
SSID/VLAN/Security

The AP provides several security features to protect your network from unauthorized access. This section gives an overview of VLANs and then discusses the SSID/VLAN/Security configuration options in the AP:

- [VLAN Overview](#)
- [Management VLAN](#)
- [Security Profile](#)
- [MAC Access](#)
- [Wireless](#)

The AP also provides Broadcast SSID/Closed System and Rogue Scan to protect your network from unauthorized access. See the [Broadcast SSID and Closed System](#) and [Rogue Scan](#) sections for more information.

VLAN Overview

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to clients) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify traffic flow between clients and their frequently-used or restricted resources.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

AP devices are fully VLAN-ready; however, by default VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured, and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

Once enabled, VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
 - Improve network performance and reduce latency
- Increase security
 - Secure network restricts members to resources on their own VLAN
 - Clients roam without compromising security

VLAN tagged data is collected and distributed through an AP's wireless interface(s) based on Network Name (SSID). An Ethernet port on the access point connects a wireless cell or network to a wired backbone. The access points communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports. On the wired network, a RADIUS server authenticates traffic and a DHCP server manages IP addresses for the VLAN(s). Resources like servers and printers may be present, and a hub may include multiple APs, extending the network over a larger area.

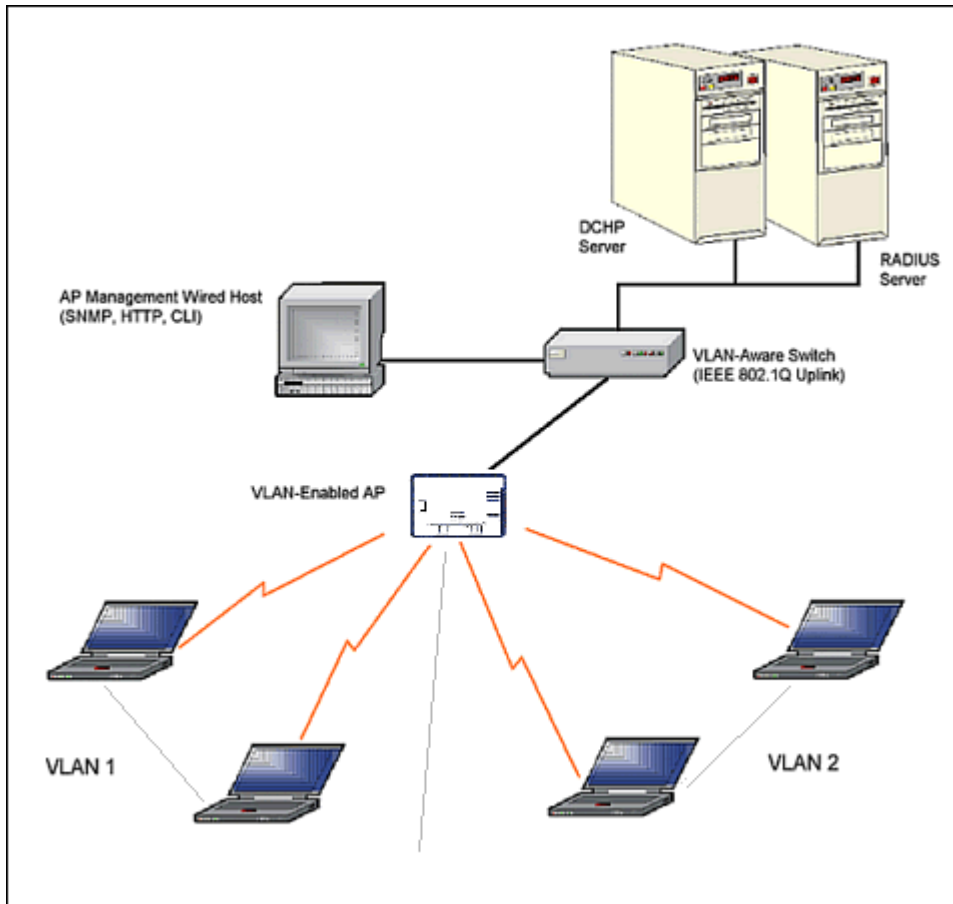


Figure 4-36 Components of a Typical VLAN

VLAN Workgroups and Traffic Management

Access Points that are not VLAN-capable typically transmit broadcast and multicast traffic to all wireless Network Interface Cards (NICs). This process wastes wireless bandwidth and degrades throughput performance. In comparison, a VLAN-capable AP is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 16 SSIDs, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a workgroup; for example, one VLAN could be used for an EMPLOYEE workgroup and the other for a GUEST workgroup.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as EMPLOYEE or GUEST, depending on which wireless NIC received it. The AP would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the EMPLOYEE workgroup to the appropriate corporate resources such as printers and servers. Packets from the GUEST workgroup could be restricted to a gateway that allowed access to only the Internet. A member of the GUEST workgroup could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

Typical User VLAN Configurations

VLANs segment network traffic into workgroups, which enable you to limit broadcast and multicast traffic. Workgroups enable clients from different VLANs to access different resources using the same network infrastructure. Clients using the same physical network are limited to those resources available to their workgroup.

The AP can segment users into a maximum of 16 different workgroups per radio, based on an SSID/VLAN grouping (also referred as a VLAN Workgroup or a Sub-network).

The primary scenarios for using VLAN workgroups are as follows:

1. VLAN disabled: Your network does not use VLANs, and you cannot configure the AP to use multiple SSIDs.
2. VLAN enabled, each VLAN workgroup uses a different VLAN ID Tag.
3. VLAN enabled, a mixture of Tagged and Untagged workgroups exist.
4. VLAN enabled, all VLANs untagged: VLAN is enabled in order to use SSID. (Note that typical use of SSIDs assumes actual use of VLANs.)

NOTE: VLAN must be enabled to configure security per SSID.

Management VLAN

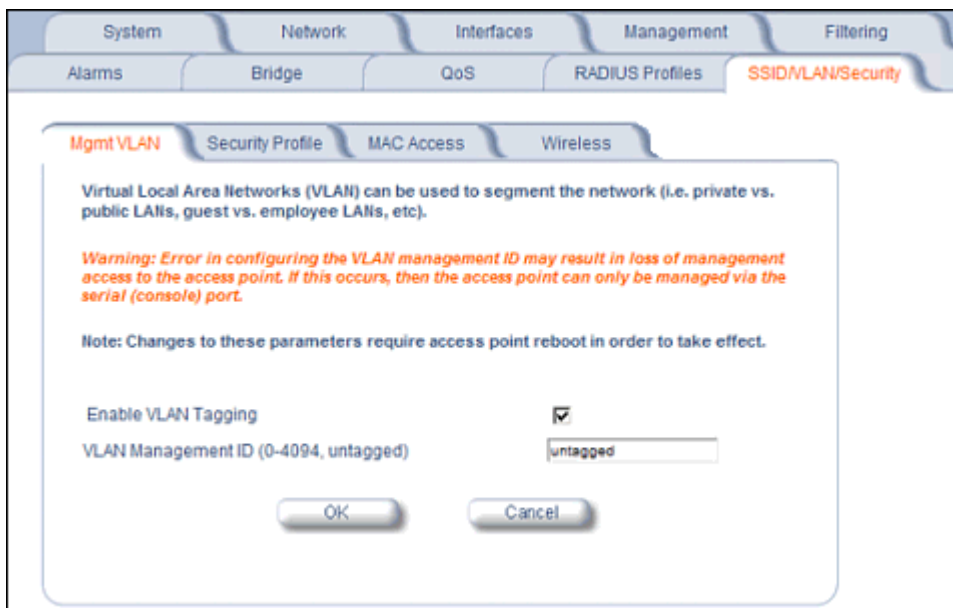


Figure 4-37 Mgmt VLAN

VLAN Tagging Management

Control Access to the AP

Management access to the AP can easily be secured by making management stations or hosts and the AP itself members of a common VLAN. Simply configure a non-zero management VLAN ID and enable VLAN to restrict management of the AP to members of the same VLAN.

CAUTION: If a non-zero management VLAN ID is configured then management access to the AP is restricted to wired or wireless hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the AP.

1. Click **Configure** > **SSID/VLAN/Security** > **Mgmt VLAN**.
2. Set the VLAN Management ID to a value of between 1 and 4094. (A value of -1 disables VLAN Tagging).

3. Place a check mark in the **Enable VLAN Tagging** box.

Provide Access to a Wireless Host in the Same Workgroup

The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN User ID, then those wireless clients who are members of that VLAN will have AP management access.

CAUTION: *Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.*

1. Click **Configure > SSID/VLAN/Security > Mgmt VLAN**.
2. Set the **VLAN Management ID** to use the same VLAN ID as one of the configured SSIDs.
3. Place a check mark in the **Enable VLAN Tagging** box.

Disable VLAN Tagging

1. Click **Configure > SSID/VLAN/Security > Mgmt VLAN**.
2. Remove the check mark from the **Enable VLAN Tagging** box (to disable all VLAN functionality) or set the **VLAN Management ID** to -1 (to disable VLAN Tagging only).

NOTE: *If you disable VLAN Tagging, you will be unable to configure security per SSID.*

Security Profile

The AP supports the following security features:

- **WEP Encryption:** The original encryption technique specified by the IEEE 802.11 standard.
- **802.1x Authentication:** An IEEE standard for client authentication.
- **Wi-Fi Protected Access (WPA/802.11i [WPA2]):** A new standard that provides improved encryption security over WEP.

NOTE: *The AP does not support shared key 802.11 MAC level authentication. Clients with this MAC level feature must disable it.*

WEP Encryption

The IEEE 802.11 standards specify an optional encryption feature, known as Wired Equivalent Privacy or WEP, that is designed to provide a wireless LAN with a security level equal to what is found on a wired Ethernet network. WEP encrypts the data portion of each packet exchanged on an 802.11 network using an Encryption Key (also known as a WEP Key).

When Encryption is enabled, two 802.11 devices must have the same Encryption Keys and both devices must be configured to use Encryption in order to communicate. If one device is configured to use Encryption but a second device is not, then the two devices will not communicate, even if both devices have the same Encryption Keys.

802.1x Authentication

IEEE 802.1x is a standard that provides a means to authenticate and authorize network devices attached to a LAN port. A port in the context of IEEE 802.1x is a point of attachment to the LAN, either a physical Ethernet connection or a wireless link to an Access Point. 802.1x requires a RADIUS server and uses the Extensible Authentication Protocol (EAP) as a standards-based authentication framework, and supports automatic key distribution for enhanced security. The EAP-based authentication framework can easily be upgraded to keep pace with future EAP types.

Popular EAP types include:

- **EAP-Message Digest 5 (MD5):** Username/Password-based authentication; does not support automatic key distribution
- **EAP-Transport Layer Security (TLS):** Certificate-based authentication (a certificate is required on the server and each client); supports automatic key distribution

- EAP-Tunneled Transport Layer Security (TTLS): Certificate-based authentication (a certificate is required on the server; a client's username/password is tunneled to the server over a secure connection); supports automatic key distribution
- PEAP - Protected EAP with MS-CHAP: Secure username/password-based authentication; supports automatic key distribution

Different servers support different EAP types and each EAP type provides different features. See the documentation that came with your RADIUS server to determine which EAP types it supports.

NOTE: The AP supports the following EAP types when Security Mode is set to 802.1x, WPA, or 802.11i (WPA2): EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, and EAP-SIM.

Authentication Process

There are three main components in the authentication process. The standard refers to them as:

1. Supplicant (client PC)
2. Authenticator (Access Point)
3. Authentication server (RADIUS server)

When the Security Mode is set to 802.1x Station, WPA Station, or 802.11i Station you need to configure your RADIUS server for authentication purposes.

Prior to successful authentication, an unauthenticated client PC cannot send any data traffic through the AP device to other systems on the LAN. The AP inhibits all data traffic from a particular client PC until the client PC is authenticated. Regardless of its authentication status, a client PC can always exchange 802.1x messages in the clear with the AP (the client begins encrypting data after it has been authenticated).

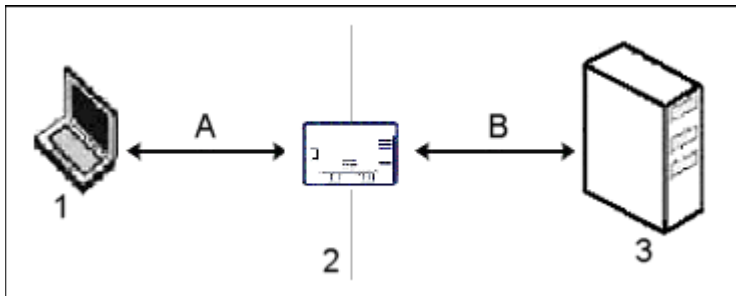


Figure 4-38 RADIUS Authentication Illustrated

The AP acts as a pass-through device to facilitate communications between the client PC and the RADIUS server. The AP (2) and the client (1) exchange 802.1x messages using an EAPOL (EAP Over LAN) protocol (A). Messages sent from the client station are encapsulated by the AP and transmitted to the RADIUS (3) server using EAP extensions (B).

Upon receiving a reply EAP packet from the RADIUS, the message is typically forwarded to the client, after translating it back to the EAPOL format. Negotiations take place between the client and the RADIUS server. After the client has been successfully authenticated, the client receives an Encryption Key from the AP (if the EAP type supports automatic key distribution). The client uses this key to encrypt data after it has been authenticated.

For 802.11a and 802.11b/g clients that communicate with an AP, each client receives its own unique encryption key; this is known as Per User Per Session Encryption Keys.

Wi-Fi Protected Access (WPA/802.11i [WPA2])

Wi-Fi Protected Access (WPA) is a security standard designed by the Wi-Fi Alliance in conjunction with the Institute of Electrical and Electronics Engineers (IEEE). The AP supports 802.11i (WPA2), based on the IEEE 802.11i security standard.

WPA is a replacement for Wired Equivalent Privacy (WEP), the encryption technique specified by the original 802.11 standard. WEP has several vulnerabilities that have been widely publicized. WPA addresses these weaknesses and provides a stronger security system to protect wireless networks.

WPA provides the following new security measures not available with WEP:

- Improved packet encryption using the Temporal Key Integrity Protocol (TKIP) and the Michael Message Integrity Check (MIC).
- Per-user, per-session dynamic encryption keys:
 - Each client uses a different key to encrypt and decrypt unicast packets exchanged with the AP
 - A client's key is different for every session; it changes each time the client associates with an AP
 - The AP uses a single global key to encrypt broadcast packets that are sent to all clients simultaneously
 - Encryption keys change periodically based on the **Re-keying Interval** parameter
 - WPA uses 128-bit encryption keys
- Dynamic Key distribution
 - The AP generates and maintains the keys for its clients
 - The AP securely delivers the appropriate keys to its clients
- Client/server mutual authentication
 - 802.1x
 - Pre-shared key (for networks that do not have an 802.1x solution implemented)

The AP supports the following WPA security modes:

- **WPA:** The AP uses 802.1x to authenticate clients and TKIP for encryption. You should only use an EAP that supports mutual authentication and session key generation, such as EAP-TLS, EAP-TTLS, and PEAP. See [802.1x Authentication](#) for details.
- **WPA-PSK (Pre-Shared Key):** For networks that do not have 802.1x implemented, you can configure the AP to authenticate clients based on a Pre-Shared Key. This is a shared secret that is manually configured on the AP and each of its clients. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits or 32 alphanumeric characters. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the TKIP Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).
- **802.11i** (also known as WPA2): The AP provides security to clients according to the 802.11i draft standard, using 802.1x authentication, a CCMP cipher based on AES, and re-keying.
- **802.11i-PSK** (also known as WPA2 PSK): The AP uses a CCMP cipher based on AES, and encrypts frames to clients based on a Pre-Shared Key. The Pre-Shared Key must be 256 bits long, which is either 64 hexadecimal digits or 32 alphanumeric characters. The AP also supports a **PSK Pass Phrase** option to facilitate the creation of the Pre-Shared Key (so a user can enter an easy-to-remember phrase rather than a string of characters).

NOTE: For more information on WPA, see the Wi-Fi Alliance Web site at <http://www.wi-fi.org>.

Authentication Protocol Hierarchy

There is a hierarchy of authentication protocols defined for the AP.

The hierarchy is as follows, from Highest to lowest:

- 802.1x authentication
- MAC Access Control via RADIUS Authentication
- MAC Access Control through individual APs' MAC Access Control Lists

If you have both 802.1x and MAC authentication enabled, the 802.1x results will take effect. This is required in order to propagate the WEP keys to the clients in such cases. Once you disable 802.1x on the AP, you will see the effects of MAC authentication.

VLANs and Security Profiles

The AP-700 allows you to segment wireless networks into multiple sub-networks based on Network Name (SSID) and VLAN membership. A Network Name (SSID) identifies a wireless network. Clients associate with Access Points that share an SSID. During installation, the Setup Wizard prompts you to configure a Primary Network Name for each wireless interface.

After initial setup and once VLAN is enabled, the AP can be configured to support up to 16 SSIDs per wireless interface to segment wireless networks based on VLAN membership.

Each VLAN can be associated to a Security Profile and RADIUS Server Profiles. A Security Profile defines the allowed wireless clients, and authentication and encryption types. See the following sections for configuration details.

Configuring Security Profiles

Security policies can be configured and applied on the AP as a whole, or on a per VLAN basis. When VLAN is disabled on the AP, the user can configure a security profile for each interface of the AP. When VLANs are enabled and Security per SSID is enabled, the user can configure a security profile for each VLAN.

The user defines a security policy by specifying one or more values for the following parameters:

- Wireless STA types (WPA station, 802.11i (WPA2) station, 802.1x station, WEP station, WPA-PSK, and 802.11i-PSK) that can associate to the AP.
- Authentication mechanisms (802.1x, RADIUS MAC authentication) that are used to authenticate clients for each type of station.
- Cipher Suites (CCMP, TKIP, WEP, None) used for encapsulating the wireless data for each type of station.

Up to 16 security profiles can be configured.

1. Click **Configure** > **SSID/VLAN/Security** > **Security Profile**.

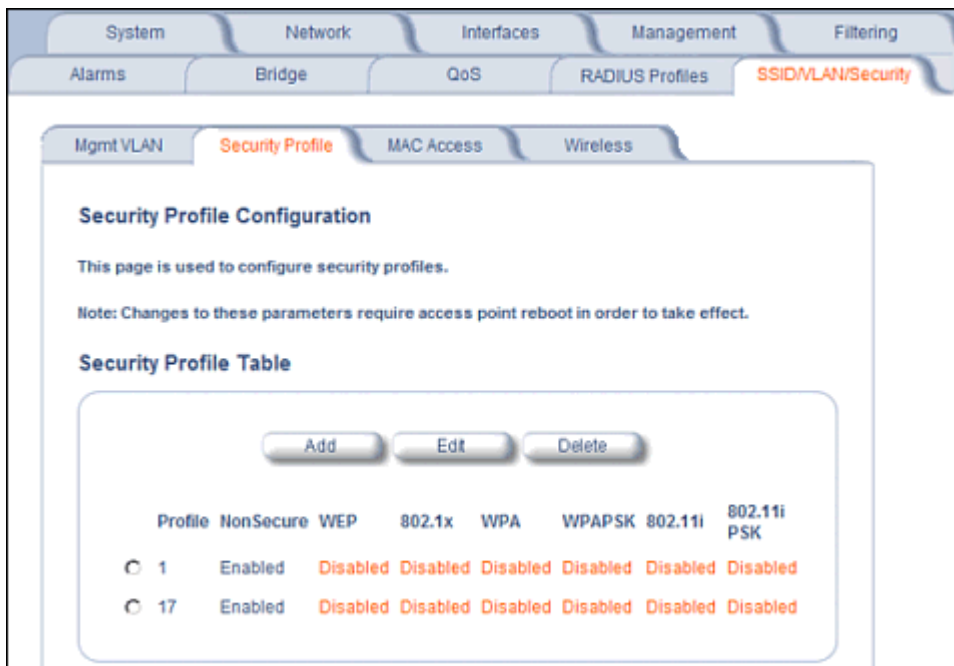


Figure 4-39 Security Profile Configuration

2. Click **Add** in the Security Profile Table to create a new entry. To modify an existing profile, select the profile and click **Edit**. To delete an existing profile, select the profile and click **Delete**. You cannot delete a Security Profile used in an SSID. Also, the first Security Profile cannot be deleted.

3. Configure one or more types of wireless stations (security modes) that are allowed access to the AP under the security profile. The WEP/PSK parameters are separately configurable for each security mode. To enable a security mode in the profile (Non Secure Station, WEP Station, 802.1x Station, WPA Station, WPA-PSK Station, 802.11i (WPA2) Station, 802.11i-PSK Station), check the box next to the mode. See [Figure 4-40 on page 112](#).

If the security mode selected in a profile is WEP, WPA-PSK, or 802.11i-PSK, then you must configure the WEP or Pre-Shared Keys.

NOTE: *If an 802.1x client that has already been authenticated attempts to switch to WEP, or if a WEP client that has already been connected attempts to switch to 802.1x, the AP will not allow the client to switch immediately. If this happens, either reboot the AP or disable the client/roam to a new AP for five minutes, and then attempt to reconnect to the AP. If the client is still unable to connect after waiting five minutes, reboot the AP.*

4. Configure the parameters as follows for each enabled security mode. See [Figure 4-40 on page 112](#).
 - **Non Secure Station:**
 - Authentication Mode: None. The AP allows access to Stations without authentication.
 - Non secure station should be used only with WEP or 802.1x security mode.
 - Cipher: None
 - **WEP Station:**
 - Authentication Mode: None
 - Cipher: WEP
 - Encryption Key 0, Encryption Key 1, Encryption Key 2, Encryption Key 3
 - Encryption Key Length: 64, 128, or 152 Bits.
 - For 64-bit encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters (see [ASCII Character Chart](#)).
 - For 128-bit encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.
 - For 152-bit encryption, an encryption key is 32 hexadecimal characters or 16 ASCII characters.
 - Encryption Transmit Key: select Key 0, Key 1, Key 2, or Key 3
 - **802.1x Station:**
 - Authentication Mode: 802.1x
 - Cipher: WEP
 - Encryption Key Length: 64 or 128 Bits.
 - If 802.1x is enabled simultaneously with WEP, the 802.1x Station's encryption key length is determined by the WEP encryption key.
 - **WPA Station:**
 - Authentication Mode: 802.1x
 - Cipher: TKIP
 - **WPA-PSK Station:**
 - Authentication Mode: PSK
 - Cipher: TKIP
 - PSK Passphrase: an 8-63 character user-defined phrase. It is recommended a passphrase of at least 13 characters, including both letters and numbers, and upper and lower case characters, be used to ensure that the generated key cannot be easily deciphered by network infiltrators.
 - **802.11i Station:**
 - Authentication Mode: 802.1x
 - Cipher: CCMP based on AES
 - **802.11i-PSK Station:**
 - Authentication Mode: PSK

- Cipher: CCMP based on AES
 - PSK Passphrase: an 8-63 character user-defined phrase. It is recommended a passphrase of at least 13 characters, including both letters and numbers, and upper and lower case characters, to ensure that the generated key cannot be easily deciphered by network infiltrators.
5. When finished configuring all parameters, click **OK**.
 6. If you selected a Security Mode of 802.1x Station, WPA Station, or 802.11i Station, you must configure a RADIUS 802.1x/EAP server. See the [Configuring Radius Profiles](#) section.
Security Profile 1 will be used by default for all wireless interfaces.
 7. Reboot the AP.

System
Network
Interfaces
Management
Filtering

Alarms
Bridge
QoS
RADIUS Profiles
SSID/VLAN/Security

Security Profile Table - Add Entries

This page is used to edit a Security Profile.

If the WEP security mode is configured, then the appropriate key size must be configured. The access point supports 64, 128, and 152 bit encryption keys. The following table provides information on how to configure encryption keys using HEX or ASCII values.

	Configuration in Hex	Configuration in ASCII
64 bit encryption key	10 characters (0-F)	5 alphanumeric characters
128 bit encryption key	26 characters (0-F)	13 alphanumeric characters
152 bit encryption key	32 characters (0-F)	16 alphanumeric characters

If the WPA/PSK or 802.11i/PSK security mode is configured, then the appropriate PSK pass phrase must be configured. The PSK pass phrase consists of a alphanumeric string from 8 to 63 characters.

802.1x, WPA or 802.11i security mode can be configured only if an EAP RADIUS server profile is configured and enabled. Certain security modes and their combinations may not be available depending on the security capabilities of the wireless interface.

Note: Changes to these parameters require access point reboot in order to take effect.

Non Secure Station

	Authentication Mode	None
	Cipher	None

WEP Station

	Authentication Mode	None
	Cipher	WEP
	Encryption Key 0	<input type="text"/>
	Encryption Key 1	<input type="text"/>
	Encryption Key 2	<input type="text"/>
	Encryption Key 3	<input type="text"/>
	Encryption Transmit Key	Key 0 <input type="text"/>

802.1x Station

	Authentication Mode	802.1x
	Cipher	WEP
	Encryption Key Length	64 Bits <input type="text"/>

WPA Station

	Authentication Mode	802.1x
	Cipher	TKIP

WPA-PSK Station

	Authentication Mode	PSK
	Cipher	TKIP
	PSK Passphrase	<input type="text"/>

802.11i Station

	Authentication Mode	802.1x
	Cipher	AES

802.11i-PSK Station

	Authentication Mode	PSK
	Cipher	AES
	PSK Passphrase	<input type="text"/>

Figure 4-40 Security Profile Table - Add Entries