is visible on the network, any security and QoS parameters defined for each SSID, associated VLAN IDs, radio availability, and DHCP pools defined per SSID. Click on an SSID's name to jump to the edit page for the SSID. There are no configuration options available on this page, but if you are experiencing problems or reviewing SSID management parameters, you may want to print this page for your records.

For a complete discussion of implementing Voice over Wi-Fi on the Array, see the Xirrus ***Voice over Wireless Application Note*** *in the Xirrus* ***Resource Center****.*

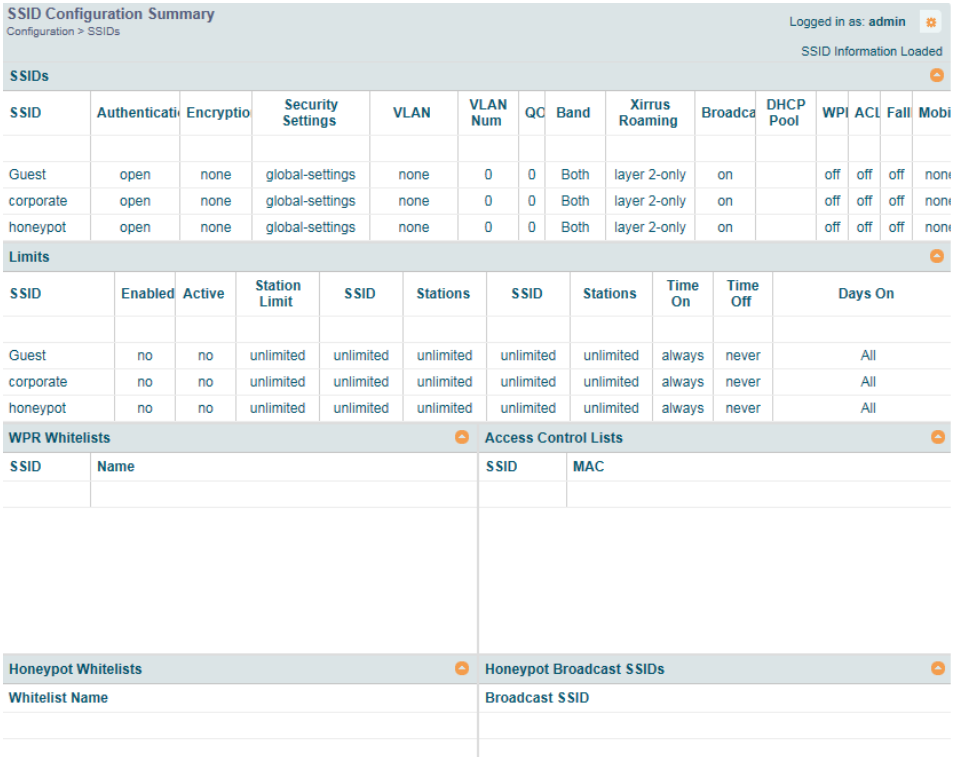


Figure 141. SSIDs

The read-only **Limits** section of the SSIDs window allows you to review any limitations associated with your defined SSIDs. For example, this window shows the current state of an SSID (enabled or not), how much SSID and station traffic is allowed, time on and time off, days on and off, and whether each SSID is currently active or inactive.

For information to help you understand SSIDs and how multiple SSIDs are managed by the Wireless Array, go to "Understanding SSIDs" on page 255 and the Multiple SSIDs section of "Frequently Asked Questions" on page 492. For a description of how QoS operates on the Array, see "Understanding QoS Priority on the Wireless Array" on page 256.

SSIDs are managed with the following windows:

- **"SSID Management" on page 262**
- **"Active IAPs" on page 275**
- **"Per-SSID Access Control List" on page 276**
- **"Honeypots" on page 278**

SSIDs are discussed in the following topics:

- **"Understanding SSIDs" on page 255**
- **"Understanding QoS Priority on the Wireless Array" on page 256**
- **"High Density 2.4G Enhancement—Honeypot SSID" on page 261**

Understanding SSIDs

The SSID (Service Set Identifier) is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining SSIDs).

Multiple SSIDs

A BSSID (Basic SSID) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS. A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS via a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or "wireless network name") identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. Wireless Arrays support the ability to define and use multiple SSIDs simultaneously.

Using SSIDs

The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- The wireless security mode needed to join this SSID.
- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest Quality of Service (QoS) definition. This SSID might also forward traffic to specific VLANs on the wired network.

See Also

SSID Management
SSIDs
Understanding SSIDs

Understanding QoS Priority on the Wireless Array

For a complete discussion of implementing Voice over Wi-Fi on the Array, see the Xirrus ***Voice over Wireless Application Note*** *in the Xirrus* ***Resource Center*** .

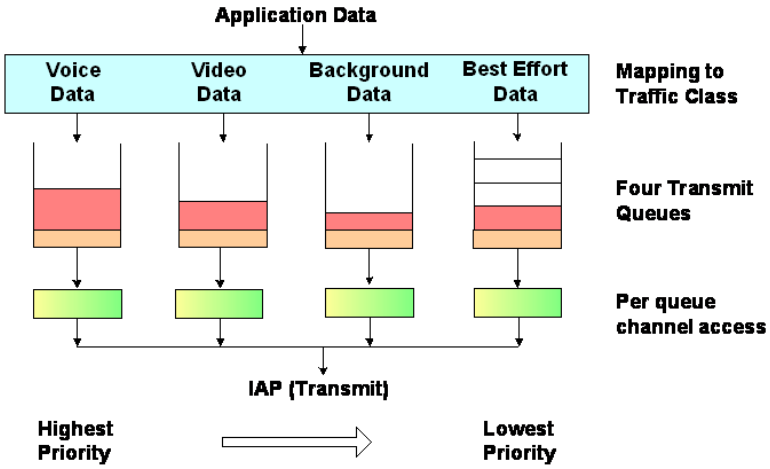


Figure 142. Four Traffic Classes

The Wireless Array's Quality of Service Priority feature (QoS) allows traffic to be prioritized according to your requirements. For example, you typically assign the highest priority to voice traffic, since this type of traffic requires delay to be under 10 ms. The Array has four separate queues for handling wireless traffic at different priorities, and thus it supports four traffic classes (QoS levels).

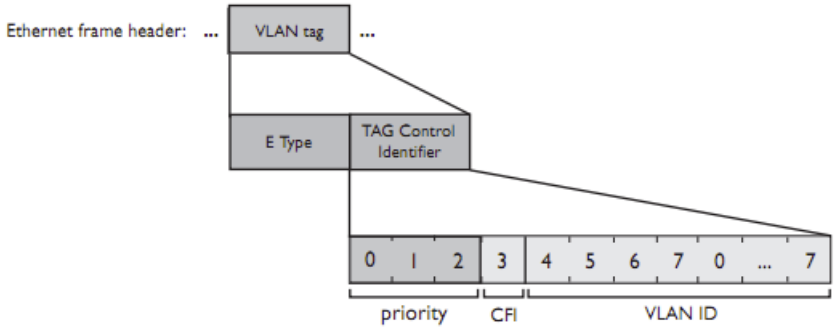


Figure 143. Priority Level—IEEE 802.1p (Layer 2)

IEEE802.1p uses three bits in an Ethernet frame header to define eight priority levels at the MAC level (Layer 2) for wired networks. Each data packet may be

tagged with a priority level, i.e., a **user priority** tag. Since there are eight possible user priority levels and the Array implements four wireless QoS levels, user priorities are mapped to QoS as described below.

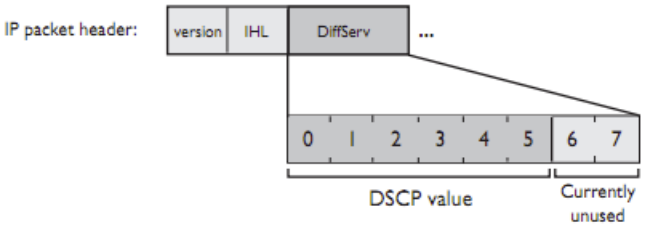


Figure 144. Priority Level—DSCP (DiffServ - Layer 3)

DSCP (Differentiated Services Code Point or DiffServ) uses 6 bits in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies a Layer 3 packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

The description below describes how both of these priority levels are mapped to the Array's four traffic classes.

End-to-End QoS Handling

Wired QoS - Ethernet Port:

- Egress: Outgoing wired packets are IEEE 802.1p tagged at the Ethernet port for upstream traffic, thus enabling QoS at the edge of the network.

FROM Array QoS (Wireless)	TO Priority Tag 802.1p (Wired)
1 (Lowest priority)	1
0	0
2 (Default)	5
3 (Highest priority)	6

- Ingress: Incoming wired packets are assigned QoS priority based on their SSID and 802.1p tag (if any), as shown in the table below. This table follows the mapping recommended by IEEE802.11e.

FROM Priority Tag 802.1p (Wired)	TO Array QoS (Wireless)	Typical Use
0	0 (Lowest priority)	Best Effort
1	1	Background—explicitly designated as low-priority and non-delay sensitive
2	1	Spare
3	0	Excellent Effort
4	2	Controlled Load
5	2	Video
6	3	Voice - requires delay <10ms
7 (Highest priority)	3 (Highest priority)	Network control

Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 2 is the default. See "SSID Management" on page 262. If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.
- The Array supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.
- How QoS is set for a packet in case of conflicting values:

a. If an SSID has a QoS setting, and an incoming wired packet's user priority tag is mapped to a higher QoS value, then the higher QoS value is used.

b. If a group or filter has a QoS setting, this overrides the QoS value above. See "Groups" on page 280, and "Filters" on page 365.

c. Voice packets have the highest priority (see Voice Support, below).

d. If **DSCP to QoS Mapping Mode** is enabled, the IP packet is mapped to QoS level 0 to 3 as specified in the DSCP Mappings table. This value overrides any of the settings in cases a to c above.

   In particular, by default:

   - DSCP 8 is set to QoS level 1.
   - DSCP 40 is typically used for video traffic and is set to QoS level 2.
   - DSCP 48 is typically used for voice traffic and is set to QoS level 3—the highest level
   - All other DSCP values are set to QoS level 0 (the lowest level—Best Effort).

Packet Filtering QoS classification

- Filter rules can be used to redefine the QoS priority level to override defaults. See "Filter Management" on page 368. This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

- The QoS priority implementation on the Array gives voice packets the highest priority to support voice applications.

High Density 2.4G Enhancement—Honeypot SSID

Some situations pose problems for all wireless APs. For example, iPhones will remember every SSID and flood the airwaves with probes, even when the user doesn't request or desire this behavior. In very high density deployments, these probes can consume a significant amount of the available wireless bandwidth.

The Array "honeypot" SSID targets this problem. Simply create an SSID named **honeypot** (lower-case) on the Array, with no encryption or authentication (select **None/Open**). Once this SSID is created and enabled, it will respond to any station probe looking for a named open SSID (unencrypted and unauthenticated) that is *not* configured on the Array. It will make the station go through its natural authentication and association process. See "Honeypots" on page 278.

The following SSIDs are excluded from being honeypotted:

- Explicitly whitelisted SSIDs. See "Honeypots" on page 278.
- SSIDs that are encrypted and/or authenticated.
- SSIDs that are configured on this Array, whether or not they are enabled.

Traffic for a station connected to the honeypot SSID may be handled in various ways using other Array features:

- Traffic may be directed to WPR (captive portal) to display a splash page or offer the user the opportunity to sign in to your service (see "Web Page Redirect (Captive Portal) Configuration" on page 269);
- Traffic may be filtered (see "Filters" on page 365);
- or it may be dead-ended by defining a specific dead-end VLAN on the honeypot SSID to "trap" stations (see "VLANs" on page 204).

Use the honeypot feature carefully as it could interfere with legitimate SSIDs and prevent clients from associating to another available network. You may define a whitelist of allowed SSIDs which are not to be honeypotted. See "Honeypots" on page 278. Th Honey pots page also allows you to change the SSID name that is broadcast for the honeypot SSID.

SSID Management

This window allows you to manage SSIDs (create, edit and delete), assign security parameters and VLANs on a per SSID basis, and configure the Web Page Redirect (WPR captive portal) functionality.

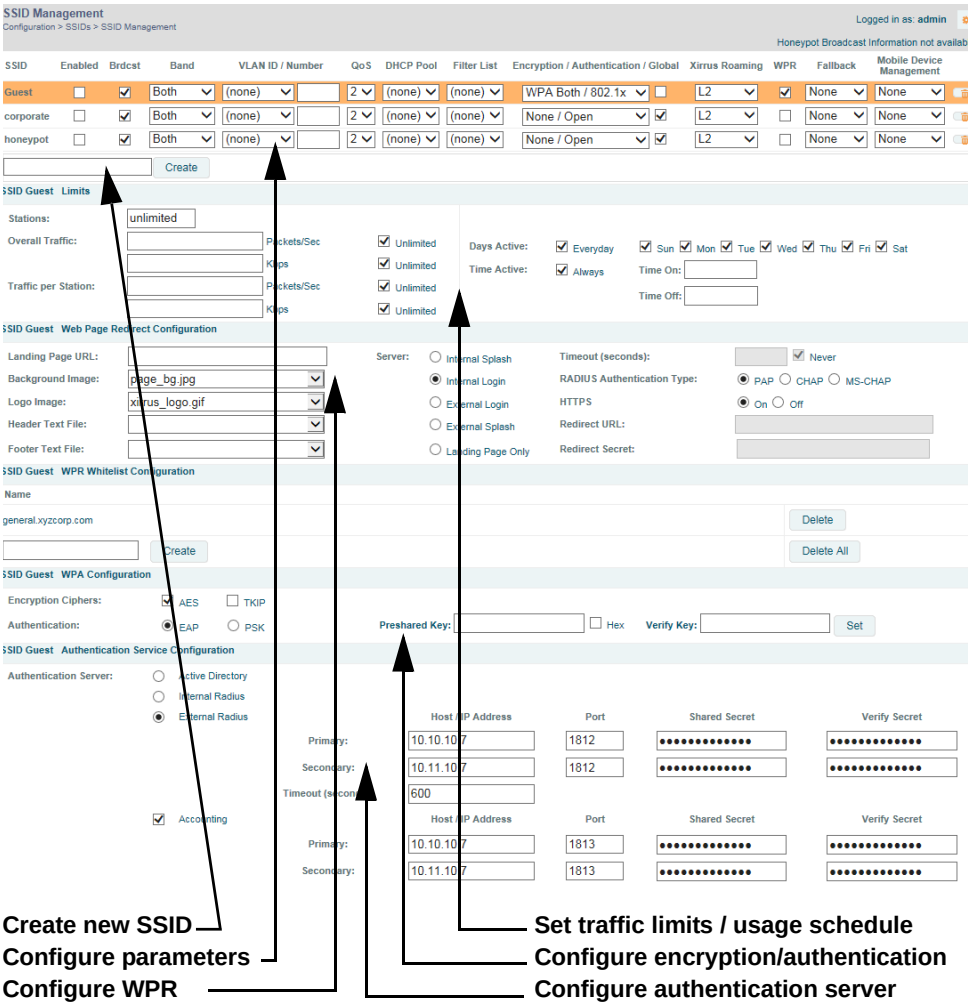


Figure 145. SSID Management

Procedure for Managing SSIDs

1. **New SSID Name:** To create a new SSID, enter a new SSID name to the left of the Create button (Figure 145), then click **Create**. SSID names are case sensitive and may only consist of the characters A-Z, a-z, 0-9, dash, and underscore. You may create up to 16 SSIDs (up to 8 on the XR-500 Series and on the XR-620). You may create a special SSID named **honeypot** (lower-case) to reduce the amount of unnecessary traffic caused by stations probing for open SSID names that they have learned in the past—see "High Density 2.4G Enhancement—Honeypot SSID" on page 261. In this case, a **Honeypot Service Whitelist Configuration** section will appear below (see Step 1 on page 279).

SSID List (top of page)

2. **SSID**: Shows all currently assigned SSIDs. When you create a new SSID, the SSID name appears in this table. Click any SSID in this list to select it.
3. **Enabled**: Check this box to activate this SSID or clear it to deactivate it.
4. **Brdcast**: Check this box to make the selected SSID visible to all clients on the network. Although the Wireless Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Clear this box if you do not want this SSID to be visible on the network.
5. **Band**: Choose which wireless band the SSID will be beaconed on. Select either **5 GHz**—802.11an, **2.4 GHz**—802.11bgn or **Both**.
6. **VLAN ID / Number**: From the pull-down list, select a VLAN that you want this traffic to be forwarded to on the wired network. Select **numeric** to enter the number of a previously defined VLAN in the **Number** field (see "VLANs" on page 204). This step is optional.
7. **QoS**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:
   - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without

compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.

- 1—Medium, with QoS prioritization aggregated across all traffic types.
- 2—High, normally used to give priority to video traffic.
- 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic, as described in "Understanding QoS Priority on the Wireless Array" on page 256. The default value for this field is 2.

8. **DHCP Pool**: If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull--down list. An internal DHCP pool must be created before it can be assigned. To create an internal DHCP pool, go to "DHCP Server" on page 194.

9. **Filter List**: If you wish to apply a set a filters to this SSID's traffic, select the desired Filter List. See "Filters" on page 365.

10. **Authentication**: The following authentication options are available (only valid encryption/authentication combinations are offered):

    - **Open:** This option provides no authentication and is not recommended.
    - **RADIUS MAC:** Uses an external RADIUS server to authenticate stations onto the wireless network, based on the user's MAC address. Accounting for these stations is performed according to the accounting options that you have configured specifically for this SSID or globally (see Step 12 below).

If this SSID is on a VLAN, the VLAN must have management turned on in order to pass CHAP authentication challenges from the client station to the RADIUS server.

    - **802.1x:** Authenticates stations onto the wireless network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the Wireless Array) or external.

11. **Encryption**: Choose the encryption that will be required—specific to this SSID—either **None**, **WEP**, **WPA**, **WPA2** or **WPA-Both**. The None option provides no security and is not recommended; WPA2 provides the best Wi-Fi security.

    Each SSID supports only one encryption type at a time (except that WPA and WPA2 are both supported on an SSID if you select WPA-Both). If you need to support other encryption types, you must define additional SSIDs. The encryption used with WPA or WPA2 is selected in "Global Settings" on page 236. For an overview of the security options, see "Security Planning" on page 50 and "Understanding Security" on page 214.

12. **Global**: Check this box if you want this SSID to use the security settings established at the global level (see "Global Settings" on page 236). Clear this box if you want the settings established here to take precedence.

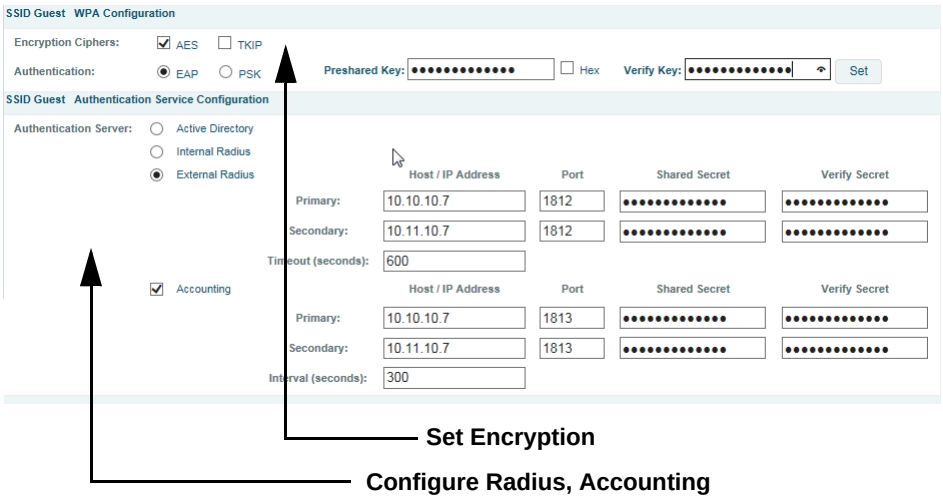


Figure 146. SSID Management—Encryption, Authentication, Accounting

Additional sections will be displayed to allow you to configure encryption, authentication server, and RADIUS accounting settings.

- The **WPA Configuration** encryption settings have the same parameters as those described in "Procedure for Configuring Network Security" on page 236.
- To configure **Active Directory** settings, see "Active Directory" on page 246).
- The **External RADIUS** and **Accounting** settings are configured in the same way as for an external RADIUS server (see "Procedure for Configuring an External RADIUS Server" on page 241). Note that external RADIUS servers may be specified using IP addresses or domain names.

13. **Roaming**: For this SSID, select whether to enable fast roaming between IAPs or Arrays at **L2&L3** (Layer 2 and Layer 3), at **L2** (Layer 2 only), or disable roaming (**Off**). You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings (IAP). See "Understanding Fast Roaming" on page 288.

14. **WPR (Web Page Redirect**, also called captive portal**)**: Check the checkbox to enable the Web Page Redirect functionality, or clear it to disable this option. If enabled, WPR configuration fields will be displayed under the SSID Limits section. This feature may be used to provide an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. For example, some wireless devices and users may not have a correctly configured 802.1x (RADIUS) supplicant. Utilizing WPR's Web-based login, users may be authenticated without using an 802.1x supplicant. See "Web Page Redirect (Captive Portal) Configuration" on page 269 for details of WPR usage and configuration.

    You may specify "Whitelist" entries—a list of web sites to which users have unrestricted access, without needing to be redirected to the WPR page first. See "Whitelist Configuration for Web Page Redirect" on page 273 for details.

*When using WPR, it is particularly important to adhere to the SSID naming restrictions detailed in **Step 1**.*

15. **Fallback**: Network Assurance checks network connectivity for the Array. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the Array will automatically disable this SSID. This will disassociate current clients, and prevent new clients from associating. Since the Array's network connectivity has failed, this gives clients a chance to connect to other, operational parts of the wireless network. No changes are made to WDS configuration. See Step a on page 230 for more information on Network Assurance.
16. **Mobile Device Management** (MDM): If you are an AirWatch customer and wish to have AirWatch manage mobile device access to the wireless network on this SSID, select **AirWatch** from the drop-down list. Before selecting this option, you must configure your AirWatch settings. See "AirWatch" on page 380.

Note that you cannot use MDM and WPR on the same SSID.

The lower part of the window contains a few sections of additional settings to configure for the currently selected SSID, depending on the values chosen for the settings described above.

- **"SSID Limits" on page 267**
- **"Web Page Redirect (Captive Portal) Configuration" on page 269**
- **"Whitelist Configuration for Web Page Redirect" on page 273**
- **"WPA Configuration" on page 274**
- **"Authentication Service Configuration" on page 274**

SSID Limits

See "Group Limits" on page 285 for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

17. **Stations**: Enter the maximum number of stations allowed on this SSID. This step is optional. Note that the IAPs - Global Settings window also has a station limit option—**Max Station Association per IAP**, and the windows for Global Settings .11an and Global Settings .11bgn also have **Max Stations** settings. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

18. **Overall Traffic**: Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.

19. **Traffic per Station**: Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Packets/Sec** field or the **Kbps** field to force a traffic restriction. If you set both values, the Array will enforce the limit it reaches first.

20. **Days Active**: Choose **Everyday** if you want this SSID to be active every day of the week, or select only the specific days that you want this SSID to be active. Days that are not checked are considered to be the inactive days.

21. **Time Active**: Choose **Always** if you want this SSID active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that this SSID is active.

22. **Web Page Redirect Configuration**: see "Web Page Redirect (Captive Portal) Configuration" on page 269.

23. To delete an SSID, click its **Delete** button .

24. Click the **Save** button if you wish to make your changes permanent.

Web Page Redirect (Captive Portal) Configuration

If you enable WPR, the SSID Management window displays additional fields that must be configured.

If enabled, WPR displays a splash or login page when a user associates to the wireless network and opens a browser to any URL (provided the URL does not point to a resource directly on the user's machine). The user-requested URL is captured, the user's browser is redirected to the splash or login page, and then the browser is redirected either to your specified landing page, if any, or else back to the captured URL. The landing page may be specified for a user group as well. See "Group Management" on page 282. Note that if you change the management HTTPS port, WPR uses that port, too. See "HTTPS" on page 230.

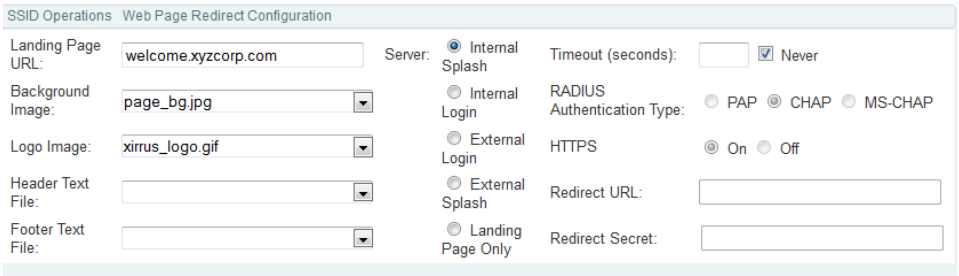


Figure 147. WPR Internal Splash Page Fields (SSID Management)

Note that when users roam between Arrays, their WPR Authentication will follow them so that re-authentication is not required.

You may select among five different modes for use of the Web Page Redirect feature, each displaying a different set of parameters that must be entered:

- Internal Login page

  This option displays a login page (residing on the Array) instead of the first user-requested URL. There is an upload function that allows you to replace the default login page, if you wish. Please see "Web Page Redirect (Captive Portal)" on page 396 for more information.

  To set up internal login, set **Server** to **Internal Login**. Set **HTTPS** to **On** for a secure login, or select **Off** to use HTTP. You may also customize the

login page with logo and background images and header and footer text. See "Customizing an Internal Login or Splash page" on page 272.

The user name and password are obtained by the login page. Authentication occurs according to your selection—**PAP**, **CHAP**, or **MS-CHAP**. Note that if you select CHAP, then you cannot select **Active Directory** in "Authentication Service Configuration" on page 274.

After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

Both the Internal Login and External Login options of WPR perform authentication using your configured RADIUS servers.

- Internal Splash page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Array. Note that there is an upload function that allows you to replace the default splash page, if you wish. Please see "Web Page Redirect (Captive Portal)" on page 396 for more information. You may also customize the splash page with logo and background images and header and footer text. See "Customizing an Internal Login or Splash page" on page 272.

  To use an internal splash page, set **Server** to **Internal Splash**. Enter a value in the **Timeout** field to define how many seconds the splash screen is displayed before timing out, or select **Never** to prevent the page from timing out automatically. After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

- External Login page

  This option redirects the user to a login page on an external web server for authentication, instead of the first user-requested URL. Login information (user name and password) must be obtained by that page, and returned to the Array for authentication.

Authentication occurs according to your configured RADIUS information. These parameters are configured as described in "Procedure for Configuring Network Security" on page 236, except that the **RADIUS Authentication Type** is selected here, as described below. After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

To set up external login page usage, set **Server** to **External Login**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

Select the **RADIUS Authentication Type**. This is the protocol used for authentication of users, **CHAP** or **PAP** (the default).

- **PAP** (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
- **CHAP** (Challenge-Handshake Authentication Protocol) is a more secure Protocol. The login request is sent using a one-way hash function.

- External Splash page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on an external web server.

  To set up external splash page usage, set **Server** to **External Splash**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

  After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

- Landing Page Only

  This option redirects the user to a specific landing page. If you select this option, enter the desired address in **Landing Page URL**.

Customizing an Internal Login or Splash page

You may customize these pages with a logo and/or background image, and header and/or footer text, as shown below in Figure 148.

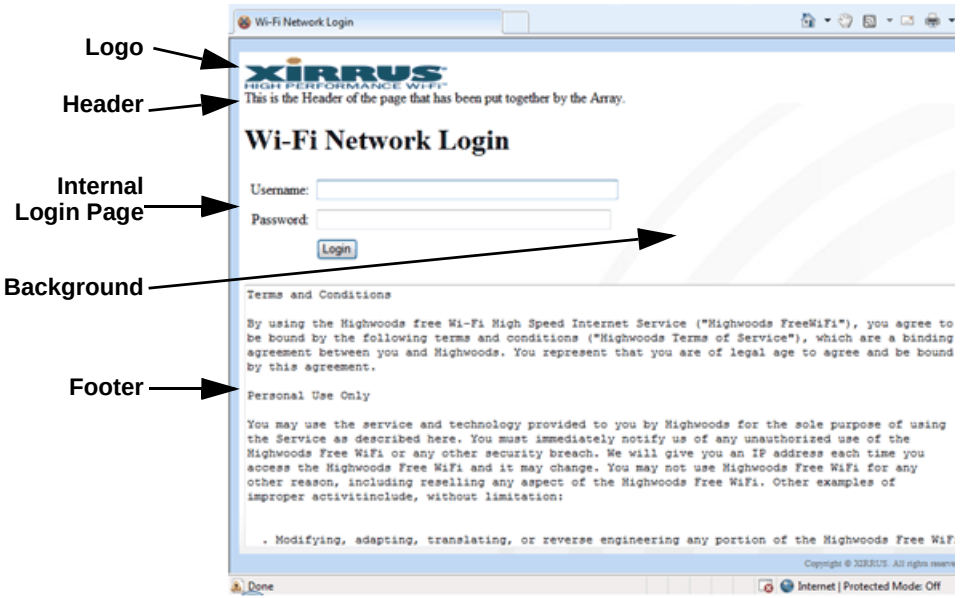


Figure 148. Customizing an Internal Login or Splash Page

- **Background Image**—specify an optional jpg, gif, or png file to display in the background of the page. Other customizations (logo, header, footer) will overlay the background, so that it will not be visible in those areas.
- **Logo Image**—specify an optional jpg, gif, or png file to display at the top of the page.
- **Header Text File**—specify an optional .txt file to display at the top of the page (beneath the logo, if any).
- **Footer Text File**—specify an optional .txt file to display at the bottom of the page.

Whitelist Configuration for Web Page Redirect

On a per-SSID basis, the whitelist allows you to specify Internet destinations that stations can access without first having to pass the WPR (captive portal) login/splash page. Note that a whitelist may be specified for a user group as well. See "Group Management" on page 282.

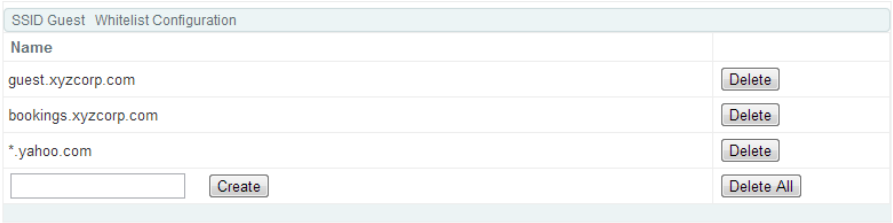


Figure 149. Whitelist Configuration for WPR

To add a web site to the whitelist for this SSID, enter it in the provided field, then click **Create**. You may enter an IP address or a domain name. Up to 32 entries may be created.

Example whitelist entries:

- Hostname: www.yahoo.com (but not www.yahoo.com/abc/def.html)
- Wildcards are supported: *.yahoo.com
- IP address: 121.122.123.124

Some typical applications for this feature are:

- to add allowed links to the WPR page
- to add a link to terms of use that may be hosted on another site
- to allow embedded video on WPR page

Note the following details of the operation of this feature:

- The list is configured on a per-SSID basis. You must have **WPR** enabled for the SSID to see this section of the SSID Management page.
- When a station that has not yet passed the WPR login/splash page attempts to access one of the white-listed addresses, it will be allowed access to that site as many times as requested.

- The station will still be required to pass through the configured WPR flow for all other Internet addresses.
- The whitelist will work against all traffic -- not just http or https
- Indirect access to other web sites is not permitted. For example, if you add www.yahoo.com to the whitelist, you can see that page, but not all the ads that it attempts to display.
- The whitelist feature does not cause traffic to be redirected to the whitelist addresses.

WPA Configuration

If you set **Encryption** for this SSID to one of the WPA selections (Step 11 on page 265) and you did not check the **Global** checkbox (Step 12), this section will be displayed. The **WPA Configuration** encryption settings have the same parameters as those described in "Procedure for Configuring Network Security" on page 236

Authentication Service Configuration

The RADIUS settings section will be displayed if you set **Authentication** (Step 10 on page 264) to anything but **OPEN,** and you set **Encryption** (Step 11) to anything but **WEP**, and you did not check the **Global** checkbox (Step 12). This means that you wish to set up a RADIUS server or Active Directory server to be used for this particular SSID. If **Global** is checked, then the security settings (including the RADIUS server, if any) established at the global level are used instead (see "Global Settings" on page 236).

The RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see "Procedure for Configuring an External RADIUS Server" on page 241). If you select **Active Directory**, then the settings are configured in "Active Directory" on page 246. Note that if you select **Active Directory**, then you cannot use CHAP authentication.

See Also

DHCP Server
External Radius
Global Settings (IAP)

Internal Radius
Security Planning
SSIDs
Understanding QoS Priority on the Wireless Array
AirWatch

Active IAPs

By default, when a new SSID is created, that SSID is active on all IAPs. This window allows you to specify which IAPs will offer that SSID. Put differently, you can specify which SSIDs are active on each IAP.

This feature is useful in conjunction with WDS. You may use this window to configure the WDS link IAPs so that only the WDS link SSIDs are active on them.

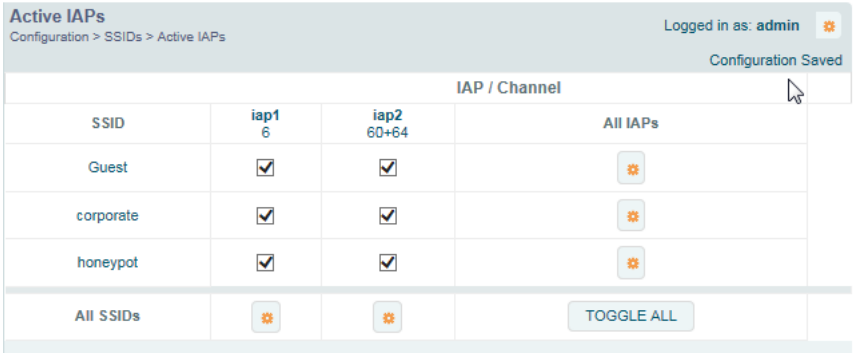


Figure 150. Setting Active IAPs per SSID

Procedure for Specifying Active IAPs

1. **SSID:** For a given SSID row, check the IAPs that should offer that SSID to clients. Uncheck any IAPs which should not offer that SSID.
2. **All IAPs**: This button, in the last column, may be used to allow or deny this SSID on all IAPs, i.e., switch all IAPs between allow or deny.
3. **All SSIDs**: This button, in the bottom row, may be used to allow or deny all SSIDs on this IAP.

4. **Toggle All**: This button, on the lower left, may be used to allow or deny all SSIDs on all IAPs.

5. Click the **Save** button if you wish to make your changes permanent.

Per-SSID Access Control List

This window allows you set up Access Control Lists (ACLs) on a per-SSID basis, to control whether a station with a particular MAC address may associate to a particular SSID. You may create access control list entries and delete existing entries, and control the type of list (allow or deny).

There is one ACL per SSID, and you may select whether its type is an **Allow** list or a **Deny** list, or whether use of this list is **Disabled**. You may create up to 1000 entries per SSID.

There is also a global ACL (see "Access Control List" on page 234). If the same MAC address is listed in both the global ACL and in an SSID's ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

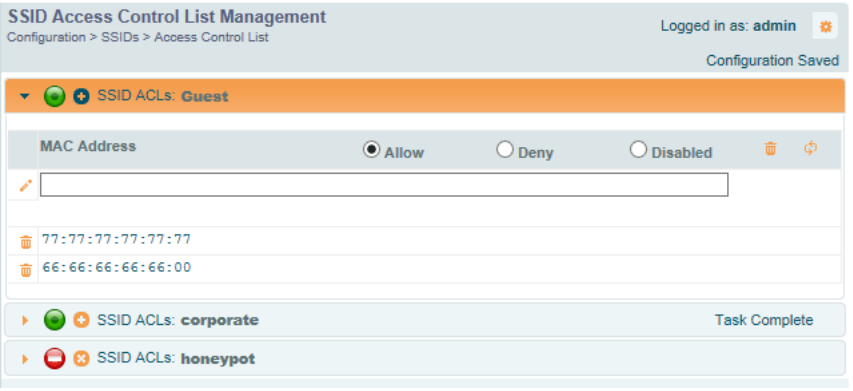


Figure 151. Per-SSID Access Control List

Procedure for Configuring Access Control Lists

1. **SSID**: Select the line for the SSID whose ACL you wish to manage. Click the line to hide or expand (display) the list.
2. **Access Control List Type**: Select **Disabled** to disable use of the Access Control List for this SSID, or select the ACL type—either **Allow** or **Deny**.
   - **Allow**: Only allows the listed MAC addresses to associate to the Array. All others are denied. The plus symbol appears before the SSID name for an allow list.
   - **Deny List**: Denies the listed MAC addresses permission to associate to the Array. All others are allowed. The minus symbol appears before the SSID name for a deny list.
   - **Disabled**: A red dot appears before the SSID name for a disabled list. A green dot appears before the SSID name for an allow or deny list.

     In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

3. **MAC Address**: If you want to add a MAC address to the ACL for the selected SSID, enter the new MAC address. You may use a wildcard (*) for one or more digits to match a range of addresses. **Delete**: You may delete selected MAC addresses from this list by clicking their **Delete** buttons .
4. Click the **Save** button if you wish to make your changes permanent.

Honeypots

Use the honeypot feature carefully as it could interfere with legitimate SSIDs.

The Xirrus honeypot SSID feature prevents the airwaves from being crowded with probes for named SSIDs. These probes are automatically generated by some popular wireless devices. When you create and enable a honeypot SSID on an Array, it responds to any station probe looking for a named open SSID (unencrypted and unauthenticated) that is *not* configured on the Array. For more details, see "High Density 2.4G Enhancement—Honeypot SSID" on page 261.

This page allows you to create a honeypot SSID, enter a whitelist of SSID names that are not to be honeypotted, and define alternate names for the SSID that will be broadcast instead of "honeypot".

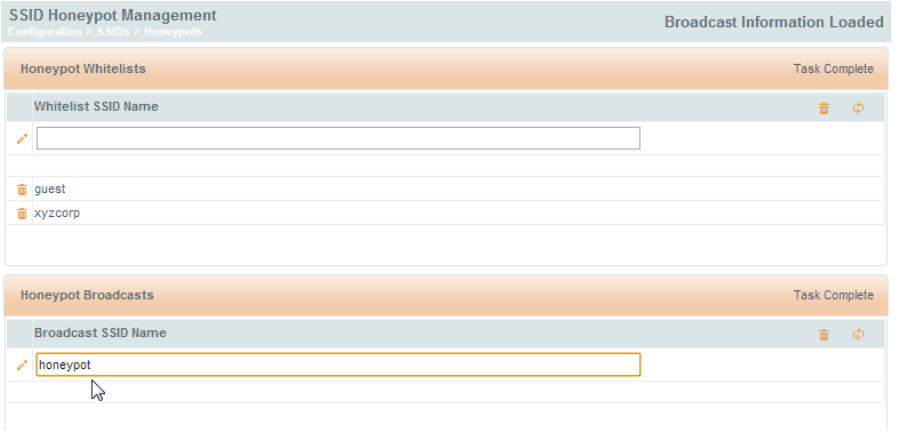


Figure 152. Honeypot Whitelist

Procedure for Configuring Honeypot Whitelists

1. **Create a honeypot:** If you have not already created an SSID named **honeypot**, you will be asked whether you wish to create one. Click **Yes**. You must have an SSID named honeypot to use this feature.

2. **Honeypot Whitelists**: This section only appears if you have created an SSID named honeypot. You may define a whitelist of allowed SSIDs which are not to be honeypotted, as described in "High Density 2.4G Enhancement—Honeypot SSID" on page 261. Type in each SSID name, and click **Create** to add it to the whitelist. Up to 50 SSIDs may be listed. The SSID names entered in this list are not case-sensitive.

   You may use the "*****" character as a wildcard to match any string at this position. For example, xir* matches any string that starts with **XIR** or **xir**. You may use a **?** as a wildcard to match a single character by surrounding the SSID name in quotes. For example, "**xirru?**" will match any six-character long string that starts with **xirru** (again, the match is not case-sensitive). If you do not use a wildcard, then the SSID name entered must be matched exactly in order to be whitelisted (except that case is not considered).

3. **Honeypot Broadcasts**: This section only appears if you have created an SSID named honeypot. You may define one or more alias names for this SSID. They will be broadcast *instead of* the name **honeypot**.

Groups

This is a status-only window that allows you to review user (i.e., wireless client) Group assignments. It includes the group name, Radius ID, Device ID, VLAN IDs and QoS parameters and roaming layer defined for each group, and DHCP pools and web page redirect information defined for the group. You may click on a group's name to jump to the edit page for the group. There are no configuration options available on this page, but if you are experiencing problems or reviewing group management parameters, you may want to print this page for your records.

The **Limits** section of this window shows any limitations configured for your defined groups. For example, this window shows the current state of a group (enabled or disabled), how much group and per-station traffic is allowed, time on and time off, and days on and off.

For information to help you understand groups, see Understanding Groups below.

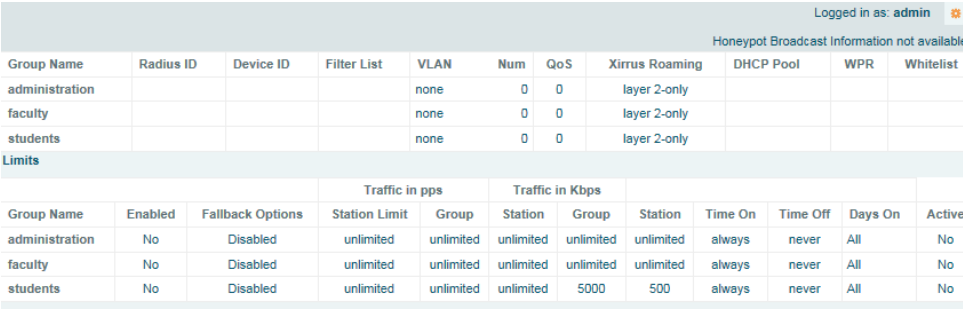


Figure 153. Groups

Understanding Groups

User groups allow administrators to assign specific network parameters to users (wireless clients) through RADIUS privileges rather than having to map users to an SSID tailored for that set of privileges. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs.

A group allows you to define a set of parameter values to be applied to selected users. For example, you might define the user group **Students**, and set its VLAN, security parameters, web page redirect (WPR), and traffic limits. When a new user

is created, you can apply all of these settings just by making the user a member of the group. The group allows you to apply a uniform configuration to a set of users in one step.

In addition, you can restrict the group so that it only applies its settings to group members who are connecting using a specific device type, such as iPad or phone. Thus, you could define a group named **Student-Phone** with **Device ID** set to **Phone**, and set the group's **VLAN Number** to 100. This group's settings will only be applied to group members who connect using a phone, and they will all use VLAN 100. Note that settings for the group in the RADIUS server will override any settings on this WMI page.

Almost all of the parameters that can be set for a group are the same as SSID parameters. This allows you to configure features at the user group level, rather than for an entire SSID. If you set parameter values for an SSID, and then enter different values for the same parameters for a user group, the **user group values have priority** (i.e., group settings will override SSID settings).

Group names are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining Groups).

Using Groups

User accounts are used to authenticate wireless clients that want to associate to the Array. These accounts are established in one of two ways, using the **Security> Internal Radius** window or the **Security> External Radius** window. In either case, you may select a user group for the user, and that user group's settings will apply to the user:

- Internal Radius—when you add or modify a user entry, select a user group to which the user will belong.
- External Radius—when you add or modify a user account, specify the **Radius ID** for the user group to which the user will belong. This must be the same Radius ID that was entered in the Group Management window. When the user is authenticated, the external Radius server will send the Radius ID to the Array. This will allow the Array to identify the group to which the user belongs.

See Also

External Radius
Internal Radius
SSIDs
Understanding QoS Priority on the Wireless Array
Web Page Redirect (Captive Portal) Configuration
Understanding Fast Roaming

Group Management

This window allows you to manage groups (create, edit and delete), assign usage limits and other parameters on a per group basis, and configure the Web Page Redirect (captive portal) functionality.

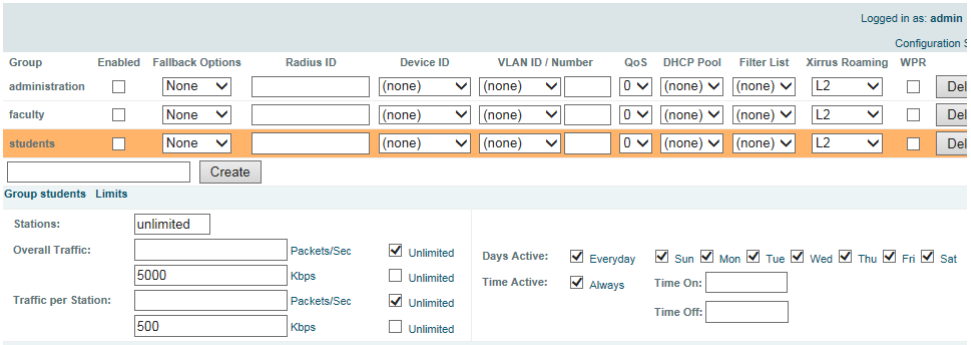


Figure 154. Group Management

Procedure for Managing Groups

1. **New Group Name:** To create a new group, enter a new group name next to the Create button, then click **Create**. You may create up to 16 groups (up to 8 on the XR-500 Series and on the XR-620).

   To configure and enable this group, proceed with the following steps.

2. **Group**: This column lists currently defined groups. When you create a new group, the group name appears in this list. Click on any group to select it, and then proceed to modify it as desired.

3. **Enabled**: Check this box to enable this group or leave it blank to disable it. When a group is disabled, users that are members of the group will behave as if the group did not exist. In other words, the options configured for the SSID will apply to the users, rather than the options configured for the group.

4. **Fallback**: Network Assurance checks network connectivity for the Array. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the Array will automatically disable users in this group. This will disassociate current clients, and prevent them from re-associating. Since the Array's network connectivity has failed, this gives clients a chance to connect to other, operational parts of the wireless network. See Step a on page 230 for more information on Network Assurance.

5. **Radius ID**: Enter a unique Radius ID for the group, to be used on an external Radius server. When adding a user account to the external server, this Radius ID value should be entered for the user. When the user is authenticated, Radius sends this value to the Array. This tells the Array that the user is a member of the group having this Radius ID.

6. **Device ID**: You may select a device type from this drop-down list, for example, **Notebook**, **phone**, **iPhone**, or **Android**. This allows you to apply the group settings only if a station authenticates as a user that is a member of the group and the station's device type matches **Device ID. Select none** if you do not want to consider the device type. If you have a Radius ID you should not enter a Device ID.

7. **VLAN ID**: (Optional) From the pull-down list, select a VLAN for this user's traffic to use. Select **numeric** and enter the number of a previously defined VLAN (see "VLANs" on page 204). This user group's VLAN settings supersede Dynamic VLAN settings (which are passed to the Array by the Radius server). To avoid confusion, we recommend that you avoid specifying the VLAN for a user in two places.

8. **QoS Priority**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:

- 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
- 1—Medium; QoS prioritization is aggregated across all traffic types.
- 2—High, normally used to give priority to video traffic.
- 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this group versus other traffic, as described in "Understanding QoS Priority on the Wireless Array" on page 256. The default value for this field is 2.

9. **DHCP Pool**: (Optional) To associate an internal DHCP pool to this group, select it from the pull--down list. Only one pool may be assigned. An internal DHCP pool must be created before it can be assigned. To create a DHCP pool, go to "DHCP Server" on page 194.

10. **Filter List**: (Optional) If you wish to apply a set of filters to this user group's traffic, select the desired Filter List. See "Filters" on page 365.

11. **Xirrus Roaming**: (Optional) For this group, select roaming behavior. Select **L2&L3** to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3. If you select **L2**, then roaming uses Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings (IAP). You may select **Off** to disable fast roaming. See "Understanding Fast Roaming" on page 288.

12. **WPR (Web Page Redirect)**: (Optional) Check this box if you wish to enable the Web Page Redirect (captive portal) functionality. This will open a **Web Page Redirect** details section in the window, where your WPR parameters may be entered. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. See "Web Page Redirect (Captive Portal) Configuration" on page 269 for details of WPR configuration. Note that the Group Management window only allows you to set up an **Internal Splash** page and a **Landing Page URL**.

The authentication options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the Array by a Radius server, this means the user has already been authenticated.

You may create a WPR Whitelist on a per-group basis if you wish. See "Whitelist Configuration for Web Page Redirect" on page 273 for details of WPR Whitelist usage and configuration.

Group Limits

The Limits section allows you to limit the traffic or connection times allowed for this user group. Note that the IAPs—Global Settings window and the SSID management windows also have options to limit the number of stations, limit traffic, and/or limit connection times. If limits are set in more than one place, all limits will be enforced:

- As soon as any station limit is reached, no new stations can associate until some other station has terminated its association.
- As soon as any traffic limit is reached, it is enforced.
- If any connection date/time restriction applies, it is enforced.

You can picture this as a logical AND of all restrictions. For example, suppose that a station's SSID is available MTWTF between 8:00am and 5:00pm, and the User Group is available MWF between 6:00am and 8:00pm, then the station will be allowed on MWF between 8:00am and 5:00pm.

To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

13. **Stations**: Enter the maximum number of stations allowed on this group. The default is 1536.
14. **Overall Traffic**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic for this group, or enter a value in the Packets/Sec field and make sure that the Unlimited box is unchecked to force a traffic restriction.

15. **Traffic per Station**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic per station for this group, or enter a value in the **Packets/Sec** or **Kbps** field and make sure that the Unlimited box is unchecked to force a traffic restriction.
16. **Days Active**: Choose **Everyday** if you want this group to be active every day of the week, or select only the specific days that you want this group to be active. Days that are not checked are considered to be the inactive days.
17. **Time Active**: Choose **Always** if you want this group active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that group members may associate.
18. To delete an entry, click its **Delete** button.
19. Click the **Save** button if you wish to make your changes permanent.

See Also

DHCP Server
External Radius
Internal Radius
Security Planning
SSIDs

IAPs

This status-only window summarizes the status of the Integrated Access Point (radios). For each IAP, it shows whether it is up or down, the channel and wireless mode, the antenna that it is currently using, its cell size and transmit and receive power, how many users (stations) are currently associated to it, whether a WDS link distance has been set for it, and its BSSID (MAC address).

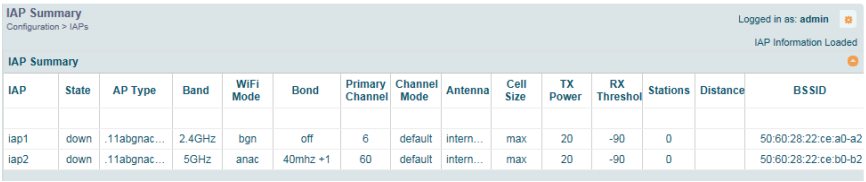
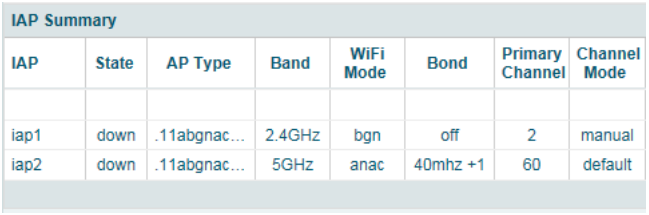


Figure 155. IAPs

The **Channel Mode** column displays some status information that is not found elsewhere: the source of a channel setting. (Figure 156) If you set a channel manually (via IAP Settings), it will be listed as **manual**. If an autochannel operation changed a channel, then it is labeled as **auto**. If the channel is set to the current factory default setting, the source will be **default**. This column also shows whether the channel selection is **locked**, or whether the IAP was automatically switched to this channel because the Array detected the signature of **radar** in operation on a conflicting channel (see also, Step 8 on page 297).



IAP Summary

IAP	State	AP Type	Band	WiFi Mode	Bond	Primary Channel	Channel Mode
iap1	down	.11abgnac...	2.4GHz	bgn	off	2	manual
iap2	down	.11abgnac...	5GHz	anac	40mhz +1	60	default

Figure 156. Source of Channel Setting

There are no configuration options in this window, but if you are experiencing problems or simply reviewing the IAP assignments, you may print this window for your records. Click any IAP name to open the associated configuration page.

Arrays have a fast roaming feature, allowing them to maintain sessions for applications such as voice, even while users cross boundaries between Arrays. Fast roaming is set up in the Global Settings (IAP) window and is discussed in:

- **"Understanding Fast Roaming" on page 288**

IAPs are configured using the following windows:

- **"IAP Settings" on page 290**
- **"Global Settings (IAP)" on page 295**
- **"Global Settings .11an" on page 311**
- **"Global Settings .11bgn" on page 316**
- **"Global Settings .11n" on page 322**
- **"Global Settings .11u" on page 327**
- **"Global Settings .11ac" on page 325**
- **"Advanced RF Settings" on page 333**
- **"Hotspot 2.0" on page 342**
- **"NAI Realms" on page 344**
- **"NAI EAP" on page 346**
- **"Intrusion Detection" on page 348**
- **"LED Settings" on page 354**
- **"DSCP Mappings" on page 355**
- **"Roaming Assist" on page 356**

See Also

IAP Statistics Summary

Understanding Fast Roaming

To maintain sessions for real-time data traffic, such as voice and video, users must be able to maintain the same IP address through the entire session. With traditional networks, if a user crosses VLAN or subnet boundaries (i.e., roaming between domains), a new IP address must be obtained.

Mobile wireless users are likely to cross multiple roaming domains during a single session (especially wireless users of VoIP phones). **Layer 3 roaming** allows a user to maintain the same IP address through an entire real-time data session. The user may be associated to any of the VLANs defined on the Array. The Layer 3 session is maintained by establishing a tunnel back to the originating Array. You should decide whether or not to use Layer 3 roaming based on your wired network design. Layer 3 roaming incurs extra overhead and may result in additional traffic delays.

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your Array, see Step 29 to Step 31 in "Global Settings (IAP)" on page 295. To choose which of the enabled options are used by an SSID or Group, see "Procedure for Managing SSIDs" on page 263 (Step 13) or "Procedure for Managing Groups" on page 282.

IAP Settings

This window allows you to enable/disable IAPs, define the wireless mode for each IAP, specify the channel and bond width and the cell size for each IAP, lock the channel selection, establish transmit/receive parameters, and reset channels. Buttons at the top of the list allow you to **Reset Channels**, **Enable All IAPs,** or **Disable All IAPs**. When finished, click the **Save** button if you wish to make your changes permanent.

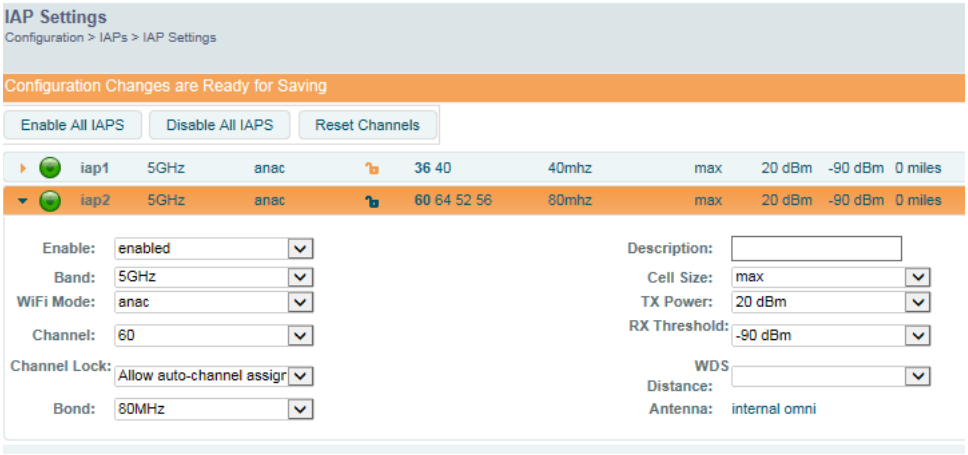


Figure 157. IAP Settings

You may also access this window by clicking on the Array image at the lower left of the WMI window—click the orange Xirrus logo in the center of the Array. See "User Interface" on page 85.

Procedure for Auto Configuring IAPs

You can auto-configure channel and cell size of radios by clicking on the **Auto Configure** buttons on the appropriate WMI page as shown below (auto configuration only applies to enabled radios):

- For all radios, go to "Advanced RF Settings" on page 333.
- For all 802.11a settings, go to "Global Settings .11an" on page 311.
- For all 802.11bg settings, go to "Global Settings .11bgn" on page 316.

- For all 802.11n settings, go to "Global Settings .11n" on page 322.
- For all 802.11ac settings, go to "Global Settings .11ac" on page 325.

Procedure for Manually Configuring IAPs

1. The row for each IAP summarizes its settings. Click to expand it and display the settings. Click again to collapse the entry.
2. In the **Enable** field select **enabled**, or select **disabled** if you want to turn off the IAP. The state of the channel is displayed with a green dot if enabled, and a red dot if disabled.
3. In the **Band** field, select the wireless band for this IAP from the choices available in the pull-down menu, either **2.4GHz** or **5 GHz**. Choosing the **5GHz** band will automatically select an adjacent channel for bonding. If the band displayed is **auto**, the **Band** is about to be changed based on a new **Channel** selection that you made that requires the change.

For XR-520 Series Arrays only:
*—iap**1** may be set to either band or to monitor (also see the Timeshare option in "RF Monitor" on page 334).*
*—iap**2** is permanently set to 5 GHz.*

One of the IAPs must be set to **monitor** mode if you wish to support Spectrum Analyzer, Radio Assurance (loopback testing), and Intrusion Detection features. Monitoring has a **Timeshare** mode option, which is especially useful for small Arrays with two IAPs allowing one IAP to be shared between monitoring the airwaves for problems and providing services to stations. See **RF Monitor Mode** in "Advanced RF Settings" on page 333 to set this option.

4. In the **WiFi Mode** field, select the IEEE 802.11 wireless mode (or combination) that you want to allow on this IAP. The drop-down list will only display the appropriate choices for the selected **Band**. For example, the 5 GHz band allows you to select **ac-only**, **anac**, **an**, **a-only**, or **n-only**,

while 2.4GHz includes 802.11b and 802.11g choices. When you select a WiFi Mode for an IAP, your selection in the **Channel** column will be checked to ensure that it is a valid choice for that WiFi Mode.

By selecting appropriate WiFi Modes for the radios on your Arrays, you can greatly improve wireless network performance. For example, if you have 802.11n and 802.11ac stations using the same IAP, throughput on that radio is reduced greatly for the 802.11ac stations. By supporting 802.11n stations only on selected radios in your network, the rest of your 802.11ac IAPs will have greatly improved performance. Take care to ensure that your network provides adequate coverage for the types of stations that you need to support.

5. In the **Channel** field, select the channel you want this IAP to use from the channels available in the pull-down list. The list shows the channels available for the IAP selected (depending on which band the IAP is using). Channels that are shown in gray are unavailable. They are either already in use, or not offered for the selected Band.

   The channels that are available for assignment to an IAP will differ, depending on the country of operation. If **Country** is set to **United States** in the Global Settings (IAP) window, then 21 channels are available to 802.11an radios.

As mandated by FCC/IC law, Arrays continually scan for signatures of radar. If such a signature is detected, the Array will switch operation from conflicting channels to new ones. The Array will switch back to the original channel after 30 minutes if the channel is clear. If a radio was turned off because there were no available channels not affected by radar, the Array will now bring that radio back up after 30 minutes if that channel is clear. The 30 minute time frame complies with FCC/IC regulations.

6. Set **Channel Lock** to **Block auto-channel assignment** if you want to lock in your channel selection so that an autochannel operation (see Advanced RF Settings) can't change it. A locked padlock will be displayed for the IAP.

7. The **Bond** field works together with the **Channel** selected above. (For 802.11n IAPs, it also obeys the bonding options selected on the Global Settings .11n page.) Also see the discussion in "80 MHz and 160 MHz Channel Widths (Bonding)" on page 43. Bonding is available on all Arrays, including two-radio models. For 802.11n, two 20MHz channels may be bonded to create one 40 MHz channel with double the data rate. 802.11ac offers an additional option to bond four 20MHz channels to create one 80MHz channel with four times the data rate.

   - **Channel number**—If a channel number appears, then this channel is already bonded to the listed channel.
   - **Off**—Do not bond his channel to another channel.
   - **40 MHz**—Bond this channel to an adjacent channel. The bonded channel is selected automatically by the Array based on the **Channel** (Step 5). The choice of banded channel is static—fixed once the selection is made.
   - **80 MHz**—Bond this channel to three adjacent channels. The bonded channels are selected automatically by the Array based on the **Channel** (Step 5). The choice of bonded channels is static—fixed once the selection is made.

   The top line for the IAP will show the channels that have been assigned based on the width of the bond.

8. In the **Cell Size** field, select **auto** to allow the optimal cell size to be automatically computed (see also, "RF Power & Sensitivity" on page 336). To set the cell size yourself, choose either **small**, **medium**, **large**, or **max** to use the desired pre-configured cell size, or choose **manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx Power** (transmit) and **Rx Threshold** (receive) fields. The default is **max**. If you select a value other than **auto**, the cell size will not be affected by cell size auto configuration. Note that ultra low power **Tx dBm** settings are possible. Values from -15dB to 5dB are provided specifically to help in high density 2.4 GHz environments.

When other Arrays are within listening range of this one, setting cell sizes to **Auto** allows the Array to change cell sizes so that coverage between cells is maintained. Each cell size is optimized to limit interference between sectors of other Arrays on the same channel. This eliminates the need for a network administrator to manually tune the size of each cell when installing multiple Arrays. In the event that an Array or a radio goes offline, an adjacent Array can increase its cell size to help compensate.

The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the Array's cell diameter. In a large office, or if multiple Arrays are in use, you may choose **Small** cells to achieve a higher data rate, since walls and other objects will not define the cells naturally.

For additional information about cell sizes, go to "Coverage and Capacity Planning" on page 30.

9. If you are using WDS to provide backhaul over an extended distance, use **WDS Distance (Miles)** to prevent timeout problems associated with long transmission times. Set the approximate distance in miles between this IAP and the connected Array in this column. This increases the wait time for frame transmission accordingly.
10. The **Antenna** field displays the antenna that has automatically been selected for this IAP.
11. If desired, enter a description for this IAP in the **Description** field.
12. You may reset all of the enabled IAPs by clicking the **Reset Channels** button at the top of the list. A message will inform you that all enabled radios have been taken down and brought back up.
13. Buttons at the top of the list allow you to **Enable All IAPs** or **Disable All IAPs**.
14. Click the **Save** button if you wish to make your changes permanent.

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
Global Settings .11ac
Advanced RF Settings
IAPs
IAP Statistics Summary
LED Settings

Global Settings (IAP)

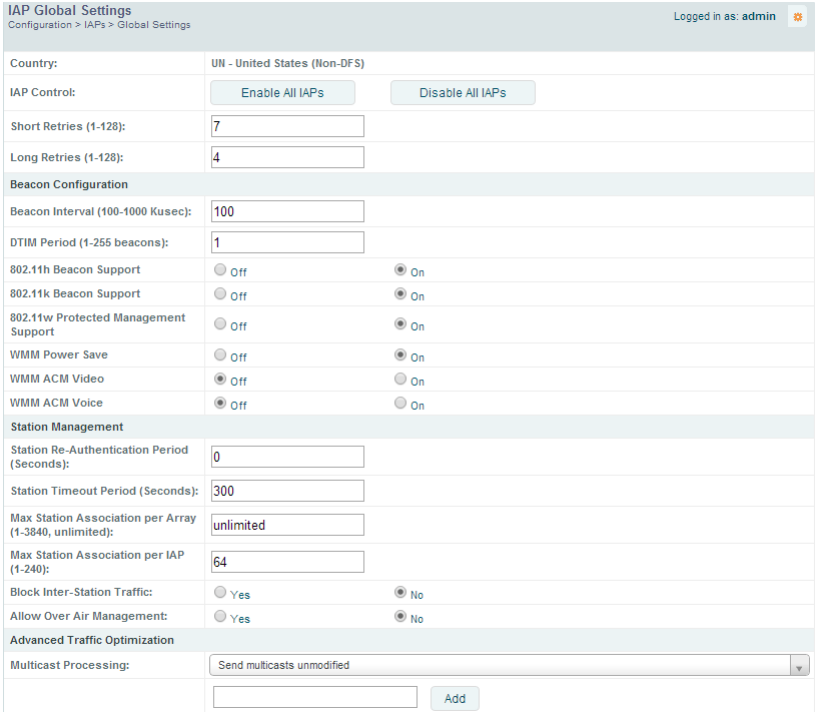


Figure 158. Global Settings (IAPs)

This window allows you to establish global IAP settings. Global IAP settings include enabling or disabling all IAPs (regardless of their operating mode), and changing settings for beacons, station management, and advanced traffic optimization—including multicast processing, load balancing, and roaming. Changes you make on this page are applied to all IAPs, without exception.

Procedure for Configuring Global IAP Settings

1. **Country**: This is a display-only value. Once a country has been set, it may not be changed.

   The channels that are available for assignment to an IAP will differ, depending on the country of operation. If **Country** is set to **United States**, then 21 channels are available for 802.11a/n.

   If no country is displayed, the channel set defaults to channels and power levels that are legal worldwide—this set only includes the lower eight 5 GHz channels.

2. **IAP Control**: Click on the **Enable All IAPs** button to enable all IAPs for this Array, or click on the **Disable All IAPs** button to disable all IAPs.

3. **Short Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value (1 to 128) in the **Short Retry Limit** field if you want to increase or decrease this attribute.

4. **Long Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value (1 to 128) in the **Long Retry Limit** field if you want to increase or decrease this attribute.

5. **Wi-Fi Alliance Mode**: Set this **On** if you need Array behavior to conform completely to Wi-Fi Alliance standards. This mode is normally set to **Off**.

Beacon Configuration

6. **Beacon Interval**: When the Array sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000 Kusecs. A Kusec is 1000 microseconds = 1 millisecond. The value you enter here is applied to all IAPs.

7. **DTIM Period**: A DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by the Array to a client device in sleep mode, alerting the device to broadcast traffic awaiting delivery. The **DTIM Period** is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all IAPs.

8. **802.11h Beacon Support**: This option enables beacons on all of the Array's radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.

9. **802.11k Beacon Support**: 802.11k offers faster and more efficient roaming. When enabled, each beacon lists the channels that nearby APs offer. This supports improved channel scanning, resulting in faster roam times and increased battery life due to shorter scan times since the station knows where to look for nearby APs. The Array will also respond to requests from stations for an 802.11K Neighbor Report with additional information about nearby APs. This setting is enabled by default.

10. **802.11w Protected Management Support**: This option protects the wireless network infrastructure against spoofing by outside APs. Authenticate, De-authenticate, Associate, and Dis-associate management frames are sent in a secured manner when this option is enabled.

11. **WMM Power Save**: Click **On** to enable Wireless Multimedia Power Save support, as defined in IEEE802.11e. This option saves power and increases battery life by allowing the client device to doze between packets to save power, while the Array buffers downlink frames. The default setting is **On**.

12. **WMM ACM Video**: Click **On** to enable Wireless Multimedia Admission Control for video traffic. When admission control for video is enabled, the Array evaluates a video request from a client device against the network load and channel conditions. If the network is not congested, it accepts the request and grants the client the medium time for its traffic stream. Otherwise, it rejects the request. This enables the Array to maintain QoS when the WLAN becomes congested after a connection has already been established. Some clients contain sufficient intelligence to decide to either delay the traffic stream, associate with a different AP, or establish a best-effort traffic stream outside the operation of WMM-Admission Control. The default setting is **Off**. Note that the QoS priority of traffic queues is voice, video, best effort, background—this gives the highest priority to voice transmissions.

13. **WMM ACM Voice**: Click **On** to enable Wireless Multimedia Admission Control for voice calls. As for **WMM ACM Video** above, when admission control for voice is enabled, the Array evaluates a voice request from a client device against the network load and channel conditions. If the network is not congested, it accepts the request and grants the client the medium time for its call. Otherwise, it rejects the request. Some clients contain sufficient intelligence to decide to either delay the traffic stream, associate with a different AP, or establish a best-effort traffic stream outside the operation of WMM-Admission Control. The default setting is **Off**.

Station Management

14. **Station Re-Authentication Period**: This specifies an interval (in seconds) for station reauthentications. This is the minimum time period between station authentication attempts, enforced by the Array. This feature is part of the Xirrus Advanced RF Security Manager (RSM).

15. **Station Timeout Period**: Specify a time (in seconds) in this field to define the timeout period for station associations.

16. **Max Station Association per Array**: This option allows you to define how many station associations are allowed per Array, or enter **unlimited**. Note that the **Max Station Association per IAP** limit (below) may not be exceeded, so entering **unlimited**, in practice, will stop at the per-IAP limit. If you have an unlicensed Array, this value is set to 1, which simply allows you to test the ability to connect to the Array.

17. **Max Station Association per IAP**: This defines how many station associations are allowed per IAP. The maximum is 240 (up to 128 on the XR-500 and XR-600 Series). Note that the SSIDs > SSID Management window also has a station limit option—**Station Limit**, and the windows for Global Settings .11an and Global Settings .11bgn also have **Max Stations** settings. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

18. **Block Inter-Station Traffic:** This option allows you to block or allow traffic between wireless clients that are associated to the Array. Choose either **Yes** (to block traffic) or **No** (to allow traffic).

19. **Allow Over Air Management**: Choose **Yes** to enable management of the Array via the IAPs, or choose **No** (recommended) to disable this feature.

Advanced Traffic Optimization

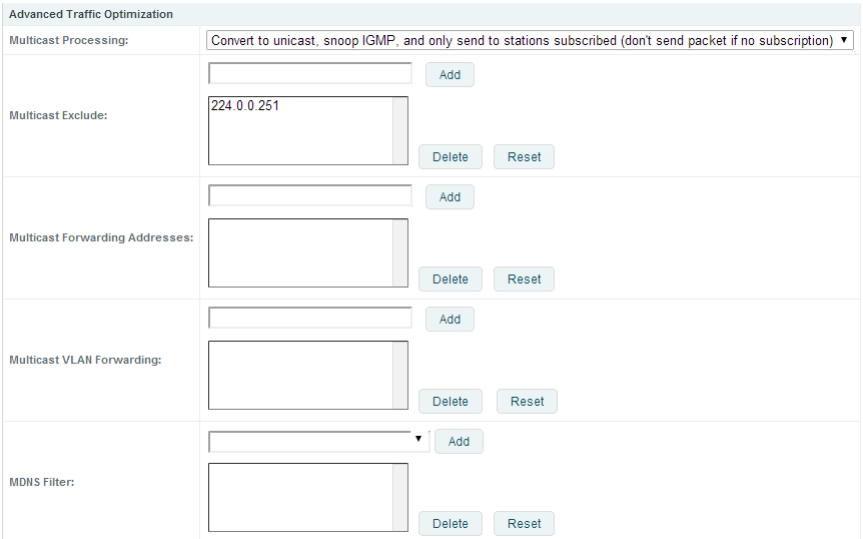


Figure 159. Multicast Processing

20. **Multicast Processing:** This sets how multicast traffic is handled. Multicast traffic can be received by a number of subscribing stations at the same time, thus saving a great deal of bandwidth. In some of the options below, the Array uses IGMP snooping to determine the stations that are subscribed to the multicast traffic. IGMP (Internet Group Management Protocol) is used to establish and manage the membership of multicast groups.

    Multicast handling options are only applicable to traffic transmitted from the Array to wireless stations. Select one of the following options:

    - **Send multicasts unmodified**. This is useful when multicast is not needed because no video or audio streaming is required or when it is used only for discovering services in the network. Some situations where you might use this option are:
        - for compatibility with ordinary operation, i.e., there is no optimization or modification of multicast traffic.

- if you have an application where many subscribers need to see the multicast—a large enough number that it would be less efficient to convert to unicast and better just to send out multicast even though it must be sent out at the speed of the slowest connected station.

An example of a situation that might benefit from the use of this mode is ghosting all the laptops in a classroom using multicast. One multicast stream at, say, 6 Mbps is probably more efficient than thirty unicast streams.

The next three options convert multicast to unicast. Packets are sent directly to the stations at the best possible data rates. This approach significantly improves the quality of the voice and video multicast streams.

- **Convert to unicast and send unicast packets to all stations**. This may be useful in link-local multicast situations.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (send as multicast if no subscription)**. This option is useful when you need to stream voice or video multicast traffic to all stations, but some stations are capable of subscribing to multicast groups while other stations are not. The stations that do not subscribe will not benefit from conversion to unicast; their video or voice quality may be compromised.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription)**. This option is useful in well controlled environments when you need to stream voice or video multicast traffic only to stations that are capable of subscribing to multicast groups and there is no need for the rest of the stations to receive the data stream.

21. **Multicast Exclude:** This is a list of multicast IP addresses that will not be subject to multicast-to-unicast conversion. This list is useful on networks where applications such as those using multicast Domain Name System (mDNS) are in use. For example, Apple Bonjour finds local network devices such as printers or other computers using mDNS. By default, the

list contains the IPv4 multicast address for Apple Bonjour mDNS: 224.0.0.251. For an additional discussion of optimizing Apple Bonjour handling, see the *Bonjour Director Application Note* in the Xirrus ***Resource Center***.

To add a new IP address to the list, type it in the top field and click the **Add** button to its right. You may only enter IP addresses—host names are not allowed. This is because mDNS is a link local multicast address, and does not require IGMP to the gateway.

To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

22. **Multicast Forwarding**

Multicast Forwarding is a Xirrus feature that forwards selected multicast traffic between wired VLANs and wireless SSIDs. For example, Apple devices use mDNS to advertise and find services, using local network multicasts that are not routed. This creates an issue when you are using Apple devices on the Wireless LAN, and have other devices that provide services connected on the wired infrastructure in a different VLAN, for example, printers and AppleTV devices. One way to address this issue is to set up multicast forwarding between the wireless SSID and the wired VLAN. This requires the wired VLAN to be trunked to the Array. Once configured correctly, mDNS traffic will be forwarded from the specified wireless network(s) to the specified wired VLANs and vice-versa, subject to any mDNS service filtering defined (Step 24).

Use multicast forwarding together with multicast VLAN forwarding (Step 23) and mDNS filtering (Step 24) to make services available across VLANs as follows:

- In **Multicast Forwarding Addresses**, enter a list of multicast addresses that you want forwarded, for example, 224.0.0.251 (the multicast address for Bonjour).
- In **Multicast VLAN Forwarding**, enter a list of VLANs that participate in the multicast forwarding.

- In **MDNS Filter**, specify the mDNS service types that are allowed to be forwarded.
  - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed*.
  - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed **only** for the listed service types*.

  Note that mDNS filtering may be used to filter the mDNS packet types that are forwarded within the same VLAN. Also, in conjunction with multicast forwarding, it may be used to filter the mDNS packet types that are forwarded across configured VLANs.

After you have entered these settings, when multicast packets arrive from the wired network from one of the **Multicast Forwarding Addresses** on any VLAN specified in **Multicast VLAN Forwarding,** they are forwarded to the corresponding wireless SSID for that VLAN.

Multicast packets coming in from the wireless network on an SSID tied to one of the specified VLANs and matching one of the **Multicast Forwarding Addresses** are forwarded to the specified VLANs on the wired network.

No modifications are made to the forwarded packets – they are just forwarded between specified VLANs and associated SSIDs.

*Xirrus strongly recommends the use of MDNS Filters (*Step 24*) when using multicast forwarding. Only allow required services to be forwarded.*

Carefully monitor results, as forwarding may flood your network with multicast traffic. Experience has shown Bonjour devices to be very chatty. Also note that since this is link local multicast traffic, it will be sent to every wired port in the VLAN, as IGMP snooping does not work with link local multicast addresses.

To specify **Multicast Forwarding Addresses:** enter each IP address in the top field and click the **Add** button to its right. You may only enter IPv4 multicast addresses - host names are not allowed. To remove an entry,

select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

23. **Multicast VLAN Forwarding:** This is a list of VLANs that participate in the multicast forwarding. Please see the description of multicast forwarding in Step 22 above.

The VLANs you enter must be explicitly defined (see "VLANs" on page 204) in order to participate in multicast forwarding. In fact, the Array discards packets from undefined VLANs.

Multicast VLAN Forwarding operates as follows:

- If you leave this field blank, then there is ***no*** filter, and *Multicast Forwarding traffic is passed across all VLANs*.
- If you enter VLANs, then this acts as an allow filter, and *Multicast Forwarding traffic is passed **only** to the listed VLANS*.

To add a new VLAN to the list, enter its number or name in the top field and click the **Add** button to its right. You may enter multiple VLANs at once, separated by a space. To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

These VLANs must be trunked to the Array from the LAN switch, and be defined on the Array. See "VLAN Management" on page 206 and "SSID Management" on page 262.

Note that Multicast Forwarding and mDNS Filtering capabilities also work if both devices are wireless. For example, let's say that AppleTV is using wireless to connect to an SSID that is associated with VLAN 56, and the wireless client is on an SSID that is associated with VLAN 58. Normally the wireless client would not be able to use Bonjour to discover the AppleTV because they are on separate VLANs. But if you add 224.0.0.251 to the ***Multicast Forwarding Addresses****, then add VLANs 56 and 58 to the* ***Multicast VLAN Forwarding*** *list, then the wireless client will be able to discover the AppleTV. In this same scenario you could add AppleTV to the* ***MDNS Filter*** *list so that only MDNS packets for the AppleTV service type would be forwarded between VLANs 56 and 58.*

Note that all the VLANs that you add to this list do not have to be associated with SSIDs. As an example, say that AppleTV is on the wired network on VLAN 56, while the wireless device is connected to an SSID that is associated to VLAN 58. In this case, VLAN 56 and 58 need to be defined on the Array but only VLAN 58 needs to be associated to a SSID.

24. **MDNS Filter:** There are many different types of services that may be specified in multicast query and response packets. The mDNS filters let you restrict forwarding, so that multicast packets are forwarded only for the services that you explicitly specify. This list may be used to restrict the amount of Apple Bonjour multicast traffic forwarding. For example, you may restrict forwarding to just AppleTV and printing services. Please see the description of multicast forwarding in Step 22 above.

    The **MDNS Filter** operates as follows:

    - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed*.
    - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed* ***only*** *for the listed service types*.

    To add an mDNS packet type to the list of packets that may be forwarded, select it from the drop-down list in the top field and click the **Add** button to its right. The drop-down list offers packet types such as **AirTunes**,

Apple-TV, **iChat**, **iPhoto**, **iTunes**, **iTunes-Home-Sharing**, **Internet-Printing**, **Mobile-Device-Sync**, and **Secure-Telnet**.

For example, to allow mirroring of an iPad on an Apple-TV, select **Apple-TV**.

You may define your own type if you do not see the service you want in the drop-down list. Simply enter the mDNS service name that you would like to allow through. Custom mDNS packet types must be prefixed with an underscore, e.g., **_airvideoserver**.

To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

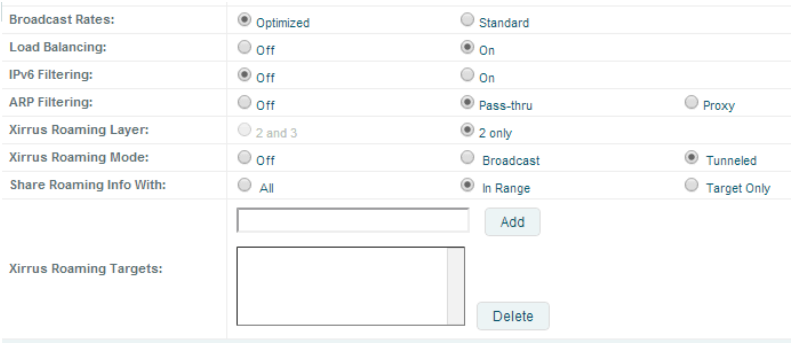


Figure 160. Additional Optimization Settings

25. **Broadcast Rates**: This changes the rates of broadcast traffic sent by the Array (including beacons). When set to **Optimized**, each broadcast or multicast packet that is transmitted on each radio is sent at the lowest transmit rate used by any client associated to that radio at that time. This results in each IAP broadcasting at the highest Array TX data rate that can be heard by all associated stations, improving system performance. The rate is determined dynamically to ensure the best broadcast/multicast performance possible. The benefit is dramatic. Consider a properly

designed network (having -70db or better everywhere), where virtually every client should have a 54Mbps connection. In this case, broadcasts and multicasts will all go out at 54Mbps vs. the standard rate. Thus, with broadcast rate optimization on, broadcasts and multicasts use between 2% and 10% of the bandwidth that they would in Standard mode.

When set to **Standard** (the default), broadcasts are sent out at the lowest basic rate only—6 Mbps for 5GHz clients, or 1 Mbps for 2.4GHz clients. The option you select here is applied to all IAPs.

26. **Load Balancing (ACExpress™)**: Wi-Fi is a shared medium and only one device can transmit data at any time. Faster devices supporting 802.11ac standards have to wait until the slower devices finish transmitting data. This brings down the overall throughput of the network. For example, an 802.11n client operates more than four times slower than an 802.11ac client, and thus will take four times more air time to communicate a given amount of data. This starves the available bandwidth from faster clients, reducing performance significantly. Xirrus solves this issue with ACExpress™ that automatically separates devices onto different IAPs by their speeds and capability.

    ACExpress identifies station capabilities based on fingerprinting and automatically groups devices by performance. It works on all modes (802.11a/b/g/n/ac) and bands (2.4GHz and 5GHz). This results in improved performance for every WLAN client and optimized use of wireless radio resources. Factors including wireless band, number of spatial streams, 802.11ac and 802.11n capability, and signal to noise ratio are considered.

    This feature also provides automatic load balancing designed to distribute wireless stations across multiple radios rather than having stations associate to the closest radios with the strongest signal strength, as they normally would. In wireless networks, the station selects the radio to which it will associate. The Array/AP cannot actually force load balancing, however it can “encourage” stations to associate in a more optimal fashion to underused radios of the most advantageous type. This option enables or disables active load balancing between the Array IAPs.

If you select **On** and an IAP is not the best choice for network performance, that IAP will send an "AP Full" message in response to Probe, Association, or Authentication requests. This deters persistent clients from forcing their way onto overloaded IAPs.

Note that ACExpress load balancing is **not** used if:

- A station is re-associating—if it was already associated to this IAP, it is allowed back on this IAP immediately. This prevents the station from being bounced between different IAPs.
- The IAP's **Band**, **WiFi Mode,** and **Channel** settings are not at their default values. For example, if an IAP's WiFi mode is set to 11n-only, load balancing will not be used. See "IAP Settings" on page 290.
- If station counts (specified at the IAP, SSID, or band level) are already exceeded.
- If a station has already been turned down a number of times when attempting to associate, i.e., the station will eventually be allowed onto an IAP after a number of attempts have failed.

Choose **Off** to disable load balancing.

27. **ARP Filtering:** Address Resolution Protocol finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. ARP filtering allows you to reduce the proliferation of ARP messages by restricting how they are forwarded across the network.

    You may select from the following options for handling ARP requests:

    - **Off**: ARP filtering is disabled. ARP requests are broadcast to radios that have stations associated to them.
    - **Pass-thru**: The Array forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it. This is the default value.
    - **Proxy**: The Array replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

Note that the Array has a broadcast optimization feature that is always on (it is not configurable). Broadcast optimization restricts all broadcast packets (not just ARP broadcasts) to only those radios that need to forward them. For instance, if a broadcast comes in from VLAN 10, and there are no VLAN 10 users on a radio, then that radio will not send out that broadcast. This increases available air time for other traffic.

28. **IPv6 Filtering:** this setting allows blocking of IPv6 traffic which may be a concern for IT managers. The Xirrus Array currently bridges IPv6 traffic. Set IPv6 filtering **On** if you wish to prevent the forwarding of IPv6 packets through the Array in both directions—wired network to wireless and wireless network to wired. The default is **Off**.

29. **Xirrus Roaming Layer:** Select whether to enable roaming capabilities between IAPs or Arrays at Layer **2 and 3**, or at Layer **2 only**. Depending on your wired network, you may wish to allow fast roaming at Layer 3. This may result in delayed traffic.

30. **Xirrus Roaming Mode:** This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3 (as specified in Step 31), while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see "Understanding Fast Roaming" on page 288 for a discussion of this feature). XRP uses a discovery process to identify other Xirrus Arrays as fast roaming targets. This process has two modes:

    - **Broadcast**—the Array uses a broadcast technique to discover other Arrays that may be targets for fast roaming.
    - **Tunneled**—in this Layer 3 technique, fast roaming target Arrays must be explicitly specified.

    To enable fast roaming, choose **Broadcast** or **Tunneled**, and set additional fast roaming attributes (Step 31). To disable fast roaming, choose **Off**. If you enable Fast Roaming, the following ports **cannot** be blocked:

    - **Port 22610**—reserved for Layer 2 roaming using UDP to share PMK information between Arrays.

- **Ports 15000 to 17999**—reserved for Layer 3 roaming (tunneling between subnets).

31. **Share Roaming Info With:** Three options allow your Array to share roaming information with all Arrays; just with those that are within range; or with specifically targeted Arrays. Choose either **All**, **In Range** or **Target Only**, respectively.

    a. **Xirrus Roaming Targets:** If you chose **Target Only**, use this option to add target MAC addresses. Enter the MAC address of each target Array, then click on **Add** (add as many targets as you like). To find a target's MAC address, open the Array **Info** window on the target Array and look for IAP **MAC Range**, then use the starting address of this range.

       To delete a target, select it from the list, then click **Delete**.

See Also

Coverage and Capacity Planning
Global Settings .11ac
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
Advanced RF Settings
IAPs
IAP Statistics Summary
LED Settings
IAP Settings

Global Settings .11an

This window allows you to establish global 802.11a IAP settings. These settings include defining which 802.11a data rates are supported, enabling or disabling all 802.11an IAPs, auto-configuration of channel allocations for all 802.11an IAPs, and specifying the fragmentation and RTS thresholds for all 802.11an IAPs.

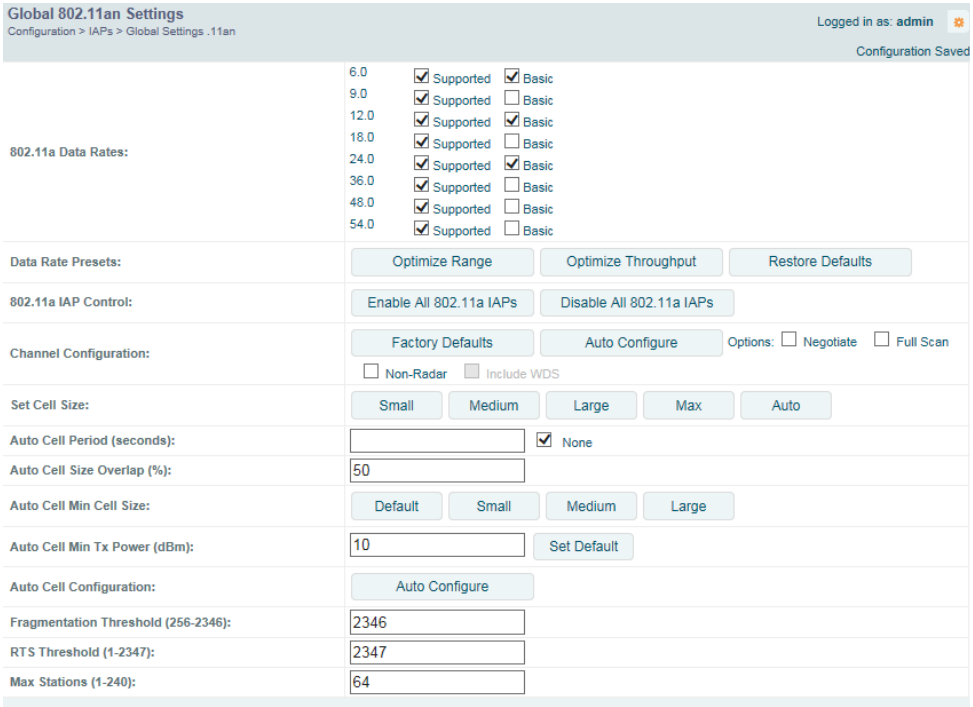


Figure 161. Global Settings .11an

Procedure for Configuring Global 802.11an IAP Settings

1. **802.11a Data Rates:** The Array allows you to define which data rates are supported for all 802.11an radios. Select (or deselect) data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.

- **Supported Rate**—data rates that can be used to transmit to clients.

2. **Data Rate Presets**: The Wireless Array can optimize your 802.11a data rates automatically, based on range or throughput. Click **Optimize Range** to optimize data rates based on range, or click **Optimize Throughput** to optimize data rates based on throughput. The **Restore Defaults** button will take you back to the factory default rate settings.

3. **802.11a IAP Control**: Click **Enable 802.11a IAPs** to enable all 802.11an IAPs for this Array, or click **Disable 802.11a IAPs** to disable all 802.11an IAPs.

4. **Channel Configuration**: Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11an IAP and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11a channel allocation (see "RF Spectrum Management" on page 337).

   Click **Factory Defaults** if you wish to instruct the Array to return all IAPs to their factory preset channels. As of release 6.3, Arrays no longer all use the same factory preset values for channel assignments. Instead, if the Array has been deployed for a while and already has data from the spectrum analyzer and Xirrus Roaming Protocol about channel usage on neighboring Arrays, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the Array has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On the XR-500/600 and XR-1000 Series Arrays, the **Factory Defaults** button will not restore iap1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **Timeshare Mode** again - see "RF Monitor" on page 334.*

The following options may be selected for auto configuration:

- **Non-Radar**: give preference to channels that are not required to use dynamic frequency selection (DFS) to avoid communicating in the same frequency range as some radar (also see Step 8 on page 297).

Channels Required to Use DFS Radar Avoidance in USA			
36+40	Non-radar	116+120	DFS required
44+48	Non-radar	124+128	DFS required
52+56	DFS required	132+136	DFS required
60+64	DFS required	149+153	Non-radar
100+104	DFS required	157+161	Non-radar
108+112	DFS required		

- **Negotiate**: negotiate air-time with other Arrays before performing a full scan.
- **Full Scan**: perform a full traffic scan on all channels on all IAPs to determine the best channel allocation.
- **Include WDS**: automatically assign 5GHz to WDS client links.

To use the Auto Cell Size feature, the following additional settings are required:

RF Monitor Mode must be turned ***On****. See* ***"RF Monitor" on page 334***

One of the radios must be in ***monitor*** *mode with the default* ***RxdBm*** *setting of* ***-95****, and all other IAPs that will use Auto Cell must have* ***Cell Size*** *set to* ***auto****. See* ***"Procedure for Manually Configuring IAPs" on page 291****.*

5. **Set Cell Size**: Cell Size may be set globally for all 802.11an IAPs to **Auto**, **Large, Medium, Small**, or **Max** using the buttons.

For an overview of RF power and cell size settings, please see "RF Power & Sensitivity" on page 336, "Capacity and Cell Sizes" on page 32, and "Fine Tuning Cell Sizes" on page 33.

6. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

7. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

8. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large, Medium,** or **Small**.

9. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

10. **Auto Cell Configuration**: Click this button to instruct the Array to determine and set the best cell size for each 802.11an IAP whose **Cell Size** is **auto** on the IAP Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the IAP Settings window to view the cell size settings that were applied.

11. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11an radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here.

Smaller fragmentation numbers can help to "squeeze" packets through in noisy environments. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346.

12. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

13. **Max Stations**: This defines how many station associations are allowed per 802.11an IAP. Note that the IAPs > Global Settings window and SSIDs—SSID Management window also have station limit settings—**Max Station Association per IAP** (page 299) and **Station Limit** (page 268), respectively. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association. Array

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11bgn
Global Settings .11n
IAPs
IAP Statistics Summary
Advanced RF Settings
IAP Settings

Global Settings .11bgn

This window allows you to establish global 802.11b/g IAP settings. These settings include defining which 802.11b and 802.11g data rates are supported, enabling or disabling all 802.11b/g IAPs, auto-configuring 802.11b/g IAP channel allocations, and specifying the fragmentation and RTS thresholds for all 802.11b/g IAPs.

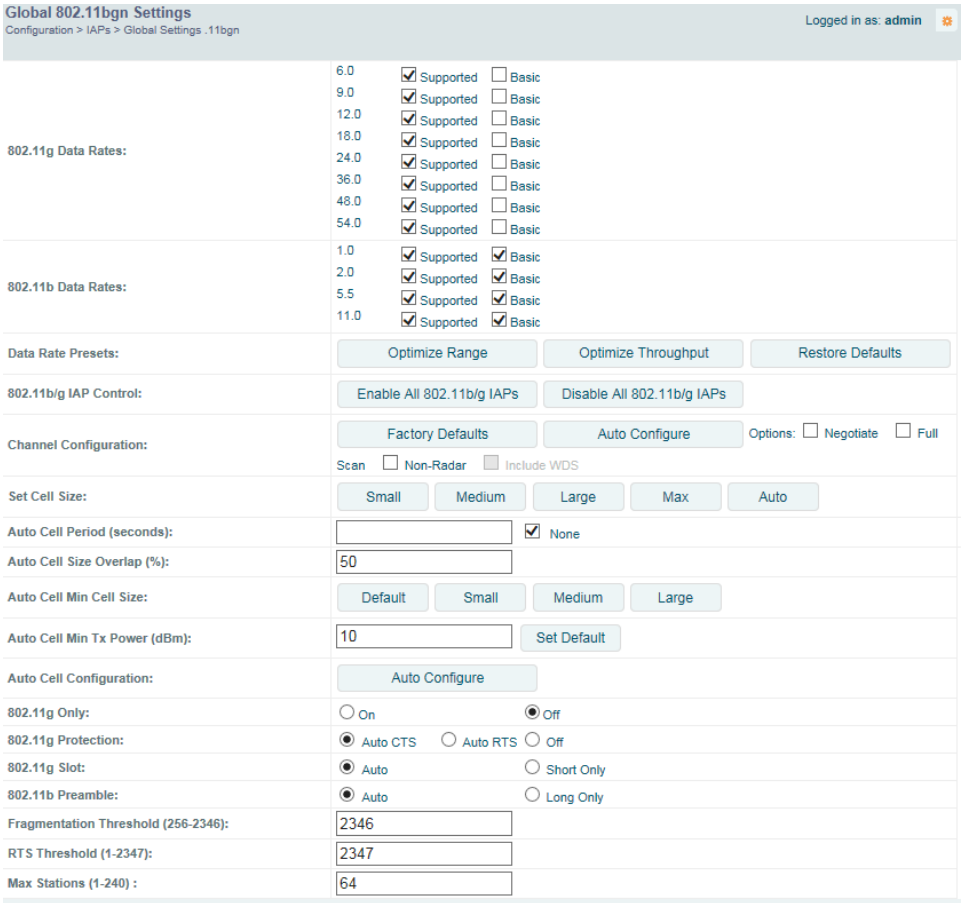


Figure 162. Global Settings .11bgn

Procedure for Configuring Global 802.11b/g IAP Settings

1. **802.11g Data Rates:** The Array allows you to define which data rates are supported for all 802.11g radios. Select (or deselect) 11g data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
    - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
    - **Supported Rate**—data rates that can be used to transmit to clients.
2. **802.11b Data Rates**: This task is similar to Step 1, but these data rates apply only to 802.11b IAPs.
3. **Data Rate Presets**: The Wireless Array can optimize your 802.11b/g data rates automatically, based on range or throughput. Click **Optimize Range** button to optimize data rates based on range, or click on the **Optimize Throughput** to optimize data rates based on throughput. **Restore Defaults** will take you back to the factory default rate settings.
4. **802.11b/g IAP Control**: Click **Enable All 802.11b/g IAPs** to enable all 802.11b/g IAPs for this Array, or click **Disable All 802.11b/g IAPs** to disable them.
5. **Channel Configuration**: Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11b/g IAP and select the channel automatically, based on changes in the environment. This is the recommended method for channel allocation (see "RF Spectrum Management" on page 337).

    Click **Factory Defaults** if you wish to instruct the Array to return all IAPs to their factory preset channels. As of release 6.3, Arrays no longer all use the same factory preset values for channel assignments. Instead, if the Array has been deployed for a while and already has data from the spectrum analyzer and Xirrus Roaming Protocol about channel usage on neighboring Arrays, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the Array has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior

data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On the XR-500/600 and XR-1000 Series Arrays, the **Factory Defaults** button will not restore iap1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **Timeshare Mode** again - see "RF Monitor" on page 334.*

The following options may be selected for auto configuration:

- **Negotiate**: negotiate air-time with other Arrays before performing a full scan.
- **Full Scan**: perform a full traffic scan on all channels on all IAPs to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in "Procedure for Configuring Global 802.11an IAP Settings" on page 311.
- **Include WDS**: automatically assign 5GHz to WDS client links.

To use the Auto Cell Size feature, the following additional settings are required:

*RF Monitor Mode must be turned **On**. See **"RF Monitor" on page 334***

*One of the radios must be in **monitor** mode with the default **RxdBm** setting of **-95**, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See **"Procedure for Manually Configuring IAPs" on page 291**.*

6. **Set Cell Size/ Autoconfigure**: Cell Size may be set globally for all 802.11b/g IAPs to **auto**, **large, medium, small**, or **max** using the drop down menu.

   For an overview of RF power and cell size settings, please see "RF Power & Sensitivity" on page 336, "Capacity and Cell Sizes" on page 32, and "Fine Tuning Cell Sizes" on page 33.

7. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

8. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

9. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large, Medium,** or **Small**.

10. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

11. **Auto Cell Configuration**: Click **Auto Configure** to instruct the Array to determine and set the best cell size for each enabled 802.11b/g IAP whose **Cell Size** is **auto** on the IAP Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the IAP Settings window to view the cell size settings that were applied.

12. **802.11g Only**: Choose **On** to restrict use to 802.11g mode only. In this mode, no 802.11b rates are transmitted. Stations that only support 802.11b will not be able to associate.

13. **802.11g Protection**: You should select **Auto CTS** or **Auto RTS** to provide automatic protection for all 802.11g radios in mixed networks (802.11 b and g). You may select **Off** to disable this feature, but this is not recommended. Protection allows 802.11g stations to share an IAP with

older, slower 802.11b stations. Protection avoids collisions by preventing 802.11b and 802.11g stations from transmitting simultaneously. When **Auto CTS** or **Auto RTS** is enabled and any 802.11b station is associated to the IAP, additional frames are sent to gain access to the wireless network.

- Auto CTS requires 802.11g stations to send a slow Clear To Send frame that locks out other stations. Automatic protection reduces 802.11g throughput when 802.11b stations are present—Auto CTS adds less overhead than Auto RTS. The default value is Auto CTS.
- With Auto RTS, 802.11g stations reserve the wireless media using a Request To Send/Clear To Send cycle. This mode is useful when you have dispersed nodes. It was originally used in 802.11b only networks to avoid collisions from "hidden nodes"—nodes that are so widely dispersed that they can hear the Array, but not each other.

When there are no 11b stations associated and an auto-protection mode is enabled, the Array will not send the extra frames, thus avoiding unnecessary overhead.

14. **802.11g Slot**: Choose **Auto** to instruct the Array to manage the 802.11g slot times automatically, or choose **Short Only**. Xirrus recommends using **Auto** for this setting, especially if 802.11b devices are present.
15. **802.11b Preamble**: The preamble contains information that the Array and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble. A short preamble improves the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video. Select **Auto** to instruct the Array to manage the preamble (long and short) automatically, or choose **Long Only**.
16. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11b/g IAP. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value, between 256 and 2346.

17. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

18. **Max Stations**: This defines how many station associations are allowed per 802.11bgn IAP. Note that the IAPs > Global Settings window and SSIDs > SSID Management window also have station limit settings—**Max Station Association per IAP** (page 299) and **Station Limit** (page 268), respectively. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11an
Global Settings .11n
Advanced RF Settings
LED Settings
IAP Settings
IAP Statistics Summary

Global Settings .11n

This window allows you to establish global 802.11n IAP settings. These settings include enabling or disabling 802.11n mode for the entire Array, specifying the number of transmit and receive chains (data stream) used for spatial multiplexing, setting a short or standard guard interval, auto-configuring channel bonding, and specifying whether auto-configured channel bonding will be static or dynamic.

Before changing your settings for 802.11n, please read the discussion in "About IEEE 802.11ac" on page 37.

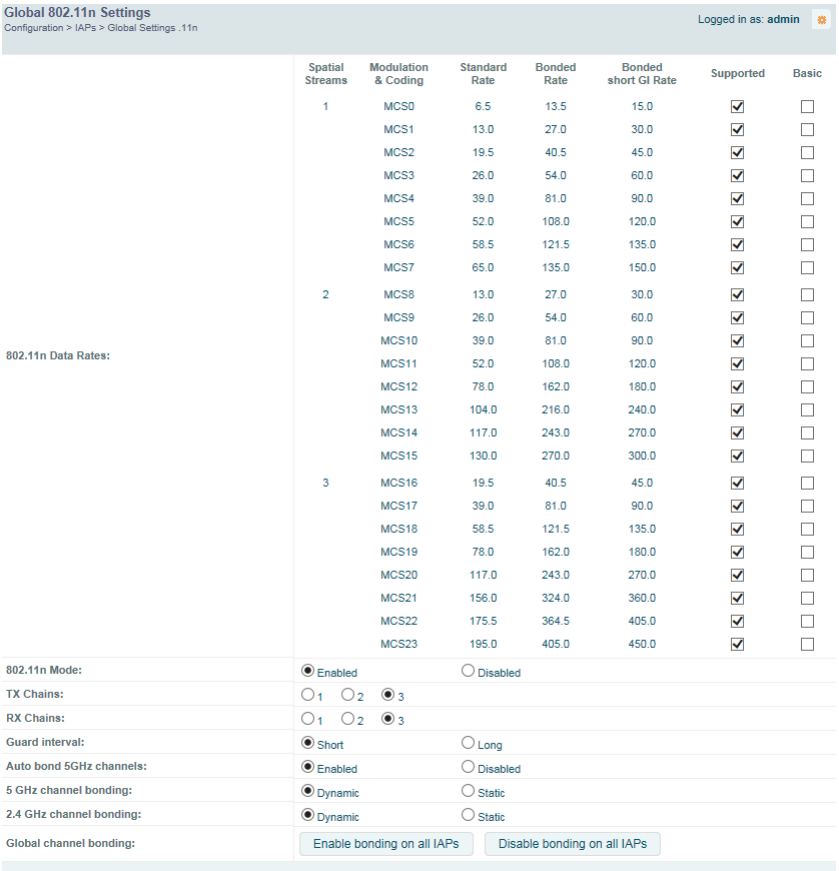


Figure 163. Global Settings .11n

Procedure for Configuring Global 802.11n IAP Settings

1. **802.11n Data Rates**: The Array allows you to define which data rates are supported for all 802.11n radios. Select (or deselect) 11n data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
    - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
    - **Supported Rate**—data rates that can be used to transmit to clients.
2. **802.11n Mode**: Select **Enabled** to allow the Array to operate in 802.11n mode.

    If you select **Disabled**, then 802.11n operation is disabled on the Array.
3. **TX Chains**: Select the number of separate data streams transmitted by the antennas of each IAP. The maximum number of chains is determined by whether the XR Series Array has 2x2 or 3x3 radios. The default value is always the maximum supported by the radio type. See "Up to Eight Simultaneous Data Streams—Spatial Multiplexing" on page 39.
4. **RX Chains**: Select the number of separate data streams received by the antennas of each IAP. This number should be greater than or equal to **TX Chains**. The maximum number of chains is determined by whether the XR Series Array has 2x2 or 3x3 radios. The default value is always the maximum supported by the radio type. See "Up to Eight Simultaneous Data Streams—Spatial Multiplexing" on page 39.
5. **Guard interval**: Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short.
6. **Auto bond 5 GHz channels**: Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**. See "80 MHz and 160 MHz Channel Widths (Bonding)" on page 43.

7. **5 GHz channel bonding**: Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**. See "80 MHz and 160 MHz Channel Widths (Bonding)" on page 43.

8. **2.4 GHz channel bonding**: Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The default is **Dynamic**. See "80 MHz and 160 MHz Channel Widths (Bonding)" on page 43.

9. **Global channel bonding**: These buttons allow you to turn channel bonding on or off for all IAPs in one step. The effect of using one of these buttons will be shown if you go to the **IAP Settings** window and look at the **Bond** column. Clicking **Enable bonding on all IAPs** causes all IAPs to be bonded to their auto-bonding channel immediately, if appropriate. For example, an IAP will not be bonded if it is set to monitor mode, and 2.4 GHz radios will not be bonded. Click **Disable bonding on all IAPs** to turn off bonding on all IAPs immediately. See "80 MHz and 160 MHz Channel Widths (Bonding)" on page 43. Settings in Step 7 and Step 8 are independent of global channel bonding.

Global Settings .11ac

This window allows you to establish global 802.11ac IAP settings. These settings include enabling or disabling 802.11ac mode for the entire Array, specifying the number of data streams used in spatial multiplexing, and setting a short or long guard interval.

Before changing your settings for 802.11ac, please read the discussion in "About IEEE 802.11ac" on page 37.

Global 802.11ac Radio Settings
Configuration > IAPs > Global Settings .11ac
Logged in as: **admin**

802.11ac Mode:	(•) Enabled	( ) Disabled
80 Mhz Guard interval:	(•) Short	( ) Long
Max MCS - 1 Spatial Stream:	MCS9	
Max MCS - 2 Spatial Streams:	MCS9	
Max MCS - 3 Spatial Streams:	MCS9	

801.11ac Supported Rates

One Spatial Stream

802.11ac Modulation & Coding Schema				MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
Frequenc	Type	Guard	Rate										
20MHz	channel	long	GI	6.5	13.0	19.5	26.0	39.0	52.0	58.5	65.0	78.0	-
20MHz	channel	short	GI	7.2	14.4	21.7	28.9	43.3	57.8	65.0	72.2	86.7	-
40MHz	bonded	long	GI	13.5	27.0	40.5	54.0	81.0	108.0	121.5	135.0	162.0	180.0
40MHz	bonded	short	GI	15.0	30.0	45.0	60.0	90.0	120.0	135.0	150.0	180.0	200.0
80MHz	bonded	long	GI	29.3	58.5	87.8	117.0	175.5	234.0	263.3	292.5	351.0	390.0
80MHz	bonded	short	GI	32.5	65.0	97.5	130.0	195.0	260.0	292.5	325.0	390.0	433.3

Two Spatial Streams

802.11ac Modulation & Coding Schema				MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
Frequenc	Type	Guard	Rate										
20MHz	channel	long	GI	13.0	26.0	39.0	52.0	78.0	104.0	117.0	130.0	156.0	-
20MHz	channel	short	GI	14.4	28.9	43.3	57.8	86.7	115.6	130.0	144.4	173.3	-
40MHz	bonded	long	GI	27.0	54.0	81.0	108.0	162.0	216.0	243.0	270.0	324.0	360.0
40MHz	bonded	short	GI	30.0	60.0	90.0	120.0	180.0	240.0	270.0	300.0	360.0	400.0
80MHz	bonded	long	GI	58.5	117.0	175.5	234.0	351.0	468.0	526.5	585.0	702.0	780.0
80MHz	bonded	short	GI	65.0	130.0	195.0	260.0	390.0	520.0	585.0	650.0	780.0	866.7

Three Spatial Streams

802.11ac Modulation & Coding Schema				MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
Frequenc	Type	Guard	Rate										
20MHz	channel	long	GI	19.5	39.0	58.5	78.0	117.0	156.0	175.5	195.0	234.0	260.0

Figure 164. Global Settings .11ac

Procedure for Configuring Global 802.11ac IAP Settings

1. **802.11ac Mode**: Select **Enabled** to allow the Array to operate in 802.11ac mode. **If you select Disabled, then 802.11ac operation is disabled on the Array.**

2. **80 MHz Guard interval**: This is the length of the interval between transmission of symbols (the smallest unit of data transfer) when you are using 80MHz bonded channels. (See "80 MHz and 160 MHz Channel Widths (Bonding)" on page 43.) Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short.

3. **Max MCS**: Select the highest Modulation and Coding Scheme level that may be used with **1** or **2 Spatial Streams**. For models with 3x3 radios, there is also a setting for **3 Spatial Streams**. This setting may be used to limit the highest level of modulation to 64-QAM, or allow 256-QAM with its higher data rate. It also determines the coding scheme used for error correction. Higher MCS levels allocate fewer bits to error correction, and thus a higher proportion is used for data transfer. The default **Max MCS** value is **MCS9**.

   The higher the MCS values, the higher the data rate, as shown in **802.11ac Supported Rates**, below. Higher MCS levels require higher signal-to-noise ratios (i.e., a less noisy environment) and shorter transmission distances. See "Higher Precision in the Physical Layer" on page 42.

   The maximum number of separate data streams that may be transmitted by the antennas of each IAP is determined by whether the XR Series Array has 2x2 or 3x3 radios. For a device that has 2x2 radios, such as the XR-620, the settings for three spatial streams are not shown.See "Up to Eight Simultaneous Data Streams—Spatial Multiplexing" on page 39.

4. **802.11ac Supported Rates**: This list shows the optimum data rates that can be expected, based on the number of spatial streams that a station can handle, and on your settings for Max MCS, Guard Interval, and the use of bonded channels, up to 80MHz wide.

Global Settings .11u

Understanding 802.11u

As the number of access points available in public venues increases, mobile devices users have a harder time distinguishing usable SSIDs from the tens, if not hundreds of access points visible. Using the 802.11u protocol, access points may broadcast information about the services and access that they offer and to respond to queries for additional information related to the facilities that the downstream service network provides.

The type of information broadcast or available from 802.11u-compliant access points includes:

- **Access Network Type**. Indicates the type of network available. For example: public or private, free or charged, etc.
- **Internet Connectivity**. Indicates whether the network provides Internet connectivity.
- **Authentication**. Indicates whether additional authentication steps will be required to use the network as well as the network authentication types that are in use.
- **Venue Information**. The type and name of the location where the access point is found.
- **Identification**. A globally unique identification for the access point.
- **IPv4/IPv6 Addressing.** Indicate the type of IP addressing (IPv4 and/or IPv6) and NATing that is performed by the network.
- **Roaming Consortium.** The service network may be connected to one or more roaming providers, called consortia, that allow access points from multiple service providers to be used transparently through a single paid service. The access point may advertise multiple consortia to mobile devices.
- **Domain Names.** A list of domain names to which the mobile user may end up belonging based on authentication credentials used.

- **Cellular Networks.** The service network may have arrangements with one or more cellular service providers who can transparently provide wireless and Internet connectivity.

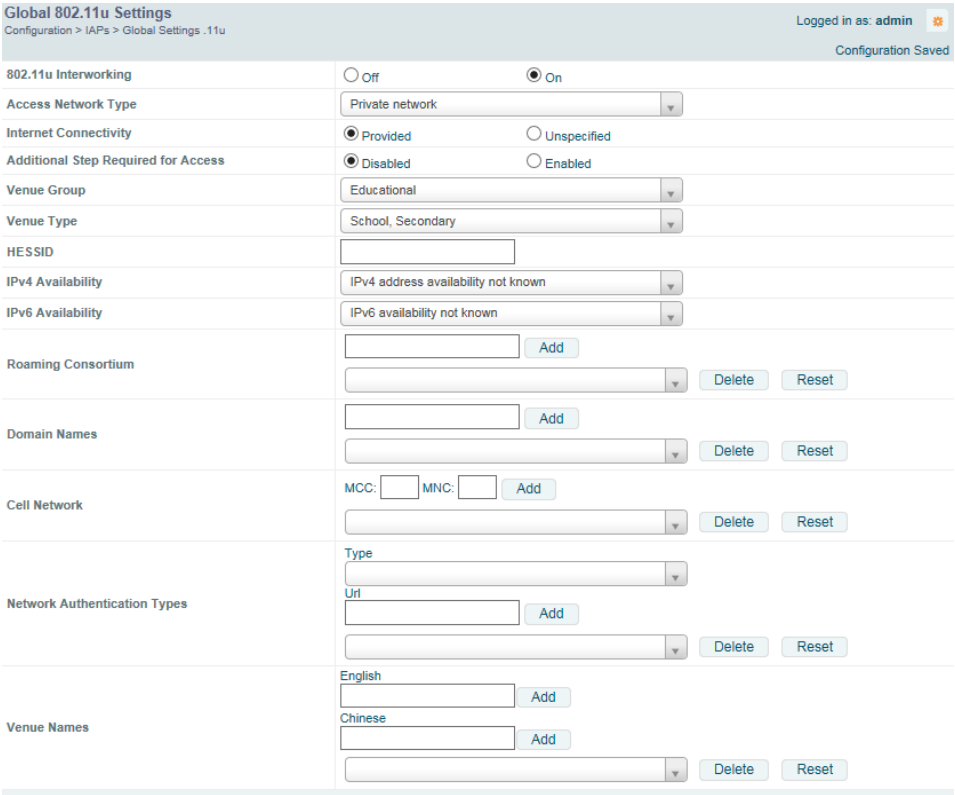


Figure 165. 802.11u Global Settings

Procedure for Configuring 802.11u Settings

Use this window to establish the 802.11u configuration.

1. **802.11u Internetworking.** Click **On** to enable 802.11u protocol operation.
2. **Access Network Type**: This indicates the type of network supported by the access point. The choices are:

a. **Chargeable public network**

b. **Emergency services only network**

c. **Free public network**

d. **Personal device network**

e. **Private network with guest access**

f. **Test or experimental network**

g. **Wildcard**—all of the networks above are supported.

3. **Internet Connectivity.** Click **Provided** if Internet connectivity is available through the access point from the back end provider to which the mobile user ends up belonging. Click **Unspecified** otherwise—for example, depending on the SLAs (service level agreements) of the mobile user, Internet access may or may not be provided.

4. **Additional Step Required for Access.** Click **Disabled** if no additional authentication steps will be required to complete the connection and **Enabled** otherwise. The available authentication techniques are described in the **Network Authentication Types** field (Step 13).

5. **Venue Group.** Select the general type of venue that the access point is located in. Various choices are available, including **Business, Residential,** and **Outdoor.** For each **Venue Group**, a further set of sub-choices are available in the **Venue Type** field below. The particular name of the venue is specified in the **Venue Names** field (Step 14).

6. **Venue Type**. For each of the **Venue Group** choices, a further set of sub-choices are available. For example, if you set **Venue Group** to **Assembly**, the choices include **Amphitheater, Area, Library,** and **Theatre.**

7. **HESSID**. Enter the globally unique homogeneous ESS ID. This SSID is marked as being HotSpot 2.0 capable. This SSID attribute is global—if 802.11u is enabled and HotSpot 2.0 is enabled, then all SSIDs will have HotSpot 2.0 capability.

8. **IPv4 Availability.** Select the type of IPv4 addressing that will be assigned by the network upon connection. NATed addresses are IP addresses that have been changed by mapping the IP address and port number to IP addresses and new port numbers routable by other networks. **Double NATed** addresses go through two levels of NATing. **Port restricted IPv4 addresses** refer to specific UDP and TCP port numbers associated with standard Internet services; for example, port 80 for web pages. The choices for this field are:
   a. **Double NATed private IPv4 address available**
   b. **IPv4 address not available**
   c. **IPv4 address availability not known**
   d. **Port-restricted IPv4 address available**
   e. **Port-restricted IPv4 address and double NATed IPv4 address available**
   f. **Port-restricted IPv4 address and single NATed IPv4 address available**
   g. **Public IPv4 address available**
   h. **Single NATed private IPv4 address available**
9. **IPv6 Availability.** Select the type of IPv6 addressing that is available from the network upon connection.
   a. **IPv6 address not available**
   b. **IPv6 address availability not known**
   c. **IPv6 address available**
10. **Roaming Consortium.** Each of the roaming consortia has an organizational identifier (OI) obtained from IEEE that unique identifies the organization. This is similar to the OUI part of a MAC address. Use this control to build up a list of OIs for the consortia available. Enter the OI as a hexadecimal string of between 6 and 30 characters in the **Add** field

and click **Add**. The OI will appear in the list. An OI may be deleted by selecting it in the list and clicking **Delete**. All OIs may be deleted by clicking **Reset**.

11. **Domain Names.** Use this control to build up a list of domain names. Enter the name in the **Add** field and click **Add**, and it will appear in the list. A name may be deleted by selecting it in the list and clicking **Delete**. All names may be deleted by clicking **Reset**.

12. **Cell Network.** Each of the cell networks is identified by a mobile country code (MCC) and mobile network code (MNC). Use this control to build up a list of cell networks. Enter the MCC as a three digit number and the MNC as a two or three digit number and click **Add**. The cell network will appear in the list. A cell network may be deleted by selecting it in the list and clicking **Delete**. All networks may be deleted by clicking **Reset**.

13. **Network Authentication Types**. Each network authentication that is in use on the network should be specified in this list. The choices are:

    a. **Acceptance of terms and conditions.** This choice displays a web page asking for the user's acceptance of terms and conditions of use. The URL should be specified in the URL field before clicking **Add.**

    b. **DNS redirection.** Rather than use the DNS server on the network, the redirection points to a different server.

    c. **HTTP/HTTPS redirection.** This choice causes the user's first web page reference to be redirected to a different URL for login or other information. The URL should be specified in the URL field before clicking **Add.**

    d. **On-line enrollment supported.** This choice indicates that the user may sign up for network access as part of the authentication process.

    When **Add** is clicked the authentication type and optional URL will appear in the list. An authentication type may be deleted by selecting it in the list and clicking **Delete**. All authentication types may be deleted by clicking **Reset**.

14. **Venue Names.** The list of names associated with the venue are specified here. A venue name may be added to the list in English or Chinese. Enter the name in the appropriate field and click **Add.** The name will appear in the list. A name may be deleted by selecting it in the list and clicking **Delete**. All names may be deleted by clicking **Reset**.

Advanced RF Settings

This window allows you to establish RF settings, including automatically configuring channel allocation and cell size, and configuring radio assurance and standby modes. Changes you make on this page are applied to all IAPs, without exception.

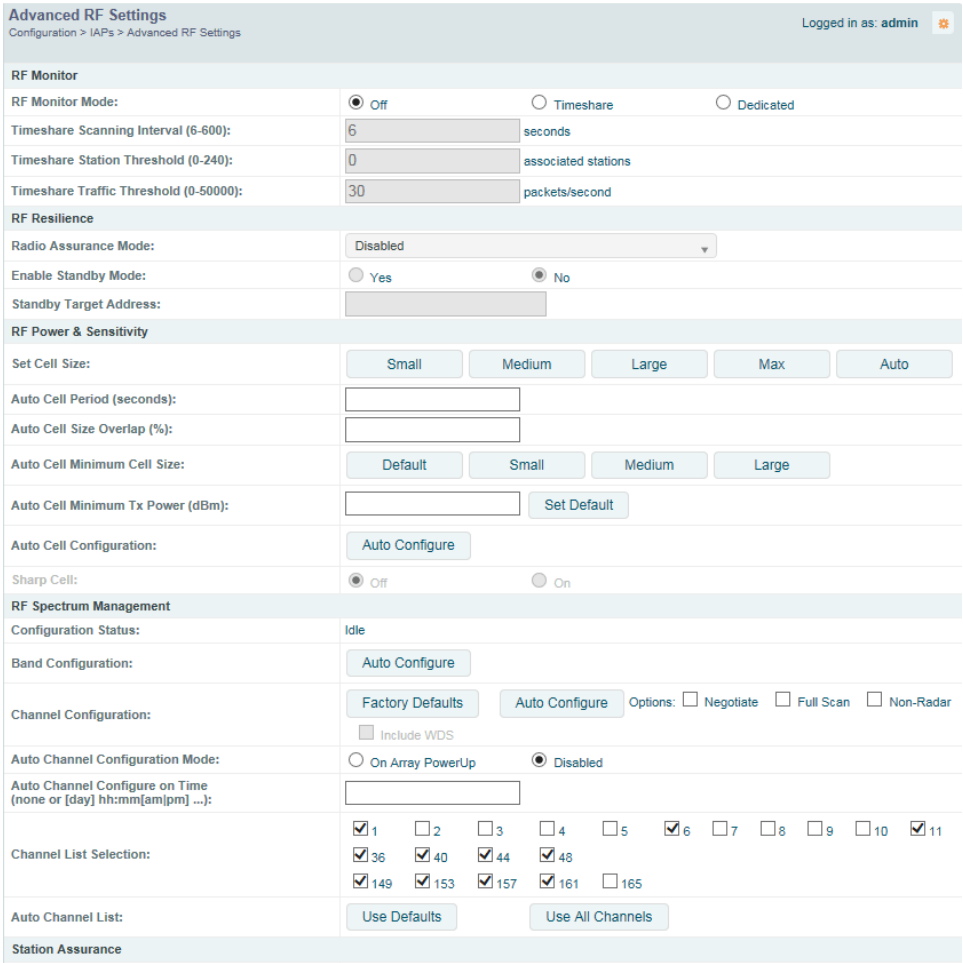


Figure 166. Advanced RF Settings

About Standby Mode

Standby Mode supports the Array-to-Array fail-over capability. When you enable Standby Mode, the Array functions as a backup unit, and it enables its radios if it detects that its designated target Array has failed. The use of redundant Arrays to provide this fail-over capability allows Arrays to be used in mission-critical applications. In Standby Mode, an Array monitors beacons from the target Array. When the target has not been heard from for 40 seconds, the standby Array enables its radios until it detects that the target Array has come back online. Standby Mode is off by default. Note that you must ensure that the configuration of the standby Array is correct. This window allows you to enable or disable Standby Mode and specify the primary Array that is the target of the backup unit. See also, "Failover Planning" on page 47.

Procedure for Configuring Advanced RF Settings

RF Monitor

1. **RF Monitor Mode:** RF monitoring permits the operation of features like intrusion detection. The monitor may operate in **Dedicated** mode, or in **Timeshare** mode which allows the radio to divide its time between monitoring and acting as a standard radio that allows stations to associate to it. **Timeshare** mode is especially useful for small Arrays with two IAPs, such as the XR-500/600 and XR-1000 Series, allowing one IAP to be shared between monitoring the airwaves for problems and providing services to stations. Settings allow you to give priority to monitoring or wireless services, depending on your needs. The default Monitor Mode is **Off** for the XR-500 and XR-600 Series, **Timeshare** mode for XR-1000 Series, and **Dedicated** for XR-2000 and above.

   If **Timeshare** mode is selected, you may adjust the following settings:

   - **Timeshare Scanning Interval (6-600)**: number of seconds between monitor (off-channel) scans.
   - **Timeshare Station Threshold (0-240)**: when the number of stations associated to the monitor radio exceeds this threshold, scanning is halted.

- **Timeshare Traffic Threshold (0-50000)**: when the number of packets per second handled by the monitor radio exceeds this threshold, scanning is halted.

RF Resilience

2. **Radio Assurance Mode**: When this mode is enabled, the monitor radio performs loopback tests on the Array. This mode requires RF Monitor Mode to be enabled (Step 1) to enable self-monitoring functions. It also requires a radio to be set to monitoring mode (see "Enabling Monitoring on the Array" on page 500).

   Operation of Radio Assurance mode is described in detail in "Array Monitor and Radio Assurance Capabilities" on page 500.

   The Radio Assurance mode scans and sends out probe requests on each channel, in turn. It listens for all probe responses and beacons. These tests are performed continuously (24/7). If no beacons or probe responses are observed from a radio for a predetermined period, Radio Assurance mode will take action according to the preference that you have specified:

   - **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
   - **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of one or all of the radios if needed.
   - **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets, and schedule reboots if needed.
   - **Disabled**—Disable IAP radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.

3. **Enable Standby Mode**: Choose **Yes** to enable this Array to function as a backup unit for the target Array, or choose **No** to disable this feature. See "About Standby Mode" on page 334.

4. **Standby Target Address**: If you enabled the Standby Mode, enter the MAC address of the target Array (i.e., the address of the primary Array that is being monitored and backed up by this Array). To find this MAC address, open the Array Info window on the target Array, and use the Gigabit1 MAC Address.

RF Power & Sensitivity

For an overview of RF power and cell size settings, please see "Capacity and Cell Sizes" on page 32 and "Fine Tuning Cell Sizes" on page 33.

To use the Auto Cell Size feature, the following additional settings are required:

RF Monitor Mode must be turned ***On****. See* ***"RF Monitor" on page 334.***

One of the radios must be in ***monitor*** *mode, and all other IAPs that will use Auto Cell must have* ***Cell Size*** *set to* ***auto****. See* ***"Procedure for Manually Configuring IAPs" on page 291****.*

5. **Set Cell Size**: Cell Size may be set globally for all enabled IAPs to **Auto**, **Large, Medium, Small**, or **Max** using the buttons.

6. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

7. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

8. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large, Medium,** or **Small**.

9. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

10. **Auto Cell Configuration**: Click this button to instruct the Array to determine and set the best cell size for each enabled IAP whose **Cell Size** is **auto** on the IAP Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the IAP Settings window to view the cell size settings that were applied.

11. **Sharp Cell:** This feature reduces interference between neighboring Arrays or other Access Points by limiting to a defined boundary (cell size) the trailing edge bleed of RF energy. Choose **On** to enable the Sharp Cell functionality, or choose **Off** to disable this feature. See also, "Fine Tuning Cell Sizes" on page 33. This feature is available on all Arrays.

    The Sharp Cell feature only works when the cell size is Small, Medium, or Large (or Auto)—but not Max. If an IAP cell size is set to Max, the Sharp Cell feature will be disabled for that radio.

RF Spectrum Management

12. **Configuration Status**: Shows the status of auto channel configuration. If an operation is in progress, the approximate time remaining until completion is displayed; otherwise **Idle** is displayed.

13. **Band Configuration**: Automatic band configuration is the recommended method for assigning bands to the abgn IAPs. It runs only on command, assigning IAPs to the 2.4GHz or 5GHz band when you click the **Auto Configure** button. The Array uses its radios to listen for other APs on the same channel, and it assigns bands based on where it finds the least interference.

Auto band assigns as many IAPs to the 5 GHz band as possible when there are other Arrays within earshot. It does this by determining how many Arrays are in range and then picking the number of radios to place in the 2.4 GHz band. Note that for another Array to be considered to be in range, the other Array must be visible via both the wireless and wired networks—the Array must be listed in the Network Map table, its entry must have **In Range** set to **Yes**, and it must have at least one active IAP with an SSID that has broadcast enabled.

Auto band runs separately from auto channel configuration. If the band is changed for an IAP, associated stations will be disconnected and will then reconnect.

14. **Channel Configuration**: Automatic channel configuration is the recommended method for channel allocation. When the Array performs auto channel configuration, you may optionally instruct it to first negotiate with any other nearby Arrays that have been detected, to determine whether to stagger the start time for the procedure slightly. Thus, nearby Arrays will not run auto channel at the same time. This prevents Arrays from interfering with each other's channel assignments.

    The **Configuration Status** field displays whether an Auto Configure cycle is currently running on this Array or not.

    Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each enabled IAP and select the channel automatically, based on changes in the environment. This is the recommended method for channel allocation (see "RF Spectrum Management" on page 337). The following options may be selected for auto configuration:

    - **Negotiate**: negotiate air-time with other Arrays before performing a full scan. Negotiating is slower, but if multiple Arrays are configuring channels at the same time the Negotiate option ensures that multiple Arrays don't select the same channels. Turning off the Negotiate option allows the **Auto Configure** button to manually perform auto

channel without waiting, and may be used when you know that no other nearby Arrays are configuring their channels.

- **Full Scan**: perform a full traffic scan on all channels on all IAPs to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in "Procedure for Configuring Global 802.11an IAP Settings" on page 311.
- **Include WDS**: automatically assign 5GHz to WDS client links.

Click **Factory Defaults** if you wish to instruct the Array to return all IAPs to their factory preset channels. As of release 6.3, Arrays no longer all use the same factory preset values for channel assignments. Instead, if the Array has been deployed for a while and already has data from the spectrum analyzer and Xirrus Roaming Protocol about channel usage on neighboring Arrays, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the Array has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On XR-500/600 and XR-1000 Series Arrays, the **Factory Defaults** button will not restore iap1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **RF Monitor Mode** to **Timeshare Mode** again - see "RF Monitor" on page 334.*

15. **Auto Channel Configuration Mode**: This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP when the Array is powered up. Choose **On Array PowerUp** to enable this feature, or choose **Disabled** to disable this feature.

16. **Auto Channel Configure on Time**: This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here. Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated. Time is specified in hours and minutes, using the format: **[day]hh:mm [am | pm]**. If you omit

the optional **day** specification, channel configuration will run daily at the specified time. If you do not specify am or pm, time is interpreted in 24-hour military time. For example, Sat 11:00 pm and Saturday 23:00 are both acceptable and specify the same time.

17. **Channel List Selection**: This list selects which channels are available to the auto channel algorithm. Channels that are not checked are left out of the auto channel selection process. Note that channels that have been locked by the user are also not available to the auto channel algorithm.

18. **Auto Channel List**: **Use All Channels** selects all available channels (this does not include locked channels). **Use Defaults** sets the auto channel list back to the defaults. This omits newer channels (100-140)—many wireless NICs don't support these channels.

Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the wireless network. You can quickly detect stations that are having problems and take steps to correct them. Use these settings to establish threshold values for errors and other problems. Station assurance is enabled by default, with a set of useful default thresholds that you may adjust as desired.

When a connection is experiencing problems and reaches one of these thresholds in the specified period of time, the Array responds with several actions: an event is triggered, a trap is generated, and a Syslog message is logged. For example, if a client falls below the threshold for **Min Average Associated Time**, this "bouncing" behavior might indicate roaming problems with the network's RF design, causing the client to bounce between multiple Arrays and not stay connected longer than the time to re-associate and then jump again. This can be corrected with RF adjustments. Station assurance alerts you to the fact that this station is encountering problems.

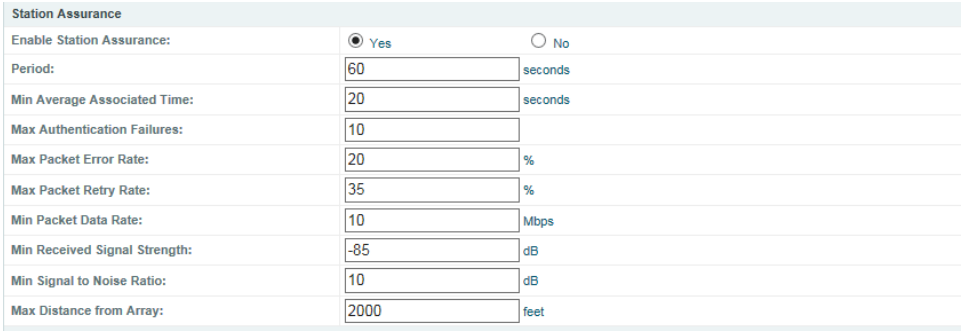


Figure 167. Station Assurance (Advanced RF Settings)

19. **Enable Station Assurance**: This is enabled by default. Click No if you wish to disable it, and click Yes to re-enable it. When station assurance is enabled, the Array will monitor connection quality indicators listed below and will display associated information on the Station Assurance Status page. When a threshold is reached, an event is triggered, a trap is generated, and a Syslog message is logged.
20. **Period**: In seconds, the period of time for a threshold to be reached. For example, the Array will check whether Max Authentication Failures has been reached in this number of seconds.
21. **Min Average Associated Time**: (seconds) Station assurance detects whether the average length of station associations falls below this threshold during a period.
22. **Max Authentication Failures**: Station assurance detects whether the number of failed login attempts reaches this threshold during a period.
23. **Max Packet Error Rate**: (%) Station assurance detects whether the packet error rate percentage reaches this threshold during a period.
24. **Max Packet Retry Rate**: (%) Station assurance detects whether the packet retry rate percentage reaches this threshold during a period.
25. **Min Packet Data Rate**: (Mbps) Station assurance detects whether the packet data rate falls below this threshold during a period.

26. **Min Received Signal Strength**: (dB) Station assurance detects whether the strength of the signal received from the station falls below this threshold during a period.
27. **Min Signal to Noise Ratio**: (dB) Station assurance detects whether the ratio of signal to noise received from the station falls below this threshold during a period.
28. **Max Distance from Array**: **Min Received Signal Strength**: (feet) Station assurance detects whether the distance of the station from the Array reaches this threshold during a period.

See Also

Coverage and Capacity Planning
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
IAPs
IAP Settings
Radio Assurance

Hotspot 2.0

Understanding Hotspot 2.0

Hotspot 2.0 is a part of the Wi-Fi Alliance's Passpoint certification program. It specifies additional information above and beyond that found in 802.11u, which allows mobile clients to automatically discover, select, and connect to networks based on preferences and network optimization. Mobile clients that support Hotspot 2.0 are informed of an access point's support via its beacon message.

Hotspot 2.0 messages forward several types of information to clients, including:

- **Uplink and Downlink Speeds**
- **Link Status**
- **Friendly Name**
- **Connection Capabilities** The access point will restrict the protocols that can be used by a specification of protocol and port numbers.

Procedure for Hotspot 2.0 Settings

Use this window to establish the Hotspot 2.0 configuration.

1. **Hotspot 2.0.** Click **Enabled to** enable Hotspot 2.0 operation**.**
2. **Downstream Group-addressed Forwarding.** Click **Enabled** to allow the access point to forward group-addressed traffic (broadcast and multicast) to all connected devices. Click **Disabled** to cause the access point to convert group-addressed traffic to unicast messages.
3. **WAN Downlink Speed.** Enter the WAN downlink speed in kbps into the field.
4. **WAN Uplink Speed.** Enter the WAN uplink speed in kbps into the field.

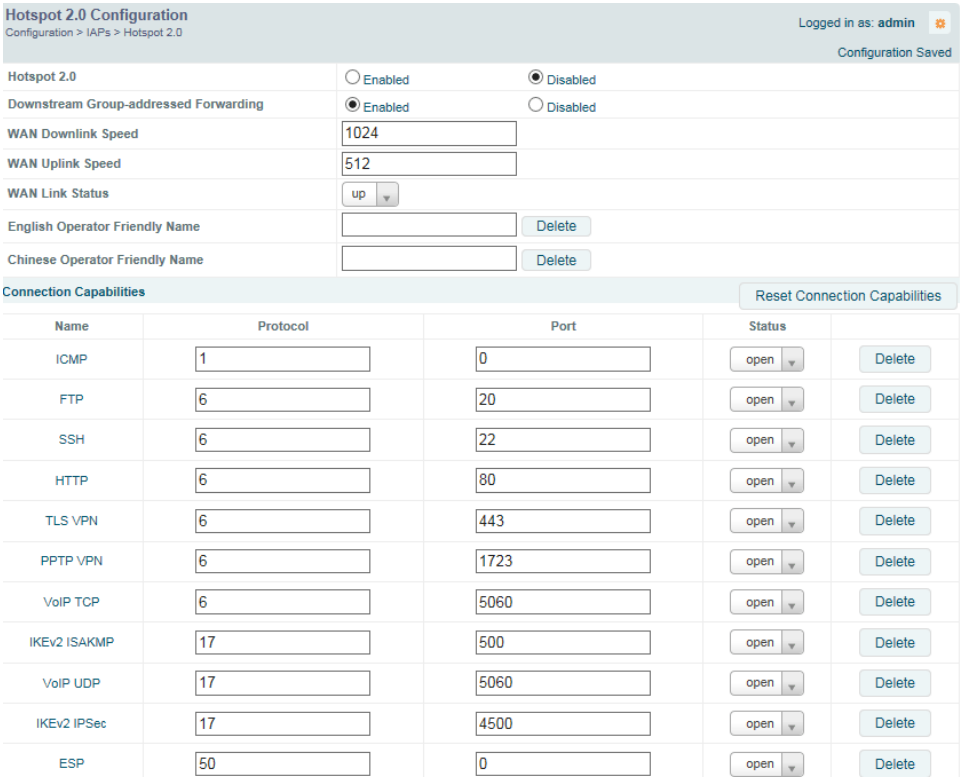


Figure 168. Hotspot 2.0 Settings

5. **English/Chinese Operator Friendly Name.** Enter an English or Chinese name into one of the fields. An incorrectly entered name can be deleted by clicking the corresponding **Delete.**

6. **Connection Capabilities.** A Hotspot 2.0 access point limits the particular protocols that clients may use. The set of default protocols is shown initially. This table specifies the protocols in terms of:

   a. A common **Name**, such as FTP or HTTP.

   b. A **Protocol** number. For example 1 for ICMP, 6 for TCP, 17 for UDP, and 50 for Encapsulated Security Protocol in IPsec VPN connections.

   c. **Port** number for UDP/TCP connection.

   d. **Status**: one of **open, closed** or **unknown.**

   Any of the entries may be deleted by clicking the corresponding **Delete** button. New entries may be created by entering the name of the protocol in the box beside the **Create** button, and then clicking **Create.** The new protocol will be added to the list with zeros in the protocol fields and **unknown** for the status. Enter the appropriate **Protocol** and **Port** values before setting the **Status** field to **open.**

NAI Realms

Understanding NAI Realm Authentication

A network access identifier (NAI) is a specification of a particular user. A NAI takes the general form of an e-mail address. Examples of NAIs are:

```
joe@example.com
fred@foo-9.example.com
jack@3rd.depts.example.com
fred.smith@example.com
```

Figure 169. NAI Realms

The **NAI Realm** is the part of the NAI following the @ sign. For example, you might enter: **example.com**, **3rd.depts.example.com**, and **foo-9.example.com**. Use the **NAI Realms** page, in conjunction with the **NAI EAP** page, to specify the authentication techniques to be used to access that realm with appropriate parameters.

Procedure for NAI Realms Settings

Use this window to establish the names of the supported realms.

1. **Enter the realm name.** Enter the name of a realm in the box to the left of the **Create** button and click **Create**. The realm will be added to the **NAI Realms** list. Any of the realms may be deleted by clicking the corresponding **Delete** button**.**
2. **Enter Authentication Information.** The NAI EAP page is used to specify authentication for a realm. Click on the name of a realm to go to the NAI EAP page for that realm. See "NAI EAP" on page 346.

NAI EAP

This window allows specification of the authentication techniques for a realm.

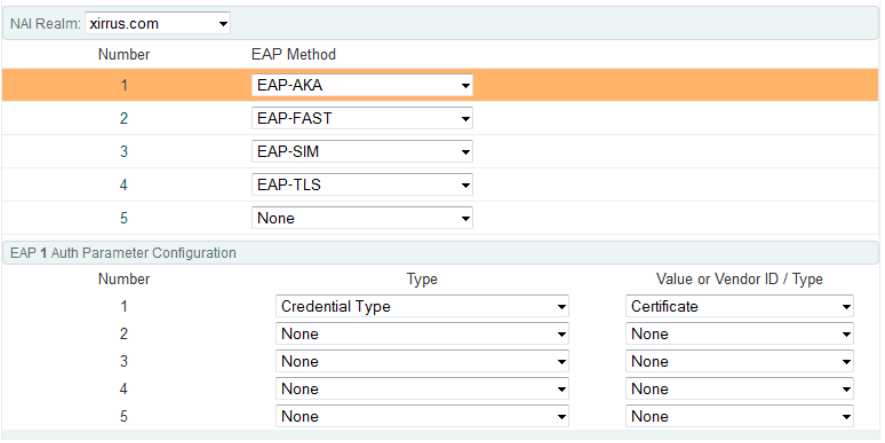


Figure 170. NAI EAP

Procedure for NAI Realms Settings

1. Select the realm to be configured in the **NAI Realm** drop down.
2. Select **EAP Methods**. Each realm may support up to five EAP authentication methods. Beside each of the five numbers (1, 2, 3, 4, 5) select the method from the drop down. The choices are:
   - **EAP-AKA**
   - **EAP-AKA' (EAP-AKA prime)**
   - **EAP-FAST**
   - **EAP-MSCHAP-V2**
   - **EAP-SIM**
   - **EAP-TLS**
   - **EAP-TTLS**
   - **GTC**
   - **MD5-Challenge**
   - **None**

- **PEAP**

3. **Specify Authentication Parameters.** Each of the authentication methods may specify up to five authentication parameters. To specify the parameters click on the number corresponding to the authentication method; i.e. **1, 2, 3, 4,** or **5.** This displays the **EAP n Auth Parameter Configuration** below the list of **EAP Methods**. For up to five of the parameters, select the **Type** and **Value or Vendor ID / Type.** The choices for the **Type** are:

   - **Credential Type**
   - **Expanded EAP Method**
   - **Expanded Inner EAP Method**
   - **Inner Authentication EAP Method Type**
   - **Non-EAP Inner Authentication Type**
   - **None**
   - **Tunneled EAP Method Credential Type**

   For each type, a value or a vendor ID and type must be specified, as applicable.

Intrusion Detection

The Xirrus Array employs a number of IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) strategies to detect and prevent malicious attacks on the wireless network. Use this window to adjust intrusion detection settings.

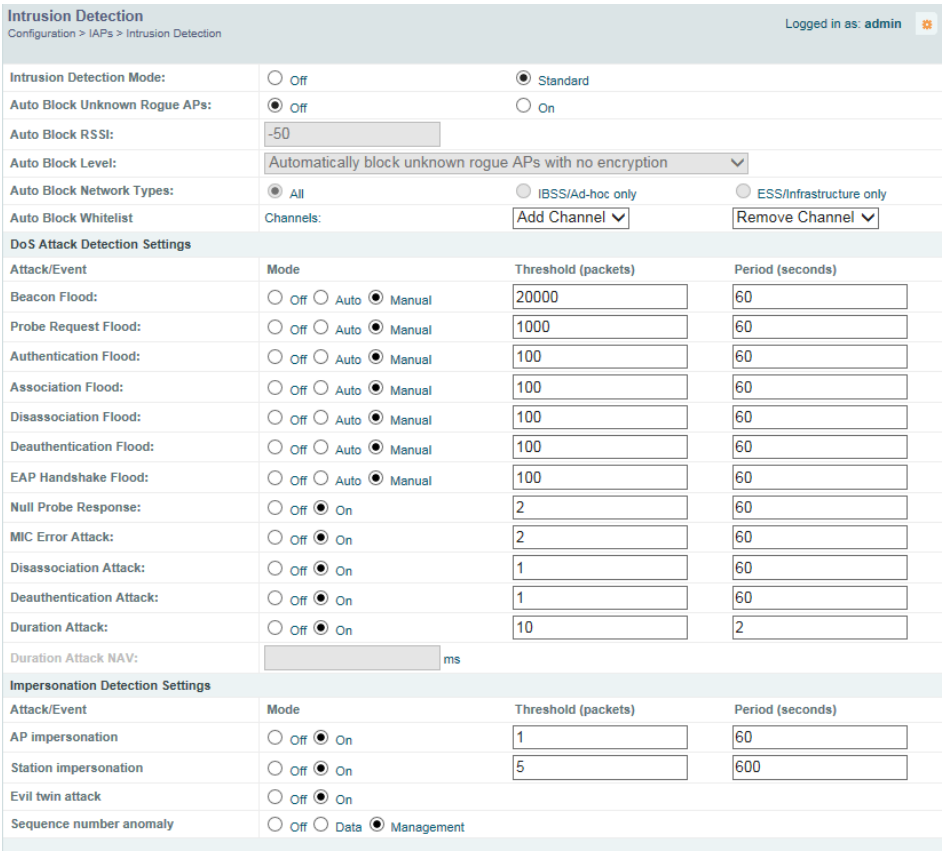


Figure 171. Intrusion Detection Settings

The Array provides a suite of intrusion detection and prevention options to improve network security. You can separately enable detection of the following types of problems:

- **Rogue Access Point Detection and Blocking**

  Unknown APs are detected, and may be automatically blocked based on a number of criteria. See "About Blocking Rogue APs" on page 351.

- **Denial of Service (DoS) or Availability Attack Detection**

  A DoS attack attempts to flood an Array with communications requests so that it cannot respond to legitimate traffic, or responds so slowly that it becomes effectively unavailable. The Array can detect a number of types of DoS attacks, as described in the table below. When an attack is detected, the Array logs a Syslog message at the Alert level.

- **Impersonation Detection**

  These malicious attacks use various techniques to impersonate a legitimate AP or station, often in order to eavesdrop on wireless communications. The Array detects a number of types of impersonation attacks, as described in the table below. When an attack is detected, the Array logs a Syslog message at the Alert level.

Type of Attack	Description
DoS Attacks	
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.
Probe Request Flood	Generating thousands of counterfeit 802.11 probe requests to overburden the Array.
Authentication Flood	Sending forged Authenticates from random MAC addresses to fill the Array's association table.
Association Flood	Sending forged Associates from random MAC addresses to fill the Array's association table.

Type of Attack	Description
Disassociation Flood	Flooding the Array with forged Disassociation packets.
Deauthentication Flood	Flooding the Array with forged Deauthenticates.
EAP Handshake Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.
Null Probe Response	Answering a station probe-request frame with a null SSID. Many types of popular NIC cards cannot handle this situation, and will freeze up.
MIC Error Attack	Generating invalid TKIP data to exceed the Array's MIC error threshold, suspending WLAN service.
Disassociation Attack (Omerta)	Sending forged disassociation frames to all stations on a channel in response to data frames.
Deauthentication Attack	Sending forged deauthentication frames to all stations on a channel in response to data frames.
Duration Attack (Duration Field Spoofing)	Injecting packets into the WLAN with huge duration values. This forces the other nodes in the WLAN to keep quiet, since they cannot send any packet until this value counts down to zero. If the attacker sends such frames continuously it silences other nodes in the WLAN for long periods, thereby disrupting the entire wireless service.
Impersonation Attacks	
AP impersonation	Reconfiguring an attacker's MAC address to pose as an authorized AP. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Station impersonation	Reconfiguring an attacker's MAC address to pose as an authorized station. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Evil twin attack	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.

Type of Attack	Description
Sequence number anomaly	A sender may use an Add Block Address request (ADDBA - part of the Block ACK mechanism) to specify a sequence number range for packets that the receiver can accept. An attacker spoofs an ADDBA request, asking the receiver to reset its sequence number window to a new range. This causes the receiver to drop legitimate frames, since their sequence numbers will not fall in that range.

About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see "Rogue Control List" on page 250), then the Array will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue it sends out a broadcast "deauth" signal using the rogue's BSSID and source address. This has the effect of disconnecting all of a rogue AP's clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

The Advanced RF Settings window allows you to set up **Auto Block** parameters so that unknown APs get the same treatment as explicitly blocked APs. This is basically a "shoot first and ask questions later" mode. By default, auto blocking is turned off. Auto blocking provides two parameters for qualifying blocking so that APs must meet certain criteria before being blocked. This keeps the Array from blocking every AP that it detects. You may:

- Set a minimum RSSI value for the AP—for example, if an AP has an RSSI value of -90, it is probably a harmless AP belonging to a neighbor and not in your building.
- Block based on encryption level.
- Block based on whether the AP is part of an ad hoc network or infrastructure network.
- Specify channels to be whitelisted. Rogues discovered on these channels are excluded from auto blocking. This allows specified channels to be freely used by customer or guests for their APs.

Procedure for Configuring Intrusion Detection

RF Intrusion Detection and Auto Block Mode

1. **Intrusion Detection Mode:** This option allows you to choose the **Standard** intrusion detection method, or you can choose **Off** to disable this feature. See "Array Monitor and Radio Assurance Capabilities" on page 500 for more information.
   - **Standard**—enables the monitor radio to collect Rogue AP information.
   - **Off**—intrusion detection is disabled.
2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see "About Blocking Rogue APs" on page 351). Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block Unknown Rogue APs to **On**. Then the remaining Auto Block fields will be active.
3. **Auto Block RSSI:** Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.
4. **Auto Block Level:** Select rogue APs to block based on the level of encryption that they are using. The choices are:
   - Automatically block unknown rogue APs regardless of encryption.
   - Automatically block unknown rogue APs with no encryption.
   - Automatically block unknown rogue APs with WEP or no encryption.
5. **Auto Block Network Types:** Select rogues to automatically block by applying the criteria above only to networks of the type specified below. The choices are:
   - **All**—the unknown rogues may be part of any wireless network.
   - **IBSS/AD Hoc only**—only consider auto blocking rogues if they belong to an ad hoc wireless network (a network of client devices

without a controlling Access Point, also called an Independent Basic Service Set—IBSS).

- **ESS/Infrastructure only**—only consider auto blocking rogue APs if they are in infrastructure mode rather than ad hoc mode.

6. **Auto Block Whitelist:** Use this list to specify channels to be excluded from automatic blocking. If you have enabled **Auto Block**, it will not be applied to rogues detected on the whitelisted channels. Use the **Add Channel** drop-down to add entries to the **Channels** list, one at a time. You can delete entries from the list by selecting them from the **Remove Channel** drop-down list.

DoS Attack Detection Settings

7. **Attack/Event**: The types of DoS attack that you may detect are described in the Type of Attack Table page 349. Detection of each attack type may be separately enabled or disabled. For each attack, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the Array declares that an attack has been detected. You may modify the **Threshold** and **Period**.

   For the Flood attack settings, you also have a choice of **Auto** or **Manual**.

   - **Manual** mode—threshold and period settings are used to detect a flood. Packets received are simply counted for the specified time period and compared against the flood threshold. The default for all of the floods is **Manual** mode.
   - **Auto** mode—the Array analyzes current traffic for packets of a given type versus traffic over the past hour to determine whether a packet flood should be detected. In this mode, threshold and period settings are ignored. This mode is useful for floods like beacon or probe floods, where the numbers of such packets detected in the air can vary greatly from installation to installation.

8. **Duration Attack NAV (ms)**: For the duration attack, you may also modify the default duration value that is used to determine whether a packet may be part of an attack. If the number of packets having at least this duration value exceeds the **Threshold** number in the specified **Period**, an attack is detected.

Impersonation Detection Settings

9. **Attack/Event**: The types of impersonation attack that you may detect are described in Impersonation Attacks page 350. Detection of each attack type may be turned **On** or **Off** separately. For **AP** or **Station Impersonation** attacks, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the Array declares that an attack has been detected. You may modify the **Threshold** and **Period**.

10. **Sequence number anomaly**: You may specify whether to detect this type of attack in **Data** traffic or in **Management** traffic, or turn **Off** this type of detection.

LED Settings

This window assigns behavior preferences for the Array's IAP LEDs.

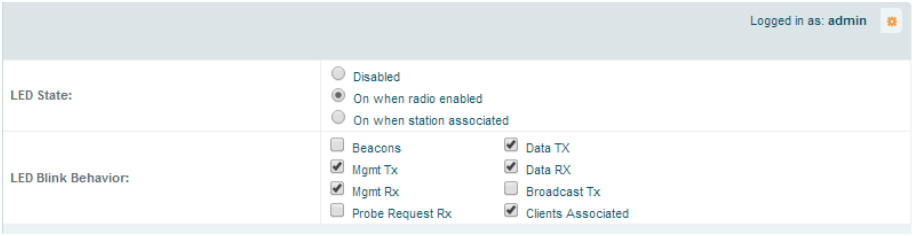


Figure 172. LED Settings

Procedure for Configuring the IAP LEDs

1. **LED State:** This option determines which event triggers the LEDs, either when an IAP is enabled or when an IAP first associates with the network.

Choose **On Radio Enabled** or **On First Association**, as desired. You may also choose Disabled to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.

2. **LED Blink Behavior**: This option allows you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink. For default behavior, see "Array LED Operating Sequences" on page 67.

3. Click the **Save** button if you wish to make your changes permanent.

See Also

Global Settings (IAP)
Global Settings .11an
Global Settings .11bgn
IAPs
LED Boot Sequence

DSCP Mappings

DSCP is the 6-bit Differentiated Services Code Point (DiffServ) field in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies the packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

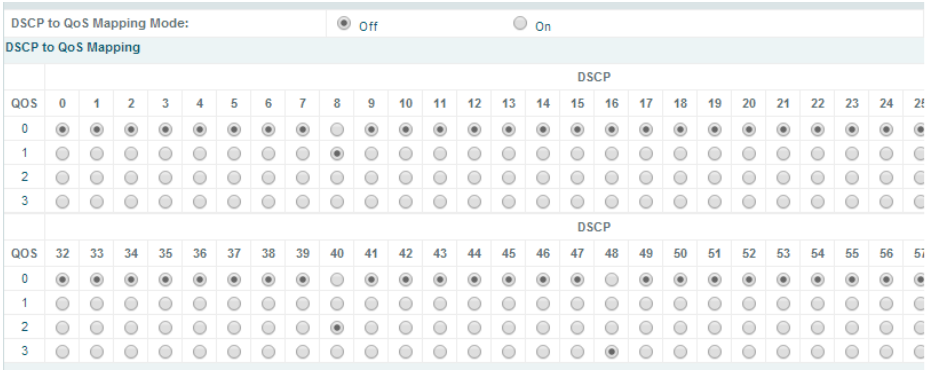


Figure 173. DSCP Mappings

The DSCP Mappings page shows the default mapping of each of the 64 DSCP values to one of the Array's four QoS levels, and allows you to change these mappings.

For a detailed discussion of the operation of QoS and DSCP mappings on the Array, please see "Understanding QoS Priority on the Wireless Array" on page 256.

Procedure for Configuring DSCP Mappings

1. **DSCP to QoS Mapping Mode:** Use the **On** and **Off** buttons to enable or disable the use of the DSCP mapping table to determine the QoS level applied to each packet.
2. **DSCP to QoS Mapping:** The radio buttons in this table show all DSCP values (0 to 63), and the QoS level to which each is mapped. To change the QoS level applied to a DSCP value, click the desired QoS level (0 to 3) underneath it.

Roaming Assist

Roaming assist is a Xirrus feature that helps clients roam to Arrays that will give them high quality connections. Some smart phones and tablets will stay connected to a radio with poor signal quality, even when there's a radio with better signal strength within range. When roaming assist is enabled, the Array "assists" the device by deauthenticating it when certain parameters are met. This encourages a client with a high roaming threshold (i.e., a device that may not roam until signal quality has seriously dropped) to move to an Array that gives it a better signal. The deauthentication is meant to cause the client to choose a different radio. You can specify the device types that will be assisted in roaming.

The roaming threshold is the difference in signal strength between radios that will trigger a deauthentication. If the client's signal is lower than the sum of the threshold and the stronger neighbor radio's RSSI, then we "assist" the client. For example:

Threshold = -5
RSSI of neighbor Array = -65

RSSI of client = -75
-75 < (-5 + -65) : Client will roam

Another example:

Threshold = -15
RSSI of neighbor Array = -60
RSSI of station = -70
-70 > (-15 + -60) : Client will not roam

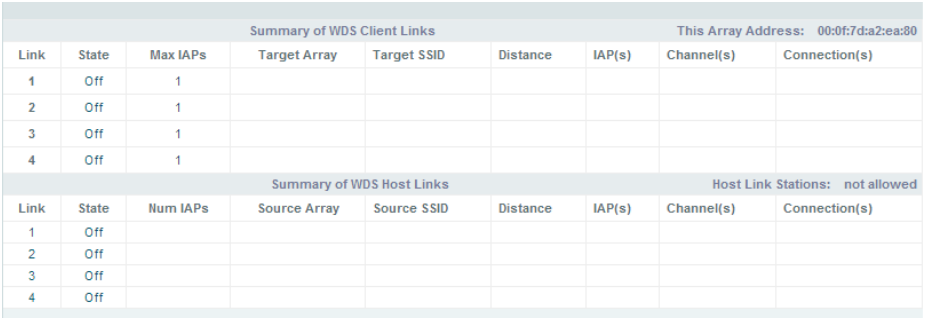
Procedure for Configuring Roaming Assist

1. **Enable Roaming Assist:** Use the **Yes** and **No** buttons to enable or disable this feature.
2. **Backoff Period**: After deauthenticating a station, it may re-associate to the same radio. To prevent the Array from repeatedly deauthenticating the station when it comes back, there is a backoff period. This is the number of seconds the station is allowed to stay connected before another deauthentication.
3. **Roaming Threshold**: This is the difference in signal strength between radios that will trigger a deauthentication, as described in the discussion above. In most cases, this will be a negative number.

WDS

WDS is not available for Arrays or Access Points featuring 802.11ac IAPs.

This is a status-only window that provides an overview of all WDS links that have been defined. WDS (Wireless Distribution System) is a system that enables the interconnection of access points wirelessly, allowing your wireless network to be expanded using multiple access points without the need for a wired backbone to link them. The **Summary of WDS Client Links** shows the WDS links that you have defined on this Array and identifies the target Array for each by its base MAC address. The **Summary of WDS Host Links** shows the WDS links that have been established on this Array as a result of client Arrays associating to this Array (i.e., the client Arrays have this Array as their target). The summary identifies the source (client) Array for each link. Both summaries identify the IAPs that are part of the link and whether the connection for each is up or down. See "WDS Planning" on page 57 for an overview.



Summary of WDS Client Links — This Array Address: 00:0f:7d:a2:ea:80

Link	State	Max IAPs	Target Array	Target SSID	Distance	IAP(s)	Channel(s)	Connection(s)
1	Off	1						
2	Off	1						
3	Off	1						
4	Off	1						

Summary of WDS Host Links — Host Link Stations: not allowed

Link	State	Num IAPs	Source Array	Source SSID	Distance	IAP(s)	Channel(s)	Connection(s)
1	Off							
2	Off							
3	Off							
4	Off							

Figure 174. WDS

About Configuring WDS Links

A WDS link connects a client Array and a host Array (see Figure 175 on page 359). The host must be the Array that has a wired connection to the LAN. Client links from one or more Arrays may be connected to the host, and the host may also have client links. See "WDS Planning" on page 57 for more illustrations.

The configuration for WDS is performed on the client Array only, as described in "WDS Client Links" on page 361. No WDS configuration is performed on the host Array. First you will set up a client link, defining the target (host) Array and SSID, and the maximum number of IAPs in the link. Then you will select the IAPs to be used in the link. When the client link is created, each member IAP will associate to an IAP on the host Array.

You may wish to consider configuring the WDS link IAPs so that only the WDS link SSIDs are active on them. See "Active IAPs" on page 275.

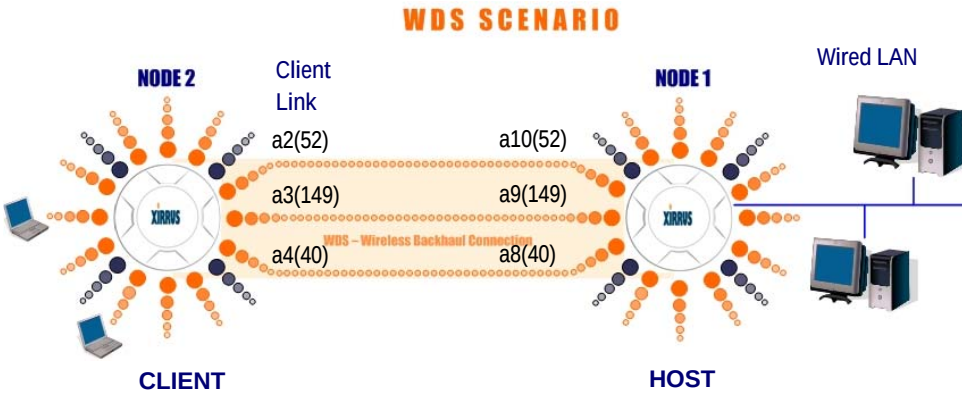


Figure 175. Configuring a WDS Link

Once an IAP has been selected to act as a WDS client link, you will not be allowed to use auto-configured cell sizing on that IAP (since the cell must extend all the way to the other Array).

When configuring WDS, if you use WPA-PSK (Pre-Shared Key) as a security mechanism, ensure that EAP is disabled. Communication between two Arrays in WDS mode will not succeed if the client Array has both PSK and EAP enabled on the SSID used by WDS. See ***SSID Management****.*

TKIP encryption does not support high throughput rates, per IEEE 802.11n. TKIP should ***never*** *be used for WDS links on XR Arrays.*

WDS is available on all Xirrus Arrays, including XR-500/600 and XR-1000 Series Arrays with two radios (WDS will operate on either of the radios).

Long Distance Links

If you are using WDS to provide backhaul over an extended distance, use the **WDS Dist. (Miles)** setting to prevent timeout problems associated with long transmission times. (See "IAP Settings" on page 290) Set the approximate distance in miles between this IAP and the connected Array in the **WDS Dist. (Miles)** column. This will increase the wait time for frame transmission accordingly.

See Also

SSID Management
Active IAPs
WDS Client Link IAP Assignments:
WDS Client Links
WDS Statistics

WDS Client Links

WDS is not available for Arrays or Access Points featuring 802.11ac IAPs.

This window allows you to set up a maximum of four WDS client links.

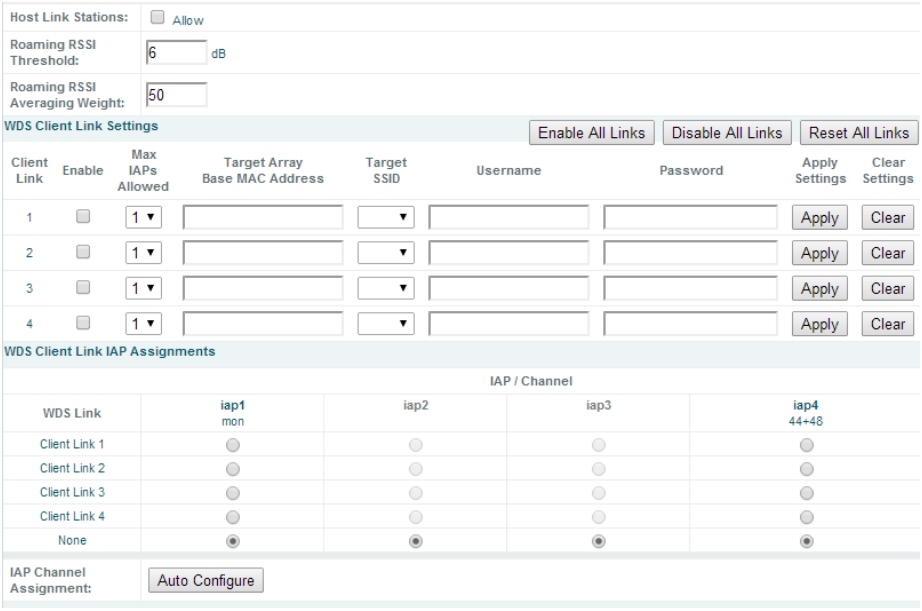


Figure 176. WDS Client Links

Procedure for Setting Up WDS Client Links

WDS Client Link Settings:

1. **Host Link Stations**: Check the **Allow** checkbox to instruct the Array to allow stations to associate to IAPs on a host Array that participates in a WDS link. The WDS host IAP will send beacons announcing its availability to wireless clients. This is disabled by default.

Once an IAP has been selected to act as a WDS client link, no other association will be allowed on that IAP. However, wireless associations will be allowed on the WDS host side of the WDS session.

In situations like the one in the next step, where WDS is used by an Array mounted on a high speed train, STP can add significant delay (often on the order of 30 to 60 seconds) while initially analyzing network topology. In such a situation, it may be desirable to disable STP. See "Management Control" on page 226.

Caution: If Spanning Tree Protocol ("Management Control" on page 226) is disabled and a network connection is made on the WDS Client Array's Gigabit link that can reach the WDS Host Array, broadcast and multicast packets will not be blocked. A broadcast storm may cause a network outage.

2. **Roaming RSSI Threshold**: If an Array is deployed on a mobile site (on a train, for example), you can use WDS to implement a wireless backhaul that will roam between Arrays at fixed locations. When another candidate Array for WDS host target is found, the client link will roam to the new Array if its RSSI is stronger than the RSSI of the current host connection by at least the **Roaming RSSI Threshold.** The default is 6 dB.

3. **Roaming RSSI Averaging Weight**: This weight changes how much the latest RSSI reading influences the cumulative weighted RSSI value utilized in checking the threshold (above) to make a roaming decision. The higher the weight, the lower the influence of a new RSSI reading. This is not exactly a percentage, but a factor in the formula for computing the current RSSI value based on new readings:

   StoredRSSI = (StoredRSSI * RoamingAvgWeight
   + NewRSSIReading * (100 - RoamingAvgWeight)) / 100

   This prevents erroneous or out-of-line RSSI readings from causing the WDS link to jump to a new Array. Such readings can result from temporary obstructions, external interference, etc.

4. Click the **Save** button after you are finished making changes on this page if you wish to make your changes permanent.

WDS Client Link IAP Setting:

5. **Enable/Disable/Reset All Links**: Click the appropriate button to:

- **Enable All Links**—this command activates all WDS links configured on the Array.
- **Disable All Links**—this command deactivates all WDS links configured on the Array. It leaves all your settings unchanged, ready to re-enable.
- **Reset All Links**—this command tears down all links configured on the Array and sets them back to their factory defaults, effective immediately.

6. **Client Link**: Shows the ID (1 to 4) of each of the four possible WDS links.
7. **Enabled**: Check this box if you want to enable this WDS link, or uncheck the box to disable the link.
8. **Max IAPs Allowed (1-3)**: Enter the maximum number of IAPs for this link, between 1 and 3.
9. **Target Array Base MAC Address**: Enter the base MAC address of the target Array (the host Array at the other side of this link). To find this MAC address, open the **WDS** window on the ***target*** Array, and use **This Array Address** located on the right under the Summary of WDS Host Links. To allow any Xirrus Array to be accepted as a WDS target, enter the Xirrus OUI: **00:0f:7d:00:00:00** or **50:60:28:00:00:00** (this is useful for roaming in a mobile deployment, as described in Step 2 on page 362).
10. **Target SSID**: Enter the SSID that the target Array is using.
11. **Username**: Enter a username for this WDS link. A username and password is required if the SSID is using PEAP for WDS authentication from the internal RADIUS server.
12. **Password**: Enter a password for this WDS link.
13. **Clear Settings**: Click on the **Clear** button to reset all of the fields on this line.

WDS Client Link IAP Assignments:

14. For each desired client link, select the IAPs that are part of that link. The IAP channel assignments are shown in the column headers.

15. **IAP Channel Assignment**: Click **Auto Configure** to instruct the Array to automatically determine the best channel allocation settings for each IAP that participates in a WDS link, based on changes in the environment. These changes are executed immediately, and are automatically applied.

See Also

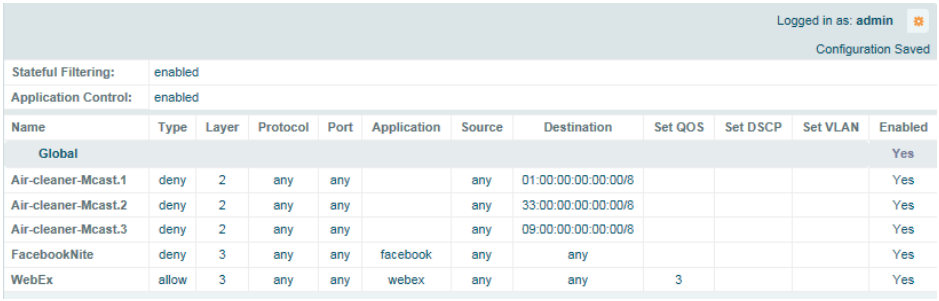
SSID Management
WDS Planning
WDS
WDS Statistics

Filters

The Wireless Array's integrated firewall uses stateful inspection to speed the decision of whether to allow or deny traffic. Filters are used to define the rules used for blocking or passing traffic. Filters can also set the VLAN and QoS level for selected traffic.

The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic. See "Air Cleaner" on page 438.

Filters may be used based on your experience with Application Control Windows to eliminate or cap the amount of traffic allowed for less desirable applications.



Logged in as: **admin**

Configuration Saved

Stateful Filtering:	enabled
Application Control:	enabled

Name	Type	Layer	Protocol	Port	Application	Source	Destination	Set QOS	Set DSCP	Set VLAN	Enabled
Global											Yes
Air-cleaner-Mcast.1	deny	2	any	any		any	01:00:00:00:00:00/8				Yes
Air-cleaner-Mcast.2	deny	2	any	any		any	33:00:00:00:00:00/8				Yes
Air-cleaner-Mcast.3	deny	2	any	any		any	09:00:00:00:00:00/8				Yes
FacebookNite	deny	3	any	any	facebook	any	any				Yes
WebEx	allow	3	any	any	webex	any	any	3			Yes

Figure 177. Filters

User connections managed by the firewall are maintained statefully—once a user flow is established through the Array, it is recognized and passed through without application of all defined filtering rules. Stateful inspection runs automatically on the Array. The rest of this section describes how to view and manage filters.

Filters are organized in groups, called Filter Lists. A filter list allows you to apply a uniform set of filters to SSIDs or Groups very easily.

The read-only Filters window provides you with an overview of all filter lists that have been defined for this Array, and the filters that have been created in each list. Filters are listed in the left side column by name under the filter list to which they belong. Each filter entry is a link that takes you to its Filter Management entry,

and the list includes information about the type of filter, the protocol it is filtering, which port it applies to, source and destination addresses, and QoS and VLAN assignments.

Filter Lists

This window allows you to create filter lists. The Array comes with one predefined list, named **Global**, which cannot be deleted. Filter lists (including Global) may be applied to SSIDs or to Groups. Only one filter list at a time may be applied to a group or SSID (although the filter list may contain a number of filters). All filters are created within filter lists.

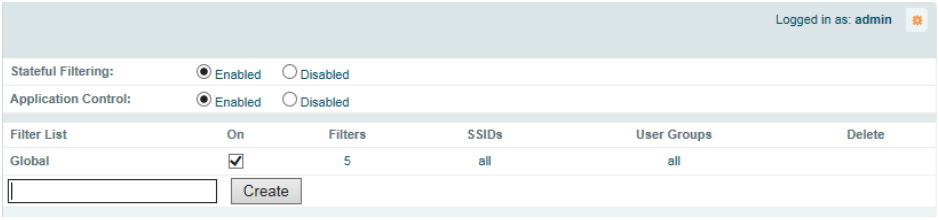


Figure 178. Filter Lists

Procedure for Managing Filter Lists

1. **Stateful Filtering:** Stateful operation of the integrated firewall can be **Enabled** or **Disabled**. If you have a large number of filters and you don't want to apply them in a stateful manner, you may use this option to turn the firewall off.
2. **Application Control:** Operation of the Application Control feature may be **Enabled** or **Disabled**. See "Application Control Windows" on page 146.

*The Application Control feature is only available if the Array license includes **Application Control**. If a setting is unavailable (grayed out), then your license does not support the feature. See **"About Licensing and Upgrades" on page 387**.*

3. **New Filter List Name**: Enter a name for the new filter list in this field, then click on the Create button to create the list. All new filters are disabled when they are created. The new filter list is added to the Filter List table in the window. Click on the filter list name, and you will be taken to the Filter Management window for that filter list. You may create up to 16 filter lists (up to 8 on the XR-500 Series and on the XR-620).
4. **On**: Check this box to enable this filter list, or leave it blank to disable the list. If the list is disabled, you may still add filters to it or modify it, but none of the filters will be applied to data traffic.
5. **Filters**: This read-only field displays the number of filters that belong to this filter list.
6. **SSIDs**: This read-only field lists the SSIDs that use this filter list.
7. **User Groups**: This read-only field lists the Groups that use this filter list.
8. **Delete**: Click this button to delete this filter list. The **Global** filter list may not be deleted.
9. Click the **Save** button if you wish to make your changes permanent.
10. Click a filter list to go to the Filter Management window to create and manage the filters that belong to this list.

Filter Management

This window allows you to create and manage filters that belong to a selected filter list, based on the filter criteria you specify. Filters are an especially powerful feature when combined with the intelligence provided by the "Application Control Windows" on page 146.

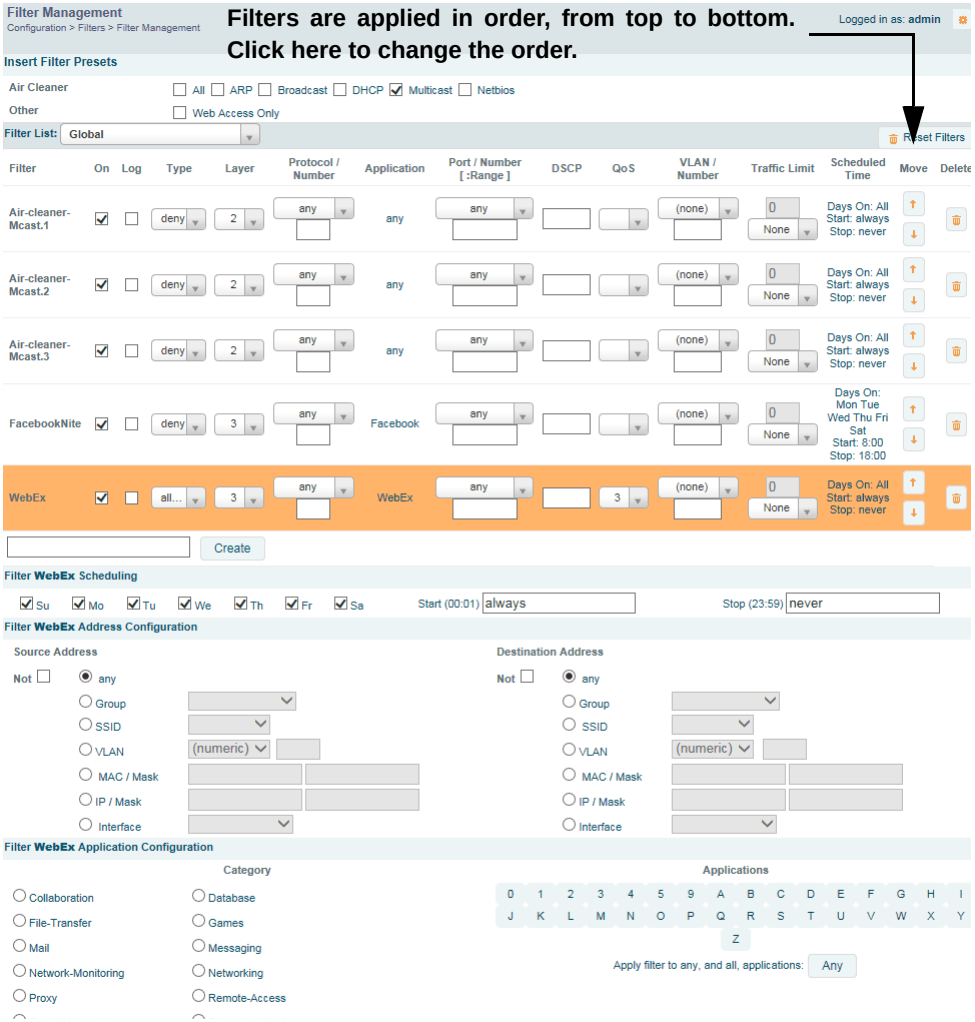


Figure 179. Filter Management

Based on Application Control's analysis of your wireless traffic, you can create filters to enhance wireless usage for your business needs:

- Usage of non-productive and risky applications like BitTorrent can be restricted.
- Traffic for mission-critical applications like VoIP and WebEx may be given higher priority (QoS).
- Non- critical traffic from applications like YouTube may be given lower priority (QoS) or bandwidth allowed may be capped per station or for all stations.
- Traffic flows for specific applications may be controlled by sending them into VLANs that are designated for that type of traffic.
- Filters may be applied at specified times—for example, no games allowed from 8 AM to 6 PM.

Note that filtering is secondary to the stateful inspection performed by the integrated firewall. Traffic for established connections is passed through without the application of these filtering rules.

Procedure for Managing Filters

1. **Filter List:** Select the filter list to display and manage on this window. All of the filters already defined for this list are shown, and you may create additional filters for this list. You may create up to 50 filters per list (up to 25 per list on the XR-500 Series and on the XR-620).
2. **Add Preset Filter**: A number of predefined "Air Cleaner" filters are available using these buttons. You can use these rules to eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. For more information, please see "Air Cleaner" on page 438.
3. **New Filter Name**: To add a new filter, enter its name in the field next to the **Create** button at the bottom of the list, then click **Create**. All new filters are added to the table of filters in the window. The filter name must be unique within the list, but it may have the same name as a filter in a

different filter list. Two filters with the same name in different filter lists will be completely unrelated to each other—they may be defined with different parameter values.

Viewing or modifying existing filter entries:

4. **Filter**: Select a filter entry if you wish to modify it. Source and destination details are displayed below the bottom of the list.
5. **On**: Use this field to enable or disable this filter.
6. **Log**: Log usage of this filter to Syslog.
7. **Type**: Choose whether this filter will be an **Allow** filter or a **Deny** filter. If you define the filter as an Allow filter, then any associations that meet the filter criteria will be allowed. If you define the filter as a Deny filter, any associations that meet the filter criteria will be denied.
8. **Layer**: Select network layer **2** or **3** for operation of this filter.
9. **Protocol/Number**: Choose a specific filter protocol from the pull-down list, or choose **numeric** and enter a **Number**, or choose **any** to instruct the Array to use the best filter. This is a match criterion.
10. **Application**: Shows an application to filter, based on settings from Step 22 and Step 23. If an application has been selected, you should not enter **Protocol** or **Port**—application filters have intelligence built into them, and perform filtering that you cannot accomplish with just port and protocol. See "Application Control Windows" on page 146.
11. **Port/Number**: This is a match criterion. From the pull-down list, choose the target port type for this filter. Choose **any** to instruct the Array to apply the filter to any port, or choose **1-65534** and enter a **Number**.

    To enter a **Range** of port numbers, separate the start and end numbers with a colon as shown: **Start # : End #**.
12. **DSCP**: (Differentiated Services Code Point or DiffServ—Optional) Set packets ingressing from the wireless network that match the filter criteria to this DSCP level (0 to 63) before sending them out on the wired network. Select the level from the pull-down list. Level 0 has the lowest

priority; level 63 has the highest priority. By default, this field is blank and the filter does not modify DSCP level. See "Understanding QoS Priority on the Wireless Array" on page 256.

13. **QoS**: (Optional) Set packets ingressing from the wired network that match the filter criteria to this QoS level (0 to 3) before sending them out on the wireless network. Select the level from the pull-down list. Level 0 has the lowest priority; level 3 has the highest priority. By default, this field is blank and the filter does not modify QoS level. See "Understanding QoS Priority on the Wireless Array" on page 256.

14. **VLAN/Number**: (Optional) Set packets that match the filter criteria to this VLAN. Select a VLAN from the pull-down list, or select **numeric** and enter the number of a previously defined VLAN (see "VLANs" on page 204).

15. **Traffic Limit**: Instead of prohibiting or allowing the specified traffic type, you may cap the amount of traffic allowed that matches this filter. First choose the units for the limit: kbps for all stations in total or per station, or packets per second (pps) for all stations in total or per station. Then enter the numeric limit in the field to the left.

16. **Scheduled Time**: shows the times at which this filter is active, if you have established a schedule in Step 19.

17. **Move Up/Down**: The filters are applied in the order in which they are displayed in the list, with filters on the top applied first. To change an entry's position in the list, just click its **Up** or **Down** button.

18. To delete a filter, click its **Delete** button.

Select an existing filter entry in the list to view or modify **Scheduling** or **Address Configuration,** shown below the list of filters:

19. **Scheduling**: Use these fields if you wish to specify a scheduled time for this filter to be active. Check the checkboxes for the days that the filter is to be active. By default, the filter is active all day on each selected day.

You may also specify a time of day for the filter to be active by entering a **Start** and **Stop** time in 24:00 hour format (i.e., 6:30 PM is 18:30). To use this feature, you must enter both a Start and a Stop time.

You cannot apply one filter for two or more scheduled periods, but you can create two filters to achieve that. For example, one filter could deny the category Games from 9:00 to 12:00, and another could deny them from 13:00 to 18:00. Similarly, you might create two rules for different days—one to deny Games Mon-Fri 8:00 to 18:00, and another to deny them on Sat. from 8:00 to 12:00.

20. **Source Address**: Define a source address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.

21. **Destination Address**: Define a destination address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **any** to use any source address. Check **Not** to match any address except for the specified address.

Below the Source and Destination Addresses, you may enter a **Category** or an **Application** to be matched by the filter:

22. **Category**: If you wish this filter to apply to a particular category of application, such as **File-Transfer** or **Database**, select it from the listed options.

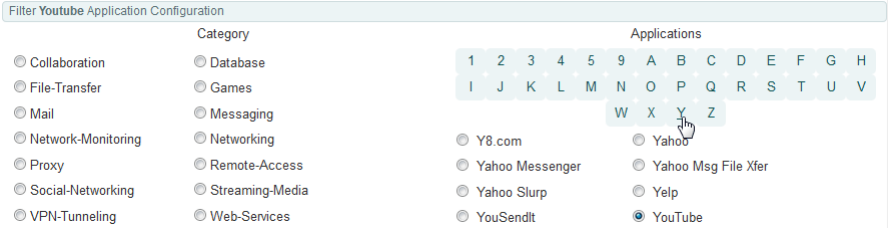


Figure 180. Filter Category or Application

23. **Applications**: If you wish this filter to apply to a specific application, such as **WebEx**, click the letter or number that it starts with. Then select the desired application. You may select a **Category** or an **Application**, but not both.

24. Click the **Save** button if you wish to make your changes permanent.

See Also

Filters
Filter Statistics
Understanding QoS Priority on the Wireless Array
VLANs

Clusters

An XR-500 or XR-600 or XR-1000 Series Array cannot act as the Cluster controller. It will operate correctly as a member of a cluster.

Clusters allow you to configure multiple Arrays at the same time. Using WMI (or CLI), you may define a set of Arrays that are members of the cluster. Then you may enter Cluster mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member Arrays. When you exit cluster mode, configuration commands revert to applying only to the Array to which you are connected.

The read-only Clusters window provides you with an overview of all clusters that have been defined for this Array, and the Arrays that have been added to each. Arrays are listed in the left hand column by name under the cluster to which they belong. Each Array entry displays its IP Address, Username, and Password.

Name	IP Address	Username	Password	Arrays
North				1
XR4012802207C	192.168.1.56	admin	*****	

Figure 181. Clusters

Clusters are discussed in the following topics:

- **Cluster Definition**
- **Cluster Management**
- **Cluster Operation**

Cluster Definition

An XR-500 or XR-1000 Series Array cannot act as the Cluster controller. It will operate correctly as a member of a cluster.

This window allows you to create clusters. All existing clusters are shown, along with the number of Arrays currently in each. Up to 16 clusters may be created, with up to 50 Arrays in each.

Figure 182. Cluster Definition

Procedure for Managing Cluster Definition

1. **New Cluster Name:** Enter a name for the new cluster in the field to the left of the **Create** button, then click **Create** to add this entry. The new cluster is added to the list in the window. Click on the cluster name, and you will be taken to the Cluster Management window for that cluster.
2. **Delete**: To delete a cluster, click its **Delete** button.
3. Click the **Save** button if you wish to make your changes permanent.
4. Click a cluster to go to the Cluster Management window to add or remove Arrays in the cluster.

Cluster Management

An XR-500 or XR-1000 Series Array cannot act as the Cluster controller. It will operate correctly as a member of a cluster.

This window allows you to add Arrays to or delete them from a selected cluster. A cluster may include a maximum of 50 Arrays.

Note that the Array on which you are currently running WMI is not automatically a member of the cluster. If you would like it to be a member, you must add it explicitly.

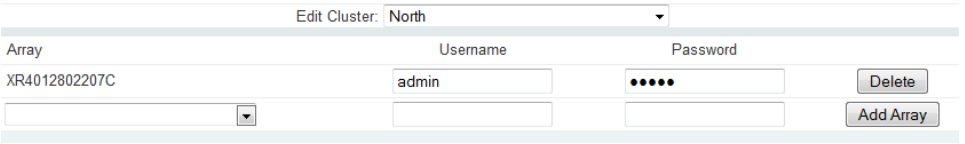


Figure 183. Cluster Management

Procedure for Managing Clusters

1. **Edit Cluster:** Select the cluster to display and manage on this window. All of the Arrays already defined for this cluster are shown, and you may add additional Arrays to this list.
2. Array: Enter the hostname or IP address of the Array that you wish to add to this cluster.
3. **Username/Password**: In these columns, enter the administrator name and password for access to the Array.
4. Click the **Add Array** button to enter the Array.
5. To delete an Array, click its **Delete** button.
6. Click the **Save** button if you wish to make your changes permanent.

Cluster Operation

This window puts WMI into Cluster Mode. In this mode, all configuration operations that you execute in WMI or CLI are performed on the members of the cluster. They are **not** performed on the Array where you are running WMI, unless it is a member of the cluster.

An XR-500 or XR-1000 Series Array cannot act as the Cluster controller. It will operate correctly as a member of a cluster.

You must use the **Save** button at the top of configuration windows to permanently save your changes in Cluster Mode, just as you would in normal operation. When you are done configuring Arrays in the cluster, return to this window and click the **Exit** button to leave Cluster Mode.

Figure 184. Cluster Mode Operation

Procedure for Operating in Cluster Mode

1. **Operate:** Click the **Operate** button to the right of the desired cluster. A message informs you that you are operating in cluster mode. Click **OK**. The **Operate** button is replaced with an **Exit** button.

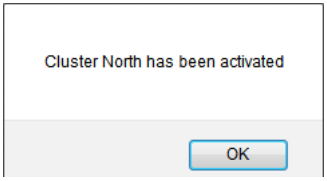


Figure 185. Cluster Mode Activation

2. Select a WMI window for settings that you wish to configure for the cluster, and proceed to make the desired changes.
3. Proceed to any additional pages where you wish to make changes.

4. Some Status and Statistics windows will present information for all Arrays in the cluster.
5. Click the **Save** button when done if you wish to save changes on the cluster member Arrays.
6. **Exit:** Click the **Exit** button to the right of the operating cluster to terminate Cluster Mode. The WMI returns to normal operation—managing only the Array to which it is connected.

Status and Statistics Windows in Cluster Mode

In Cluster Mode, many of the Status and Statistics windows will display information for all of the members of the cluster. You can tell whether a window displays cluster information—if so, it will display the Cluster Name near the top, as shown in Figure 186.

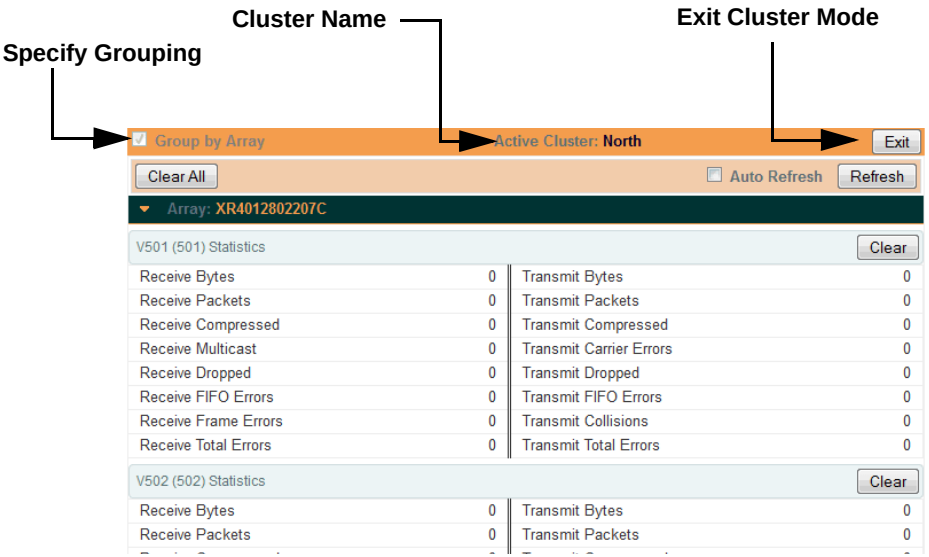


Figure 186. Viewing Statistics in Cluster Mode

You have the option to show aggregate information for the cluster members, or click the **Group by Array** check box to separate it out for each Array.

You may terminate cluster mode operation by clicking the **Exit** button to the right of the **Group by Array** check box.

Mobile

Mobile Device Management (MDM) servers enable you to manage large-scale deployments of mobile devices. They may include capabilities to handle tasks such as enrolling devices in your environment, configuring and updating device settings over-the-air, enforcing security policies and compliance, securing mobile access to your resources, and remotely locking and wiping managed devices.

Xirrus Arrays/APs support the AirWatch MDM, using an AirWatch API call to determine the status of a user's device and allow access to the wireless network only if the device is enrolled and compliant with the policies of the service.

AirWatch

Individual SSIDs may be configured to require AirWatch enrollment and compliance before a mobile device such as a smartphone or tablet is admitted to the wireless network. The Array uses the AirWatch API with the settings below to request that AirWatch check whether the mobile device is enrolled and compliant with your wireless policies.

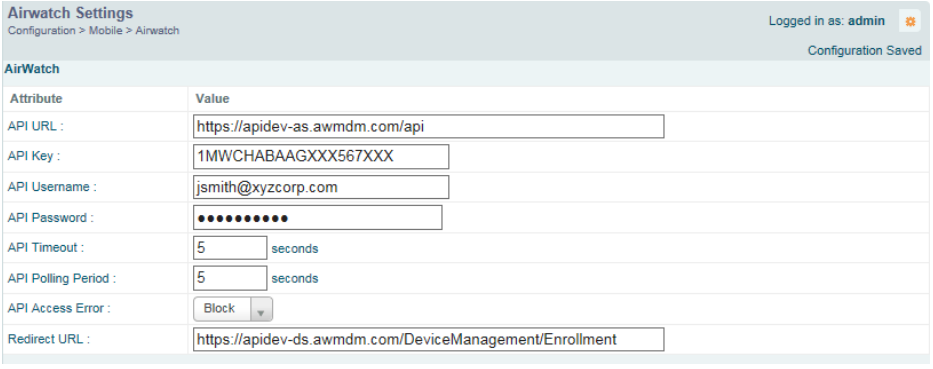


Figure 187. AirWatch Settings

Before configuring AirWatch settings on the Array, you must have an AirWatch account, already set up with your organization's compliance policies and other configuration as required by AirWatch.

The Array settings entered on this page are mostly taken from AirWatch. Once you have entered these settings, your users will be constrained to follow a set of

steps to access the wireless network, as described in "User Procedure for Wireless Access" on page 382.

Procedure for Managing AirWatch

If you have configured the **Mobile Device Management** setting on one or more SSIDs to use **AirWatch**, then the API specified below will be used to determine the admissibility of a mobile device requesting a connection to the wireless network.

1. **API URL**: Obtain this from your AirWatch server's **System / Advanced / Site URLs** page. Copy the **REST API URL** string into this field. This specifies the AirWatch API that the Array will call to determine the enrollment and compliance status of a mobile device attempting to connect to the Array. The steps that the user will need to take are described in "User Procedure for Wireless Access" on page 382.
2. **API Key**: Obtain this from your AirWatch server. Go to the **System / Advanced / API / REST** page, **General** tab, and copy the **API Key** string into this field. The key is required for access to the API.
3. **API Username**: Enter the user name for your account on the AirWatch server.
4. **API Password**: Enter the password for your account on the AirWatch server.
5. **API Timeout**: (seconds) If AirWatch does not respond within this many seconds, the request fails.
6. **API Polling Period**: (seconds) Mobile device enrollment and compliance status will be checked via polling at this interval. Note that there may thus be a delay before the mobile device will be admitted.
7. **API Access Error**: Specify whether or not to allow access if AirWatch fails to respond. The default is to **Block** access.
8. **Redirect URL**: Obtain this from your AirWatch server. Go to the **System / Advanced / Site URLs** page, and copy the **Enrollment URL** string into this field. When a mobile device that is not currently enrolled with

AirWatch attempts to connect to the Array, the device displays a page directing the user to install the AirWatch agent and go to the AirWatch enrollment page. Note that Android devices will need another form of network access (i.e. cellular) to download the agent, since un-enrolled devices will not have access to download it via the Array. See "User Procedure for Wireless Access" on page 382 for more details.

9. You must configure the **Mobile Device Management** setting on one or more SSIDs to use **AirWatch**, as described in Procedure for Managing SSIDs (see Step 16 on page 267).

User Procedure for Wireless Access

1. A user attempts to connect a mobile device to an SSID that uses AirWatch.
2. The device will authenticate according to the SSID's authentication settings (Open, Radius MAC, 802.1x).
3. The user browses to any destination on the Internet.

   The Array asks the user to wait while it checks device enrollment and compliance status by querying the AirWatch API with the device MAC address.

Device enrollment and compliance status will be checked via polling so there may be a delay before the device will be allowed in. That delay will depend on the API Polling Period setting.

4. If AirWatch responds that the device is enrolled and compliant, the device will be allowed into the network. The device will be considered compliant if AirWatch finds that the device does not violate any applicable policies for that device. (If no policies are assigned to the device in AirWatch, then the device is compliant by default.)
5. If the device is not enrolled, all user traffic will be blocked, except that HTTP traffic is redirected to an intermediate page on the Array that tells the user to download and install the AirWatch agent. The page displays a link to the AirWatch-provided device enrollment URL. This link is a pass-

though that allows the user to go through the enrollment process. The user will need to enter your organization's AirWatch Group ID and individual account credentials when requested.

Once the agent is installed, the user must start again at Step 1.

Android devices must go to the PlayStore to install the agent BEFORE they can go through the enrollment process. This means un-enrolled devices need another form of network access (i.e., cellular or an unrestricted SSID) to download this agent, as they are not permitted access to the PlayStore.

Once the agent is installed, the user must start again at Step 1.

6. If the device is enrolled with AirWatch but not compliant with applicable policies, all traffic will be blocked as in Step 5 above, and the HTTP traffic will be redirected to an intermediate page on the Array that tells the user which policies are out of compliance.

   This page contains a button for the user to click when the compliance issues have been corrected. This button causes AirWatch to again check device compliance. The user's browser is redirected to a "wait" page until the Array has confirmed compliance with AirWatch. The user's browser is then redirected to a page announcing that the device is now allowed network access.

7. If the Array is unable to access AirWatch to obtain enrollment and compliance status (for example, due to bad credentials, timeout, etc.), device access to the network will be granted according to the **API Access Error** setting (**Allow** or **Block**). If this field is set to **Block**, traffic will be blocked as in Step 5 above and HTTP traffic will be redirected to an informational page that informs the user that AirWatch cannot be contacted at this time and advises the user to contact the network administrator. If this field is set to **Allow**, then the device will be allowed network access.

Using Tools on the Wireless Array

These WMI windows allow you to perform administrative tasks on your Array, such as upgrading software, rebooting, uploading and downloading configuration files, and other utility tasks. Tools are described in the following sections:

- **"System Tools" on page 386**
- **"CLI" on page 399**
- **"API Documentation" on page 401**
- **"Options" on page 406**
- **"Logout" on page 407**

Note that the **Tools** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See Figure 39 on page 86)

This section does not discuss using status or configuration windows. For information on those windows, please see:

- **"Viewing Status on the Wireless Array" on page 91**
- **"Configuring the Wireless Array" on page 157**

System Tools

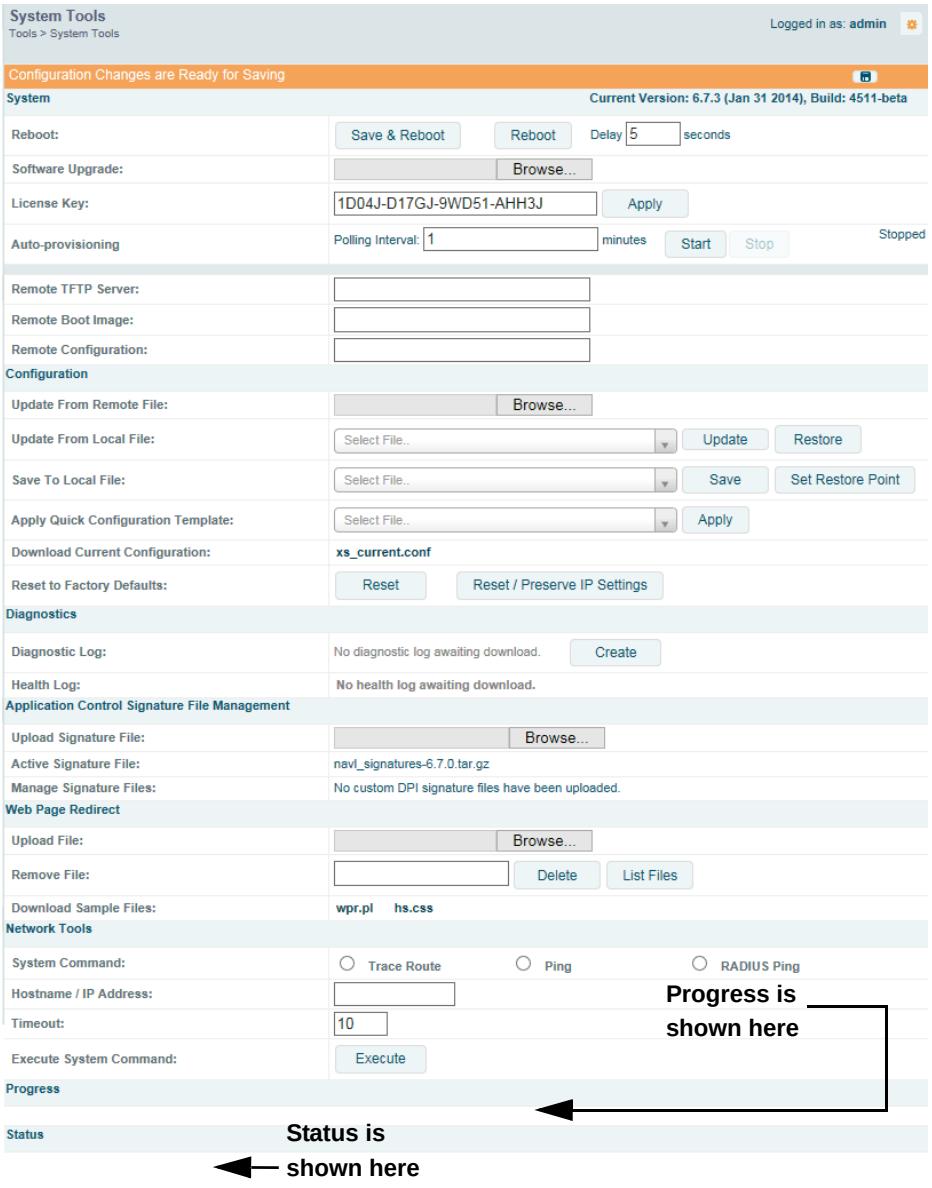


Figure 188. System Tools

This window allows you to manage files for software images, configuration, and Web Page Redirect (WPR), manage the system's configuration parameters, reboot the system, and use diagnostic tools.

About Licensing and Upgrades

If you are a customer using XMS, when you upgrade an Array from XMS, your license will automatically be updated for you first.

The Array's license determines some of the features that are available on the Array. For example, the Application Control feature is an option that must be separately licensed. To check the features supported by your license, see "Array Information" on page 98.

When upgrading the Array for a new major release, the Array needs the new license key that enables the operation of that release before upgrading. If you do not obtain the new license first, the Array will display a message and revert to the previous software image, rather than trying to run new software for which it is not licensed. Major releases will need a new license key, but minor releases will not. For example, to upgrade from ArrayOS Release 6.0.5 to Release 6.1, you must enter a new license key. To upgrade from ArrayOS Release 6.0.1 to Release 6.0.3, use your existing license key.

If you are not using XMS to perform a software upgrade, you may use the **Auto-provisioning Start** button to get an updated license from Xirrus before performing an upgrade.

If you will be entering license keys and performing upgrades on many Arrays, the effort will be streamlined by using the Xirrus Management System (XMS), especially if you are using XMS Cloud.

Procedure for Configuring System Tools

These tools are broken down into the following sections:

- **System**
- **Configuration**
- **Diagnostics**
- **Diagnostics**

- **Web Page Redirect (Captive Portal)**
- **Network Tools**
- **Progress and Status Frames**

System

1. **Save & Reboot** or **Reboot**: Use **Save & Reboot** to save the current configuration and then reboot the Array. The LEDs on the Array indicate the progress of the reboot, as described in "Powering Up the Wireless Array" on page 66. Alternatively, use the **Reboot** button to discard any configuration changes which have not been saved since the last reboot. You may specify an optional **Delay** period in seconds to wait before the reboot starts.

2. **Software Upgrade**: This feature upgrades the ArrayOS to a newer version provided by Xirrus. **Please note that you typically will need an updated license key to cover the upgrade's features before clicking the Upgrade button.** If you are a customer using XMS-9000-CL-x, your license will be updated for you automatically; with other XMS versions, you can easily upgrade all members of a profile network to a new ArrayOS release. See "About Licensing and Upgrades" on page 387 for details.

   Enter the filename and directory location (or click on the **Browse** button to locate the software upgrade file), then click on the **Upgrade** button to upload the new file to the Array. Progress of the operation will be displayed below, in the **Progress** section. Completion status of the operation is shown in the **Status** section.

   This operation does not run the new software or change any configured values. The existing software continues to run on the Array until you reboot, at which time the uploaded software will be used. An upgrade will, however, automatically save a copy of the current configuration of the Array. See Step 8 on page 391.

If you have difficulty upgrading the Array using the WMI, see ***"Upgrading the Array via CLI" on page 506*** *for a lower-level procedure you may use.*

Software Upgrade always uploads the file in binary mode. If you transfer any image file to your computer to have it available for the Software Upgrade command, it is ***critical*** *to remember to transfer it (ftp, tftp) in* ***binary*** *mode!*

3. **License Key/Auto-provisioning**:

If you are a customer using XMS-9000-CL-x, your license will be updated for you automatically; with other XMS versions, you can easily upgrade all members of a profile network to a new ArrayOS release, including updating license keys.

If you need an updated license (for example, if you are upgrading an Array to a new major release—say, from 6.4 to 6.5, and you are not using XMS to perform network-wide updates), you may obtain one through **Auto-provisioning**. Click the **Start** button, and the Array will contact the Xirrus Mobilize server with its serial number and MAC address to obtain and install its latest license. If the Array is unable to access the activation server, it will continue to attempt to contact the server at intervals specified by the **Polling Interval** (the default value is one minute). Click the **Stop** button if you wish to stop contacting the server.

If you need to enter a new license key manually, use the **License Key** field to enter it, then click the **Apply** button to the right.

A valid license is required for Array operation, and it controls the features available on the Array. If you upgrade your Array for additional features, you will be provided with a license key to activate those capabilities.

A license update will automatically save a copy of the current configuration of the Array. See Step 8 on page 391.

If you attempt to enter an invalid key, you will receive an error message and the current key will not be replaced.

Trial licenses: If you enter a trial license to try new premium features, then when the trial expires the perpetual license will be restored automatically without requiring a reboot. When the trial expires, the current Array configuration will not be lost.

Automatic Updates from Remote Image or Configuration File

The Array software image or configuration file can be downloaded from an external server. In large deployments, all Arrays can be pointed to one TFTP server instead of explicitly initiating software image uploads to all Arrays. When the Array boots, the Array will download the software image from the specified TFTP server. Similarly, if you decide to change a setting in the Arrays, you can simply modify a single configuration file. After the Arrays are rebooted, they will automatically download the new configuration file from a single location on the specified TFTP server.

4. **Remote TFTP Server**: This field defines the path to a TFTP server to be used for automated remote update of software image and configuration files when rebooting. You may specify the server using an IP address or host name.

5. **Remote Boot Image**: When the Array boots up, it fetches the software image file specified here from the TFTP server defined above, and upgrades to this image before booting. This must be an Array image file with a **.bin** extension.

   Make sure to place the file on the TFTP server. If you disable the remote boot image (by blanking out this field) or if the image can't be transferred, the Array will fall back to booting whatever image is on the compact flash.

The Remote Boot Image or Remote Configuration update happens every time that the Array reboots. If you only want to fetch the remote image or configuration file one time, be sure to turn off the remote option (blank out the field on the System Tools page) after the initial download. When a remote boot image is used, the image is transferred directly into memory and is never written to the compact flash.

6. **Remote Configuration:** When the Array boots up, it fetches the specified configuration file from the TFTP server defined above, and applies this configuration **after** the local configuration is applied. The remote configuration must be an Array configuration file with a **.conf** extension. Make sure to place the file on the TFTP server.

   A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your Arrays but don't want to have the same IP address for each Array, you may remove the **ipaddr** line from the file. You can then load the file on each Array and the local IP addresses will not change.

   A remote configuration is never saved to the compact flash unless you issue a Save command.

Configuration

7. **Update from Remote File**: This field allows you to define the path to a configuration file (one that you previously saved—see Step 9 and Step 10 below). Click on the **Browse** button if you need to browse for the location of the file, then click **Update** to update your configuration settings.

8. **Update from Local File**: This field updates Array settings from a local configuration file on the Array. Select one of the following files from the drop-down list:

   - **factory.conf**: The factory default settings.
   - **lastboot.conf**: The setting values from just before the last reboot.
   - **saved.conf**: The last settings that were explicitly saved using the **Save** button at the top of each window.

- **history/saved-yyyymmdd-pre-update.conf**:
  history/saved-yyyymmdd-post-update.conf:

  Two files are automatically saved for a software upgrade or for a license change (including the setting values from just before the upgrade/change was performed, and the initial values afterward. The filename includes the date.

- **history/saved-yyyymmdd-auto.conf**: Each time you use the **Save** button, an "auto" file is saved with the settings current at that time.
- **history/saved-yyyymmdd-pre-reset.conf**:
  history/saved-yyyymmdd-post-reset.conf:

  Each time you use one of the **Reset to Factory Default** buttons, two files are saved: the setting values from just before the reset, and the initial values afterward. The filename includes the reset date.

- **history/saved-yyyymmdd-hhmm.conf**: The setting values that were explicitly saved using the **Set Restore Point** button (see Step 9 below).

Click **Update** to update your configuration settings by appending to the current Array configuration. Click **Restore** to replace the Array configuration with the configuration file selected.

Note that the History folder allows a maximum of 16 files. The oldest file is automatically deleted to make room for each new file.

9. **Save to Local File:** There are a few options for explicitly requesting the Array to save your current configuration to a file on the Array:

   - To view the list of configuration files currently on the Array, click the down arrow to the right of this field. If you wish to replace one of these files (i.e., save the current configuration under an existing file name), select the file, then click **Save**. Note that you cannot save to the file names f**actory.conf**, **lastboot.conf**, and **saved.conf** - these files are write-protected.
   - You may enter the desired file name, then click **Save**.

- Click **Set Restore Point** to save a copy of the current configuration, basing the file name on the current date and time. For example:

  history/saved-20100318-1842.conf

Note that the configuration is automatically saved to a file in a few situations, as described in Step 8 above.

Important! *When you have initially configured your Array, or have made significant changes to its configuration, we strongly recommend that you save the configuration to a file in order to have a safe backup of your working configuration.*

10. **Download Current Configuration:** Click on the link titled **xs_current.conf** to download the Array's current configuration settings to a file (that you can upload back to the Array at a later date). The system will prompt you for a destination for the file. The file will contain the Array's current configuration values.

11. **Reset to Factory Defaults**: Click on the **Reset/Preserve IP Settings** button to reset the system's current configuration settings to the factory default values, *except for the Array's management IP address which is left unchanged*. This function allows you to maintain management connectivity to the Array even after the reset. This will retain the Gigabit Ethernet port's IP address (see "Network Interfaces" on page 166), or if you have configured management over a VLAN it will maintain the management VLAN's IP address (see "VLAN Management" on page 206). *All other previous configuration settings will be lost*.

    Click **Reset** to reset all of the system's current configuration settings to the factory default values, including the management IP address—*all previous configuration settings will be lost*. The Array's Gigabit Ethernet ports default to using DHCP to obtain an IP address.

If the IP settings change, the connection to the WMI may be lost.

Diagnostics

12. **Diagnostic Log**: Click the **Create** button to save a snapshot of Array information for use by Xirrus Customer Support personnel. The Progress and Status Frames show the progress of this operation. When the process is complete, the filename `xs_diagnostic.log` will be displayed in blue and provides a link to the newly created log file. Click the link to download this file. You will be asked to specify the location for saving the file. (Figure 189)

Figure 189. Saving the Diagnostic Log

This feature is only used at the request of Customer Support. It saves all of the information regarding your Array, including status, configuration, statistics, log files, and recently performed actions.

The diagnostic log is always saved as a file named `xs_diagnostic.log` on your `C:\` drive, so you should immediately rename the file to save it. This way, it will not be lost the next time you save a diagnostic log. Often, Customer Support will instruct you to save two diagnostic logs about ten minutes apart so that they can examine the difference in statistics between the two snapshots (for example, to see traffic and error statistics for the interval). Thus, you must rename the first diagnostic log file.

All passwords are stored on the array in an encrypted form and will not be exposed in the diagnostic log.

13. **Health Log**: This file is created automatically, but only if the Array encounters unexpected and serious problems. Normally this file will not exist. The Diagnostic Log **Create** button has no effect on this file

whatsoever. When a health log exists, the filename **xs_health.log.bz2** is displayed in blue and provides a link to the log file. Click the link to download this file or to open it with your choice of application. This file is normally only used at the request of Customer Support.

Application Control Signature File Management

Application Control recognizes applications using a file containing the signatures of hundreds of applications. This file may be updated regularly to keep up as Internet usage evolves over time. The latest signature file is available from the same location that you use to download the latest ArrayOS release: Xirrus ArrayOS - XR Platform Latest Release . Note that new ArrayOS releases will automatically contain the latest signature file available at the time of the build.

See "Application Control Windows" on page 146 for more information about using Application Control.

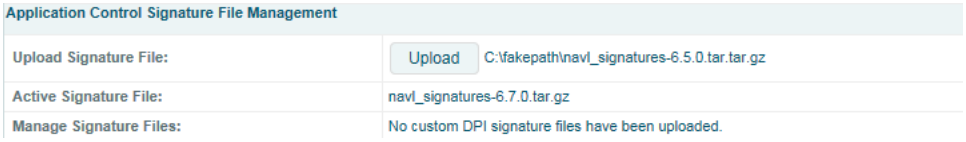


Figure 190. Managing Application Control Signature files

14. **Upload Signature File**: First, download the latest signature file from the Xirrus Customer Support site: Xirrus ArrayOS - XR Platform Latest Release to your file system. Click the **Browse** button, then browse to locate the new signature file. Click the **Upload** button when it appears. The new file will be uploaded to the Array and will be used for identifying applications. **You must turn Application Control off and back on again** on the Filter Lists page to make the new signature file take effect. See "Filter Lists" on page 366. No reboot is required.

    Upload Signature File shows which file is currently being used by Application Control. If you have installed any custom DPI signature files, you may use **Manage Signature Files**.

Web Page Redirect (Captive Portal)

The Array uses a Perl script and a cascading style sheet to define the default splash/login Web page that the Array delivers for WPR. You may replace these files with files for one or more custom pages of your own. See Step 17 below to view the default files. See Step 14 page 266 for more information about WPR and how the splash/login page is used.

Each SSID that has WPR enabled may have its own page. Custom files for a specific SSID **must** be named based on the SSID name. For example, if the SSID is named **Public**, the default `wpr.pl` and `hs.css` files should be modified as desired and renamed to `wpr-Public.pl` and `hs-Public.css` before uploading to the Array. If you modify and upload files named `wpr.pl` and `hs.css`, they will replace the factory default files and will be used for any SSID that does not have its own custom files, per the naming convention just described. Be careful not to replace the default files unintentionally.

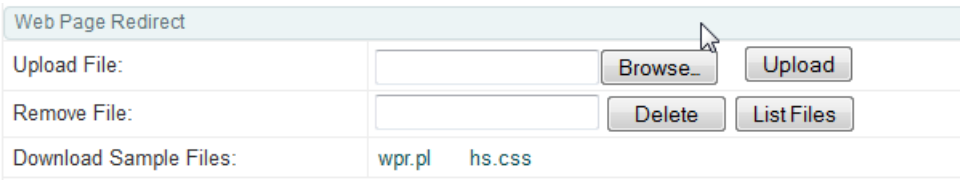


Figure 191. Managing WPR Splash/Login page files

15. **Upload File**: Use this to install files for your own custom WPR splash/login page (as described above) on the Array. Note that uploaded files are not immediately used - you must reboot the Array first. At that time, the Array looks for and uses these files, if found.

    Enter the filename and directory location (or click **Browse** to locate the splash/login page files), then click on the **Upload** button to upload the new files to the Array. You must reboot to make your changes take effect.

16. **Remove File**: Enter the name of the WPR file you want to remove, then click on the **Delete** button. You can use the **List Files** button to show you a list of files that have been saved on the Array for WPR. The list is displayed in the **Status** section at the bottom of the WMI window. You must reboot to make your changes take effect.

17. **Download Sample Files**: Click on a link to access the corresponding sample WPR files:

    - **wpr.pl**—a sample Perl script.
    - **hs.css**—a sample cascading style sheet.

Network Tools

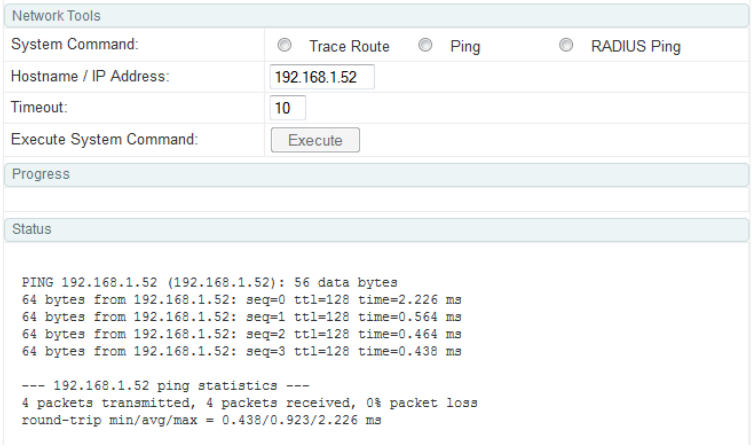


Figure 192. System Command (Ping)

18. **System Command**: Choose **Trace Route**, **Ping.**, or **RADIUS Ping**. For Trace Route and Ping, fill in **IP Address** and **Timeout**. Then click the **Execute** button to run the command.

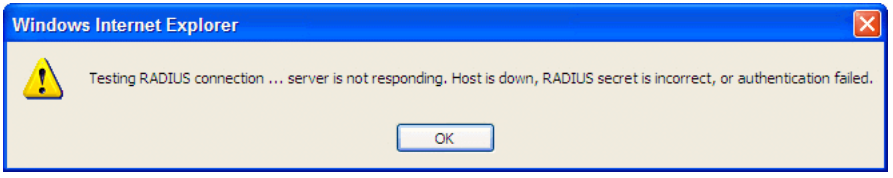
    The RADIUS Ping command is a simple utility that tests connectivity to a RADIUS server by attempting to log in with the specified Username and Password. When using a RADIUS server, this command allows you to verify that the server configuration is correct and whether a particular Username and Password are set up properly. If a client is having trouble

accessing the network, you can quickly determine if there is a basic RADIUS problem by using the RADIUS Ping tool. For example, in Figure 193 (A), RADIUS Ping is unable to contact the server. In Figure 193 (B), RADIUS Ping verifies that the host information and secret for a RADIUS server are correct, but that the user account information is not.

Select RADIUS allows you to select a RADIUS server that you have already configured. When you make a choice in this field, additional fields will be displayed. Set **Select RADIUS** to External Radius, Internal Radius, or a server specified for a particular SSID, or select **Other Server** to specify another server by entering its **Host** name or IP address, **Port**, and shared **Secret**.

Enter the **RADIUS Credentials**: **Username** and **Password**. Select the **Authentication Type**, **PAP** or **CHAP**. Click the **Execute** button to run the command. The message **Testing RADIUS connection** appears. Click **OK** to proceed.

A



B

Figure 193. Radius Ping Output

19. **IP Address**: For Ping or Trace Route, enter the IP address of the target device.
20. **Timeout**: For Ping or Trace Route, enter a value (in seconds) before the action times out.

21. **Execute System Command**: Click **Execute** to start the specified command. Progress of command execution is displayed in the **Progress** frame. Results are displayed in the **Status** frame.

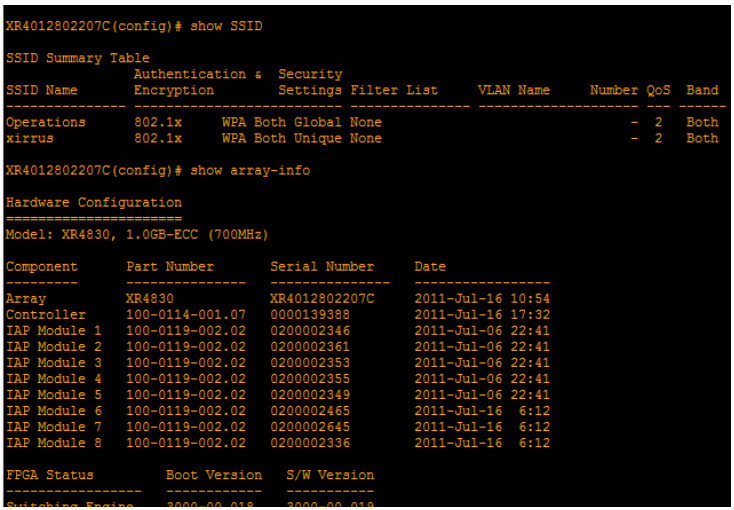
Progress and Status Frames

The **Progress** frame displays a progress bar for commands such as Software Upgrade and Ping. The **Status** frame presents the output from system commands (Ping and Trace Route), as well as other information, such as the results of software upgrade.

22. If you want to save the parameters you established in this window for future sessions, click the **Save** button .

CLI

The WMI provides this window to allow you to use the Array's Command Line Interface (CLI). You can enter commands to configure the Array, or display information using show commands. You will not need to log in - you already logged in to the Array when you started the WMI.



```
XR4012802207C(config)# show SSID

SSID Summary Table
                Authentication &  Security
SSID Name       Encryption        Settings Filter List     VLAN Name     Number QoS  Band
--------------- ------------------------- --------------- -------------------- --- ------
Operations      802.1x     WPA Both Global None                              -  2   Both
xirrus          802.1x     WPA Both Unique None                              -  2   Both

XR4012802207C(config)# show array-info

Hardware Configuration
======================
Model: XR4830, 1.0GB-ECC (700MHz)

Component      Part Number       Serial Number     Date
---------      ---------------   ---------------   -----------------
Array          XR4830            XR4012802207C     2011-Jul-16 10:54
Controller     100-0114-001.07   0000139388        2011-Jul-16 17:32
IAP Module 1   100-0119-002.02   0200002346        2011-Jul-06 22:41
IAP Module 2   100-0119-002.02   0200002361        2011-Jul-06 22:41
IAP Module 3   100-0119-002.02   0200002353        2011-Jul-06 22:41
IAP Module 4   100-0119-002.02   0200002355        2011-Jul-06 22:41
IAP Module 5   100-0119-002.02   0200002349        2011-Jul-06 22:41
IAP Module 6   100-0119-002.02   0200002465        2011-Jul-16  6:12
IAP Module 7   100-0119-002.02   0200002645        2011-Jul-16  6:12
IAP Module 8   100-0119-002.02   0200002336        2011-Jul-16  6:12

FPGA Status         Boot Version   S/W Version
-----------------   ------------   -----------
```

Figure 194. CLI Window

To enter a command, simply type it in. The command is echoed and output is shown in the normal way—that is, the same way it would be if you were using the CLI directly. You may use the extra scroll bar inside the right edge of the window to scroll through your output. If output runs past the right edge of the screen, there is also a horizontal scroll bar at the bottom of the page.

This window has some minor differences, compared to direct use of the CLI via the console or an SSH connection:

- The CLI starts in **config** mode. All configuration and show commands are available in this mode. You can "drill down" the mode further in the usual way. For example, you can type **interface iap** to change the mode to **config-iap**. The prompt will indicate the current command mode, for example:

  ```
  My-Array(config-iap) #
  ```

- You can abbreviate a command and it will be executed if you have typed enough of the command to be unambiguous. The command will not auto-complete, however. Only the abbreviated command that you actually typed will be shown. You can type a partial command and press Tab to have the command auto-complete. If the partial command is ambiguous a list of legal endings is displayed.
- Entering **quit** will return you to the previously viewed WMI page.
- Most, but not all, CLI commands can be run in this window. Specifically the **run-test** menu of commands is **not** available in this window. To use the run-test command, please connect using SSH and use CLI directly, or use the System Tools described in this chapter, such as Trace Route, Ping, and RADIUS Ping.

Help commands (the **?** character) are available, either at the prompt or after you have typed part of a command.

API Documentation

Arrays provide an API interface conforming to the RESTful API model. Developers may use this read-only API to read status, statistics, and settings from the Array. The interactive API Documentation page provides documentation for the API.

You may use the Array's API for purposes such as integrating with third party applications or creating your own applications for network monitoring and analysis. Using the RESTful API eliminates the need to use CLI scripting, or to use SNMP which can be cumbersome for polling large amounts of data. Results are returned in JSON format (JavaScript Object Notation), a text-based open standard designed for human-readable data interchange. The API documentation is tightly integrated with the server code. The API Documentation page allows you to interact with the API in a sandbox UI that gives clear insight into how the API responds to parameters and options.

Security for the API is provided with OAuth, as described in "OAuth 2.0 Management" on page 251. Once registration is completed and a permanent token for this Array has been obtained, your application may access the RESTful API using the **client_id** and the **token** at the following URL:

```
https://[Array hostname or IP address]/api/v1/[api-name]
```

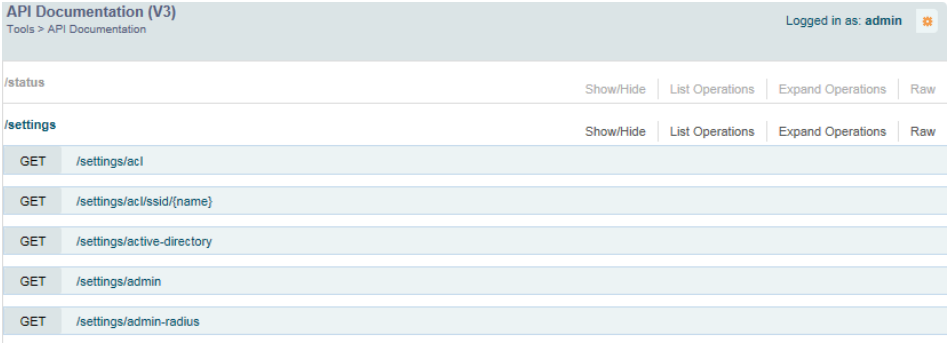


Figure 195. API Documentation

The API Documentation page lists all of the APIs that are available, lists their calling parameters, if any, and allows you to perform sample calls and view sample output.

Status/Settings

The RESTful API on the Array is broken into these two main headings: **status** and **settings**. Each is a node that may be clicked to expand or collapse the list of corresponding API requests available on the Array. Since this is a read-only API, the list consists exclusively of GET operations.

The figure below shows part of the list displayed by clicking **/settings**. Click again to collapse (hide) the list.

Status requests include **GET** requests for many of the status and statistics items described in the chapter titled, "Viewing Status on the Wireless Array" on page 91. **Settings** requests include **GET** requests for many of the settings described in the chapter titled, "Configuring the Wireless Array" on page 157

GET Requests

Each request name in the list is a link. Click it to see more information and to try the API and see its output.

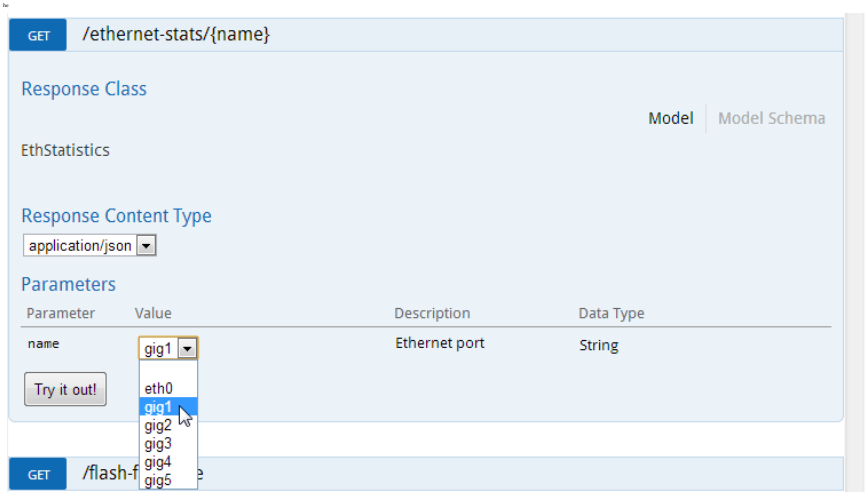


Figure 196. API — GET Request Details

The figure above shows the GET request for **ethernet-stats{name}**. Click again to collapse (hide) the API details.

High-level details are shown, including the **Response Class** name and the **Response Content Type** (limited to JSON at this time).

Trying a GET Request

The **Try it out!** button allows you to send the GET request to the Array API and see its response. Developers can use this feature to design and implement applications that use this response.

Enter any necessary **Parameters** and click the **Try it out!** button. Most GET requests do not use any parameters. If they are required, their names will be listed and there will be a field or a drop-down list to specify each one. An example is shown in Figure 196. In some cases, there may be two versions of a request, with and without parameters. For example, **GET /ethernet-stats/{name}** returns status and statistics for a particular Ethernet port, while **GET /ethernet-stats/** returns information for all Ethernet ports.

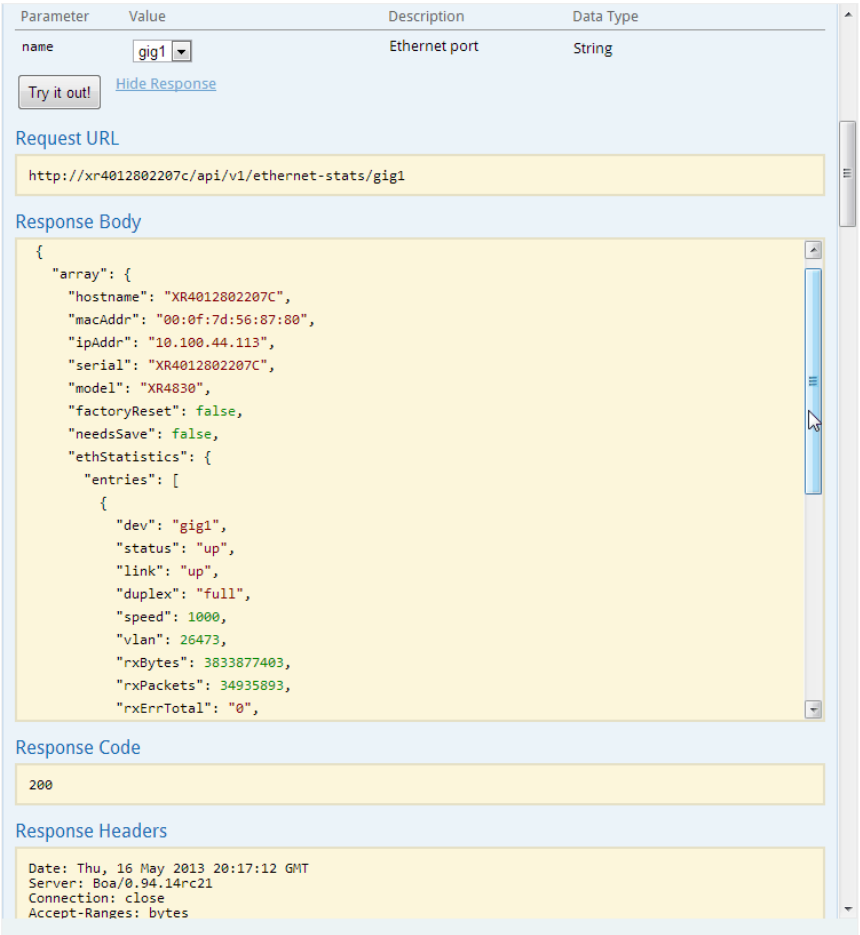


Figure 197. API — GET Request Response

The figure above shows the response for **ethernet-stats{name}**. The response is produced in the human-readable JSON format. The status and statistics data shown are as described in "Viewing Status on the Wireless Array" on page 91. Click **Hide Response** if you wish to hide the output.

The **Response Code** and the **Response Header** are standard for HTTP(S).

API Documentation Toolbar

Figure 198. API Documentation Toolbar

The Status and Settings sections each have a toolbar as shown above, offering the following options.

- **Show/Hide**—expands or collapses this list of GET requests. Hiding and then showing again displays the requests as they were before, i.e., expanded GET requests will still be expanded when displayed again.
- **List Operations**—expands this list of GET requests. Each individual entry is collapsed.
- **Expand Operations**—shows all of the GET requests in this list. Each individual entry is expanded.
- **Raw**—shows the source XML code for this list of GET requests. Click the link for the API Documentation page again to return to the normal display.

Options

This window allows you to customize the behavior of the WMI. ~~Array~~

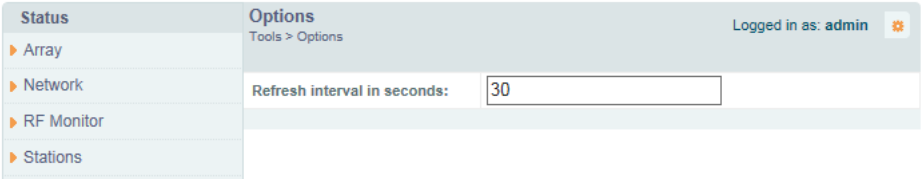


Figure 199. WMI Display Options

Procedure for Configuring Options

1. **Refresh Interval in Seconds**: Many of the windows in the Status section of the WMI have an Auto Refresh option. You may use this setting to change how often a status or statistics window is refreshed, if its auto refresh option is enabled. Enter the desired number of seconds between refreshes. The default refresh interval is 30 seconds.

Logout

Click on the Logout button to terminate your session. When the session is terminated, you are presented with the login window.

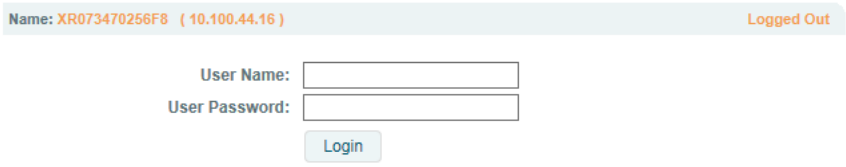


Figure 200. Login Window

The Command Line Interface

This section covers the commands and the command structure used by the Wireless Array's Command Line Interface (CLI), and provides a procedure for establishing an SSH connection to the Array. Topics discussed include:

- **"Establishing a Secure Shell (SSH) Connection" on page 409**.
- **"Getting Started with the CLI" on page 411.**
- **"Top Level Commands" on page 413.**
- **"Configuration Commands" on page 422.**
- **"Sample Configuration Tasks" on page 466.**

*Some commands are only available if the Array's license includes appropriate Xirrus **Advanced Feature Sets**. If a command is unavailable, an error message will notify you that your license does not support the feature. See **"About Licensing and Upgrades" on page 387**.*

See Also

Zero-Touch Provisioning and Ongoing Management
Network Map
System Tools

Establishing a Secure Shell (SSH) Connection

Use this procedure to initialize the system and log in to the Command Line Interface (CLI) via a Secure Shell (SSH) utility, such as PuTTY. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. Make sure that your SSH utility is set up to use SSH-2.

1. Start your SSH session and communicate with the Array via its IP address.
   - If the Array is connected to a network that uses DHCP, use the address assigned by DHCP. We recommend that you have the

network administrator assign a reserved address to the Array for ease of access in the future.

- If the network does not use DHCP, use the factory default address 10.0.2.1 to access either the Gigabit 1 or Gigabit 2 Ethernet port. You may need to change the IP address of the port on your computer that is connected to the Array—change that port's IP address so that it is on the same 10.0.2.xx subnet as the Array port.

2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the Array's Command Line Interface.

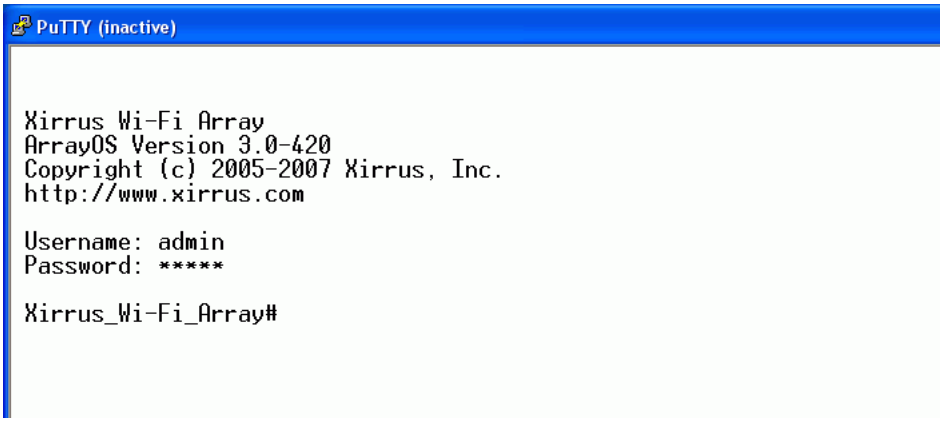


Figure 201. Logging In

Getting Started with the CLI

The root command prompt (**Root Command Prompt**) is the first prompt you see after logging in to the CLI. If you are at a level other than the root command prompt you can return to this prompt at any time by using the **exit** command to step back through each command prompt level. The root command prompt you see in the CLI window is determined by the host name you assigned to your Array. The prompt Xirrus_**Wi-Fi_Array** is displayed throughout this document simply because this is the host name assigned to the Array used for development. To terminate your session at any time, use the **quit** command.

Inputting Commands

When inputting commands you need only type as many characters as the system requires before it recognizes your input. For example, you can type the abbreviated term **config** to access the configure prompt.

Getting Help

The CLI offers the following two levels of assistance:

- help Command

  The **help** command is only available at the root command prompt. Initiating this command generates a window that provides information about the types of help that are available with the CLI.

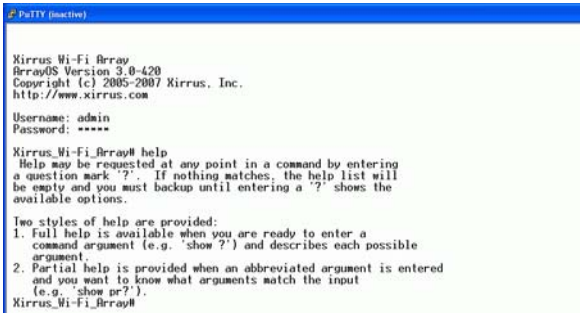


Figure 202. Help Window

- ? Command

  This command is available at any prompt and provides either FULL or PARTIAL help. Using the **?** (question mark) command when you are ready to enter an argument will display all the possible arguments (full help). Partial help is provided when you enter an abbreviated argument and you want to know what arguments will match your input.

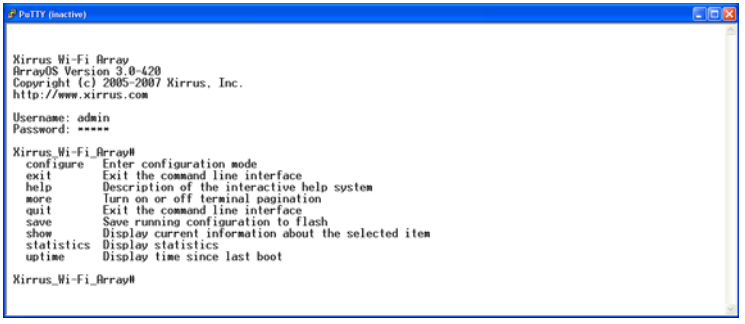


Figure 203. Full Help

Figure 204 shows an example of how the Help system can provide the argument and format when specifying the time zone under the **date-time** command.

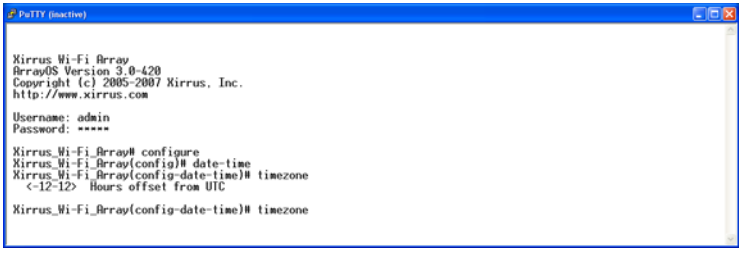


Figure 204. Partial Help

Top Level Commands

This section offers an at-a-glance view of all top level commands—organized alphabetically. Top level commands are defined here as commands that are directly accessible from the root command prompt that consists of the name of the Array followed by a "#" sign (e.g. **MyAP#**). When inputting commands, be aware that all commands are **case-sensitive**.

All other commands are considered second level configuration commands—these are the commands you use to configure specific elements of the Array's features and functionality. For a listing of these commands with examples of command formats and structure, go to "Configuration Commands" on page 422.

Root Command Prompt

The following table shows the top level commands that are available from the root command prompt [**MyAP**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
configure	Enter the configuration mode. See "Configuration Commands" on page 422.
exit	Exit the CLI and terminate your session—if this command is used at any level other than the root command prompt you will simply exit the current level (step back) and return to the previous level.
help	Show a description of the interactive help system. See also, "Getting Help" on page 411.
history	List history of commands that have been executed.
more	Turn terminal pagination ON or OFF.
quit	Exit the Command Line Interface (from any level).
search	Search for pattern in show command output.

Command	Description
show	Display information about the selected item. See "show Commands" on page 417.
statistics	Display statistical data about the Array. See "statistics Commands" on page 420.
uptime	Display the elapsed time since the last boot.
xms-override	Override XMS managed mode and allow local configuration changes according to your user privileges. See "Managing Arrays Locally or via XMS" on page 81.

configure Commands

The following table shows the second level commands that are available with the top level **configure** command [**MyAP(config)#**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
acl	Configure the Access Control List.
admin	Define administrator access parameters.
auth	Configure Oauth tokens.
cdp	Configure Cisco Discovery Protocol settings.
clear	Remove/clear the requested elements.
cluster	Make configuration changes to multiple Arrays.
contact-info	Contact information for assistance on this Array.
date-time	Configure date and time settings.
dhcp-server	Configure the DHCP Server.
dns	Configure the DNS settings.

Command	Description
end	Exit the configuration mode.
exit	Go UP one mode level.
file	Manage the file system.
filter	Define protocol filter parameters.
group	Define user groups with parameter settings
help	Description of the interactive Help system.
history	List history of commands that have been executed.
hostname	Host name for this Array.
interface	Select the interface to configure.
load	Load running configuration from flash
location	Location name for this Array.
location-reporting	Configure location server settings.
management	Configure Array management parameters
mdm	Configure mobile device management server settings.
more	Turn ON or OFF terminal pagination.
netflow	Configure NetFlow data collector.
no	Disable (if enabled) or set to default value.
quick-config	Apply configuration template for typical deployment scenario.
quit	Exit the Command Line Interface.
authentication-server	Configure the RADIUS server parameters.

Command	Description
reboot	Reboot the Array.
reset	Reset all settings to their factory default values and reboot.
restore	Reset all settings to their factory default values and reboot.
revert	Revert to saved configuration after specified delay in seconds if configuration not saved.
run-tests	Run selective tests.
save	Save the running configuration to FLASH.
search	Search for pattern in show command output.
security	Set the security parameters for the Array.
show	Display current information about the selected item.
snmp	Enable, disable or configure SNMP.
ssid	Configure the SSID parameters.
statistics	Display statistics.
syslog	Enable, disable or configure the Syslog Server.
tunnel	Configure tunnels.
uptime	Display time since the last boot.
vlan	Configure VLAN parameters.
wifi-tag	Configure VLAN parameters.
xms-override	Override XMS managed mode and allow local configuration changes according to your user privileges. See "Managing Arrays Locally or via XMS" on page 81.

show Commands

The following table shows the second level commands that are available with the top level **show** command [**MyAP# show**].

Command	Description
acl	Display the Access Control List.
admin	Display the administrator list or login information.
array-info	Display system information.
associated-stations	Display stations that have associated to the Array.
boot-env	Display Boot loader environment variables.
capabilities	Display detailed station capabilities.
cdp	Display Cisco Discovery Protocol settings.
channel-list	Display list of Array's 802.11an and bgn channels.
clear-text	Display and enter passwords and secrets in the clear.
conntrack	Display the Connection Tracking table.
console	Display terminal settings.
contact-info	Display contact information.
date-time	Display date and time settings summary.
dhcp-leases	Display IP addresses (leases) assigned to stations by the DHCP server.
dhcp-pool	Display internal DHCP server settings summary information.
diff	Display the difference between configurations.
dns	Display DNS summary information.

Command	Description
error-numbers	Display the detailed error number in error messages.
ethernet	Display Ethernet interface summary information.
external-radius	Display summary information for the external RADIUS server settings.
factory-config	Display the Array factory configuration information.
filters	Display filter information.
iap	Display IAP configuration information.
internal-radius	Display the users defined for the embedded RADIUS server.
lastboot-config	Display Array configuration at the time of the last boot-up.
management	Display settings for managing the Array, plus Standby, FIPS, and other information.
network-map	Display network map information.
realtime-monitor	Display realtime statistics for all IAPs.
rogue-ap	Display rogue AP information.
route	Display the routing table.
rssi-map	Display RSSI map by IAP for station.
running-config	Display configuration information for the Array currently running.
saved-config	Display the last saved Array configuration.
security	Display security settings summary information.
self-test	Display self test results.
snmp	Display SNMP summary information.

Command	Description
spanning-tree	Display spanning tree information.
spectrum-analyzer	Display spectrum analyzer measurements.
ssid	Display SSID summary information.
stations	Display station information.
statistics	Display statistics.
syslog	Display the system log.
syslog-settings	Display the system log (Syslog) settings.
temperature	Display the current board temperatures.
unassociated-stations	Display unassociated station information.
vlan	Display VLAN information.
wds	Display WDS information.
<cr>	Display configuration or status information.

statistics Commands

The following table shows the second level commands that are available with the top level **statistics** command [**MyAP# statistics**].

Command	Description
ethernet	Display statistical data for all Ethernet interfaces.
Ethernet Name **eth0**, **gig1**, **gig2**	Display statistical data for the defined Ethernet interface (either eth0, gig1 or gig2). FORMAT: **statistics gig1**
filter	Display statistics for defined filters (if any). FORMAT: **statistics filter [detail]**
filter-list	Display statistics for defined filter list (if any). FORMAT: **statistics filter <filter-list>**
iap	Display statistical data for the defined IAP. FORMAT: **statistics iap iap2**
station	Display statistical data about associated stations. FORMAT: **statistics station billw**
vlan	Display statistical data for the defined VLAN. You must use the VLAN number (not its name) when defining a VLAN. FORMAT: **statistics vlan 1**

Command	Description
wds	Display statistical data for the defined active WDS (Wireless Distribution System) links. FORMAT: **statistics wds 1**
<cr>	Display configuration or status information.

Configuration Commands

All configuration commands are accessed by using the **configure** command at the root command prompt (**MyAP#**). This section provides a brief description of each command and presents sample formats where deemed necessary. The commands are organized alphabetically. When inputting commands, be aware that all commands are **case-sensitive**.

To see examples of some of the key configuration tasks and their associated commands, go to "Sample Configuration Tasks" on page 466.

acl

The **acl** command [**MyAP(config)# acl**] is used to configure the Access Control List.

Command	Description
add	Add a MAC address to the list. FORMAT: **acl add AA:BB:CC:DD:EE:FF**
del	Delete a MAC address from the list. FORMAT: **acl del AA:BB:CC:DD:EE:FF**
disable	Disable the Access Control List FORMAT: **acl disable**
enable	Enable the Access Control List FORMAT: **acl enable**
reset	Delete all MAC addresses from the list. FORMAT: **acl reset**

admin

The **admin** command **[MyAP(config-admin)#]** is used to configure the Administrator List.

Command	Description
add	Add a user to the Administrator List. FORMAT: **admin add [userID]**
del	Delete a user to the Administrator List. FORMAT: **admin del [userID]**
edit	Modify user in the Administrator List. FORMAT: **admin edit [userID]**
radius	Define a RADIUS server to be used for authenticating administrators. FORMAT: **admin radius [disable | enable | off | on | timeout <seconds> | auth-type [PAP | CHAP]]** **admin radius [primary |secondary] port <portid> server [<ip-addr> | <host>] secret <shared-secret>**
reset	Delete all users and restore the default user. FORMAT: **admin reset**

auth

The **auth** command [**MyAP(config)# auth**] is used to configure Oauth tokens. See

Command	Description
add	Add an Oauth token. FORMAT: **auth add <token> client <client> grant <grant> expiration <expiration> code <code> type <type> [agent <agent>] [scope <scope>]**
del	Delete an Oauth token. FORMAT: **auth del <Oauth token>**
reset	Delete all Oauth tokens. FORMAT: **auth reset**

also, "OAuth 2.0 Management" on page 251.

cdp

The **cdp** command [**MyAP(config)# cdp**] is used to configure the Cisco Discovery Protocol.

Command	Description
disable	Disable the Cisco Discovery Protocol FORMAT: **cdp disable**
enable	Enable the Cisco Discovery Protocol FORMAT: **cdp enable**

Command	Description
hold-time	Select CDP message hold time before messages received from neighbors expire. FORMAT: **cdp hold-time [# seconds]**
interval	The Array sends out CDP announcements at this interval. FORMAT: **cdp interval [# seconds]**
off	Disable the Cisco Discovery Protocol FORMAT: **cdp off**
on	Enable the Cisco Discovery Protocol FORMAT: **cdp on**

clear

The **clear** command [**MyAP(config)# clear**] is used to clear requested elements.

Command	Description
arp	Clear the arp table entry for a requested IP address, or clear all entries if no IP address is entered. FORMAT: **clear arp [ipaddress]**
authentication	Deauthenticate a station (specified by MAC address, hostname, or IP address). If you specify the permanent option, then the station is deauthenticated and put on the access control list. FORMAT: **clear authentication [permanent] [authenticated station]**
history	Clear the history of CLI commands executed. FORMAT: **clear history**
screen	Clear the screen where you're viewing CLI output. FORMAT: **clear screen**
station-assurance	Clear all station assurance data, but continue to collect new data. FORMAT: **clear station-assurance**
statistics	Clear the statistics for thee change, but it won't show up requested element. FORMAT: **clear statistics [ethname | all-eth | applications | filters |iap | station | vlan | wds]**

Command	Description
syslog	Clear all Syslog messages, but continue to log new messages. FORMAT: **clear syslog**

cluster

The **cluster** command [Xirrus_**Wi-Fi_Array(config)# cluster**] is used to create and operate clusters. Clusters allow you to configure multiple Arrays at the same time. Using CLI (or WMI), you may define a set of Arrays that are members of the cluster. Then you may switch the Array to Cluster operating mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member Arrays. When you exit cluster mode, configuration commands revert to applying only to the Array to which you are connected.

For more information, see "Clusters" on page 374.

Command	Description
add	Create a new Array cluster. Enters edit mode for that cluster to allow you to specify the Arrays that belong to the cluster. FORMAT: **cluster add [cluster-name]**
del	Delete an Array cluster. Type **del ?** to list the existing clusters. FORMAT: **cluster del [cluster-name]**
edit	Enter edit mode for selected cluster to add or delete Arrays that belong to the cluster. FORMAT: **cluster edit [cluster-name]**
end	Exit Cluster configuration mode. Configuration returns to normal operation, affecting this Array only. FORMAT: **cluster end**

Command	Description
operate	Enter Cluster operation mode. All configuration commands are applied to all of the selected cluster's member Arrays until you give the **end** command (see above). FORMAT: **cluster operate [cluster-name]**
reset	Delete all clusters. FORMAT: **cluster reset**

contact-info

The **contact-info** command **[MyAP(config)# contact-info]** is used for managing administrator contact information.

Command	Description
email	Add an email address for the contact (must be in quotation marks). FORMAT: **contact-info email ["contact@mail.com"]**
name	Add a contact name (must be in quotation marks). FORMAT: **contact-info name ["Contact Name"]**
phone	Add a telephone number for the contact (must be in quotation marks). FORMAT: **contact-info phone ["8185550101"]**

date-time

The **date-time** command [**MyAP(config-date-time)#**] is used to configure the date and time parameters. Your Array supports the Network Time Protocol (NTP) in order to ensure that the Array's internal time is accurate. NTP is set to UTC time by default; however, you can set the time zone so that your Array will display local time. This is done by defining an offset from the UTC value. For example, Pacific Standard Time is 8 hours behind UTC time, so the offset from UTC time would be -8.

Command	Description
dst_adjust	Enable adjustment for daylight savings. FORMAT: **date-time dst_adjust**
no	Disable daylight savings adjustment. FORMAT: **date-time no dst_adjust**
ntp	Enable the NTP server. FORMAT: **date-time ntp on** (or **off** to disable)
offset	Set an offset from Greenwich Mean Time. FORMAT: **date-time no dst_adjust**
set	Set the date and time for the Array. FORMAT: **date-time set [10:24 10/23/2007]**
timezone	Configure the time zone. FORMAT: **date-time timezone [-8]**

dhcp-server

The **dhcp-server** command **[MyAP(config-dhcp-server)#]** is used to add, delete and modify DHCP pools.

Command	Description
add	Add a DHCP pool. FORMAT: **dhcp-server add [dhcp pool]**
del	Delete a DHCP pool. FORMAT: **dhcp-server del [dhcp pool]**
edit	Edit a DHCP pool FORMAT: **dhcp-server edit [dhcp pool]**
reset	Delete all DHCP pools. FORMAT: **dhcp-server reset**

dns

The **dns** command **[MyAP(config-dns)#]** is used to configure your DNS parameters.

Command	Description
domain	Enter your domain name. FORMAT: **dns domain [www.mydomain.com]**
server1	Enter the IP address of the primary DNS server. FORMAT: **dns server1 [1.2.3.4]**
server2	Enter the IP address of the secondary DNS server. FORMAT: **dns server1 [2.3.4.5]**
server3	Enter the IP address of the tertiary DNS server. FORMAT: **dns server1 [3.4.5.6]**

file

The **file** command [**MyAP(config-file)#**] is used to manage files.

Command	Description
active-image	Validate and commit a new array software image.
backup-image	Validate and commit a new backup software image.
check-image	Validate a new array software image.
chkdsk	Check flash file system.
copy **cp**	Copy a file to another file. FORMAT: **file copy [sourcefile destinationfile]**
dir	List the contents of a directory. FORMAT: **file dir [directory]**
erase	Delete a file from the FLASH file system. FORMAT: **file erase [filename]**
format	Format flash file system.
ftp	Open an FTP connection with a remote server. Files will be transferred in binary mode. FORMAT: **file ftp host {<hostname> | <ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the Array, it **must** be transferred in binary mode, or the file may be corrupted.

Command	Description
http-get	Perform an HTTP file download. This is the preferred method of downloading files for XMS Cloud. FORMAT: **http-get [no-cert-check] <url> [<local_file>]** **no-cert-check** causes the array to download the file even if the SSL certificate is invalid, expired, or not signed by a recognized CA **<url>** is a standard HTTP URL, e.g. https://file.example.com:8080/mydir/myfile.ext. ● **http://** or **https://** may be omitted, in which case HTTP is assumed **<local_file>** is an optional parameter that describes the path and name where the file should be saved ● if no local_file is specified, the file will be saved in the root of the flash storage ● the local_file does support specifying a directory, which will be created if it doesn't already exist
list	List the contents of a file. FORMAT: **file list [filename]**

Command	Description
remote-config	When the Array boots up, it fetches the specified configuration file from the TFTP server defined in the **file remote-server** command, and uses this configuration. This must be an Array configuration file with a **.conf** extension. A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your Arrays but don't want to have the same IP address for each Array, you may remove the **ipaddr** line from the file. You can then load the file on each array and the local IP addresses will not change. FORMAT: **file remote-config <config-file.conf>** **Note:** If you enter **file remote-config ?**, the help response suggests possibilities by listing all of the configuration files that are currently in the Array's flash.
remote-image	When the Array boots up, it fetches the named image file from the TFTP server defined in the **file remote-server** command, and upgrades to this file before booting. This must be an Array image file with a **.bin** extension. FORMAT: **file remote-image <image-file.bin>** **Note**: This will happen every time that the Array reboots. If you only want to fetch the remote-image one time be sure to turn off the remote image option after the initial download.
remote-server	Sets up a TFTP server to be used for automated remote update of software image and configuration files when rebooting. FORMAT: **file remote-server A.B.C.D**
rename	Rename a file.

Command	Description
scp	Copy a file to or from a remote system. You may specify the port to use.
tftp	Open a TFTP connection with a remote server. FORMAT: **file tftp host {<hostname> | <ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the Array, it **must** be transferred in binary mode, or the file may be corrupted.

filter

The **filter** command [**MyAP(config-filter)#**] is used to manage protocol filters and filter lists.

Command	Description
add	Add a filter. Details about the air cleaner feature are after the end of this table. FORMAT: **filter add [air-cleaner |name]**
add-list	Add a filter list. FORMAT: **filter add-list [name]**
del	Delete a filter. FORMAT: **filter del [name]**
del-list	Delete a filter list. FORMAT: **filter del-list [name]**
edit	Edit a filter. FORMAT: **filter edit [name type]**
edit-list	Edit a filter list FORMAT: **filter edit-list [name type]**
enable	Enable a filter list. FORMAT: **filter enable**
move	Change a filter priority. FORMAT: **filter move [name priority]**

Command	Description
off	Disable a filter list. FORMAT: **filter off**
on	Enable a filter list. FORMAT: **filter on**
reset	Delete all protocol filters and filter lists. FORMAT: **filter reset**
stateful	Enable or disable stateful filtering (firewall). FORMAT: **Stateful [enable | disable | on |off]**

Air Cleaner

The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. You may select **all** of the air cleaner rules for the greatest effect, or only specific rules, such as **broadcast** or **multicast**, to eliminate only a particular source of traffic. The following options are offered:

```
MyArray(config)# filter add air-cleaner
  all         All air cleaner filters
  arp         Eliminate station to station ARPs over the air
  broadcast   Eliminate broadcast traffic from the air
  dhcp        Eliminate stations serving DHCP addresses from the air
  multicast   Eliminate chatty multicast traffic from the air
  netbios     Eliminate NetBIOS traffic from the air
```

If you select all, the rules shown in Figure 205 are added to the predefined filter list named **Global**. These rules assume that you have station-to-station blocking enabled, that a DHCP server is on the Array's wired connection, and that you want to block most all multicast and all broadcast traffic not vital to normal

operation. If you find that there is a particular type of multicast or broadcast traffic that you want to allow, just add a specific allow filter for it before the deny filter in this list that would normally block it. Add or delete any of the Multicast rules as necessary for a specific site. Remember that the order of the rules is important.

```
MyArray(config)# show filter

Global Filter List
                                                                                                  Set Set
Name                 Type   Layer Protocol Port         Source       Destination           Qos VLAN State
-------------------- ------ ----- -------- ------------ ------------ --------------------- --- ---- -----
Air-cleaner-Arp.1    deny     2   arp      any          iface iap    iface iap                          on
Air-cleaner-Dhcp.1   deny     2   udp      bootps       iface gig    ff:ff:ff:ff:ff:ff/48               on
Air-cleaner-Dhcp.2   deny     2   udp      bootpc-dhcp  iface iap    ff:ff:ff:ff:ff:ff/48               on
Air-cleaner-Nbios.1  deny     2   udp      netbios-ns   any          any                                on
Air-cleaner-Nbios.2  deny     2   udp      netbios-dgm  any          any                                on
Air-cleaner-Nbios.3  deny     2   udp      netbios-ssn  any          any                                on
Air-cleaner-Mcast.1  deny     2   any      any          any          01:00:00:00:00:00/8                off
Air-cleaner-Mcast.2  deny     2   any      any          any          33:00:00:00:00:00/8                off
Air-cleaner-Mcast.3  deny     2   any      any          any          09:00:00:00:00:00/8                off
Air-cleaner-Bcast.1  allow    2   arp      any          any          ff:ff:ff:ff:ff:ff/48               on
Air-cleaner-Bcast.2  allow    2   udp      bootps       any          ff:ff:ff:ff:ff:ff/48               on
Air-cleaner-Bcast.3  allow    2   udp      bootpc-dhcp  any          ff:ff:ff:ff:ff:ff/48               on
Air-cleaner-Bcast.4  allow    2   udp      22610        any          ff:ff:ff:ff:ff:ff/48               on
Air-cleaner-Bcast.5  deny     2   any      any          any          ff:ff:ff:ff:ff:ff/48               on

Stateful filtering: enabled
```

Figure 205. Air Cleaner Filter Rules

Explanations of some sample rules are below.

- **Air-cleaner-Arp.1** blocks ARPs from one client from being transmitted to clients via all of the radios. The station to station block setting doesn't block this traffic, so this filter eliminates this unnecessary traffic.
- **Air-cleaner-Dhcp.1** drops all DHCP client traffic coming in from the gigabit interface. This traffic doesn't need to be transmitted by the radios since there shouldn't be any DHCP server associated to the radios and offering DHCP addresses. For large subnets the DHCP discover/request broadcast traffic can be significant.
- **Air-cleaner-Dhcp.2** drops all DHCP server traffic coming in from the radio interfaces. There should not be any DHCP server associated to the radios. These rogue DHCP servers are blocked from doing any damage with this filter. There have been quite a few cases in public venues like schools and conventions where such traffic is seen.

- **Air-cleaner-Mcast.1** drops all multicast traffic with a destination MAC address starting with 01. This filters out a lot of IP multicast traffic that starts with 224.
- **Air-cleaner-Mcast.2** drops all multicast traffic with a destination MAC address starting with 33. A lot of IPv6 traffic and other multicast traffic is blocked by this filter.
- **Air-cleaner-Mcast.3** drops all multicast traffic with a destination MAC address starting with 09. A lot of Appletalk traffic and other multicast traffic is blocked by this filter. Note that for OSX 10.6.* Snow Leopard no longer supports Appletalk.
- **Air-cleaner-Bcast.1** allows all ARP traffic (other than the traffic that was denied by **Air-cleaner-Arp.1**). This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.4** allows all XRP traffic from Arrays to be received from the wire. This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.5** drops all other broadcast traffic that hasn't previously been explicitly allowed. This filter will catch all UDP broadcast traffic as well as all other known and unknown protocol broadcast traffic.

group

The **group** command [**MyAP(config)# group**] is used to create and configure user groups. User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs. For more information, see "Groups" on page 280.

Command	Description
add	Create a new user group. FORMAT: **group add [group-name]**
del	Delete a user group. FORMAT: **group del [group-name]**
edit	Set parameters values for a group. FORMAT: **group edit [group-name]**
reset	Reset the group. FORMAT: **group reset**

hostname

The **hostname** command [Xirrus_**Wi-Fi_Array(config)# hostname**] is used to change the hostname used by the Array.

Command	Description
hostname	Change the hostname of the Array. FORMAT: **hostname [name]**

interface

The **interface** command **[MyAP(config)# interface]** is used to select the interface that you want to configure. To see a listing of the commands that are available for each interface, use the **?** command at the selected interface prompt. For example, using the **?** command at the **MyAP(config-gig1}#** prompt displays a listing of all commands for the **gig1** interface.

Command	Description
console	Select the console interface. The console interface is used for management purposes only. FORMAT: **interface console**
gig1	Select the Gigabit 1 interface. FORMAT: **interface gig1**
gig2	Select the Gigabit 2 interface. FORMAT: **interface gig2**
iap	Select an IAP. FORMAT: **interface iap**

load

The **load** command **[MyAP(config)# load]** loads a configuration file.

Command	Description
factory.conf	Load the factory settings configuration file. FORMAT: **load [factory.conf]**

Command	Description
lastboot.conf	Load the configuration file from the last boot-up. FORMAT: **load [lastboot.conf]**
[myfile].conf	If you have saved a configuration, enter its name to load it. FORMAT: **load [myfile.conf]**
saved.conf	Load the configuration file with the last saved settings. FORMAT: **load [saved.conf]**

location

The **location** command [**MyAP(config)# location**] is used to set the location descriptive string for the Array.

Command	Description
<cr>	Set the location for the Array. FORMAT: **location [newlocation]**

location-reporting

The **location-reporting** command **[MyAP(config)# location-reporting]** is used to configure Location Server settings. See also, "Location" on page 184.

Command	Description
cust-key	Set Location Server customer key. FORMAT: **location-reporting cust-key enc <loc-server-customer-key>**
disable	Disable location-reporting. FORMAT: **location-reporting disable**
enable	Enable location-reporting. FORMAT: **location-reporting enable**
period	Set Location Server reporting period (seconds). FORMAT: **location-reporting period <#-seconds>**
url	Set URL of Location Server. FORMAT: **location-reporting url <loc-server-URL>**

management

The **management** command **[MyAP(config)# management]** enters management mode, where you may configure management parameters.

Command	Description
<cr>	Enter management mode. FORMAT: **management <cr>**

The following types of settings may be configured in management mode:

- banner — Configure login banner messages
- console — Configure console management parameters
- https — Enable/disable HTTPS access
- license — Set array software license key
- load — Load running configuration from flash
- max-auth-attempts — Maximum number of authentication (login) attempts (0 means unlimited)
- network-assurance — Enable/disable network assurance
- reauth-period — Time between failed CLI login attempts
- restore — Restore to previous saved config
- revert — Revert to saved configuration after delay if configuration not saved
- save — Save running configuration to flash
- ssh — Enable/disable SSH access
- standby — Configure standby parameters
- telnet — Enable/disable telnet access
- uptime — Display time since last boot
- xircon — Enable/disable Xircon access. See Xircon *User's Guide* for more information.

mdm

The **mdm** command [**MyAP(config)# mdm**] is used to configure Mobile Device Management Server settings. See also, "Mobile" on page 380.

Command	Description
airwatch api	Set Location Server customer key. FORMAT: **mdm airwatch api** The following types of settings may be configured in management mode: • access-error Set AirWatch API access error action • key Set AirWatch API key • password Set AirWatch API password • poll-period Set AirWatch API poll period • timeout Set AirWatch API timeout • url Set AirWatch API URL • username Set AirWatch API username
redirect-url	Set URL to redirect clients to. FORMAT: **mdm airwatch redirect-url <URL-string>**

more

The **more** command [**MyAP(config)# more**] is used to turn terminal pagination ON or OFF.

Command	Description
off	Turn OFF terminal pagination. FORMAT: **more off**
on	Turn ON terminal pagination. FORMAT: **more on**

netflow

The **netflow** command [**MyAP(config-netflow)#**] is used to enable or disable, or configure sending IP flow information (traffic statistics) to the collector you specify.

Command	Description
disable	Disable netflow. FORMAT: **netflow disable**
enable	Enable netflow. FORMAT: **netflow enable**
off	Disable netflow. FORMAT: **netflow off**
on	Enable netflow. FORMAT: **netflow on**
collector	Set the netflow collector IP address or fully qualified domain name (host.domain). Only one collector may be set. If port is not specified, the default is 2055. FORMAT: **netflow collector host {<ip-addr> | <domain>} [port <port#>]**

no

The **no** command [**MyAP(config)# no**] is used to disable a selected element or set the element to its default value.

Command	Description
acl	Disable the Access Control List. FORMAT: **no acl**
dot11a	Disable all 802.11an IAPs (radios). FORMAT: **no dot11a**
dot11bg	Disable all 802.11bgn IAPs (radios). FORMAT: **no dot11bg**
https	Disable https access. FORMAT: **no https**
intrude-detect	Disable intrusion detection. FORMAT: **no intrude-detect**
management	Disable management on all Ethernet interfaces. FORMAT: **no management**
more	Disable terminal pagination. FORMAT: **no more**
ntp	Disable the NTP server. FORMAT: **no ntp**

Command	Description
snmp	Disable SNMP features. FORMAT: **no snmp**
ssh	Disable ssh access. FORMAT: **no ssh**
syslog	Disable the Syslog services. FORMAT: **no syslog**
telnet	Disable Telnet access. FORMAT: **no telnet**
ETH-NAME	Disable the selected Ethernet interface (eth0, gig1 or gig2). You cannot disable the console interface. with this command. FORMAT: **no eth0** (gig1 or gig2)

quick-config

The **quick-config** command is used to apply configuration templates to the Array for typical deployment scenarios.

Command	Description
Classroom	Configure Array for classroom deployment. FORMAT: **quick-config Classroom** Configures the array for use in classroom settings (K-12 schools, Higher education, etc.)
High-density	Configure Array for high density deployment. FORMAT: **quick-config High-density** Configures the array for use in high density settings (lecture halls, convention centers, stadiums, etc.)

quit

The **quit** command [**MyAP(config)# quit**] is used to exit the Command Line Interface.

Command	Description
<cr>	Exit the Command Line Interface. FORMAT: **quit** If you have made any configuration changes and your changes have not been saved, you are prompted to save your changes to Flash. At the prompt, answer **Yes** to save your changes, or answer **No** to discard your changes.

authentication-server

The **radius-server** command [**MyAP(config-authserver)#**] is used to configure the external and internal RADIUS server parameters.

Command	Description
external	Configure an external RADIUS server. FORMAT: **authentication-server external** To configure a RADIUS server (primary, secondary, or accounting server, by IP address or host name), and the reporting interval use: **authentication-server external accounting**
internal	Configure the external RADIUS server. FORMAT: add active directory **authentication-server internal**
use	Choose the active RADIUS server (either external or internal). FORMAT: **authentication-server use external** (or internal)

reboot

The **reboot** command **[MyAP(config)# reboot]** is used to reboot the Array. If you have unsaved changes, the command will notify you and give you a chance to cancel the reboot.

Command	Description
<cr>	Reboot the Array. FORMAT: **reboot**
delay	Reboot the Array after a delay of 1 to 60 seconds. FORMAT: **reboot delay [n]**

reset

The **reset** command **[MyAP(config)# reset]** is used to reset all settings to their default values then reboot the Array.

Command	Description
<cr>	Reset all configuration parameters to their factory default values. FORMAT: **reset** The Array is rebooted automatically.
preserve-ip-settings	Preserve all ethernet and VLAN settings and reset all other configuration parameters to their factory default values. FORMAT: **reset preserve-ip-settings** The Array is rebooted automatically.

restore

The **restore** command [**MyAP(config)# restore**] is used to restore configuration to a version that was previously saved locally.

Command	Description
?	Use this to display the list of available config files. FORMAT: **restore ?**
<filename>	Enter the name of the locally saved configuration to restore. FORMAT: **restore <config-filename>**

roaming-assist

The **roaming-assist** command **[MyAP(config)# roaming-assist]** is used to configure roaming assistance settings. See also, "Roaming Assist" on page 356.

Command	Description
data-rate	Set minimum packet data rate before roaming, in Mbps. FORMAT: **roaming-assist data-rate <1-99>**
devices	Set device types or classes to assist. FORMAT: **roaming-assist devices all | unidentified | DEVICE-CLASS <ID-string> | DEVICE-TYPE <ID-string>**
disable	Disable roaming assist. FORMAT: **roaming-assist disable**
enable	Enable roaming assist. FORMAT: **roaming-assist enable**
period	Set roaming assist backoff period (seconds). FORMAT: **roaming-assist period <#-seconds>**
threshold	Set roaming RSSI threshold in db relative to RSSI of nearest Array. FORMAT: **roaming-assist threshold <-50 to 50>**

run-tests

The **run-tests** command [**MyAP(run-tests)#**] is used to enter run-tests mode, which allows you to perform a range of tests on the Array.

Command	Description
<cr>	Enter run-tests mode. FORMAT: **run-tests**
iperf	Execute iperf utility. FORMAT: **run-tests iperf**
kill-beacons	Turn off beacons for selected single IAP. FORMAT: **run-tests kill-beacons [off | iap-name]**
kill-probe-responses	Turn off probe responses for selected single IAP. FORMAT: **run-tests kill-probe-responses [off | iap-name]**
led	LED test. FORMAT: **run-tests led [flash | rotate]**
memtest	Execute memory tests. FORMAT: **run-tests memtest**
ping	Execute ping utility. FORMAT: **run-tests ping [host-name | ip-addr]**

Command	Description
radius-ping	Special ping utility to test the connection to a RADIUS server. FORMAT: **run-tests radius-ping [external | ssid <ssidnum>] [primary | secondary] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** **run-tests radius-ping [internal | server <radserver> port <radport> secret <radsecret>] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** You may select a RADIUS server that you have already configured (**ssid** or **external** or **internal**) or specify another **server**.
rlb	Run manufacturing radio loopback test. FORMAT: **run-tests rlb {optional command line switches}**
self-test	Execute self-test. FORMAT: **run-tests self-test {logfile-name (optional)]**
site-survey	Enable or disable site survey mode. FORMAT: **run-tests site-survey [on | off | enable | disable]**
ssh	Execute ssh utility. FORMAT: **run-tests ssh [hostname | ip-addr] [command-line-switches (optional)]**
tcpdump	Execute tcpdump utility to dump traffic for selected interface or VLAN. Supports 802.11 headers. FORMAT: **run-tests tcpdump**

Command	Description
telnet	Execute telnet utility. FORMAT: **run-tests telnet [hostname | ip-addr] [command-line-switches (optional)]**
traceroute	Execute traceroute utility. FORMAT: **run-tests traceroute [host-name | ip-addr]**

security

The **security** command **[MyAP(config-security)#]** is used to establish the security parameters for the Array.

Command	Description
wep	Set the WEP encryption parameters. FORMAT: **security wep**
wpa	Set the WEP encryption parameters. FORMAT: **security wpa**

snmp

The **snmp** command [**MyAP(config-snmp)#**] is used to enable, disable, or configure SNMP.

Command	Description
v2	Enable SNMP v2. FORMAT: **snmp v2**
v3	Enable SNMP v3. FORMAT: **snmp v3**
trap	Configure traps for SNMP. Up to four trap destinations may be configured, and you may specify whether to send traps for authentication failure. FORMAT: **snmp trap**

ssid

The **ssid** command [**MyAP(config-ssid)#**] is used to establish your SSID parameters.

Command	Description
add	Add an SSID. FORMAT: **ssid add [newssid]**
del	Delete an SSID. FORMAT: **ssid del [oldssid]**
edit	Edit an existing SSID. FORMAT: **ssid edit [existingssid]**
reset	Delete all SSIDs and restore the default SSID. FORMAT: **ssid reset**

syslog

The **syslog** command [**MyAP(config-syslog)#**] is used to enable, disable, or configure the Syslog server.

Command	Description
console	Enable or disable the display of Syslog messages on the console, and set the level to be displayed. All messages at this level and lower (i.e., more severe) will be displayed. FORMAT: **syslog console [on/off] level [0-7]**
disable	Disable the Syslog server. FORMAT: **syslog disable**
email	Disable the Syslog server. FORMAT: **syslog email from [email-from-address]** **level [0-7]** **password [email-acct-password]** **server [email-server-IPaddr]** **test [test-msg-text]** **to-list [recipient-email-addresses]** **user [email-acct-username]**
enable	Enable the Syslog server. FORMAT: **syslog enable**
local-file	Set the size and/or severity level (all messages at this level and lower will be logged). FORMAT: **syslog local-file size [1-500] level [0-7]**
no	Disable the selected feature. FORMAT: **syslog no [feature]**

Command	Description
off	Disable the Syslog server. FORMAT: **syslog off**
on	Enable the Syslog server. FORMAT: **syslog on**
primary	Set the IP address of the primary Syslog server and/or the severity level of messages to be logged. FORMAT: **syslog primary [1.2.3.4] level [0-7]**
secondary	Set the IP address of the secondary (backup) Syslog server and/or the severity level of messages to be logged. FORMAT: **syslog primary [1.2.3.4] level [0-7]**

tunnel

The **tunnel** command [**MyAP(config-tunnel)#**] is used to establish your tunnel parameters.

Command	Description
add	Add a tunnel. FORMAT: **tunnel add [newtunnel]**
delete	Delete a tunnel. FORMAT: **tunnel delete [oldtunnel]**

Command	Description
edit	Modify an existing tunnel. FORMAT: **tunnel edit [existingtunnel]**
reset	Delete all existing tunnels. FORMAT: **tunnel reset**

uptime

The **uptime** command [**MyAP(config)# uptime**] is used to display the elapsed time since you last rebooted the Array.

Command	Description
<cr>	Display time since last reboot. FORMAT: **uptime**

vlan

The **vlan** command [**MyAP(config-vlan)#**] is used to establish your VLAN parameters.

Command	Description
add	Add a VLAN. FORMAT: **vlan add [newvlan]**
default-route	Assign a VLAN for the default route (for outbound management traffic). FORMAT: **vlan default-route [defaultroute]**

Command	Description
delete	Delete a VLAN. FORMAT: **vlan delete [oldvlan]**
edit	Modify an existing VLAN. FORMAT: **vlan edit [existingvlan]**
native-vlan	Assign a native VLAN (traffic is untagged). FORMAT: **vlan native-vlan [nativevlan]**
no	Disable the selected feature. FORMAT: **vlan no [feature]**
reset	Delete all existing VLANs. FORMAT: **vlan reset**

wifi-tag

The **wifi-tag** command [**MyAP(config-wifi-tag)#**] is used to enable or disable Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channels. See also "Wi-Fi Tag" on page 183.

Command	Description
disable	Disable wifi-tag. FORMAT: **wifi-tag disable**
enable	Enable wifi-tag. FORMAT: **wifi-tag enable**

Command	Description
off	Disable wifi-tag. FORMAT: **wifi-tag off**
on	Enable wifi-tag. FORMAT: **wifi-tag on**
tag-channel-bg	Set an 802.11b or g channel for listening for tags. FORMAT: **wifi-tag tag-channel-bg <1-255>**
udp-port	Set the UDP port which a tagging server will use to query the Array for tagging information. FORMAT: **wifi-tag udp-port <1025-65535>**

Sample Configuration Tasks

This section provides examples of some of the common configuration tasks used with the Wireless Array, including:

- **"Configuring a Simple Open Global SSID" on page 467.**
- **"Configuring a Global SSID using WPA-PEAP" on page 468.**
- **"Configuring an SSID-Specific SSID using WPA-PEAP" on page 469.**
- **"Enabling Global IAPs" on page 470.**
- **"Disabling Global IAPs" on page 471.**
- **"Enabling a Specific IAP" on page 472.**
- **"Disabling a Specific IAP" on page 473.**
- **"Setting Cell Size Auto-Configuration for All IAPs" on page 474**
- **"Setting the Cell Size for All IAPs" on page 475.**
- **"Setting the Cell Size for a Specific IAP" on page 476.**
- **"Configuring VLANs on an Open SSID" on page 477.**
- **"Configuring Radio Assurance Mode (Loopback Tests)" on page 478.**

To facilitate the accurate and timely management of revisions to this section, the examples shown here are presented as screen images taken from a Secure Shell (SSH) session (in this case, PuTTY). Depending on the application you are using to access the Command Line Interface, and how your session is set up (for example, font and screen size), the images presented on your screen may be different than the images shown in this section. However, the data displayed will be the same.

Some of the screen images shown in this section have been modified for clarity. For example, the image may have been "elongated" to show all data without the need for additional images or scrolling. We recommend that you use the Adobe PDF version of this User's Guide when reviewing these examples—a hard copy document may be difficult to read.

As mentioned previously, the root command prompt is determined by the host name assigned to your Array.

Configuring a Simple Open Global SSID

This example shows you how to configure a simple open global SSID.

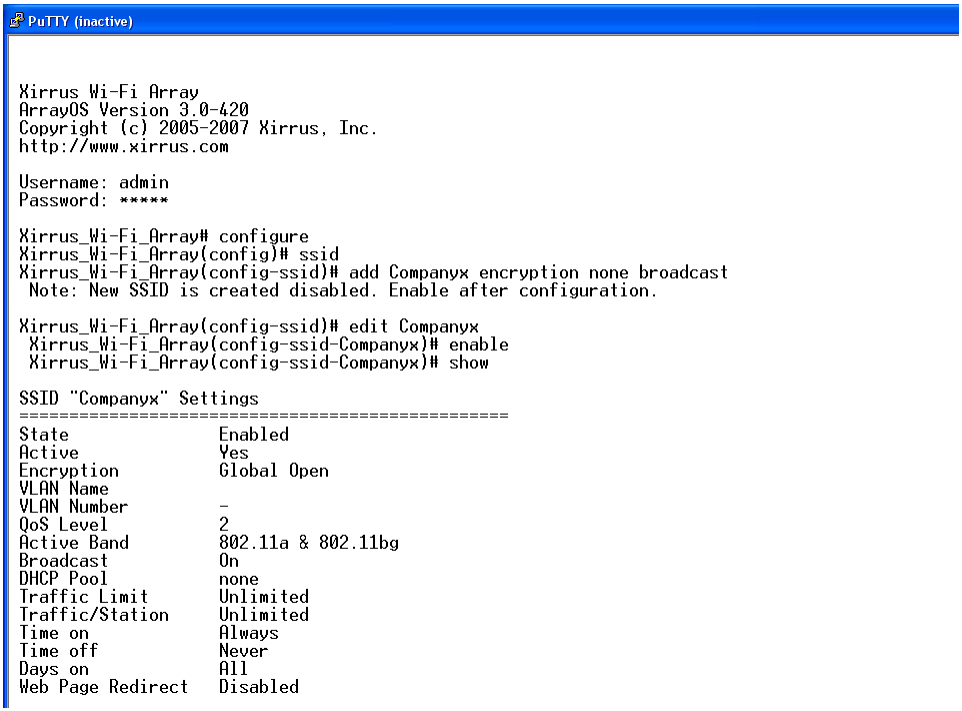


Figure 206. Configuring a Simple Open Global SSID

Configuring a Global SSID using WPA-PEAP

This example shows you how to configure a global SSID using WPA-PEAP encryption in conjunction with the Array's Internal RADIUS server.

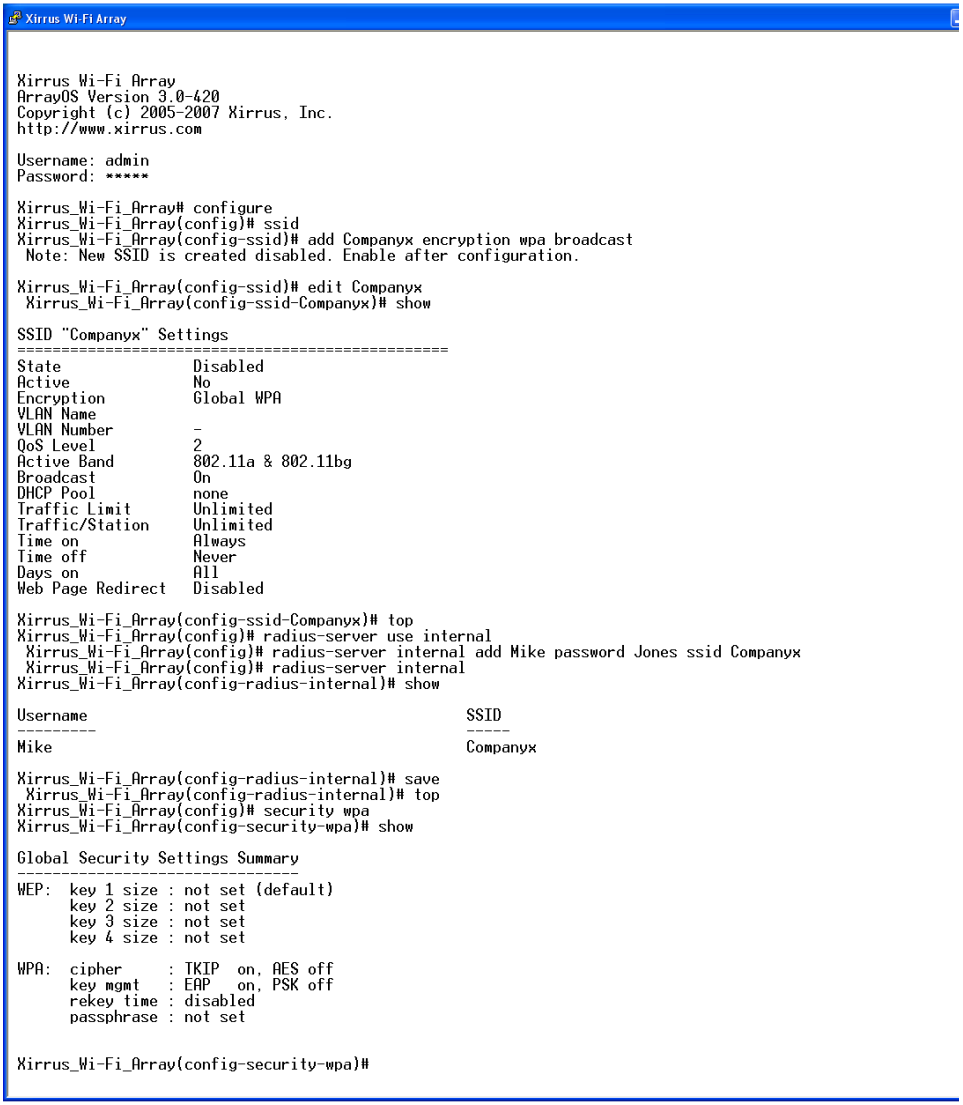


Figure 207. Configuring a Global SSID using WPA-PEAP

Configuring an SSID-Specific SSID using WPA-PEAP

This example shows you how to configure an SSID-specific SSID using WPA-PEAP encryption in conjunction with the Array's Internal RADIUS server.

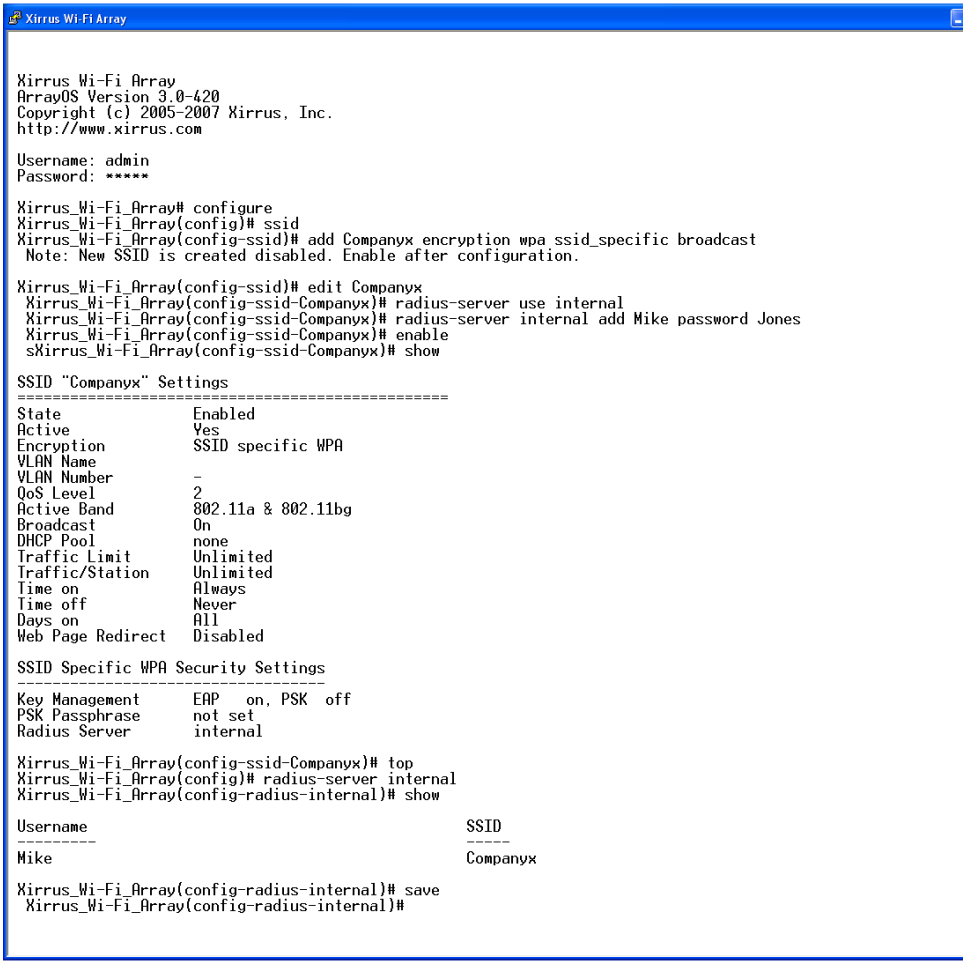
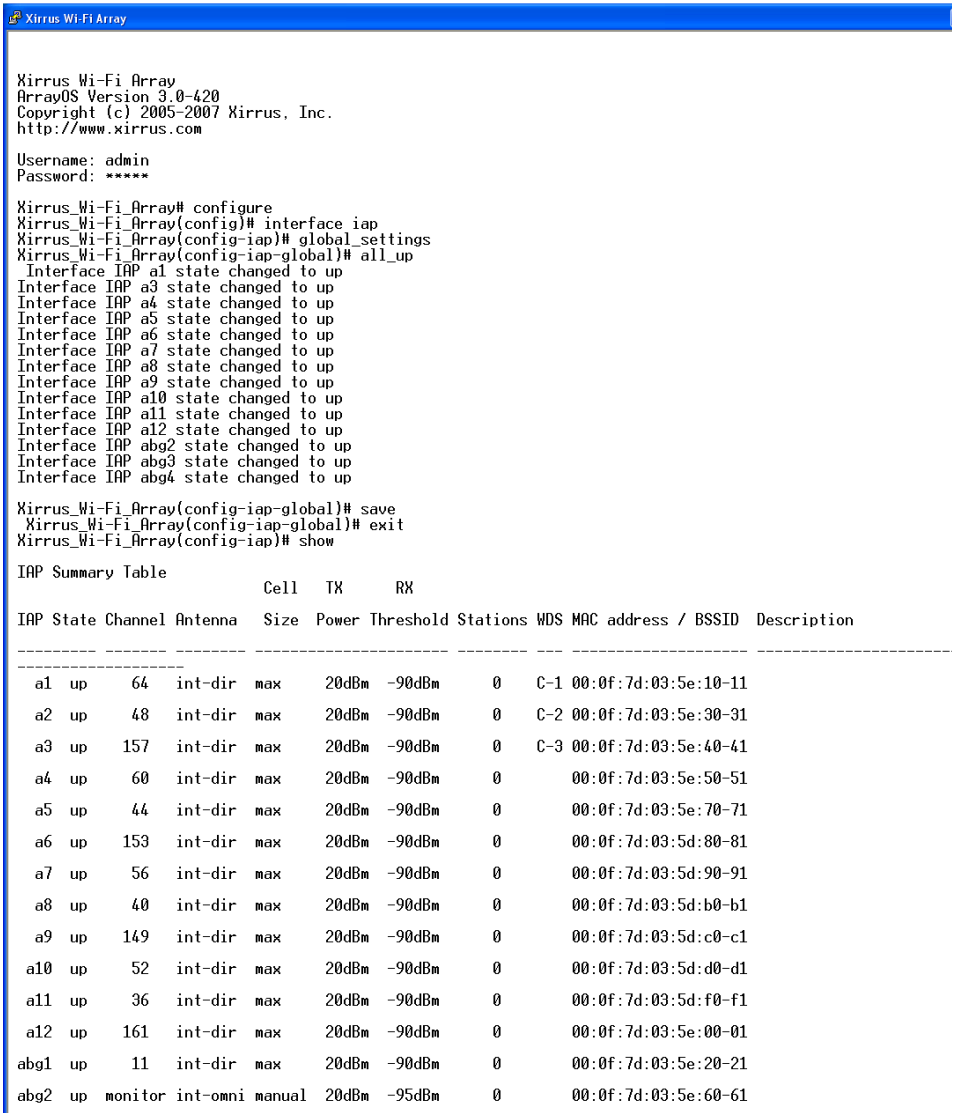


Figure 208. Configuring an SSID-Specific SSID using WPA-PEAP

Enabling Global IAPs

This example shows you how to enable all IAPs (radios), regardless of the wireless technology they use.



```
Xirrus Wi-Fi Array


Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# all_up
 Interface IAP a1 state changed to up
Interface IAP a3 state changed to up
Interface IAP a4 state changed to up
Interface IAP a5 state changed to up
Interface IAP a6 state changed to up
Interface IAP a7 state changed to up
Interface IAP a8 state changed to up
Interface IAP a9 state changed to up
Interface IAP a10 state changed to up
Interface IAP a11 state changed to up
Interface IAP a12 state changed to up
Interface IAP abg2 state changed to up
Interface IAP abg3 state changed to up
Interface IAP abg4 state changed to up

Xirrus_Wi-Fi_Array(config-iap-global)# save
 Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                              Cell   TX      RX

IAP State Channel Antenna     Size  Power Threshold Stations WDS MAC address / BSSID  Description

--------- ------- --------- ---------------------- -------- --- -------------------- -----------------------
-------------------
  a1  up     64   int-dir  max     20dBm  -90dBm      0    C-1 00:0f:7d:03:5e:10-11
  a2  up     48   int-dir  max     20dBm  -90dBm      0    C-2 00:0f:7d:03:5e:30-31
  a3  up    157   int-dir  max     20dBm  -90dBm      0    C-3 00:0f:7d:03:5e:40-41
  a4  up     60   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:50-51
  a5  up     44   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:70-71
  a6  up    153   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:80-81
  a7  up     56   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:90-91
  a8  up     40   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:b0-b1
  a9  up    149   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:c0-c1
 a10  up     52   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:d0-d1
 a11  up     36   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:f0-f1
 a12  up    161   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:00-01
abg1  up     11   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:20-21
abg2  up monitor int-omni manual  20dBm  -95dBm      0        00:0f:7d:03:5e:60-61
```

Figure 209. Enabling Global IAPs

Disabling Global IAPs

This example shows you how to disable all IAPs (radios), regardless of the wireless technology they use.

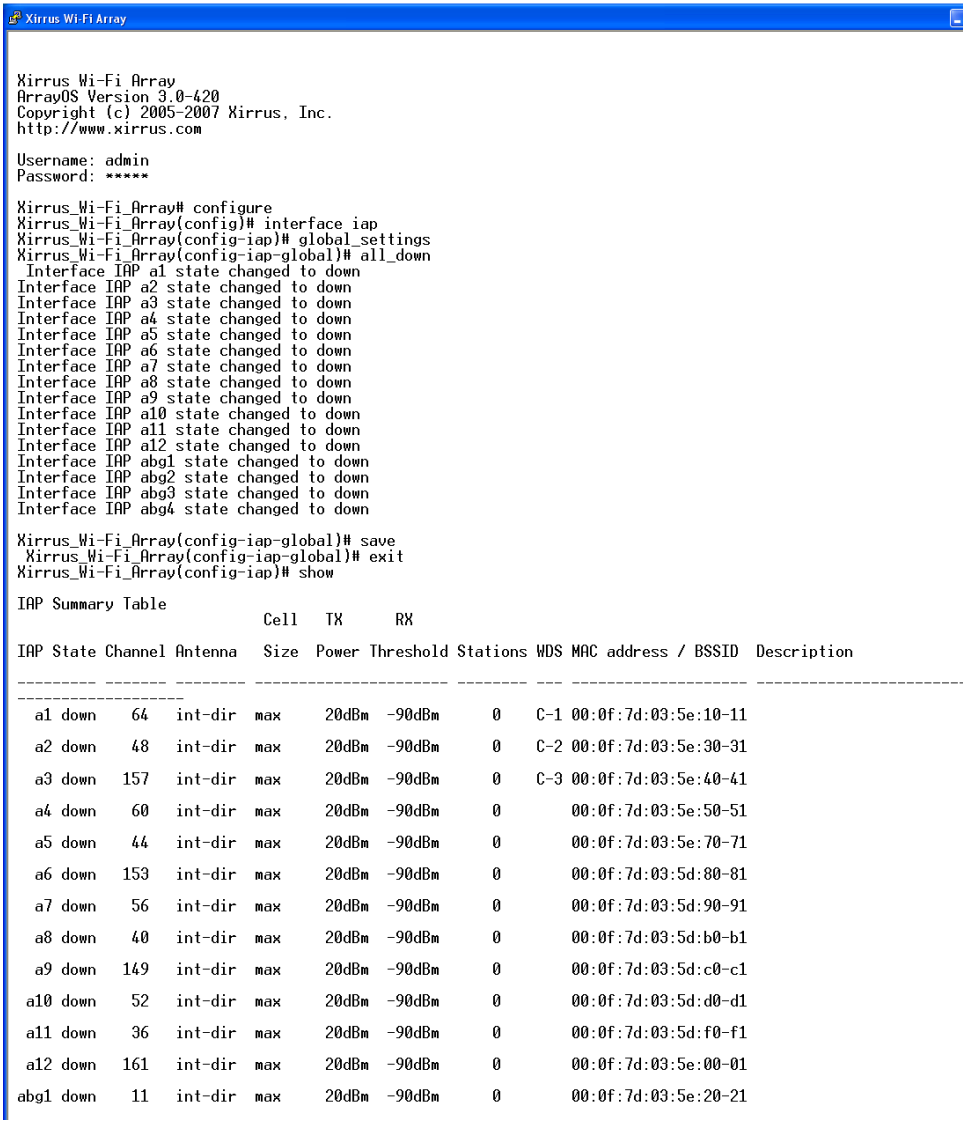
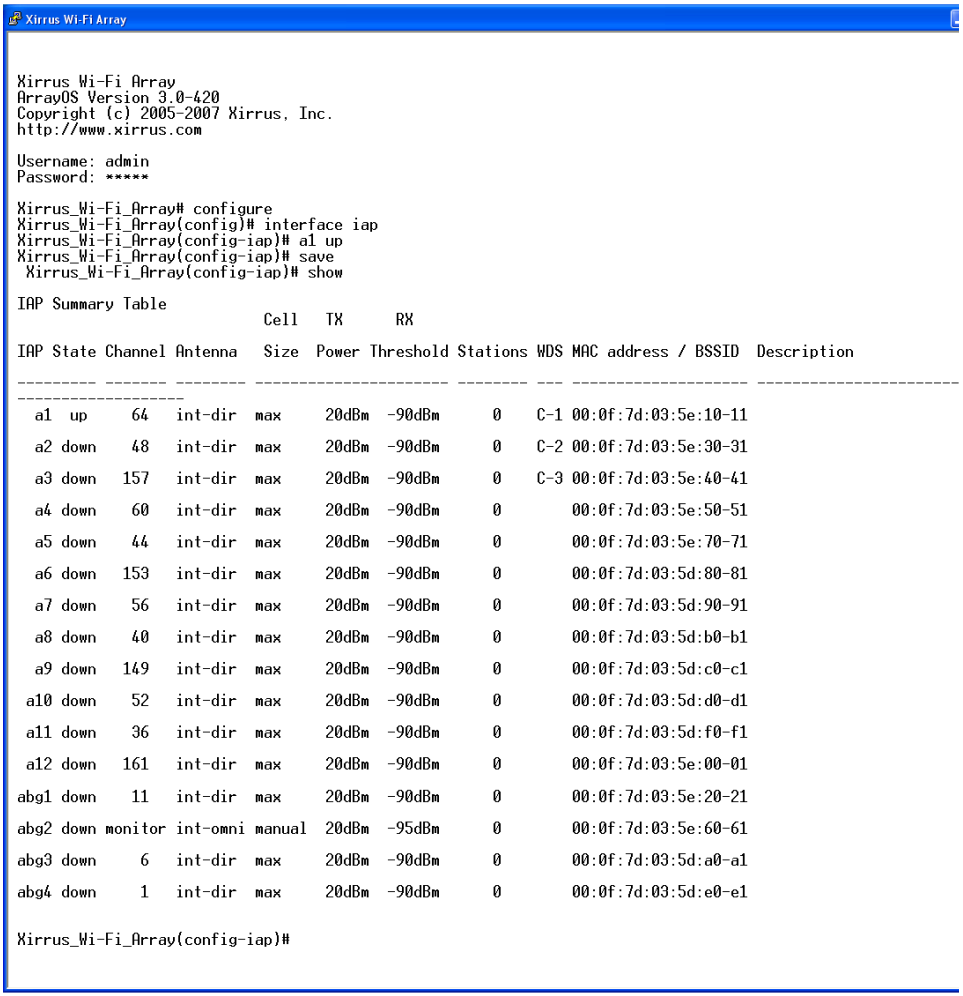


Figure 210. Disabling Global IAPs

Enabling a Specific IAP

This example shows you how to enable a specific IAP (radio). In this example, the IAP that is being enabled is **a1** (the first IAP in the summary list).

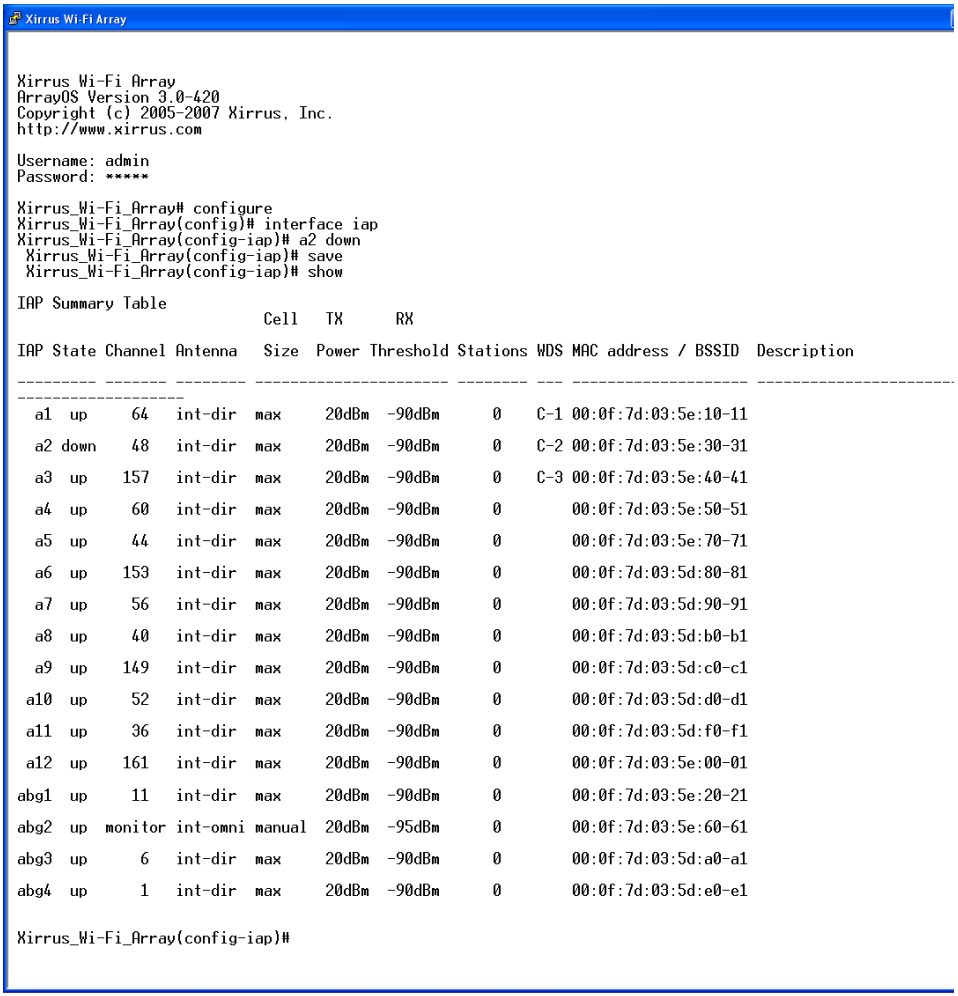


```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a1 up
Xirrus_Wi-Fi_Array(config-iap)# save
 Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                            Cell   TX      RX
IAP State Channel Antenna   Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- -------- ---------------------- -------- --- -------------------- -----------------------
-------------------
  a1  up     64   int-dir  max     20dBm  -90dBm      0    C-1 00:0f:7d:03:5e:10-11
  a2 down    48   int-dir  max     20dBm  -90dBm      0    C-2 00:0f:7d:03:5e:30-31
  a3 down   157   int-dir  max     20dBm  -90dBm      0    C-3 00:0f:7d:03:5e:40-41
  a4 down    60   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:50-51
  a5 down    44   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:70-71
  a6 down   153   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:80-81
  a7 down    56   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:90-91
  a8 down    40   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:b0-b1
  a9 down   149   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:c0-c1
 a10 down    52   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:d0-d1
 a11 down    36   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:f0-f1
 a12 down   161   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:00-01
abg1 down    11   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:20-21
abg2 down monitor int-omni manual  20dBm  -95dBm      0        00:0f:7d:03:5e:60-61
abg3 down     6   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:a0-a1
abg4 down     1   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:e0-e1

Xirrus_Wi-Fi_Array(config-iap)#
```

Figure 211. Enabling a Specific IAP

Disabling a Specific IAP

This example shows you how to disable a specific IAP (radio). In this example, the IAP that is being disabled is **a2** (the second IAP in the summary list).



```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a2 down
 Xirrus_Wi-Fi_Array(config-iap)# save
 Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                            Cell   TX      RX
IAP State Channel Antenna    Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- -------- ---------- -------- --------- --- -------------------- ------------------------
-------------------
  a1  up     64   int-dir  max     20dBm  -90dBm      0    C-1 00:0f:7d:03:5e:10-11
  a2 down    48   int-dir  max     20dBm  -90dBm      0    C-2 00:0f:7d:03:5e:30-31
  a3  up    157   int-dir  max     20dBm  -90dBm      0    C-3 00:0f:7d:03:5e:40-41
  a4  up     60   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:50-51
  a5  up     44   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:70-71
  a6  up    153   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:80-81
  a7  up     56   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:90-91
  a8  up     40   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:b0-b1
  a9  up    149   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:c0-c1
 a10  up     52   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:d0-d1
 a11  up     36   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:f0-f1
 a12  up    161   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:00-01
abg1  up     11   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5e:20-21
abg2  up monitor int-omni manual  20dBm  -95dBm      0        00:0f:7d:03:5e:60-61
abg3  up      6   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:a0-a1
abg4  up      1   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:5d:e0-e1

Xirrus_Wi-Fi_Array(config-iap)#
```

Figure 212. Disabling a Specific IAP

Setting Cell Size Auto-Configuration for All IAPs

This example shows how to set the cell size for all enabled IAPs to be auto-configured (**auto**). (See "Fine Tuning Cell Sizes" on page 33.) The **auto_cell** option may be used with **global_settings**, **global_a_settings**, or **global_bg_settings**. It sets the cell size of the specified IAPs to **auto**, and it launches an auto-configuration to adjust the sizes. Be aware that if the **intrude-detect** feature is enabled on the **monitor** radio**,** its cell size is unaffected by this command. Also, any IAPs used in WDS links are unaffected.

Auto-configuration may be set to run periodically at intervals specified by **auto_cell period** (in seconds) if **period** is non-zero. The percentage of overlap allowed between cells in the cell size computation is specified by **auto_cell overlap** (0 to 100). This example sets auto-configuration to run every 1200 seconds with an allowed overlap of 5%. It sets the cell size of all IAPs to **auto**, and runs a cell size auto-configure operation which completes successfully.

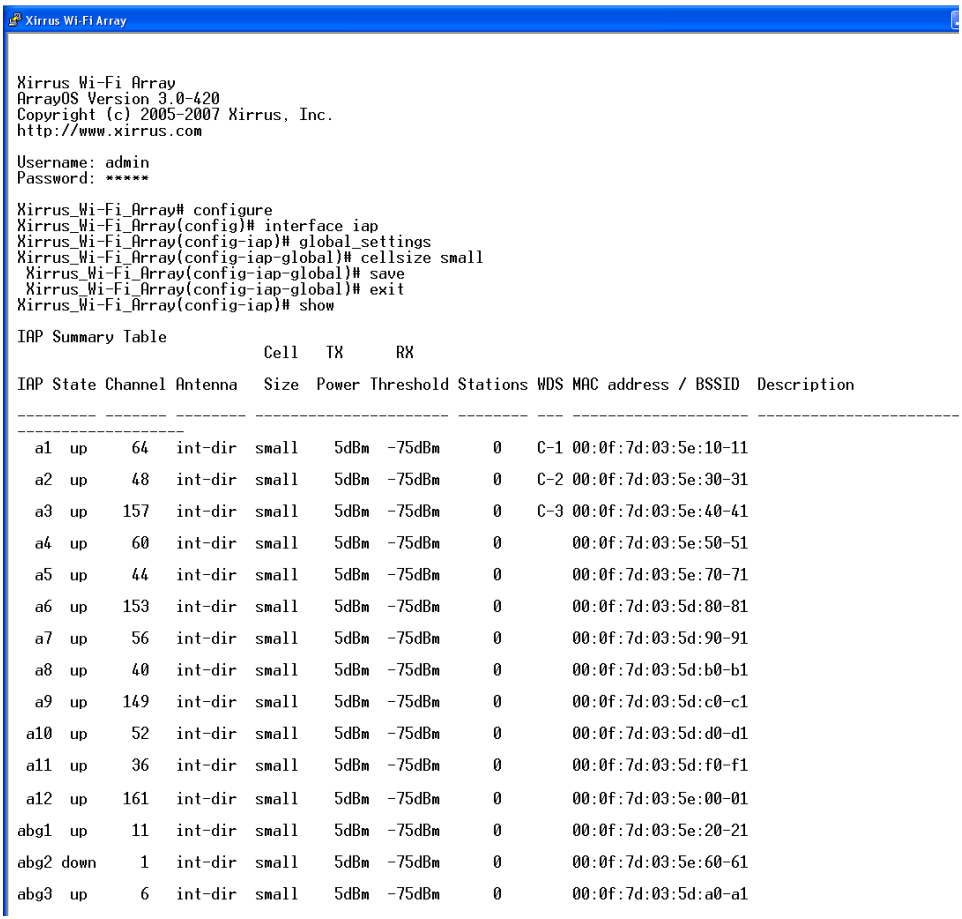
```
192.168.39.125 - PuTTY
Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# auto_cell overlap 5
Xirrus-WiFi-Array(config-iap-global)# auto_cell period 1200
Xirrus-WiFi-Array(config-iap-global)# auto_cell
Auto cell size configuration completed successfully.

Xirrus-WiFi-Array(config-iap-global)# save
Xirrus-WiFi-Array(config-iap-global)# exit
Xirrus-WiFi-Array(config-iap)# show

IAP Summary Table
                                Cell   TX      RX
IAP State Channel Antenna       Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- -------- ---------------------- -------- --- -------------------- ---------------
  a1 down    36   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:10
  a2  up     36   int-dir  auto   -10dBm  -65dBm      0        00:0f:7d:03:c3:30
  a3  up    157   int-dir  auto   -10dBm  -65dBm      0        00:0f:7d:03:c3:40
  a4  up     56   int-dir  auto   -10dBm  -65dBm      0        00:0f:7d:03:c3:50
  a5 down    56   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:70
  a6 down   157   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:80
  a7 down    44   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:90
  a8 down    60   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:b0
  a9  up    153   int-dir  auto   -10dBm  -65dBm      0        00:0f:7d:03:c3:c0
 a10 down    48   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:d0
 a11 down    64   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:f0
 a12 down   161   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:00
abg1 down     1   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:20
abg2  up  monitor int-omni manual  20dBm  -95dBm      0        00:0f:7d:03:c3:60
abg3 down    11   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:a0
abg4 down     6   int-dir  max     20dBm  -90dBm      0        00:0f:7d:03:c3:e0

Xirrus-WiFi-Array(config-iap)#
```

Figure 213. Setting the Cell Size for All IAPs

Setting the Cell Size for All IAPs

This example shows you how to establish the cell size for all IAPs (radios), regardless of the wireless technology they use. Be aware that if the **intrude-detect** feature is enabled on the monitor radio the cell size cannot be set globally—you must first disable the intrude-detect feature on the monitor radio.

In this example, the cell size is being set to **small** for all IAPs. You have the option of setting IAP cell sizes to small, medium, large, or max. See also, "Fine Tuning Cell Sizes" on page 33.



```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# cellsize small
 Xirrus_Wi-Fi_Array(config-iap-global)# save
 Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                                Cell   TX      RX

IAP State Channel Antenna   Size  Power Threshold Stations WDS MAC address / BSSID  Description

--------- ------- -------- ---------------------- -------- --- -------------------- ----------------------
-------------------
  a1  up     64   int-dir  small    5dBm  -75dBm      0    C-1 00:0f:7d:03:5e:10-11

  a2  up     48   int-dir  small    5dBm  -75dBm      0    C-2 00:0f:7d:03:5e:30-31

  a3  up    157   int-dir  small    5dBm  -75dBm      0    C-3 00:0f:7d:03:5e:40-41

  a4  up     60   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5e:50-51

  a5  up     44   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5e:70-71

  a6  up    153   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:80-81

  a7  up     56   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:90-91

  a8  up     40   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:b0-b1

  a9  up    149   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:c0-c1

 a10  up     52   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:d0-d1

 a11  up     36   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:f0-f1

 a12  up    161   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5e:00-01

abg1  up     11   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5e:20-21

abg2 down     1   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5e:60-61

abg3  up      6   int-dir  small    5dBm  -75dBm      0        00:0f:7d:03:5d:a0-a1
```

Figure 214. Setting the Cell Size for All IAPs

Setting the Cell Size for a Specific IAP

This example shows you how to establish the cell size for a specific IAP (radio). In this example, the cell size for **a2** is being set to **medium**. You have the option of setting IAP cell sizes to small, medium, large, or max (the default is max). See also, "Fine Tuning Cell Sizes" on page 33.

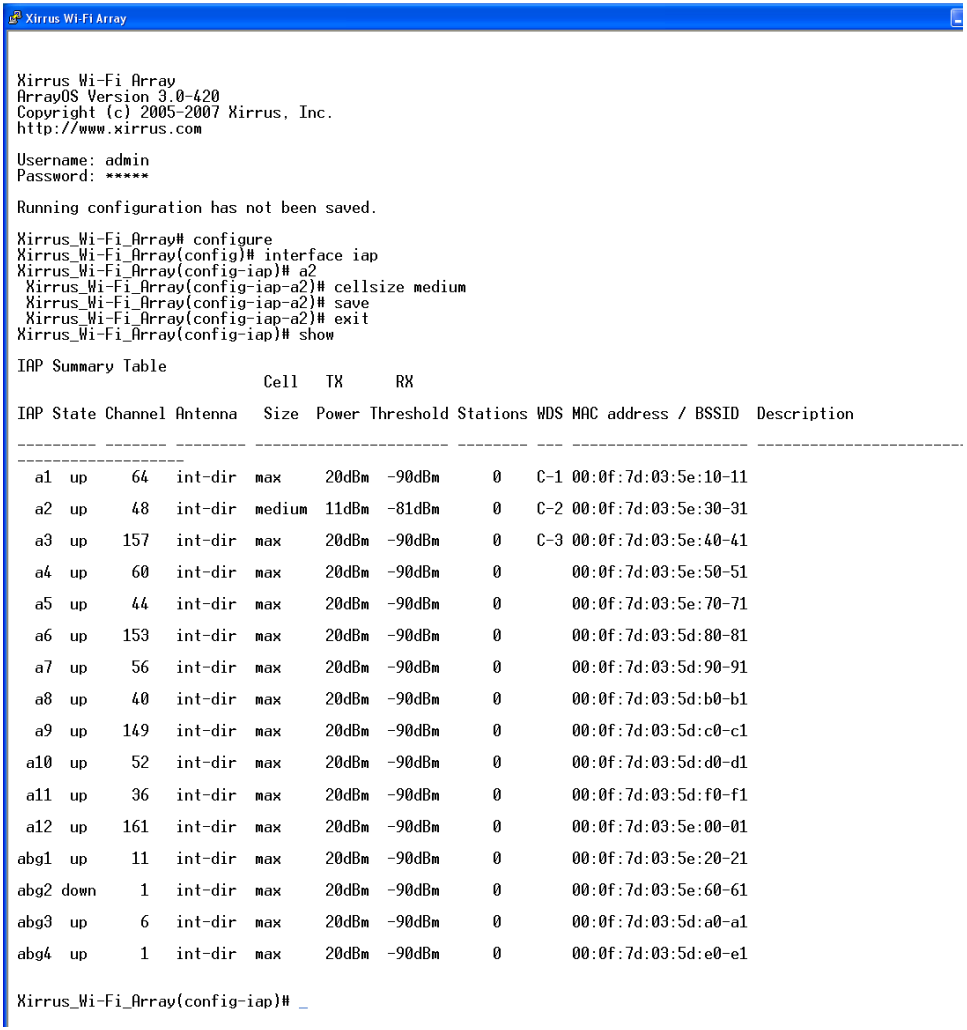
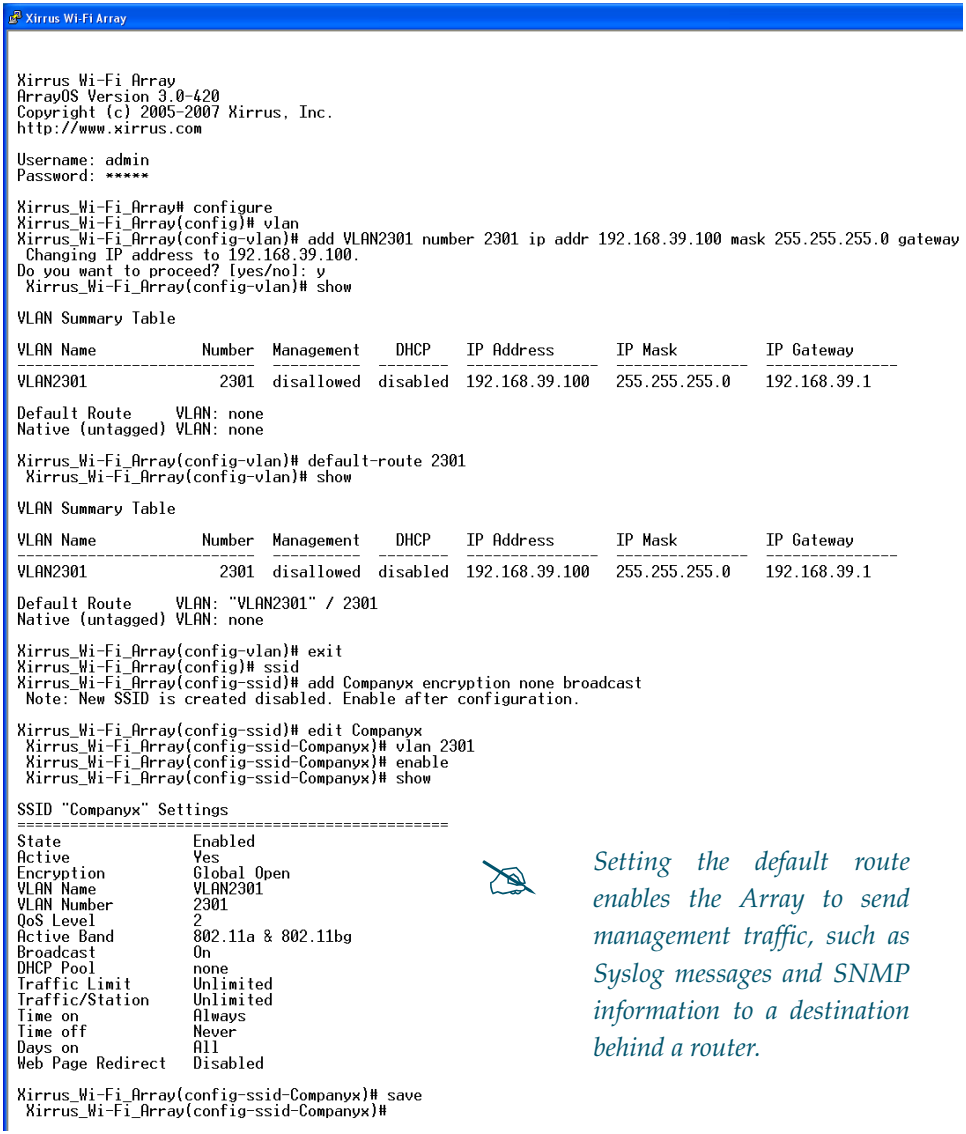


Figure 215. Setting the Cell Size for a Specific IAP

Configuring VLANs on an Open SSID

This example shows you how to configure VLANs on an Open SSID.



```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# vlan
Xirrus_Wi-Fi_Array(config-vlan)# add VLAN2301 number 2301 ip addr 192.168.39.100 mask 255.255.255.0 gateway
 Changing IP address to 192.168.39.100.
Do you want to proceed? [yes/no]: y
 Xirrus_Wi-Fi_Array(config-vlan)# show

VLAN Summary Table

VLAN Name            Number  Management    DHCP    IP Address       IP Mask          IP Gateway
-------------------------  ----------  --------  ---------------  ---------------  ---------------
VLAN2301               2301  disallowed  disabled  192.168.39.100   255.255.255.0    192.168.39.1

Default Route     VLAN: none
Native (untagged) VLAN: none

Xirrus_Wi-Fi_Array(config-vlan)# default-route 2301
 Xirrus_Wi-Fi_Array(config-vlan)# show

VLAN Summary Table

VLAN Name            Number  Management    DHCP    IP Address       IP Mask          IP Gateway
-------------------------  ----------  --------  ---------------  ---------------  ---------------
VLAN2301               2301  disallowed  disabled  192.168.39.100   255.255.255.0    192.168.39.1

Default Route     VLAN: "VLAN2301" / 2301
Native (untagged) VLAN: none

Xirrus_Wi-Fi_Array(config-vlan)# exit
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption none broadcast
 Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# vlan 2301
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
================================================
State               Enabled
Active              Yes
Encryption          Global Open
VLAN Name           VLAN2301
VLAN Number         2301
QoS Level           2
Active Band         802.11a & 802.11bg
Broadcast           On
DHCP Pool           none
Traffic Limit       Unlimited
Traffic/Station     Unlimited
Time on             Always
Time off            Never
Days on             All
Web Page Redirect   Disabled

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# save
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)#
```

Setting the default route enables the Array to send management traffic, such as Syslog messages and SNMP information to a destination behind a router.

Figure 216. Configuring VLANs on an Open SSID

Configuring Radio Assurance Mode (Loopback Tests)

The Array uses its built-in monitor radio to monitor other radios in the Array. Tests include sending probes on all channels and checking for a response, and checking whether beacons are received from the other radio. If a problem is detected, corrective actions are taken to recover. Loopback mode operation is described in detail in "Array Monitor and Radio Assurance Capabilities" on page 500.

The following actions may be configured:

- **alert-only**—the Array will issue an alert in the Syslog.
- **repair-without-reboot**—the Array will issue an alert and reset radios at the Physical Layer (Layer 1) and possibly at the MAC layer. The reset should not be noticed by users, and they will not need to reassociate.
- **reboot-allowed**—the Array will issue an alert, reset the radios, and schedule the Array to reboot at midnight (per local Array time) if necessary. All stations will need to reassociate to the Array.
- **off**—Disable IAP loopback tests (no self-monitoring occurs). Radio Assurance mode is off by default.

This is a global IAPs setting—the monitor radio will monitor all other radios according to the settings above, and it cannot be set up to monitor particular radios. Radio assurance mode requires Intrusion Detection to be set to Standard.

The following example shows you how to configure a loopback test.

```
192.168.39.125 - PuTTY

Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# intrude-detect standard
Interface IAP abg2 state changed to down
Interface IAP abg2 band changed to monitor
Interface IAP abg2 channel changed to monitor
Interface IAP abg2 antenna changed to internal omni
Interface IAP abg2 tx-power changed to 20
Interface IAP abg2 rx-threshold changed to -95
Interface IAP abg2 state changed to up

Xirrus-WiFi-Array(config-iap-global)# loopback-test
  alert-only             Enable  IAP loopback tests with failure alerts only
  off                    Disable IAP loopback tests
  reboot-allowed         Enable  IAP loopback tests with alerts & repairs & reboots if n
  repair-without-reboot  Enable  IAP loopback tests with alerts & repairs, but no reboot
  <cr>                   Set global IAP parameters

Xirrus-WiFi-Array(config-iap-global)# loopback-test repair-without-reboot
Xirrus-WiFi-Array(config-iap-global)#
Xirrus-WiFi-Array(config-iap-global)# show

Global IAP Settings Summary
---------------------------
Country code         not set (defaults to US: United States)
Beacon interval      100 Kusec
Broadcast rates      standard
DTIM period          1 beacon
Short retries        7
Long  retries        4
Total IAPs           16
Max stations/IAP     64
Max phones  /IAP     16
Station timeout      1000 sec
Station reauth time  5 sec
Management           disallowed
Station to station   forward
Load balancing       off
Intrusion detection  standard
Auto chan power up   off
Auto chan schedule   none
Auto cell period     1200 sec
Auto cell overlap    5%
Xirrus Fast Roaming  via tunnels to arrays in-range or targeted
Sharp cell TX power  off
Public Safety Band   disabled
802.11h support      on
Loopback test mode   repair w/o reboot
LED activity         on when IAP up
                     blink on data frame transmitted
                     blink on data frame received
                     blink on management frame transmitted
                     blink on management frame received
                     blink heartbeat on station associated

Xirrus-WiFi-Array(config-iap-global)#
Do you want to save changes to flash [yes/no]:
```

Figure 217. Configuring Radio Assurance Mode (Loopback Testing)

Appendices

Page is intentionally blank

Appendix A: Quick Reference Guide

This section contains product reference information. Use this section to locate the information you need quickly and efficiently. Topics include:

- **"Factory Default Settings" on page 483**.
- **"Keyboard Shortcuts" on page 489**.

Factory Default Settings

The following tables show the Wireless Array's factory default settings.

Host Name

Setting	Default Value
Host name	Serial Number (e.g., XR4012802207C

Network Interfaces

Serial

Setting	Default Value
Baud Rate	115200
Word Size	8 bits
Stop Bits	1
Parity	No parity
Time Out	10 seconds

Gigabit 1 and Gigabit 2

Setting	Default Value
Enabled	Yes
DHCP	Yes
Default IP Address	10.0.2.1
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1500
Management Enabled	Yes

Server Settings

NTP

Setting	Default Value
Enabled	No
Primary	time.nist.gov
Secondary	pool.ntp.org

Syslog

Setting	Default Value
Enabled	Yes

Setting	Default Value
Local Syslog Level	Information
Maximum Internal Records	500
Primary Server	None
Primary Syslog Level	Information
Secondary Server	None
Secondary Syslog Level	Information

SNMP

Setting	Default Value
Enabled	Yes
Read-Only Community String	xirrus_read_only
Read-Write Community String	xirrus
Trap Host	null (no setting)
Trap Port	162
Authorization Fail Port	On

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes
IP Start Range	192.168.1.2
IP End Range	192.168.1.254

Setting	Default Value
NAT	Disabled
IP Gateway	None
DNS Domain	None
DNS Server (1 to 3)	None

Default SSID

Setting	Default Value
ID	xirrus
VLAN	None
Encryption	Off
Encryption Type	None
QoS	2
Enabled	Yes
Broadcast	On

Security

Global Settings - Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)
WEP Key Length	null (all 4 keys)
Default Key ID	1

Setting	Default Value
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	Yes
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	Disabled

External RADIUS (Global)

Setting	Default Value
Enabled	Yes
Primary Server	None
Primary Port	1812
Primary Secret	xirrus
Secondary Server	null (no IP address)
Secondary Port	1812
Secondary Secret	null (no secret)
Time Out (before primary server is retired)	600 seconds
Accounting	Disabled
Interval	300 seconds
Primary Server	None
Primary Port	1813

Setting	Default Value
Primary Secret	null (no secret)
Secondary Server	None
Secondary Port	1813
Secondary Secret	null (no secret)

Internal RADIUS

Setting	Default Value
Enabled	No
The user database is cleared upon reset to the factory defaults. For the Internal RADIUS Server you have a maximum of 1,000 entries.	

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
SSH	On
SSH timeout	300 seconds
Telnet	Off
Telnet timeout	300 seconds

Setting	Default Value
Serial	On
Serial timeout	300 seconds
Management over IAPs	Off
http timeout	300 seconds

Keyboard Shortcuts

The following table shows the most common keyboard shortcuts used by the Command Line Interface.

Action	Shortcut
Cut selected data and place it on the clipboard.	**Ctrl + X**
Copy selected data to the clipboard.	**Ctrl + C**
Paste data from the clipboard into a document (at the insertion point).	**Ctrl + V**
Go to top of screen.	**Ctrl + Z**
Copy the active window to the clipboard.	**Alt + Print Screen**
Copy the entire desktop image to the clipboard.	**Print Screen**
Abort an action at any time.	**Esc**
Go back to the previous screen.	**b**
Access the Help screen.	**?**

Appendix B: FAQ and Special Topics

This appendix provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all topics below and try to determine if your problem resides with the Wireless Array or your network infrastructure. Topics include:

- **"General Hints and Tips" on page 491**
- **"Frequently Asked Questions" on page 492**
- **"Array Monitor and Radio Assurance Capabilities" on page 500**
- **"RADIUS Vendor Specific Attribute (VSA) for Xirrus" on page 503**
- **"Location Service Data Formats" on page 504**
- **"Upgrading the Array via CLI" on page 506**

General Hints and Tips

This section provides some useful tips that will optimize the reliability and performance of your Wireless Arrays.

- The Wireless Array requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.
- If using multiple Arrays in the same area, maintain a distance of at least 100 feet (30m) between Arrays if there is direct line-of-sight between the units, or at least 50 feet (15 m) if a wall or other barrier exists between the units.
- Keep the Wireless Array away from electrical devices or appliances that generate RF noise. Because the Array is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).
- If you are deploying multiple units, the Array should be oriented so that the monitor radio is oriented in the direction of the least required coverage, because when in monitor mode the radio does not function as an AP servicing stations.

- The Wireless Array should only be used with Wi-Fi certified client devices.

See Also

Multiple SSIDs
Security
VLAN Support

Frequently Asked Questions

This section answers some of the most frequently asked questions, organized by functional area.

Multiple SSIDs

Q. What Are BSSIDs and SSIDs?

A. BSSID (Basic Service Set Identifier) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS.

A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS by way of a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or "wireless network name") identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. Xirrus Wireless Arrays support the ability for multiple SSIDs to be defined and used simultaneously.

Q. What would I use SSIDs for?

A. The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- Minimum security required to join this SSID.
- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another SSID named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest possible Quality of Service (QoS) definition. This type of SSID might also forward traffic to specific VLANs on the wired network.

Q. How do I set up SSIDs?

A. Use the following procedure as a guideline. For more detailed information, go to "SSIDs" on page 254.

1. From the Web Management Interface, go to the SSID Management page.
2. Select **Yes** to make the SSID visible to all clients on the network. Although the Wireless Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
3. Select the minimum security that will be required by users for this SSID.
4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.
5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.

6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.
7. Click on the **Save** button if you wish to make your changes permanent.
8. If you need to edit any of the SSID settings, you can do so from the SSID Management page.

See Also

General Hints and Tips
Security
SSIDs
SSID Management
VLAN Support

Security

Q. How do I know my management session is secure?

A. Follow these guidelines:

- Administrator passwords
  Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.
- SSH versus Telnet
  Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY. The Array only allows SSH-2 connections, so your SSH utility must be set up to use SSH-2.

- Configuration auditing
  Do not change approved configuration settings. The optional Xirrus Management System (XMS) offers powerful management features for small or large Wireless Array deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.

Q. Which wireless data encryption method should I use?

A. Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The Wireless Array allows you to establish the following data encryption configuration options:

- Open
  This option offers no data encryption and is **not recommended**, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.

- WEP (Wired Equivalent Privacy)
  This option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.

- WPA (Wi-Fi Protected Access)
  This is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

  TKIP solves security issues with WEP. It also allows you to establish encryption keys on a per-user-basis, with key rotation for added security. In addition, TKIP provides Message Integrity Check (MIC) functionality and prevents active attacks on the wireless network.

  AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on

older wireless clients). Because AES is the strongest encryption standard currently available, it is highly recommended for Enterprise networks.

Any of the above encryption modes can be used (and can be used at the same time).

TKIP encryption does not support high throughput rates, per the IEEE 802.11n.

Q. Which user authentication method should I use?

A. User authentication ensures that users are who they say they are. For example, the most obvious example of authentication is logging in with a user name and password. The Wireless Array allows you to choose between the following user authentication methods:

- Pre-Shared Key
  Users must manually enter a key (pass phrase) on the client side of the wireless network that matches the key stored by the administrator in your Wireless Arrays.

- RADIUS 802.1x with EAP
  802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal (provided by the Wireless Array) or external. An external RADIUS server offers more functionality and is **recommended** for large Enterprise deployments.

  When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

- MAC Address ACLs (Access Control Lists)
  MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited

number of users—in this case, enter the MAC addresses of each user in the **Allow** list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the **Deny** list.

Q. Why do I need to authenticate my Wireless Array units?

A. When deploying multiple Wireless Arrays, you may need to define which units are part of which wireless network (for example, if you are establishing more than one network). In this case, you need to employ the Xirrus Management System (XMS) which can authenticate your Arrays automatically and ensure that only authorized units are associated with the defined wireless network.

Q. What is rogue AP (Access Point) detection?

A. The Wireless Array has integrated monitor capabilities, which can constantly scan the local wireless environment for rogue APs (non-Xirrus devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

See Also

General Hints and Tips
Multiple SSIDs
VLAN Support

VLAN Support

Q. What Are VLANs?

A. VLANs (Virtual Local Area Networks) are a logical grouping of network devices that share a common network broadcast domain. Members of a particular VLAN can be on any segment of the physical network but logically only members of a particular VLAN can see each other.

VLANs are defined and implemented using the wired network switches that are VLAN capable. Packets are tagged for transmission on a particular VLAN according to the IEEE 802.1Q standard, with VLAN switches processing packets according to the tag.

Q. What would I use VLANs for?

A. Logically separating different types of users, systems, applications, or other logical division aids in performance and management of different network devices. Different VLANs can also be assigned with different packet priorities to prioritize packets from one VLAN over packets from another VLAN.

VLANs are managed by software settings—instead of physically plugging in and moving network cables and users—which helps to ease network management tasks.

Q. What are Wireless VLANs?

A. Wireless VLANs allow similar functionality to the wired VLAN definitions and extend the operation of wired VLANs to the wireless side of the network.

Wireless VLANs can be mapped to wireless SSIDs so that traffic from wired VLANs can be sent to wireless users of a particular SSID. The reverse is also true, where wireless traffic originating from a particular SSID can be tagged for transmission on a particular wired VLAN.

Sixteen SSIDs can be defined on your Wireless Array, allowing a total of sixteen VLANs to be accessed (one per SSID).

As an example, to provide guest user access an SSID of **guest** might be created. This SSID could be mapped to a wired VLAN that segregates unknown users from the rest of the wired network and restricts them to Internet access only. Wireless users could then associate to the wireless network via the **guest** SSID and obtain access to the Internet through the selected VLAN, but would be unable to access other privileged network resources.

See Also

General Hints and Tips
Multiple SSIDs
Security

Array Monitor and Radio Assurance Capabilities

All models of the Wireless Array have integrated monitoring capabilities to check that the Array's radios are functioning correctly, and act as a threat sensor to detect and prevent intrusion from rogue access points.

Enabling Monitoring on the Array

Any radio may be set to monitor the Array or to be a normal IAP radio. In order to enable the functions required for intrusion detection and for monitoring the other Array radios, you **must** configure one monitor radio on the IAP Settings window as follows:

- Check the **Enabled** checkbox.
- Set **Mode** to **Monitor**.
- Set **Channel** to **Monitor**.

The settings above will automatically set the **Antenna** selection to **Internal-Omni**., also required for monitoring. See the "IAP Settings" on page 290 for more details. The values above are the factory default settings for the Array.

How Monitoring Works

When the monitor radio has been configured as just described, it performs these steps continuously (24/7) to check the other radios on the Array and detect possible intrusions:

1. The monitor radio scans all channels with a 200ms dwell time, hitting all channels about once every 10 seconds.
2. Each time it tunes to a new channel it sends out a probe request in an attempt to smoke out rogues.
3. It then listens for all probe responses and beacons to detect any rogues within earshot.
4. Array radios respond to that probe request with a probe response.

Intrusion Detection is enabled or disabled separately from monitoring. See Step 1 in "Advanced RF Settings" on page 333.

Radio Assurance

The Array is capable of performing continuous, comprehensive tests on its radios to assure that they are operating properly. Testing is enabled using the **Radio Assurance Mode** setting on the Advanced RF Settings window (Step 2 in "Advanced RF Settings" on page 333). When this mode is enabled, the monitor radio performs loopback tests on the Array. Radio Assurance Mode requires **Intrusion Detection** to be set to **Standard** (See Step 1 in "Advanced RF Settings" on page 333).

When **Radio Assurance Mode** is enabled:

1. The Array keeps track of whether or not it hears beacons and probe responses from the Array's radios.
2. After 10 minutes (roughly 60 passes on a particular channel by the monitor radio), if it has not heard beacons or probe responses from one of the Array's radios it issues an alert in the Syslog. If repair is allowed (see "Radio Assurance Options" on page 502), the Array will reset and reprogram that particular radio at the Physical Layer (PHY—Layer 1). This action takes under 100ms and stations are not deauthenticated, thus users should not be impacted.
3. After another 10 minutes (roughly another 60 passes), if the monitor still has not heard beacons or probe responses from the malfunctioning radio it will again issue an alert in the Syslog. If repair is allowed, the Array will reset and reprogram the MAC (the lower sublayer of the Data Link Layer) and then all of the PHYs. This is a global action that affects all radios. This action takes roughly 300ms and stations are not deauthenticated, thus users should not be impacted.
4. After another 10 minutes, if the monitor still has not heard beacons or probe responses from that radio, it will again syslog the issue. If reboot is allowed (see "Radio Assurance Options" on page 502), the Array will schedule a reboot. This reboot will occur at one of the following times, whichever occurs first:
   - When no stations are associated to the Array
   - Midnight

Radio Assurance Options

If the monitor detects a problem with an Array radio as described above, it will take action according to the preference that you have specified in the **Radio Assurance Mode** setting on the Advanced RF Settings window (see Step 2 page 335):

- **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
- **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of the PHY and MAC as described above.
- **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets of the PHY and MAC, and schedule reboots as described above.
- **Disabled**—Disable IAP loopback tests (no self-monitoring occurs). Loopback tests are disabled by default.

RADIUS Vendor Specific Attribute (VSA) for Xirrus

A RADIUS VSA is defined for Xirrus Arrays to control administrator privileges settings for user accounts. The RADIUS VSA is used by Arrays to define the following attribute for administrator accounts:

- **Array administrators**—the **Xirrus-Admin-Role** attribute sets the privilege level for this account. Set the value to the string defined in **Privilege Level Name** as described in "About Creating Admin Accounts on the RADIUS Server" on page 223.

Location Service Data Formats

Xirrus Arrays are able to capture and upload visitor analytics data, acting as a sensor network in addition to providing wireless connectivity. This data is sent to the location server in different formats, based on the type of server. The **Location Server URL**, **Location Customer Key**, and **Location Period** for reporting data are configured under Location settings. See "Location" on page 184 for details. If a **Location Customer Key** has been entered, data is sent encrypted using AES with that key.

Euclid Location Server

If the **Location Server URL** contains the string **euclid**, then it specifies a Euclid server. Data is sent at the specified intervals, in the proprietary format expected by the Euclid location server.

Non-Euclid Location Server

If the **Location Server URL** doesn't contain the string "euclid", then data is sent as a JSON object at the specified intervals, with the following fields.

Field			Name	Description
ln			Location Name	Array location string
ld			Location Data	Defined below
	vn		Version Number	Set to 1
	ma		MAC Address	Base IAP MAC Address
	mc		Message Count	Running message count (resets to 0 when array is rebooted)
	lt		Location Table	Table of Stations and APs heard during this window
		si	Station ID	Station MAC address (AES encrypted if cust-key is not blank)
		bi	BSSID	BSSID station is on (AES encrypted if cust-key is not blank)

Field			Name	Description
		ap	AP Flag	1=AP, 0=Station
		cn	Count	Count of frames heard from device during this window
		ot	Origin Time	Timestamp of first frame in this window (Unix time in seconds)
		ct	Current Time	Timestamp of last frame in this window (Unix time in seconds)
		cf	Current Frequency	Frequency (MHz) last frame was heard on
		il	Interval Low	Minimum interval between frames (within 24 hr period)
		ih	Interval High	Maximum interval between frames (within 24 hr period)
		sl	Signal Low	Minimum signal strength (within 24 hr period)
		sh	Signal High	Maximum signal strength (within 24 hr period)
		so	Signal Origin	Signal strength of first frame heard
		sc	Signal Current	Signal strength of last frame heard

Upgrading the Array via CLI

If you are experiencing difficulties communicating with the Array using the Web Management Interface, the Array provides lower-level facilities that may be used to accomplish an upgrade via the CLI and the Xirrus Boot Loader (XBL).

1. Download the latest software update from the Xirrus FTP site using your Enhanced Care FTP username and password. If you do not have an FTP username and password, contact Xirrus Customer Service for assistance (support@xirrus.com). The software update is provided as a zip file. Unzip the contents to a local temp directory. Take note of the extracted file name in case you need it later on—you may also need to copy this file elsewhere on the network depending on your situation.

2. Install a TFTP server software package if you don't have one running. It may be installed on any PC on your network, including your desktop or laptop. The Solar Winds version is freeware and works well.

   http://support.solarwinds.net/updates/New-customerFree.cfm?ProdId=52

   The TFTP install process creates the **TFTP-Root** directory on your C: drive, which is the default target for sending and receiving files. This may be changed if desired. This directory is where you will place the extracted Xirrus software update file(s). If you install the TFTP server on the same computer to which you extracted the file, you may change the TFTP directory to C:\xirrus if desired.

   You must make the following change to the default configuration of the Solar Winds TFTP server. In the **File/Configure** menu, select **Security**, then select **Transmit only** and click **OK**.

3. Determine the IP address of the computer hosting the TFTP server. (To display the IP address, open a command prompt and type **ipconfig**)

4. Connect your Array to the computer running TFTP using a serial cable, and open a terminal program if you haven't already. Attach a network cable to the Array's GIG1 port, if it is not already part of your network.

Boot your Array and watch the progress messages. When **Press space bar to exit to bootloader:** is displayed, press the space bar. The rest of this procedure is performed using the bootloader.

The following steps assume that you are running DHCP on your local network.

5. Type **dhcp** and hit return. This instructs the Array to obtain a DHCP address and use it during this boot in the bootloader environment.
6. Type **dir** and hit return to see what's currently in the compact flash.
7. Type **del** and hit return to delete the contents of the compact flash.
8. Type **update server <TFTP-server-ip-addr> XS-5.x-xxxx.bin** (the actual Xirrus file name will vary depending on Array model number and software version—use the file name from your software update) and hit return. The software update will be transferred to the Array's memory and will be written to the compact flash card. (See output below.)
9. Type **reset** and hit return. Your Array will reboot, running your new version of software.

Sample Output for the Upgrade Procedure:

The user actions are highlighted in the output below, for clarity.

Username: **admin**
Password: *****

Xirrus-WiFi-Array# **configure**
Xirrus-WiFi-Array(config)# **reboot**
Are you sure you want to reboot? [yes/no]: **yes**
Array is being rebooted.

Xirrus Boot Loader 1.0.0 (Oct 17 2006 - 13:11:42), Build: 2725

Processor | Motorola PowerPC, PVR=80200020 SVR=80300020
Board | Xirrus MPC8540 CPU Board
Clocks | CPU : 825 MHz DDR : 330 MHz Local Bus: 41 MHz

L1 cache | Data: 32 KB Inst: 32 KB Status : Enabled
Watchdog | Enabled (5 secs)
I2C Bus | 400 KHz
DTT | CPU:34C RF0:34C RF1:34C RF2:27C RF3:29C
RTC | Wed 2007-Nov-05 6:43:14 GMT
System DDR | 256 MB, Unbuffered Non-ECC (2T)
L2 cache | 256 KB, Enabled
FLASH | 4 MB, CRC: OK
FPGA | 2 Devices programmed
Packet DDR | 256 MB, Unbuffered Non-ECC, Enabled
Network | Mot FEC Mot TSEC1 [Primary] Mot TSEC2
IDE Bus 0 | OK
CFCard | 122 MB, Model: Hitachi XXM2.3.0
Environment | 4 KB, Initialized

In: serial
Out: serial
Err: serial

Press space bar to exit to bootloader:

XBL>**dhcp**
[DHCP] Device : Mot TSEC1 1000BT Full Duplex
[DHCP] IP Addr : 192.168.39.195
XBL>**dir**

[CFCard] Directory of /

Date	Time	Size	File or Directory name
2007-Nov-05	6:01:56	29	lastboot
2007-Apr-05	15:47:46	28210390	xs-3.1-0433.bak
2007-Mar-01	16:39:42		storage/
2007-Apr-05	15:56:38	28210430	xs-3.1-0440.bin
2007-Mar-03	0:56:28		wpr/

3 file(s), 2 dir(s)

```
XBL>del *
 [CFCard] Delete  : 2 file(s) deleted

XBL>update server 192.168.39.102 xs-3.0-0425.bin

[TFTP  ] Device  : Mot TSEC1 1000BT Full Duplex
[TFTP  ] Client  : 192.168.39.195
[TFTP  ] Server  : 192.168.39.102
[TFTP  ] File    : xs-3.0-0425.bin
[TFTP  ] Address : 0x1000000
[TFTP  ] Loading : ##################################################
[TFTP  ] Loading : ##################################################
[TFTP  ] Loading : ###### done
[TFTP  ] Complete: 12.9 sec, 2.1 MB/sec
[TFTP  ] Bytes   : 27752465 (1a77811 hex)
[CFCard] File    : xs-3.0-0425.bin
[CFCard] Address : 0x1000000
[CFCard] Saving  : ############################################## done
[CFCard] Complete: 137.4 sec, 197.2 KB/sec
[CFCard] Bytes   : 27752465 (1a77811 hex)

XBL>reset
[RESET ]


Xirrus Boot Loader 1.0.0 (Oct 17 2006 - 13:11:42), Build: 2725

Processor  | Motorola PowerPC, PVR=80200020 SVR=80300020
Board      | Xirrus MPC8540 CPU Board
Clocks     | CPU : 825 MHz   DDR : 330 MHz   Local Bus: 41 MHz
L1 cache   | Data:  32 KB    Inst:  32 KB    Status   : Enabled
Watchdog   | Enabled (5 secs)
I2C Bus    | 400 KHz
DTT        | CPU:33C  RF0:32C  RF1:31C  RF2:26C  RF3:27C
RTC        | Wed 2007-Nov-05  6:48:44 GMT
System DDR | 256 MB, Unbuffered Non-ECC (2T)
```

```
L2 cache   | 256 KB, Enabled
FLASH      |  4 MB, CRC: OK
FPGA       |  2 Devices programmed
Packet DDR | 256 MB, Unbuffered Non-ECC, Enabled
Network    | Mot FEC   Mot TSEC1 [Primary]  Mot TSEC2
IDE Bus 0  | OK
CFCard     | 122 MB, Model: Hitachi XXM2.3.0
Environment|  4 KB, Initialized

In:   serial
Out:  serial
Err:  serial

Press space bar to exit to bootloader:

[CFCard] File    : xs*.bin
[CFCard] Address : 0x1000000
[CFCard] Loading : ############################################## done
[CFCard] Complete: 26.9 sec, 1.0 MB/sec
[CFCard] Bytes   : 27752465 (1a77811 hex)
[Boot  ] Address : 0x01000000
[Boot  ] Image   : Verifying checksum .... OK
[Boot  ] Unzip   : Multi-File Image   .... OK
[Boot  ] Initrd  : Loading RAMDisk Image
[Boot  ] Initrd  : Verifying checksum .... OK
[Boot  ] Execute : Transferring control to OS

Initializing hardware ..... OK


Xirrus Wi-Fi Array
ArrayOS Version 3.0-425
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username:
```

Appendix C: Notices (Arrays except XR-500/600 and -H Models)

This Appendix contains Notices, Warnings, and Compliance information for all Array models ***except*** *for the following:*

For the XR-500/600 Series*, please see "Appendix D: Notices (XR500/600 Series Only)" on page 533.*

For models ending in H (such as the XR-520H)*, please see the* Quick Installation Guide *for that model.*

This appendix contains the following information:

- **"Notices" on page 511**
- **"EU Directive 1999/5/EC Compliance Information" on page 515**
- **"Compliance Information (Non-EU)" on page 522**
- **"Safety Warnings" on page 523**
- **"Translated Safety Warnings" on page 524**
- **"Software License and Product Warranty Agreement" on page 525**
- **"Hardware Warranty Agreement" on page 531**

Notices

Wi-Fi Alliance Certification

www.wi-fi.org

FCC Notice

This device complies with Part 15 of the FCC Rules, with operation subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause unwanted operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate RF energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following safety measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Consult the dealer or an experienced wireless technician for help.

Use of a shielded twisted pair (STP) cable must be used for all Ethernet connections in order to comply with EMC requirements.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LE-LAN devices.

Non-Modification Statement

Unauthorized changes or modifications to the device are not permitted. Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Modifications to the device will void the warranty and may violate FCC regulations. Please go to the Xirrus Web site for a list of all approved antennas.

Cable Runs for Power over Gigabit Ethernet (PoGE)

If using PoGE, the Array must be connected to PoGE networks without routing cabling to the outside plant—this ensures that cabling is not exposed to lightning strikes or possible cross over from high voltage.

Battery Warning

> ***Caution!*** *The Array contains a battery which is not to be replaced by the customer. Danger of Explosion exists if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.*

UL Statement

Use only with listed ITE product.

RF Radiation Hazard Warning

To ensure compliance with FCC and Industry Canada RF exposure requirements, this device must be installed in a location where the antennas of the device will have a minimum distance of at least 30 cm (12 inches) from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Installez l'appareil en veillant à conserver une distance d'au moins 30 cm entre les éléments rayonnants et les personnes. Cet avertissement de sécurité est conforme aux limites d'exposition définies par la norme CNR-102 at relative aux fréquences radio.

Industry Canada Notice and Marking

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

The term "IC:" before the radio certification number only signifies that Industry Canada technical specifications were met.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LELAN devices used in Canada.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250 - 5 350 MHz et 5 650 - 5 850 MHz. Ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

EU Directive 1999/5/EC Compliance Information

This Appendix contains Notices, Warnings, and Compliance information for all Array models ***except for the XR-500/600 Series and models ending in H****. For Notices, Warnings, and Compliance information for those models, see the notes at the beginning of this chapter.*

This section contains compliance information for the Xirrus Wireless Array family of products. The compliance information contained in this section is relevant to the European Union and other countries that have implemented the EU Directive 1999/5/EC.

Declaration of Conformity

Cesky [Czech]	Toto zahzeni je v souladu se základnimi požadavky a ostatnimi odpovidajcimi ustano veni mi Směrnice 1999/5/EC.
Dansk [Danish]	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]	Dieses Gerat entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtinie 1999/5/EU.
Eesti [Estonian]	See seande vastab direktiivi 1999/5/EU olulistele nõuetele ja teistele as jakohastele sätetele.
English	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spain]	Este equipo cump le con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνυκη [Greek]	Αυτός ο εξοπλτσμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και ύλλες σχετικές διατάξεις της Οδηγιας 1999/5/EC.

Français [French]	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajā prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šis įrenginys tenkina 1995/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]	Dit apparant voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1995/5/EC.
Malti [Maltese]	Dan l-apparant huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]	Ez a készülék teljesiti az alapvetö követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi mi warunkami określony mi Dyrektywą. UE:1999/5/EC.
Português [Portuguese]	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.

Slovensko [Slovenian]	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi popoji Direktive 1999/5/EC.
Slovensky [Slovak]	Toto zariadenie je v zhode so základnými požadavkami a inými prislušnými nariadeniami direktiv: 1999/5/EC.
Suomi [Finnish]	Tämä laite täyttää direktiivin 1999/5//EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Assessment Criteria

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 301 893 and EN 300 328 (if applicable)
- EMC: EN 301 489-1 and EN 301 489-17
- Safety: EN 50371 to EN 50385 and EN 60601

CE Marking

For the Xirrus Wireless Array, the CE mark and Class-2 identifier opposite are affixed to the equipment and its packaging:

CE ⓘ

Russian Certification Marking

For the Xirrus XR-500, XR-520H, XR-2000, and XR-4000 Series Wireless Arrays, the approval mark is affixed to the equipment:

EAC

WEEE Compliance

- Natural resources were used in the production of this equipment.
- This equipment may contain hazardous substances that could impact the health of the environment.
- In order to avoid harm to the environment and consumption of natural resources, we encourage you to use appropriate take-back systems when disposing of this equipment.
- The appropriate take-back systems will reuse or recycle most of the materials of this equipment in a way that will not harm the environment.
- The crossed-out wheeled bin symbol (in accordance with European Standard EN 50419) invites you to use those take-back systems and advises you not to combine the material with refuse destined for a land fill.
- If you need more information on collection, re-use and recycling systems, please contact your local or regional waste administration.
- Please contact Xirrus for specific information on the environmental performance of our products.

National Restrictions

In the majority of the EU and other European countries, the 2.4 GHz and 5 GHz bands have been made available for the use of Wireless LANs. The following table provides an overview of the regulatory requirements in general that are applicable for the 2.4 GHz and 5 GHz bands.

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor	Outdoor
2400–2483.5	100	X	X **
5250–5350 *	200	X	N/A
5470–5725*	1000	X	X

**Dynamic frequency selection and Transmit Power Control is required in these frequency bands.*

***France is indoor use only in the upper end of the band.*

The requirements for any country may change at any time. Xirrus recommends that you check with local authorities for the current status of their national regulations for both 2.4 GHz and 5 GHz wireless LANs.

The following countries have additional requirements or restrictions than those listed in the above table:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Xirrus recommends checking at *www.bipt.be* for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie www.bipt.be voor meer gegevens.

Les liasons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mèters doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez www.bipt.be pour de plus amples détails.

Greece

A license from EETT is required for the outdoor operation in the 5470 MHz to 5725 MHz band. Xirrus recommends checking *www.eett.gr* for more details.

Η δη ιουργβάικτ ωνεξωτερικο ρουστη ζ νησυ νοτ των 5470–5725 MHz ε ιτρ ετάιωνο ετάά όάδειά της EETT, ου ορηγεβτάι στερά ά ό σ φωνη γν η του ΓΕΕΘΑ. ερισσότερες λε τομ ρειεωστο www.eett.gr

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check with *www.communicazioni.it/it/* for more details.

Questo prodotto é conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti wireless LAN richiede una "autorizzazione Generale." Consultare www.communicazioni.it/it/ per maggiori dettagli.

Norway, Switzerland and Liechtenstein

Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

Calculating the Maximum Output Power

The regulatory limits for maximum output power are specified in EIRP (radiated power). The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Antennas

The Xirrus Wireless Array employs integrated antennas that cannot be removed and which are not user accessible. Nevertheless, as regulatory limits are not the same throughout the EU, users may need to adjust the conducted power setting for the radio to meet the EIRP limits applicable in their country or region. Adjustments can be made from the product's management interface—either Web Management Interface (WMI) or Command Line Interface (CLI).

Operating Frequency

The operating frequency in a wireless LAN is determined by the access point. As such, it is important that the access point is correctly configured to meet the local regulations. See National Restrictions in this section for more information.

Russia CU Approval (XR-2000/4000 Series)

If you still have questions regarding the compliance of Xirrus products or you cannot find the information you are looking for, please contact us at:

Xirrus, Inc.
2101 Corporate Center Drive
Thousand Oaks, CA 91320
USA

Tel: 1.805.262.1600
1.800.947.7871 Toll Free in the US
Fax: 1.866.462.3980

www.xirrus.com

Compliance Information (Non-EU)

*This Appendix contains Notices, Warnings, and Compliance information for all Array models **except for the XR-500/600 Series and models ending in H**. For Notices, Warnings, and Compliance information for those models, see the notes at the beginning of this chapter.*

This section contains compliance information for the Xirrus Wireless Array family of products. The compliance information contained in this section is relevant to the listed countries (outside of the European Union and other countries that have implemented the EU Directive 1999/5/EC).

Declaration of Conformity

Mexico XN16: Cofetel Cert #: RCPXIXN10-1052
XN12: Cofetel Cert #: RCPXIXN10-1052-A1
XN8: Cofetel Cert #: RCPXIXN10-1052-A2
XN4: Cofetel Cert #: RCPXIXN10-1052-A3

Thailand This telecommunication equipment conforms to NTC technical requirement.

Safety Warnings

This Appendix contains Notices, Warnings, and Compliance information for all Array models ***except for the XR-500/600 Series and models ending in H****. For Notices, Warnings, and Compliance information for those models, see the notes at the beginning of this chapter.*

Safety Warnings

Read all user documentation before powering this device. All Xirrus interconnected equipment should be contained indoors. This product is not suitable for outdoor operation. Please verify the integrity of the system ground prior to installing Xirrus equipment. Additionally, verify that the ambient operating temperature does not exceed 50°C (40°C for the XR500 Series).

Explosive Device Proximity Warning

Do not operate the XR Series Wireless Array near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

Lightning Activity Warning

Do not work on the XR Series Wireless Array or connect or disconnect cables during periods of lightning activity.

Circuit Breaker Warning

The XR Series Wireless Array relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.

Translated safety warnings appear on the following page.

Translated Safety Warnings

This Appendix contains Notices, Warnings, and Compliance information for all Array models ***except for the XR-500/600 Series and models ending in H****. For Notices, Warnings, and Compliance information for those models, see the notes at the beginning of this chapter.*

Avertissements de Sécurité

Sécurité

Lisez l'ensemble de la documentation utilisateur avant de mettre cet appareil sous tension. Tous les équipements Xirrus interconnectés doivent être installés en intérieur. Ce produit n'est pas conçu pour être utilisé en extérieur. Veuillez vérifier l'intégrité de la terre du système avant d'installer des équipements Xirrus. Vérifiez également que la température de fonctionnement ambiante n'excède pas 50°C (40°C pour XR-520).

Proximité d'appareils explosifs

N'utilisez pas l'unité XR Wireless Array à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.

Foudre

N'utilisez pas l'unité XR Wireless Array et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.

Disjoncteur

L'unité XR Wireless Array dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Software License and Product Warranty Agreement

THIS SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU ("CUSTOMER") AND LICENSOR (AS DEFINED BELOW) AND GOVERNS THE USE OF THE SOFTWARE INSTALLED ON THE PRODUCT (AS DEFINED BELOW). IF YOU ARE AN EMPLOYEE OR AGENT OF CUSTOMER, YOU HEREBY REPRESENT AND WARRANT TO LICENSOR THAT YOU HAVE THE POWER AND AUTHORITY TO ACCEPT AND TO BIND CUSTOMER TO THE TERMS AND CONDITIONS OF THIS AGREEMENT (INCLUDING ANY THIRD PARTY TERMS SET FORTH HEREIN). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT RETURN THE PRODUCT AND ALL ACCOMPANYING MATERIALS (INCLUDING ALL DOCUMENTATION) TO THE RELEVANT VENDOR FOR A FULL REFUND OF THE PURCHASE PRICE THEREFORE.

CUSTOMER UNDERSTANDS AND AGREES THAT USE OF THE PRODUCT AND SOFTWARE SHALL BE DEEMED AN AGREEMENT TO THE TERMS AND CONDITIONS GOVERNING SUCH SOFTWARE AND THAT CUSTOMER IS BOUND BY AND BECOMES A PARTY TO THIS AGREEMENT.

1.0 DEFINITIONS

1.1 "Documentation" means the user manuals and all other all documentation, instructions or other similar materials accompanying the Software covering the installation, application, and use thereof.

1.2 "Licensor" means XIRRUS and its suppliers.

1.3 "Product" means a multi-radio access point containing four or more distinct radios capable of simultaneous operation on four or more non-overlapping channels.

1.4 "Software" means, collectively, each of the application and embedded software programs delivered to Customer in connection with this Agreement. For purposes of this Agreement, the term Software shall be deemed to include any and all Documentation and Updates provided with or for the Software.

1.5 "Updates" means any bug-fix, maintenance or version release to the Software that may be provided to Customer from Licensor pursuant to this Agreement or pursuant to any separate maintenance and support agreement entered into by and between Licensor and Customer.

2.0 GRANT OF RIGHTS

2.1 Software. Subject to the terms and conditions of this Agreement, Licensor hereby grants to Customer a perpetual, non-exclusive, non-sublicenseable, non-transferable right and license to use the Software solely as installed on

the Product in accordance with the accompanying Documentation and for no other purpose.

2.2 Ownership. The license granted under Sections 2.1 above with respect to the Software does not constitute a transfer or sale of Licensor's or its suppliers' ownership interest in or to the Software, which is solely licensed to Customer. The Software is protected by both national and international intellectual property laws and treaties. Except for the express licenses granted to the Software, Licensor and its suppliers retain all rights, title and interest in and to the Software, including (i) any and all trade secrets, copyrights, patents and other proprietary rights therein or thereto or (ii) any Marks (as defined in Section 2.3 below) used in connection therewith. In no event shall Customer remove, efface or otherwise obscure any Marks contained on or in the Software. All rights not expressly granted herein are reserved by Licensor.

2.3 Copies. Customer shall not make any copies of the Software but shall be permitted to make a reasonable number of copies of the related Documentation. Whenever Customer copies or reproduces all or any part of the Documentation, Customer shall reproduce all and not efface any titles, trademark symbols, copyright symbols and legends, and other proprietary markings or similar indicia of origin (“Marks”) on or in the Documentation.

2.4 Restrictions. Customer shall not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) sell, rent, lease, license or sublicense, assign or otherwise transfer the Software, or any of Customer's rights and obligations under this Agreement except as expressly permitted herein; (ii) decompile, disassemble, or reverse engineer the Software, in whole or in part, provided that in those jurisdictions in which a total prohibition on any reverse engineering is prohibited as a matter of law and such prohibition is not cured by the fact that this Agreement is subject to the laws of the State of California, Licensor agrees to grant Customer, upon Customer's written request to Licensor, a limited reverse engineering license to permit interoperability of the Software with other software or code used by Customer; (iii) allow access to the Software by any user other than by Customer's employees and contractors who are bound in writing to confidentiality and non-use restrictions at least as protective as those set forth herein; (iv) except as expressly set forth herein, write or develop any derivative software or any other software program based upon the Software; (v) use any computer software or hardware which is designated to defeat any copy protection or other use limiting device, including any device intended to limit the number of users or devices accessing the Product; (vi) disclose information about the performance or operation of the Product or Software to any third party without the prior written consent of Licensor; or (vii) engage a third party to perform benchmark or functionality testing of the Product or Software.

3.0 LIMITED WARRANTY AND LIMITATION OF LIABILITY

3.1 Limited Warranty & Exclusions. Licensor warrants that the Software will perform in substantial accordance with the specifications therefore set forth in the Documentation for a period of ninety [90] days after Customer's acceptance of the terms of this Agreement with respect to the Software ("Warranty Period"). If during the Warranty Period the Software or Product does not perform as warranted, Licensor shall, at its option, correct the relevant Product and/or Software giving rise to such breach of performance or replace such Product and/or Software free of charge. THE FOREGOING ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE FOREGOING WARRANTY. THE WARRANTY SET FORTH ABOVE IS MADE TO AND FOR THE BENEFIT OF CUSTOMER ONLY. The warranty will apply only if (i) the Software has been used at all times and in accordance with the instructions for use set forth in the Documentation and this Agreement; (ii) no modification, alteration or addition has been made to the Software by persons other than Licensor or Licensor's authorized representative; and (iii) the Software or Product on which the Software is installed has not been subject to any unusual electrical charge.

3.2 DISCLAIMER. EXCEPT AS EXPRESSLY STATED IN THIS SECTION 3, ALL ADDITIONAL CONDITIONS, REPRESENTATIONS, AND WARRANTIES, WHETHER IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, ACCURACY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY DISCLAIMED BY LICENSOR AND ITS SUPPLIERS. THIS DISCLAIMER SHALL APPLY EVEN IF ANY EXPRESS WARRANTY AND LIMITED REMEDY OFFERED BY LICENSOR FAILS OF ITS ESSENTIAL PURPOSE. ALL WARRANTIES PROVIDED BY LICENSOR ARE SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN THIS AGREEMENT.

3.3 HAZARDOUS APPLICATIONS. THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF A NUCLEAR FACILITY, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROLS OR OTHER DEVICES OR SYSTEMS IN WHICH A MALFUNCTION OF THE SOFTWARE WOULD RESULT IN FORSEEABLE RISK OF INJURY OR DEATH TO THE OPERATOR OF THE DEVICE OR SYSTEM OR TO OTHERS ("HAZARDOUS APPLICATIONS"). CUSTOMER ASSUMES ANY AND ALL RISKS, INJURIES, LOSSES, CLAIMS AND ANY OTHER LIABILITIES ARISING OUT OF THE USE OF THE SOFTWARE IN ANY HAZARDOUS APPLICATIONS.

3.4 Limitation of Liability.

(a) TOTAL LIABILITY. NOTWITHSTANDING ANYTHING ELSE HEREIN, ALL LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMER FOR THE RELEVANT SOFTWARE, OR PORTION THEREOF, THAT GAVE RISE TO SUCH LIABILITY OR ONE HUNDRED UNITED STATES DOLLARS (US$100), WHICHEVER IS GREATER. THE LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS SECTION SHALL BE CUMULATIVE AND NOT PER INCIDENT.

(b) DAMAGES. IN NO EVENT SHALL LICENSOR, ITS SUPPLIERS OR THEIR RELEVANT SUBCONTRACTORS BE LIABLE FOR (A) ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR LOST OR DAMAGED DATA, OR ANY INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE OR (B) ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES IN EACH CASE, EVEN IF LICENSOR OR ITS SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 Exclusions. SOME JURISDICTIONS DO NOT PERMIT THE LIMITATIONS OF LIABILITY AND LIMITED WARRANTIES SET FORTH UNDER THIS AGREEMENT. IN THE EVENT YOU ARE LOCATED IN ANY SUCH JURISDICTION, THE FOREGOING LIMITATIONS SHALL APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED IN SUCH JURISDICTIONS. IN NO EVENT SHALL THE FOREGOING EXCLUSIONS AND LIMITATIONS ON DAMAGES BE DEEMED TO APPLY TO ANY LIABILITY BASED ON FRAUD, WILLFUL MISCONDUCT, GROSS NEGLIGENCE OR PERSONAL INJURY OR DEATH.

4.0 CONFIDENTIAL INFORMATION

4.1 Generally. The Software (and its accompanying Documentation) constitutes Licensor's and its suppliers' proprietary and confidential information and contains valuable trade secrets of Licensor and its suppliers (“Confidential Information”). Customer shall protect the secrecy of the Confidential Information to the same extent it protects its other valuable, proprietary and confidential information of a similar nature but in no event shall Customer use less than reasonable care to maintain the secrecy of the Confidential Information. Customer shall not use the Confidential Information except to exercise its rights or perform its obligations as set forth under this Agreement. Customer shall not disclose such Confidential Information to any third party other than subject to non-use and non-disclosure obligations at least as

protective of a party's right in such Confidential Information as those set forth herein.

4.2 Return of Materials. Customer agrees to (i) destroy all Confidential Information (including deleting any and all copies contained on any of Customer's Designated Hardware or the Product) within fifteen (15) days of the date of termination of this Agreement or (ii) if requested by Licensor, return, any Confidential Information to Licensor within thirty (30) days of Licensor's written request.

5.0 TERM AND TERMINATION

5.1 Term. Subject to Section 5.2 below, this Agreement will take effect on the Effective Date and will remain in force until terminated in accordance with this Agreement.

5.2 Termination Events. This Agreement may be terminated immediately upon written notice by either party under any of the following conditions:

(a) If the other party has failed to cure a breach of any material term or condition under the Agreement within thirty (30) days after receipt of notice from the other party; or

(b) Either party ceases to carry on business as a going concern, either party becomes the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation, which proceeding is not dismissed within ninety (90) days, or a receiver is appointed with respect to a substantial part of its assets.

5.3 Effect of Termination.

(a) Upon termination of this Agreement, in whole or in part, Customer shall pay Licensor for all amounts owed up to the effective date of termination. Termination of this Agreement shall not constitute a waiver for any amounts due.

(b) The following Sections shall survive the termination of this Agreement for any reason: Sections 1, 2.2, 2.4, 3, 4, 5.3, and 6.

(c) No later than thirty (30) days after the date of termination of this Agreement by Licensor, Customer shall upon Licensor's instructions either return the Software and all copies thereof; all Documentation relating thereto in its possession that is in tangible form or destroy the same (including any copies thereof contained on Customer's Designated Hardware). Customer shall furnish Licensor with a certificate signed by an executive officer of Customer verifying that the same has been done.

6. MISCELLANEOUS

If Customer is a corporation, partnership or similar entity, then the license to the Software and Documentation that is granted under this Agreement is expressly conditioned upon and Customer represents and warrants to Licensor that the person accepting the terms of this Agreement is authorized to bind such entity to the terms and conditions herein. If any provision of this Agreement is held to be invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect. During the course of use of the Software, Licensor may collect information on your use thereof; you hereby authorize Licensor to use such information to improve its products and services, and to disclose the same to third parties provided it does not contain any personally identifiable information. The express waiver by either party of any provision, condition or requirement of this Agreement does not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Customer and Licensor are independent parties. Customer may not export or re-export the Software or Documentation (or other materials) without appropriate United States, European Union and foreign government licenses or in violation of the United State's Export Administration Act or foreign equivalents and Customer shall comply with all national and international laws governing the Software. This Agreement will be governed by and construed under the laws of the State of California and the United States as applied to agreements entered into and to be performed entirely within California, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer Information Transactions Act (as promulgated by any State) to this Agreement. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of, the state and federal courts located in Ventura County, California. Customer may not assign this Agreement by operation of law or otherwise, without the prior written consent of Licensor and any attempted assignment in violation of the foregoing shall be null and void. This Agreement cancels and supersedes all prior agreements between the parties. This Agreement may not be varied except through a document agreed to and signed by both parties. Any printed terms and conditions contained in any Customer purchase order or in any Licensor acknowledgment, invoice or other documentation relating to the Software shall be deemed deleted and of no force or effect and any additional typed and/or written terms and conditions contained shall be for administrative purposes only, i.e. to identify the types and quantities of Software to be supplied, line item prices and total price, delivery schedule, and other similar ordering data, all in accordance with the provisions of this Agreement.

Hardware Warranty Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

LIMITED WARRANTY. Xirrus warrants that for a period of five years from the date of purchase by the original purchaser ("Customer"): (i) the Xirrus Equipment ("Equipment") will be free of defects in materials and workmanship under normal use; and (ii) the Equipment substantially conforms to its published specifications. Except for the foregoing, the Equipment is provided AS IS. This limited warranty extends only to Customer as the original purchaser. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' option, repair, replacement, or refund of the Equipment if reported (or, upon request, returned) to the party supplying the Equipment to Customer. In no event does Xirrus warrant that the Equipment is error free or that Customer will be able to operate the Equipment without problems or interruptions.

This warranty does not apply if the Equipment (a) has been altered, except by Xirrus, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Xirrus, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra-hazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL XIRRUS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE EQUIPMENT EVEN IF XIRRUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Xirrus' or its suppliers' liability to Customer,

whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer.

The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any evaluation Equipment made available for testing or demonstration purposes. All such Equipment is provided AS IS without any warranty whatsoever.

Customer agrees the Equipment and related documentation shall not be used in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or cause or permit any third party to do any of the foregoing.

All information or feedback provided by Customer to Xirrus with respect to the Product shall be Xirrus' property and deemed confidential information of Xirrus.

Equipment including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Equipment.

This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this Warranty shall remain in full force and effect. This Warranty constitutes the entire agreement between the parties with respect to the use of the Equipment.

Manufacturer is Xirrus, Inc. 2101 Corporate Center Drive Thousand Oaks, CA 91320

Appendix D: Notices (XR500/600 Series Only)

This Appendix contains Notices, Warnings, and Compliance information for ***the XR500/600 Series only.***

For Notices, Warnings, and Compliance information outdoor products, please see the Quick Installation Guide for that product.

For Notices, Warnings, and Compliance information ***for all other Arrays****, please see* "Appendix C: Notices (Arrays except XR-500/600 and -H Models)" on page 511.

This appendix contains the following information:

- **"Notices" on page 533**
- **"EU Directive 1999/5/EC Compliance Information" on page 537**
- **"Compliance Information (Non-EU)" on page 544**
- **"Safety Warnings" on page 545**
- **"Translated Safety Warnings" on page 546**
- **"Software License and Product Warranty Agreement" on page 547**
- **"Hardware Warranty Agreement" on page 553**

Notices

Wi-Fi Alliance Certification

www.wi-fi.org

FCC Notice

This device complies with Part 15 of the FCC Rules, with operation subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause unwanted operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate RF energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following safety measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced wireless technician for help.

Use of a shielded twisted pair (STP) cable must be used for all Ethernet connections in order to comply with EMC requirements.

> ! ***FCC Caution:*** *Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LE-LAN devices.

Non-Modification Statement

Unauthorized changes or modifications to the device are not permitted. Use only the supplied internal antenna, or external antennas supplied by the manufacturer.

Modifications to the device will void the warranty and may violate FCC regulations.

Cable Runs for Power over Gigabit Ethernet (PoGE)

If using PoGE, the Array must be connected to PoGE networks without routing cabling to the outside plant—this ensures that cabling is not exposed to lightning strikes or possible cross over from high voltage.

Battery Warning

> ***Caution!*** *The Array contains a battery which is not to be replaced by the customer. Danger of Explosion exists if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.*

UL Statement

Use only with listed ITE product.

RF Radiation Hazard Warning

To ensure compliance with FCC and Industry Canada RF exposure requirements, this device must be installed in a location where the antennas of the device will have a minimum distance of at least 30 cm (12 inches) from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Installez l'appareil en veillant à conserver une distance d'au moins 30 cm entre les éléments rayonnants et les personnes. Cet avertissement de sécurité est conforme aux limites d'exposition définies par la norme CNR-102 at relative aux fréquences radio.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

EU Directive 1999/5/EC Compliance Information

This Appendix contains Notices, Warnings, and Compliance information for ***the XR500/600 Series only.*** *For other models, see the notes under* *"Appendix C: Notices (Arrays except XR-500/600 and -H Models)" on page 511.*

This section contains compliance information for the Xirrus Wireless Array family of products. The compliance information contained in this section is relevant to the European Union and other countries that have implemented the EU Directive 1999/5/EC.

Declaration of Conformity

Cesky [Czech]	Toto zahzeni je v souladu se základnimi požadavky a ostatnimi odpovidajcimi ustano veni mi Směrnice 1999/5/EC.
Dansk [Danish]	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]	Dieses Gerat entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtinie 1999/5/EU.
Eesti [Estonian]	See seande vastab direktiivi 1999/5/EU olulistele nõuetele ja teistele as jakohastele sätetele.
English	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spain]	Este equipo cump le con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνυκη [Greek]	Αυτός ο εξοπλτσμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και ύλλες σχετικές διατάξεις της Οδηγιας 1999/5/EC.

Français [French]	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajā prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šis įrenginys tenkina 1995/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]	Dit apparant voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1995/5/EC.
Malti [Maltese]	Dan l-apparant huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]	Ez a készülék teljesiti az alapvetö követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi mi warunkami określony mi Dyrektywą. UE:1999/5/EC.
Português [Portuguese]	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.

Slovensko [Slovenian]	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi popoji Direktive 1999/5/EC.
Slovensky [Slovak]	Toto zariadenie je v zhode so základnými požadavkami a inými prislušnými nariadeniami direktiv: 1999/5/EC.
Suomi [Finnish]	Tämä laite täyttää direktiivin 1999/5//EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Assessment Criteria

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 301 893 and EN 300 328 (if applicable)
- EMC: EN 301 489-1 and EN 301 489-17
- Safety: EN 50371 to EN 50385 and EN 60601

CE Marking

For the Xirrus Wireless Array, the CE mark and Class-2 identifier opposite are affixed to the equipment and its packaging:

CE ⓘ

Russian Certification Marking

For the Xirrus XR-500, XR-520H, XR-2000, and XR-4000 Series Wireless Arrays, the approval mark is affixed to the equipment:

EAC

WEEE Compliance

- Natural resources were used in the production of this equipment.
- This equipment may contain hazardous substances that could impact the health of the environment.
- In order to avoid harm to the environment and consumption of natural resources, we encourage you to use appropriate take-back systems when disposing of this equipment.
- The appropriate take-back systems will reuse or recycle most of the materials of this equipment in a way that will not harm the environment.
- The crossed-out wheeled bin symbol (in accordance with European Standard EN 50419) invites you to use those take-back systems and advises you not to combine the material with refuse destined for a land fill.
- If you need more information on collection, re-use and recycling systems, please contact your local or regional waste administration.
- Please contact Xirrus for specific information on the environmental performance of our products.

National Restrictions

In the majority of the EU and other European countries, the 2.4 GHz and 5 GHz bands have been made available for the use of Wireless LANs. The following table provides an overview of the regulatory requirements in general that are applicable for the 2.4 GHz and 5 GHz bands.

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor	Outdoor
2400–2483.5	100	X	X **
5250–5350 *	200	X	N/A
5470–5725*	1000	X	X

**Dynamic frequency selection and Transmit Power Control is required in these frequency bands.*

***France is indoor use only in the upper end of the band.*

The requirements for any country may change at any time. Xirrus recommends that you check with local authorities for the current status of their national regulations for both 2.4 GHz and 5 GHz wireless LANs.

The following countries have additional requirements or restrictions than those listed in the above table:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Xirrus recommends checking at *www.bipt.be* for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie www.bipt.be voor meer gegevens.

Les liasons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mèters doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez www.bipt.be pour de plus amples détails.

Greece

A license from EETT is required for the outdoor operation in the 5470 MHz to 5725 MHz band. Xirrus recommends checking *www.eett.gr* for more details.

Η δη ιουργβάικτ ωνεξωτερικο ρουστη ζ νησυ νοτ των 5470–5725 MHz ε ιτρ ετάιωνο ετάά όάδειά της EETT, ου ορηγεβτάι στερά ά ό σ φωνη γν η του ΓΕΕΘΑ. ερισσότερες λε τομ ρειεωστο www.eett.gr

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check with *www.communicazioni.it/it/* for more details.

Questo prodotto é conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti wireless LAN richiede una "autorizzazione Generale." Consultare www.communicazioni.it/it/ per maggiori dettagli.

Norway, Switzerland and Liechtenstein

Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

Calculating the Maximum Output Power

The regulatory limits for maximum output power are specified in EIRP (radiated power). The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Antennas

The Xirrus Wireless Array employs integrated antennas that cannot be removed and which are not user accessible. Nevertheless, as regulatory limits are not the same throughout the EU, users may need to adjust the conducted power setting for the radio to meet the EIRP limits applicable in their country or region. Adjustments can be made from the product's management interface—either Web Management Interface (WMI) or Command Line Interface (CLI).

Operating Frequency

The operating frequency in a wireless LAN is determined by the access point. As such, it is important that the access point is correctly configured to meet the local regulations. See National Restrictions in this section for more information.

If you still have questions regarding the compliance of Xirrus products or you cannot find the information you are looking for, please contact us at:

Xirrus, Inc.
2101 Corporate Center Drive
Thousand Oaks, CA 91320
USA

Tel: 1.805.262.1600
1.800.947.7871 Toll Free in the US
Fax: 1.866.462.3980

www.xirrus.com

Compliance Information (Non-EU)

This Appendix contains Notices, Warnings, and Compliance information for ***the XR500/600 Series only.*** *For other models, see the notes under* *"Appendix C: Notices (Arrays except XR-500/600 and -H Models)" on page 511.*

This section contains compliance information for the Xirrus Wireless Array family of products. The compliance information contained in this section is relevant to the listed countries (outside of the European Union and other countries that have implemented the EU Directive 1999/5/EC).

Declaration of Conformity

Mexico XN16: Cofetel Cert #: RCPXIXN10-1052
XN12: Cofetel Cert #: RCPXIXN10-1052-A1
XN8: Cofetel Cert #: RCPXIXN10-1052-A2
XN4: Cofetel Cert #: RCPXIXN10-1052-A3

Thailand This telecommunication equipment conforms to NTC technical requirement.

Safety Warnings

This Appendix contains Notices, Warnings, and Compliance information for ***the XR500/600 Series only.*** *For other models, see the notes under "Appendix C: Notices (Arrays except XR-500/600 and -H Models)" on page 511.*

Safety Warnings

Read all user documentation before powering this device. All Xirrus interconnected equipment should be contained indoors. This product is not suitable for outdoor operation. Please verify the integrity of the system ground prior to installing Xirrus equipment. Additionally, verify that the ambient operating temperature does not exceed 50°C (40°C for the XR500/600 Series).

Explosive Device Proximity Warning

Do not operate the XR Series Wireless Array near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

Lightning Activity Warning

Do not work on the XR Series Wireless Array or connect or disconnect cables during periods of lightning activity.

Circuit Breaker Warning

The XR Series Wireless Array relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.

Translated safety warnings appear on the following page.

Translated Safety Warnings

This Appendix contains Notices, Warnings, and Compliance information for ***the XR500/600 Series only.*** *For other models, see the notes under* *"Appendix C: Notices (Arrays except XR-500/600 and -H Models)" on page 511.*

Avertissements de Sécurité

Sécurité

Lisez l'ensemble de la documentation utilisateur avant de mettre cet appareil sous tension. Tous les équipements Xirrus interconnectés doivent être installés en intérieur. Ce produit n'est pas conçu pour être utilisé en extérieur. Veuillez vérifier l'intégrité de la terre du système avant d'installer des équipements Xirrus. Vérifiez également que la température de fonctionnement ambiante n'excède pas 50°C (40°C pour XR-520).

Proximité d'appareils explosifs

N'utilisez pas l'unité XR Wireless Array à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.

Foudre

N'utilisez pas l'unité XR Wireless Array et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.

Disjoncteur

L'unité XR Wireless Array dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Software License and Product Warranty Agreement

THIS SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU ("CUSTOMER") AND LICENSOR (AS DEFINED BELOW) AND GOVERNS THE USE OF THE SOFTWARE INSTALLED ON THE PRODUCT (AS DEFINED BELOW). IF YOU ARE AN EMPLOYEE OR AGENT OF CUSTOMER, YOU HEREBY REPRESENT AND WARRANT TO LICENSOR THAT YOU HAVE THE POWER AND AUTHORITY TO ACCEPT AND TO BIND CUSTOMER TO THE TERMS AND CONDITIONS OF THIS AGREEMENT (INCLUDING ANY THIRD PARTY TERMS SET FORTH HEREIN). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT RETURN THE PRODUCT AND ALL ACCOMPANYING MATERIALS (INCLUDING ALL DOCUMENTATION) TO THE RELEVANT VENDOR FOR A FULL REFUND OF THE PURCHASE PRICE THEREFORE.

CUSTOMER UNDERSTANDS AND AGREES THAT USE OF THE PRODUCT AND SOFTWARE SHALL BE DEEMED AN AGREEMENT TO THE TERMS AND CONDITIONS GOVERNING SUCH SOFTWARE AND THAT CUSTOMER IS BOUND BY AND BECOMES A PARTY TO THIS AGREEMENT.

1.0 DEFINITIONS

1.1 "Documentation" means the user manuals and all other all documentation, instructions or other similar materials accompanying the Software covering the installation, application, and use thereof.

1.2 "Licensor" means Xirrus and its suppliers.

1.3 "Product" means a multi-radio access point containing four or more distinct radios capable of simultaneous operation on four or more non-overlapping channels.

1.4 "Software" means, collectively, each of the application and embedded software programs delivered to Customer in connection with this Agreement. For purposes of this Agreement, the term Software shall be deemed to include any and all Documentation and Updates provided with or for the Software.

1.5 "Updates" means any bug-fix, maintenance or version release to the Software that may be provided to Customer from Licensor pursuant to this Agreement or pursuant to any separate maintenance and support agreement entered into by and between Licensor and Customer.

2.0 GRANT OF RIGHTS

2.1 Software. Subject to the terms and conditions of this Agreement, Licensor hereby grants to Customer a perpetual, non-exclusive, non-sublicenseable, non-transferable right and license to use the Software solely as installed on

the Product in accordance with the accompanying Documentation and for no other purpose.

2.2 Ownership. The license granted under Sections 2.1 above with respect to the Software does not constitute a transfer or sale of Licensor's or its suppliers' ownership interest in or to the Software, which is solely licensed to Customer. The Software is protected by both national and international intellectual property laws and treaties. Except for the express licenses granted to the Software, Licensor and its suppliers retain all rights, title and interest in and to the Software, including (i) any and all trade secrets, copyrights, patents and other proprietary rights therein or thereto or (ii) any Marks (as defined in Section 2.3 below) used in connection therewith. In no event shall Customer remove, efface or otherwise obscure any Marks contained on or in the Software. All rights not expressly granted herein are reserved by Licensor.

2.3 Copies. Customer shall not make any copies of the Software but shall be permitted to make a reasonable number of copies of the related Documentation. Whenever Customer copies or reproduces all or any part of the Documentation, Customer shall reproduce all and not efface any titles, trademark symbols, copyright symbols and legends, and other proprietary markings or similar indicia of origin (“Marks”) on or in the Documentation.

2.4 Restrictions. Customer shall not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) sell, rent, lease, license or sublicense, assign or otherwise transfer the Software, or any of Customer's rights and obligations under this Agreement except as expressly permitted herein; (ii) decompile, disassemble, or reverse engineer the Software, in whole or in part, provided that in those jurisdictions in which a total prohibition on any reverse engineering is prohibited as a matter of law and such prohibition is not cured by the fact that this Agreement is subject to the laws of the State of California, Licensor agrees to grant Customer, upon Customer's written request to Licensor, a limited reverse engineering license to permit interoperability of the Software with other software or code used by Customer; (iii) allow access to the Software by any user other than by Customer's employees and contractors who are bound in writing to confidentiality and non-use restrictions at least as protective as those set forth herein; (iv) except as expressly set forth herein, write or develop any derivative software or any other software program based upon the Software; (v) use any computer software or hardware which is designated to defeat any copy protection or other use limiting device, including any device intended to limit the number of users or devices accessing the Product; (vi) disclose information about the performance or operation of the Product or Software to any third party without the prior written consent of Licensor; or (vii) engage a third party to perform benchmark or functionality testing of the Product or Software.

3.0 LIMITED WARRANTY AND LIMITATION OF LIABILITY

3.1 Limited Warranty & Exclusions. Licensor warrants that the Software will perform in substantial accordance with the specifications therefore set forth in the Documentation for a period of ninety [90] days after Customer's acceptance of the terms of this Agreement with respect to the Software ("Warranty Period"). If during the Warranty Period the Software or Product does not perform as warranted, Licensor shall, at its option, correct the relevant Product and/or Software giving rise to such breach of performance or replace such Product and/or Software free of charge. THE FOREGOING ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE FOREGOING WARRANTY. THE WARRANTY SET FORTH ABOVE IS MADE TO AND FOR THE BENEFIT OF CUSTOMER ONLY. The warranty will apply only if (i) the Software has been used at all times and in accordance with the instructions for use set forth in the Documentation and this Agreement; (ii) no modification, alteration or addition has been made to the Software by persons other than Licensor or Licensor's authorized representative; and (iii) the Software or Product on which the Software is installed has not been subject to any unusual electrical charge.

3.2 DISCLAIMER. EXCEPT AS EXPRESSLY STATED IN THIS SECTION 3, ALL ADDITIONAL CONDITIONS, REPRESENTATIONS, AND WARRANTIES, WHETHER IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, ACCURACY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY DISCLAIMED BY LICENSOR AND ITS SUPPLIERS. THIS DISCLAIMER SHALL APPLY EVEN IF ANY EXPRESS WARRANTY AND LIMITED REMEDY OFFERED BY LICENSOR FAILS OF ITS ESSENTIAL PURPOSE. ALL WARRANTIES PROVIDED BY LICENSOR ARE SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN THIS AGREEMENT.

3.3 HAZARDOUS APPLICATIONS. THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF A NUCLEAR FACILITY, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROLS OR OTHER DEVICES OR SYSTEMS IN WHICH A MALFUNCTION OF THE SOFTWARE WOULD RESULT IN FORSEEABLE RISK OF INJURY OR DEATH TO THE OPERATOR OF THE DEVICE OR SYSTEM OR TO OTHERS ("HAZARDOUS APPLICATIONS"). CUSTOMER ASSUMES ANY AND ALL RISKS, INJURIES, LOSSES, CLAIMS AND ANY OTHER LIABILITIES ARISING OUT OF THE USE OF THE SOFTWARE IN ANY HAZARDOUS APPLICATIONS.

3.4 Limitation of Liability.

(a) TOTAL LIABILITY. NOTWITHSTANDING ANYTHING ELSE HEREIN, ALL LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMER FOR THE RELEVANT SOFTWARE, OR PORTION THEREOF, THAT GAVE RISE TO SUCH LIABILITY OR ONE HUNDRED UNITED STATES DOLLARS (US$100), WHICHEVER IS GREATER. THE LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS SECTION SHALL BE CUMULATIVE AND NOT PER INCIDENT.

(b) DAMAGES. IN NO EVENT SHALL LICENSOR, ITS SUPPLIERS OR THEIR RELEVANT SUBCONTRACTORS BE LIABLE FOR (A) ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR LOST OR DAMAGED DATA, OR ANY INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE OR (B) ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES IN EACH CASE, EVEN IF LICENSOR OR ITS SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 Exclusions. SOME JURISDICTIONS DO NOT PERMIT THE LIMITATIONS OF LIABILITY AND LIMITED WARRANTIES SET FORTH UNDER THIS AGREEMENT. IN THE EVENT YOU ARE LOCATED IN ANY SUCH JURISDICTION, THE FOREGOING LIMITATIONS SHALL APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED IN SUCH JURISDICTIONS. IN NO EVENT SHALL THE FOREGOING EXCLUSIONS AND LIMITATIONS ON DAMAGES BE DEEMED TO APPLY TO ANY LIABILITY BASED ON FRAUD, WILLFUL MISCONDUCT, GROSS NEGLIGENCE OR PERSONAL INJURY OR DEATH.

4.0 CONFIDENTIAL INFORMATION

4.1 Generally. The Software (and its accompanying Documentation) constitutes Licensor's and its suppliers' proprietary and confidential information and contains valuable trade secrets of Licensor and its suppliers (“Confidential Information”). Customer shall protect the secrecy of the Confidential Information to the same extent it protects its other valuable, proprietary and confidential information of a similar nature but in no event shall Customer use less than reasonable care to maintain the secrecy of the Confidential Information. Customer shall not use the Confidential Information except to exercise its rights or perform its obligations as set forth under this Agreement. Customer shall not disclose such Confidential Information to any third party other than subject to non-use and non-disclosure obligations at least as

protective of a party's right in such Confidential Information as those set forth herein.

4.2 Return of Materials. Customer agrees to (i) destroy all Confidential Information (including deleting any and all copies contained on any of Customer's Designated Hardware or the Product) within fifteen (15) days of the date of termination of this Agreement or (ii) if requested by Licensor, return, any Confidential Information to Licensor within thirty (30) days of Licensor's written request.

5.0 TERM AND TERMINATION

5.1 Term. Subject to Section 5.2 below, this Agreement will take effect on the Effective Date and will remain in force until terminated in accordance with this Agreement.

5.2 Termination Events. This Agreement may be terminated immediately upon written notice by either party under any of the following conditions:

(a) If the other party has failed to cure a breach of any material term or condition under the Agreement within thirty (30) days after receipt of notice from the other party; or

(b) Either party ceases to carry on business as a going concern, either party becomes the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation, which proceeding is not dismissed within ninety (90) days, or a receiver is appointed with respect to a substantial part of its assets.

5.3 Effect of Termination.

(a) Upon termination of this Agreement, in whole or in part, Customer shall pay Licensor for all amounts owed up to the effective date of termination. Termination of this Agreement shall not constitute a waiver for any amounts due.

(b) The following Sections shall survive the termination of this Agreement for any reason: Sections 1, 2.2, 2.4, 3, 4, 5.3, and 6.

(c) No later than thirty (30) days after the date of termination of this Agreement by Licensor, Customer shall upon Licensor's instructions either return the Software and all copies thereof; all Documentation relating thereto in its possession that is in tangible form or destroy the same (including any copies thereof contained on Customer's Designated Hardware). Customer shall furnish Licensor with a certificate signed by an executive officer of Customer verifying that the same has been done.

6. MISCELLANEOUS

If Customer is a corporation, partnership or similar entity, then the license to the Software and Documentation that is granted under this Agreement is expressly conditioned upon and Customer represents and warrants to Licensor that the person accepting the terms of this Agreement is authorized to bind such entity to the terms and conditions herein. If any provision of this Agreement is held to be invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect. During the course of use of the Software, Licensor may collect information on your use thereof; you hereby authorize Licensor to use such information to improve its products and services, and to disclose the same to third parties provided it does not contain any personally identifiable information. The express waiver by either party of any provision, condition or requirement of this Agreement does not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Customer and Licensor are independent parties. Customer may not export or re-export the Software or Documentation (or other materials) without appropriate United States, European Union and foreign government licenses or in violation of the United State's Export Administration Act or foreign equivalents and Customer shall comply with all national and international laws governing the Software. This Agreement will be governed by and construed under the laws of the State of California and the United States as applied to agreements entered into and to be performed entirely within California, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer Information Transactions Act (as promulgated by any State) to this Agreement. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of, the state and federal courts located in Ventura County, California. Customer may not assign this Agreement by operation of law or otherwise, without the prior written consent of Licensor and any attempted assignment in violation of the foregoing shall be null and void. This Agreement cancels and supersedes all prior agreements between the parties. This Agreement may not be varied except through a document agreed to and signed by both parties. Any printed terms and conditions contained in any Customer purchase order or in any Licensor acknowledgment, invoice or other documentation relating to the Software shall be deemed deleted and of no force or effect and any additional typed and/or written terms and conditions contained shall be for administrative purposes only, i.e. to identify the types and quantities of Software to be supplied, line item prices and total price, delivery schedule, and other similar ordering data, all in accordance with the provisions of this Agreement.

Hardware Warranty Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

LIMITED WARRANTY. Xirrus warrants that for a period of five years from the date of purchase by the original purchaser ("Customer"): (i) the Xirrus Equipment ("Equipment") will be free of defects in materials and workmanship under normal use; and (ii) the Equipment substantially conforms to its published specifications. Except for the foregoing, the Equipment is provided AS IS. This limited warranty extends only to Customer as the original purchaser. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' option, repair, replacement, or refund of the Equipment if reported (or, upon request, returned) to the party supplying the Equipment to Customer. In no event does Xirrus warrant that the Equipment is error free or that Customer will be able to operate the Equipment without problems or interruptions.

This warranty does not apply if the Equipment (a) has been altered, except by Xirrus, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Xirrus, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra-hazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL Xirrus OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE EQUIPMENT EVEN IF Xirrus OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Xirrus' or its suppliers' liability to Customer,

whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer.

The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any evaluation Equipment made available for testing or demonstration purposes. All such Equipment is provided AS IS without any warranty whatsoever.

Customer agrees the Equipment and related documentation shall not be used in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or cause or permit any third party to do any of the foregoing.

All information or feedback provided by Customer to Xirrus with respect to the Product shall be Xirrus' property and deemed confidential information of Xirrus.

Equipment including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Equipment.

This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this Warranty shall remain in full force and effect. This Warranty constitutes the entire agreement between the parties with respect to the use of the Equipment.

Manufacturer is Xirrus, Inc. 2101 Corporate Center Drive Thousand Oaks, CA 91320

Appendix E: Medical Usage Notices

Xirrus XR-1000/2000/4000/6000 Series wireless devices have been tested and found to comply with the requirements of IEC 60601-1-2.

Section 5.2.1.1 - The Xirrus wireless device needs special precautions regarding EMC and must be installed and put into service according to the EMC information provided in this User's Guide and in the Quick Installation Guide for the Xirrus Array or AP.

Portable and mobile RF communications equipment can affect Medical Electrical Equipment.

Section 5.2.2.1 (c)

Table 1

Guidance and manufacturer's declaration – electromagnetic emissions		
The Xirrus wireless device is intended for use in the electromagnetic environment specified below. The customer or the user of the Xirrus device should assure that it is used in such an environment.		
Emissions test	**Compliance**	**Electromagnetic environment – guidance**
RF emissions CISPR 11	Group 1	The Xirrus wireless device uses RF energy only for its internal function. Therefore, its RF emissions are very low and are not likely to cause any interference in nearby electronic equipment.
RF emissions CISPR 11	Class A	Xirrus wireless devices are suitable for use in all establishments other than domestic and those directly connected to the public low-voltage power supply network that supplies buildings used for domestic purposes.
Harmonic emissions IEC 61000-3-2	Not Applicable	
Voltage fluctuations/flicker emissions IEC 61000-3-3	Not Applicable	

Section 5.2.2.1 (d) – The Xirrus wireless device should not be used adjacent to or stacked with other equipment. If adjacent or stacked use is necessary, the equipment should be observed to verify normal operation in the configuration in which it will be used.

Section 5.2.2.1 (f)

Table 2

Guidance and manufacturer's declaration – electromagnetic immunity			
Xirrus wireless devices are intended for use in the electromagnetic environment specified below. The customer or the user of the Xirrus wireless device should assure that it is used in such an environment.			
Immunity test	IEC 60601 test level	Compliance level	Electromagnetic environment - guidance
Electrostatic Discharge (ESD) IEC 61000-4-2	± 6 kV contact ± 8 kV air	± 6 kV contact ± 8 kV air	Floors should be wood, concrete or ceramic tile. If floors are covered with synthetic material, the relative humidity should be at least 30%.
Electrical fast transient/burst IEC 61000-4-4	± 2 kV for power supply lines ± 1 kV for input/output lines	Not applicable for power supply lines ± 1 kV for input/ output lines	
Surge IEC 61000-4-5	± 1 kV line(s) to line(s) ± 2 kV line(s) to earth	Not applicable	Not applicable
Voltage dips, short interruptions and voltage variations on power supply input lines IEC 61000-4-11	<5% U_t (>95% dip in U_t) for 0.5 cycle 40% U_t (60% dip in U_t) for 5 cycles 70% U_t (30% dip in U_t) for 25 cycles <5% U_t (>95% dip in U_t) for 5 s	Not applicable	Not applicable
Power frequency (50/60 Hz) magnetic field IEC 61000-4-8	3 A/m	3 A/m	Power frequency magnetic fields should be at levels characteristic of a typical location in a typical commercial or hospital environment.
NOTE U_t is the a.c. mains voltage prior to application of the test level.			

Section 5.2.2.1 (g) Xirrus Wireless devices have no essential performance per IEC 60601-1-2.

Section 5.2.2.2 – Tables 4 and 6

Table 4 for non-life supporting equipment

Guidance and manufacturer's declaration – electromagnetic immunity			
Xirrus wireless devices are intended for use in the electromagnetic environment specified below. The customer or the user of the Xirrus device should assure that it is used in such an environment.			
Immunity test	IEC 60601 test level	Compliance level	Electromagnetic environment - guidance
			Portable and mobile RF communication equipment should be no closer to any part of the Xirrus wireless device, including cables, than the recommended separation distance calculated from the equation applicable to the frequency of the transmitter. Recommended separation distance
Conducted RF IEC 61000-4-6	3 Vrms 150 kHz to 80 MHz	3 V	$d = 1.17 * \sqrt{P}$
Radiated RF IEC61000-4-3	3 V/m 80 MHz to 2.5 GHz	3 V/m	$d = 1.17 * \sqrt{P}$ 80 MHz to 800 MHz $d = 2.33 * \sqrt{P}$ 800 MHz to 2.5 GHz Where *P* is the maximum output power rating of the transmitter in watts (W) according to the transmitter manufacturer and *d* is the recommended separation distance in metres (m). Field strengths from fixed RF transmitters, as determined by an electromagnetic site survey[a], should be less than the compliance level in each frequency range[b]. Interference may occur in the vicinity of equipment marked with this symbol:

NOTE 1 At 80 MHz and 800 MHz, the higher frequency range applies.

NOTE 2 These guidelines may not apply in all situations. Electromagnetic propagation is affected by absorption and reflection from structures, objects and people.

[a] Field strengths from fixed transmitters, such as base stations for radio (cellular/cordless) telephones and land mobile radios, amateur radio, AM and FM radio broadcast and TV broadcast cannot be predicted theoretically with accuracy. To assess the electromagnetic environment due to fixed RF transmitters, an electromagnetic site survey should be considered. If the measured field strength in the location in which Xirrus wireless devices are used exceeds the applicable RF compliance level above, the Xirrus wireless device should be observed to verify normal operation. If abnormal performance is observed, additional measures maybe necessary, such as re-orienting or relocating the Xirrus wireless device.

[b] Over the frequency range 150 kHz to 80 MHz, field strengths should be less than 3 V/m.

Table 6 for non-life supporting equipment

Recommended separation distances between Medical Electrical Equipment and Xirrus Wireless Devices

Xirrus wireless devices are intended for use in an electromagnetic environment in which radiated RF disturbances are controlled. The customer or the user of the Xirrus wireless device can help prevent electromagnetic interference by maintaining a minimum distance between portable and mobile RF communication equipment (transmitters) and the Xirrus wireless device as recommended below, according to the maximum output power of the communications equipment.

Rated maximum output power of transmitter **W**	**Separation distance according to frequency of transmitter** **m**		
	150 kHz to 80 MHz $d = 1.17 * \sqrt{P}$	80 MHz to 800 MHz $d = 1.17 * \sqrt{P}$	800 MHz to 2.5 GHz $d = 2.33 * \sqrt{P}$
0.01	0.12	0.12	0.23
0.1	0.37	0.37	0.74
1	1.17	1.17	2.33
10	3.7	3.7	7.37
100	11.7	11.7	23.3

For transmitters rated a maximum output power not listed above, the recommended separation distance d in metres (m) can be estimated using the equation applicable to the frequency of the transmitter, where P is the maximum output power rating of the transmitter in watts (W) according to the transmitter manufacturer.

NOTE 1 At 80 MHz and 800 MHz, the separation distance for the higher frequency range applies.

NOTE 2 These guidelines may not apply in all situations. Electromagnetic propagation is affected by absorption and reflection for structures, objects and people.

Section 5.2.2.5

RF Channels Supported	
2.4GHz (Exact channels available will be based on country of operation)	1 2 3 4 5 6 7 8 9 10 11 12 13 14
5GHz (Exact channels available will be based on country of operation)	UNII I – Non-DFS Channels: 36 40 44 48 UNII-2A – DFS channel: 52 56 60 64 UNII-2C – DFS channels: 100 104 108 112 116 120 124 128 132 136 140 UNI III – Non-DFS Channels: 149 153 157 161 165

! *Xirrus wireless devices may be interfered with by other equipment, even if that other equipment complies with CISPR EMISSION requirements.*

Section 5.2.2.6

The regulatory limits for maximum output power are specified in EIRP (radiated power). The EIRP level is the transmit power setting for the IAP (specified in dBm). See "IAP Settings" on page 290.

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11d

A supplement to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It allows Access Points to communicate information on the permissible radio channels with acceptable power levels for user devices. Because the 802.11 standards cannot legally operate in some countries, 802.11d adds features and restrictions to allow WLANs to operate within the rules of these countries.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

802.1Q

An IEEE standard for MAC layer frame tagging (also known as encapsulation). Frame tagging uniquely assigns a user-defined ID to each frame. It also enables a switch to communicate VLAN membership information across multiple (and multi-vendor) devices by frame tagging.

AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

beacon interval

When a device in a wireless network sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. Network administrators can adjust the beacon interval—usually measured in milliseconds (ms) or its equivalent, kilo-microseconds (Kmsec).

bit rate

The transmission rate of binary symbols ('0' and '1'), equal to the total number of bits transmitted in one second.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a BSS network. See also, SSID.

CDP

(Cisco Discovery Protocol) CDP is a layer 2 network protocol which runs on most Cisco equipment and some other network equipment. It is used to share information with other directly connected network devices. Information such as the model, network capabilities, and IP address is shared. Wireless Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors.

cell

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11).

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

default gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DHCP lease

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the "domain" address for Google is: http://www.google.com, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.
- **www** is a reference to the World Wide Web.
- **google** refers to the company.
- **com** specifies that the domain belongs to a commercial enterprise.

DTIM

(Delivery Traffic Indication Message) A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

EAP

(Extensible Authentication Protocol) When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). However, LCP is somewhat inflexible because it has to specify an authentication device early in the process. EAP allows the system to gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP (for example, passwords and public keys).

EDCF

(Enhanced Distributed Coordinator Function) A QoS extension which uses the same contention-based access mechanism as current devices but adds "offset contention windows" that separate high priority packets from low priority packets (by assigning a larger random backoff window to lower priorities than to higher priorities). The result is "statistical priority," where high-priority packets usually are transmitted before low-priority packets.

encapsulation

A way of wrapping protocols such as TCP/IP, AppleTalk, and NetBEUI in Ethernet frames so they can traverse an Ethernet network and be unwrapped when they reach the destination computer.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

Fast Ethernet

A version of standard Ethernet that runs at 100 Mbps rather than 10 Mbps.

FCC

(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 establishes a computer security standard used to accredit cryptographic modules. The standard is a joint effort by the U.S. and Canadian governments.

frame

A packet encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

Gigabit 1 through 4

The Gigabit Ethernet interfaces on XR Series Arrays. XR-4000 Series Arrays have two gigabit interfaces, while XR-6000 Series and higher models have four gigabit interfaces. See also, Gigabit Ethernet.

Gigabit Ethernet

A version of Ethernet with data transfer rates of 1 Gigabit (1,000 Mbps).

Group

A user group, created to define a set of attributes (such as VLAN, traffic limits, and Web Page Redirect) and privileges (such as fast roaming) that apply to all users that are members of the group. This allows a uniform configuration to be easily applied to multiple user accounts. The attributes that can be configured for user groups are almost identical to those that can be configured for SSIDs.

host name

The unique name that identifies a computer on a network. On the Internet, the host name is in the form **comp.xyz.net**. If there is only one Internet site the host name is the same as the domain name. One computer can have more than one host name if it hosts more than one Internet site (for example, **home.xyz.net** and **comp.xyz.net)**. In this case, **comp** and **home** are the host names and **xyz.net** is the domain name.

IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs.

MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTU

(Maximum Transmission Unit) The largest physical packet size—measured in bytes—that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

PLCP

(Physical Layer Convergence Protocol) Defined by IEEE 802.6, a protocol specified within the Transmission Convergence layer that defines exactly how cells are formatted within a data stream for a particular type of transmission facility.

PoGE

This refers to the optional Xirrus-supplied Power over Gigabit Ethernet modules that provide DC power to Arrays. Power is supplied over the same Cat 5e or Cat 6 cable that supplies the data connection to your gigabit Ethernet switch, thus eliminating the need to run a power cable.

preamble

Preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. PLCP Has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

private key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

PSK

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

public key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider prioritizes or guarantees a service's performance.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SDMA

(Spatial Division Multiple Access) A wireless communications mode that optimizes the use of the radio spectrum and minimizes cost by taking advantage of the directional properties of antennas. The antennas are highly directional, allowing duplicate frequencies to be used for multiple zones.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSH

(Secure SHell) Developed by SSH Communications Security, Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. The Array only allows SSH-2 connections. SSH-2 provides strong authentication and secure communications over insecure channels. SSH-2 protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot "play back" the traffic or hijack the connection when encryption is enabled. When using SSH-2's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords. Be aware that your SSH utility must be set up to use SSH-2.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

TKIP

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven't been tampered with.

transmit power

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

User group

See Group.

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

VLAN tagging

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the 802.11n standard, traffic can be confined to VLANs that exist on multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

1. That the packet has a tag.
2. Whether the packet should have priority over other packets.
3. Which VLAN it belongs to, so that the switch can forward or filter it correctly.

WDS (Wireless Distribution System)

WDS creates wireless backhauls between arrays. These links between arrays may be used rather than having to install data cabling to each array.

WEP

(Wired Equivalent Privacy) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

Wi-Fi Alliance

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

Wireless Array

A high capacity wireless networking device consisting of multiple radios arranged in a circular array.

WPA

(Wi-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1x for authentication.

WPA2

(Wi-Fi Protected Access 2) WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.

Xirrus Management System (XMS)

A Xirrus product used for managing large Wireless Array deployments from a centralized Web-based interface.

XP1 and XP8—Power over Gigabit Ethernet modules

See PoGE.

XPS—Xirrus Power System

A family of optional Xirrus-supplied products that provides power over Gigabit Ethernet. See PoGE.

Index

Numerics

11ac
see 802.11ac 325
802.11a 3, 4, 290, 311
802.11a/b/g 28
802.11a/b/g/n 15
802.11a/n 15, 66, 262
802.11ac
WMI page 325
802.11b 3, 4, 316
802.11b/g 290, 316
802.11b/g/n 15, 66, 262
802.11e 17
802.11g 3, 4, 316
802.11i 4, 75, 159
802.11n 4
WMI page 322
802.11p 17
802.11q 17
802.1x 4, 50, 60, 75, 159, 494

A

abg(n)
nomenclature 2
abg(n)2
intrusion detection 352
self-monitoring
radio assurance (loopback mode) 334, 335
Access Control List 213
Access Control Lists 494
access control lists (ACLs) 234, 276
Access Point 159
Access Points, XR
overview 4
access points, XR 1
account, user 246
ACLs 50, 213, 494
active directory 246
active IAPs
per SSID 275
Address Resolution Protocol
window 106
Address Resolution Protocol (ARP) 308
Admin 494
Admin ID 219
admin ID
authentication via RADIUS 223
Admin Management 219
admin privileges
setting in admin RADIUS account 223
admin RADIUS account
if using Console port 223
admin RADIUS authentication 223
administration 75, 159, 213
Administrator Account 488
Advanced Encryption Standard 50, 494
Advanced RF Analysis Manager
see RAM 20
Advanced RF Performance Manager
see RPM 18
Advanced RF Security Manager
see RSM 19
AeroScout
see WiFi tag 183
AES 4, 17, 50, 60, 75, 159, 486, 494
AirWatch 380
Airwatch
CLI command 446
allow traffic
see filters 365
Analysis Manager
see RAM 20

appearance
WMI options 406
application control
update (signature file) 395
approved
setting rogues 116
APs 60, 116, 250, 251, 494
rogues, blocking 351
APs, rogue
see rogue APs 333, 352
APs, XR
overview 4
ARP filtering 308
ARP table window 106
Array 30, 66, 82, 159, 166
connecting 66
dismounting 66
management 385
mounting 66
powering up 66
securing 66
Web Management Interface 82
XR-2000 Series 8, 9
XR-2005 Series 8, 9
ArrayOS
upgrade 388
Arrays
managing in clusters 374
Arrays, XR 1
overview 4
associated users 30
assurance
network server connectivity 109, 230
assurance (radio loopback testing) 333
assurance, station
see station assurance 340
attack (DoS)
see DoS attack 353
attack (impersonation)
see impersonation attack 354
auth CLI command 424
authentication 17, 246
of admin via RADIUS 223
authentication (Oauth token)
CLI command
auth 424
authority
certificate 217, 231
auto block
rogue APs, settings 352
auto negotiate 166
auto-blocking
rogue APs 351
auto-configuration 75, 295, 311, 316
channel and cell size 333
automatic refresh
setting interval 406
automatic update from remote server
configuration files, boot image 390

B

backhaul
see WDS 57
backup unit
see standby mode 334
band association 262
beacon interval 295
Beacon World Mode 295
beam distribution 15
benefits 14
block
rogue APs, settings 349
block (rogue APs)
see auto block 352
blocking
rogue APs 351
blocking rogue APs 333
bond
mode, bridging 169

boot 388
bridging APs 169
broadcast 309
  fast roaming 309
browser
  certificate error 217, 231
BSS 492
BSSID 116, 492
buttons 87

C

capacity
  of 802.11n 45
cascading style sheet
  sample for web page redirect 397
cdp 424
CDP (Cisco Discovery Protocol)
  settings 177
cdp CLI command 424
CDP neighbors 108
cell
  sharp cell 333
cell size 30, 290
  auto-configuration 333
cell size configuration 333
certificate
  about 217, 231
  authority 217, 231
  error 217, 231
  install Xirrus authority 231
  X.509 217, 231
chain
  see bridging 169
channel
  auto-configuration 333
  configuration 333
  list selection 333
channels 30, 116, 290, 295, 311, 316
  non-overlapping 16
CHAP (Challenge-Handshake Authentication Protocol)
  Admin RADIUS settings 224
  web page redirect 271
CHAP Challenge Handshake Authentication Protocol)
  RADIUS ping 398
character restrictions 89
Chrome 26
Cisco Discovery Protocol
  see cdp 424
Cisco Discovery Protocol (CDP) 177
CLI 4, 60, 63, 69, 71, 409
  executing from WMI 399
  using to upgrade software image 506
  vs. XMS 81
CLI commands
  see commands 424
client
  web page redirect 396
cluster
  CLI command 428
clusters 374
  defining 375
  management 376
  operating in cluster mode 377
command
  wifi-tag 464
Command Line Interface 4, 56, 63, 66, 69, 71, 409, 494
  configuration commands 422
  getting help 411
  getting started 411
  inputting commands 411
  sample configuration tasks 466
  SSH 409
  top level commands 413
command, utilities
  ping, traceroute, RADIUS ping 397

commands
acl 422
admin 423
auth, authentication 424
cdp 424
clear 426
cluster 428
configure 414
contact-info 429
date-time 430
dhcp-server 431
dns 432
file 433
filter 437
group 428, 441
hostname 441
interface 442
load 442
location 443
location-reporting 444, 455
management 445
mdm (mobile device management)
Airwatch 446
more 447
netflow 448
no 449
quit 452
radius-server 451, 452
reboot 453, 463
reset 453
restore 454
run-tests 456
security 458
show 417
snmp 459
ssid 460
statistics 420
syslog 461
tunnel 462
vlan 463
Community String 485
configuration 157, 494
express setup 159
reset to factory defaults 393
configuration changes
applying 89
configuration files
automatic update from remote server 390
download 391
update from local file 391
update from remote file 391
connection
tracking window 107
connectivity
servers, see network assurance 109, 230
Console port
login via 223
coverage 30, 63
extended 15
coverage patterns 4
critical messages 86
CTS/RTS 311, 316

D

daisy chain
see bridging 169
data rate 311, 316
date/time restrictions
and interactions 285
default gateway 75, 166
default settings 483
Default Value 486
DHCP 485
defaults
reset configuration to factory defaults 393
Delivery Traffic Indication Message 295

denial of service
see DoS attack 353
deny traffic
see filters 365
deployment 28, 56, 60, 63, 494
ease of 17
detection
intrusion 352
see DoS attack 353
see impersonation attack 354
see impersonation detection 353
see intrusion detection 353, 354
device management
see Mobile Device Management 380
DHCP 30, 69, 71, 75, 159, 166, 484
default settings 485
leases window 107
DHCP Server 179
diagnostics
log, create file 394
directory, active 246
display
WMI options 406
DNS 75, 159, 176
DNS domain 176
DNS server 176
Domain Name System 176
DoS attack detection
settings 353
DTIM 295
DTIM period 295
duplex 166
dynamic VLAN
overridden by group 283

E

EAP 486, 494
EAP-MDS 17
EAP-PEAP 494
EAP-TLS 17, 50, 494
EAP-TTLS 17, 50, 494
EDCF 295
Encryption 486, 494
encryption 17
encryption method
recommended (WPA2 with AES) 215
setting 216
support of multiple methods 215
encryption method (encryption mode)
Open, WEP, WPA, WPA2, WPA-Both 215
encryption standard
AES, TKIP, both 215
setting 216
Enterprise 1, 3, 494
WLAN 3
Enterprise Class Management 4
Enterprise Class Security 4
ESS 492
ESSID 492
Ethernet 63, 66, 69, 71, 75, 159
Euclid
location service
data format 504
event log
IDS (intrusion detection) 155
see system log 146, 153
event messages 86
Express Setup 66, 75, 159
express setup 75, 159
Extended Service Set 492
Extensible Authentication Protocol 494
external RADIUS server 802.1x 27

F

factory default settings 483
factory defaults 484, 485, 486, 488
DHCP 485

reset configuration to 391
factory.conf 391
fail-over
standby mode 334
failover 47, 60
FAQs 492
Fast Ethernet 63, 69, 71, 159, 166, 483
fast roaming 17, 103, 309
about 288
and VLANs 289
features 14, 56, 166, 182, 186, 295, 494
and license key 389
feedback 87
filter list 366
filter name 368
filtering
IPv6 309
filters 365, 366, 368
stateful filtering, disabling 366
statistics 143
Firefox 26
firewall 365
and port usage 52
stateful filtering, disabling 366
fragmentation threshold 311, 316
frequently asked questions 492
FTP 494
FTP server 27

G

General Hints 491
getting started
express setup 159
Gigabit 63, 69, 71, 75, 159, 166, 483
global settings 295, 311, 316
glossary of terms 561
Google Chrome 26
Group
management 282
group 280
CLI command 428, 441
VLAN overrides dynamic VLAN 283
group limits and interactions 285
Group Rekey 486
GUI
see WMI 406

H

help 87
button, bottom of page 87
button, left frame 85
Help button 82
honeypot 278
honeypot SSID
whitelist settings 279
host name 75, 82, 159, 176
hs.css 397
HTTPS
certificate, see certificate 231
HTTPS port
web page redirect 269, 274
HyperTerminal 26, 63

I

IAP 30, 66, 75, 159, 290, 311, 316, 354
active SSIDs 275
fast roaming 288
Intrusion Detection (IDS/IPS) 348
naming 2
settings 290
IAP LED 66, 354
IAP LED settings 354
IAPs
auto block rogues 352
intrusion detection 352
IDS
see Intrusion Detection 348
IDS event log
viewing window 155

IEEE 3, 75, 159
IEEE 802.11ac
  WMI page 325
IEEE 802.11n
  capacity, increased 45
  multiple data streams 39
  spatial multiplexing 39
  WMI page 322
IEEE 802.1Q 497
image
  upgrade software image 388
impersonation attack detection
  settings 354
implementing Voice over Wi-Fi 28, 204, 256
installation 25, 61, 66, 481
  installing the MCAP-3616 63
  mounting the unit 66
  requirements 25
  workflow 61
installation workflow 61
interfaces 159
  Web 81
internal login page
  web page redirect 269
  web page redirect, customize 272
internal splash page
  web page redirect 270
  web page redirect, customize 272
Internet Explorer 26
interval
  automatic WMI refresh 406
intrusion detection 116, 352
  and auto block settings 352
  configuration 333
  setting as approved or known 116
intrusion detection (IDS)
  viewing event log 155
Intrusion Detection (IDS/IPS) 348
IP Address 30, 75, 82, 88, 116, 159, 166, 176, 186, 191, 385, 484
IP Subnet Mask 75
IPS
  see Intrusion Detection 348
IPv6
  filtering 309

K

key
  upgrade 389
key features 14
Keyboard Shortcuts 489
keyboard shortcuts 489
known
  setting rogues 116

L

lastboot.conf 391
Layer 3
  fast roaming 288
LDAP 246
lease 484
Lease Time 484
leases, DHCP
  viewing 107
LEDs 66
  sequence 66
  settings 354
license Key
  upgrading 389
limits
  group 285
  interactions 285
  station 285
  traffic 285
list, access control
  see access control list 234, 276
list, MAC access
  see access control list 234

list, SSID access
see access control list 276
local management vs. XMS 81
location
CLI command
location-reporting 444, 455
location information 75, 82, 159
location service
data formats 504
log
diagnostics, create file 394
log messages
counters 86
log, IDS(intrusion detection)
viewing window 155
log, system (event)
viewing window 146, 153
logging in 69, 71, 88
Login 88
login
via Console port 223
login page
web page redirect 269, 396
web page redirect, customize 272
logout 407
long retry limit 295
loopback
see radio assurance 478
loopback testing
radio assurance mode 333

M

MAC 50, 69, 71, 492, 494
MAC Access Control Lists 50
MAC Access List 234
MAC address 234, 492, 494
Management 488, 494
management 91, 157, 385
Array clusters 374
local vs. XMS 81
of Arrays 385
Web Management Interface (WMI) 81
management (XMS) 17
maximum lease 484
Maximum Lease Time 484
MDM
see Mobile Device Management 380
Megabit 75
Message Integrity Check 494
messages
syslog counters 86
MIC 17, 494
Mobile Device Management
AirWatch 380
mobile device management
Airwatch (CLI command) 446
Mobile Device Management (MDM) 380
Mobilize 17
mode
cluster operating mode 377
monitoring
intrusion detection 116
see intrusion detection 352
mounting 66
mounting plate 66
mounting the unit 66
MTU 166
size 166
multiple data streams 39

N

NAT
table - see connection tracking 107
neighbors, CDP 108
Netflow 182
netflow
CLI command 448

network
interfaces 165
settings 166
network assurance 109, 230
network connections 63, 88, 494
network installation 25, 481
network interface ports 69, 71
network interfaces 166, 483
network status
ARP table window 106
connection
tracking window 107
routing table window 106
viewing leases 107
Network Time Protocol 75, 159, 180
network tools
ping, traceroute, RADIUS ping 397
nomenclature 2
non-overlapping channels 16
NTP 75, 159, 180, 484
NTP Server 180

O

Oauth
CLI command
auth 424
Open (encryption method) 215
optimization, VLAN 309
options
WMI 406
overview 4

P

PAP (Password Authentication Protocol)
Admin RADIUS settings 224
RADIUS ping 398
web page redirect 271
passphrase 50, 75, 159
Password 488, 494
password 88
PEAP 17, 361
performance 14
Performance Manager
see RPM 18
Ping 385
ping 397
planning 47, 49, 50, 56
failover 47
network management 56
port failover 47
power 49
security 50
switch failover 47
WDS 57
PoGE 25
see Power over Gigabit Ethernet 12
PoGE Power Injectors 1
port failover 47
port requirements 52
power outlet 25
Power over Gigabit Ethernet 2, 25, 49, 63
Power over Gigabit Ethernet (PoGE) 12
power planning 49
pre-shared key 50, 60, 494
Print button 82
probe
see Netflow 182
product installation 25, 481
product overview 4
product specifications 24
PSK 60, 486
PuTTY 25, 56, 75, 159, 494
PuTTy 26

Q

QoS 17, 262, 486, 492, 568
conflicting values 259
levels defined 263, 283

priority 262
SSID 256, 263
about setting QoS 493
default QoS 486
user group 283
quality
of user experience 340
Quality of Service 17
see QoS 263, 283
quick reference guide 483
quick start
express setup 159

R

radio
assurance (self-test) 334, 335
radio assurance (loopback testing) 333
radio assurance (loopback) mode 334, 335
radio distribution 14
radios
naming 2
RADIUS 4, 25, 50, 60, 213, 234, 276, 484, 494
admin authentication 223
setting admin privileges 223
setting user VSAs 241
Vendor Specific Attributes (VSAs) 503
RADIUS ping
CHAP Challenge Handshake Authentication Protocol) 398
PAP (Password Authentication Protocol) 398
RADIUS Ping command 397
RADIUS Server 484
RADIUS server 27
RADIUS settings
web page redirect 271
RAM (RF Analysis Manager) 20
reauthentication 295
reboot 388
redirect (WPR) 396
refresh interval
WMI 406
remote boot image
automatic update from remote TFTP server 390
remote configuration
automatic update from remote server 390
remote TFTP server
automatic update of boot image, configuration 390
Reset 385, 484
reset configuration
to factory defaults 393
restore command 454
restrictions
date/time 285
stations 285
traffic 285
RF
intrusion detection 333
spectrum management 333
RF Analysis Manager
see RAM 20
RF configuration 333
RF management
see channel 333
RF Performance Manager
see RPM 18
RF resilience 333
RF Security Manager
see RSM 19
roaming 17, 103, 309
see fast roaming 288
Rogue AP 4, 56, 116, 250, 251, 494
rogue AP
blocking 351

settings for blocking 349
Rogue AP List 116
rogue APs
auto block settings 352
blocking 333
Rogue Control List 250, 251
rogue detection 15
rogues
setting as known or approved 116
root command prompt 413
route
trace route utility 397
routing table window 106
RPM (RF Performance Manager) 18
RSM (RF Security Manager) 19
RSSI 116
RTS 311, 316
RTS threshold 311, 316

S

Safari 26
sample Perl and CSS files for 396
save
with reboot 388
Save button 82
saved.conf 391
scalability 3
schedule
auto channel configuration 333
Secondary Port 484
Secondary Server 484
secret 484
Secure Shell 26
secure Shell 25
security 4, 17, 213, 492, 494
certificate, see certificate 231
Security Manager
see RSM 19
see group 280
self-monitoring 352
radio assurance 478
radio assurance options 334, 335
self-test
radio assurance mode 334, 335
serial port 26, 69, 71, 494
server, VTun
see VTun 208
servers
connectivity, see network assurance 109, 230
Service Set Identifier 75
Services 179, 492
servicing the unit 481
settings 159
setup, express 159
sharp cell 333
setting in WMI 337
short retry limit 295
signal processing
MIMO 39
signature file
update (application control) 395
SNMP 4, 13, 75, 159, 166, 179, 191, 485
required for XMS 191, 192
software
upgrade license key 389
software image
upgrading via CLI 506
Software Upgrade 385
software upgrade 388
spatial multiplexing 39
specifications 24
spectrum (RF) management 333
speed 3, 69, 71, 166
11 Mbps 3
54 Mbps 3
splash page
web page redirect 270, 396
web page redirect, customize 272

SSH 25, 26, 56, 75, 159, 166, 214, 488, 494
SSH-2 214
SSID 4, 75, 82, 116, 159, 251, 262, 486, 492, 497
about usage 493
active IAPs 275
honeypot 278
honeypot, whitelist 279
QoS 256, 263
about using 493
QoS, about usage 493
rogue control list 250
web page redirect settings 266
web page redirect settings, about 269, 274
web page redirect settings, whitelist 273
whitelist, honeypot 278
SSID Access List 276
SSID address 276
SSID Management 262, 486, 492
standby mode 334
stateful filtering
disabling 366
static IP 75, 159, 166
station
assurance 340
station assurance 340
station timeout period 295
Stations 492
stations
limits and interactions 285
rogues 116
statistics 144
statistics per station 145
statistics 159
filters 143
netflow 182
per-station 145
stations 144
WDS 140
status bar 82
submitting comments 87
subnet 25, 47, 75, 166
switch failover 47
synchronize 75, 159, 180
Syslog 75, 82, 159, 179, 186, 484
time-stamping 75
syslog messages
counters 86
Syslog reporting 186
Syslog Server 186
system commands
ping, trace route, RADIUS ping 397
System Configuration Reset 385
System Log 186
system log
viewing window 146, 153
System Reboot 385
System Tools 385
system tools 386

T

tag, WiFi 183
TCP
port requirements 52
technical support
frequently asked questions 492
Telnet 214, 488, 494
Temporal Key Integrity Protocol 494
TFTP server
automatic update of boot image, configuration 390
Time Out 484
time zone 75, 159, 180
timeout 295, 385
Tips 491
TKIP 17, 50, 60, 75, 159, 486, 494

TKIP encryption
and XR Arrays 237
token
CLI command
auth 424
tool
ping, trace route, RADIUS ping 397
Tools 385, 494
tools, network 397
tools, system 386
trace route utility 397
traffic
filtering 365
limits and interactions 285
transmit power 30
Trap Host 485
trap port 191, 485
tunnel
CLI command 462
tunneled
fast roaming 309
Tunnels 209
tunnels
see VTun 204, 208

U

UDP
port requirements 52
unknown
setting rogues 116
update
signature file (application control) 395
upgrade
license key 389
software image 388
upgrading software image
via CLI 506
user accounts 246
setting RADIUS VSAs 241
user group 280
QoS 283
user group limits and interactions 285
user interface 81
utilities
ping, trace route, RADIUS ping 397
utility buttons 87

V

Vendor Specific Attributes (VSAs)
RADIUS 503
RADIUS, for Xirrus 503
virtual tunnels
see VTun 208
VLAN 4, 60, 262, 486, 492, 497
broadcast optimization 309
dynamic
overridden by group 283
group (vs. dynamic VLAN) 283
vlan
CLI command 463
VLAN ID 262
VLANs 204
and fast roaming 289
voice
fast roaming 288
implementing on Array 28, 204, 256
Voice-over IP 316
VoIP 316
VoWLAN 17
VPN 75, 159, 494
VTS
Virtual Tunnel Server 204, 208
VTun
specifying tunnel server 204, 208
understanding 204

W

wall thickness considerations 28
warning messages 86
WDS 358, 361
  about 57
  long distance 294, 360
  planning 57
  statistics 140
  timeouts 294, 360
WDS Client Links 361
Web interface
  structure and navigation 85
web interface 81
Web Management Interface 56, 66, 69, 71, 88, 492
Web Management Interface (WMI) 81
web page redirect 396
  also called WPR 396
  CHAP (Challenge-Handshake Authentication Protocol) 271
  customize internal login/splash page 272
  HTTPS port 269, 274
  install files for 396
  internal login page 269
  internal splash page 270
  PAP, CHAP 271
  RADIUS settings 271
  remove files for 397
  sample WPR files 397
  SSID settings 266
  SSID settings, about 269, 274
  whitelist settings, about 273
WEP 17, 50, 75, 159, 213, 262, 486, 494
WEP (Wired Equivalent Privacy)
  encryption method 215
WEP encryption
  and XR Arrays 238
whitelist
  honeypot 278, 279
  web page redirect 273
Wi-Fi Protected Access 4, 50, 75, 159, 494
WiFi tag 183
wifi-tag
  CLI command 464
Wired Equivalent Privacy 75, 494
Wireless Distribution System 358
wireless LAN 3
wireless security 159
WLAN 159
WMI 4, 56, 60, 69, 71, 81, 290
  appearance options 406
  certificate error 217, 231
  executing CLI commands 399
  options 406
  refresh interval 406
  vs. XMS 81
workflow 61
WPA 4, 60, 75, 159, 213, 262, 486, 494
WPA (Wi-Fi Protected Access) and WPA2
  encryption method 215
WPA2 4
WPR
  see web page redirect 396
wpr.pl 396, 397

X

X.509
  certificate 217, 231
Xirrus
  certificate authority 231
Xirrus Advanced RF Analysis Manager
  see RAM 20
Xirrus Advanced RF Performance Manager
  see RPM 18
Xirrus Advanced RF Security Manager

see RSM 19
Xirrus Management System 4, 13, 17, 25, 27, 56, 494
SNMP required 191, 192
Xirrus Management System (XMS) 1
Xirrus PoGE Power Injectors 1
Xirrus Roaming Protocol 17, 103, 309
XMS 4, 13, 17, 27
port requirements 52
setting IP address of 191
SNMP required 191, 192
vs. local management 81
XMS-9000-CL-x 2
XP PoGE Power Injectors 1
XP1, XP8
see Power over Gigabit Ethernet 12
XPS 25
XR Array
management 157, 385
XR Arrays 1
overview 4
XR-2000 Series 8, 9
XR-2005 Series 8, 9
XRP 17, 103, 309
xs_current.conf 391
xs_diagnostic.log 394

XIRRUS®
High Performance Wireless Networks

1.800.947.7871 Toll Free in the US
+1.805.262.1600 Sales
+1.805.262.1601 Fax
2101 Corporate Center Drive
Thousand Oaks, CA 91320, USA

To learn more visit:
xirrus.com or
email info@xirrus.com

© 2013 Xirrus, Inc. All Rights Reserved. The Xirrus logo is a registered trademark of Xirrus, Inc.
All other trademarks are the property of their respective owners. Content subject to change without notice.

800-0022-001J