Compsee	**Apex** ***Technical Bulletin***
Doc # AP3-WLAN-051002	**Apex WLAN Security**

Apex WLAN Security

Apex obtains Extensible Authentication Protocol (EAP) Compliance for Wireless Network Security

The Apex has been verified to properly operate in a network environment running the Extensible Authentication Protocol (EAP). Cisco has termed the client side (i.e. Apex) of this protocol, "Lite Extensible Authentication Protocol" (LEAP). EAP-LEAP is an 802.1x-compliant approach developed by Cisco that provides greater security for networks incorporating wireless devices than using just the standard Wired Equivalent Privacy (WEP) encryption.

Network Elements

- Apex with Cisco 350 WLAN adapter (AIR-PCM352)
- Cisco Aironet Access Point (AIR-AP352E2C)
- Remote Authentication Dial-In User Service (RADIUS) server

  Note - The RADIUS server used for testing was a 90 day trial version of the Cisco Secure Access Control Server (ACS) downloaded from Cisco's website.

When EAP is enabled on the Access Point and the client (Apex), the RADIUS server controls authentication for the network in the following manner:

- The Apex wireless client device uses EAP to provide a network username and password.
- To authenticate the clients username and password the Access Point communicates with the EAP-compliant RADIUS server.
- If the username and password are valid, the RADIUS server sends a dynamic, session-based Wired Equivalent Privacy (WEP) encryption "Key" back to the Access Point. This "key", which is unique for the authenticated client, provides the client with network access.
- The client device (Apex) uses the WEP "Key" for all data transmissions during the session.

Network Requirements

- The Access Point must be enabled for Extensible Authentication Protocol (EAP). Set-Up Instructions for the Access Point are attached. They are also available in the documentation supplied with the Cisco Access Point.
- The Cisco Secure Access Control Server (ACS) must be loaded onto a network server and setup only if the network does not already have RADIUS capabilities. The documentation supplied with the Cisco Access Point and attached at the end of this document, lists the ACS setup requirements.
- Using the utility (AWCLEAP) the Apex configures the Cisco 350 wireless adapter for LEAP. This utility (AWCLEAP) is available from Cisco and can be preloaded on the Apex for users requiring this type of network security.

  This utility sets the username and password as defined by the network into the Cisco 350 adapter. The utility is run from the command line and could be run directly from the autoexec.bat file or as a batch file of its own. The complete list of command line parameters follows in this document.

National Sales Office
2500 Port Malabar Blvd. NE
Palm Bay, FL 32905

800-628-3888 – V
321-724-4321 – V
321-723-2895 – F
sales@compsee.com

Corporate Headquarters
400 N. Main St.
Mt. Gilead, NC 27306

Extensible Authentication Protocol and Authentication Server Setup

To enter the Access Point's authentication settings, you must use the Authentication Server Setup page. Follow this link path to reach the Authentication Server Setup page:

1. Summary Status page- click **Setup**.
2. Setup page- click **Security**.
3. Security Setup page- click **Authentication Server**.

Enabling EAP on the Access Point

Follow these steps to enable EAP on the Access Point:

1. Follow the link path to the Authentication Server Setup page.
2. Enter the name or IP address of the RADIUS server in the Server Name/IP entry field.
3. Enter the port number your RADIUS server uses for authentication. The default setting, *1812*, is the port setting for many RADIUS servers; *1645* is the port setting for Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS). Check your server's product documentation to find the correct port setting.
4. Enter the shared secret used by your RADIUS server in the Shared Secret entry field. The shared secret on the Access Point must match the shared secret on the RADIUS server.
5. Enter the number of seconds the Access Point should wait before authentication fails.
6. Click **O**K. Returns to the Security Setup page.
7. On the Security Setup page, click **Radio Data Encryption (WEP)** to browse to the AP Radio Data Encryption page.
8. Select **Network-EAP** for the Authentication Type setting. You can also enter this setting on the AP Radio Advanced page.
9. Check that at least one WEP key has been assigned a key size and has been selected as the transmit key. If a WEP key has been set up, skip to Step 13. If no WEP key has been set up, proceed to Step 10.
10. Enter a WEP key in one of the Encryption Key fields. The Access Point uses this key for multicast data signals (signals sent from the Access Point to several client devices at once). This key does not need to be set on client devices.
11. Select **128-bit** encryption from the Key Size pull-down menu.
12. Select the key as the transmit key.
13. Click **O**K. Return automatically to the Security Setup page.

National Sales Office
2500 Port Malabar Blvd. NE
Palm Bay, FL 32905

800-628-3888 – V
321-724-4321 – V
321-723-2895 – F
sales@compsee.com

Corporate Headquarters
400 N. Main St.
Mt. Gilead, NC 27306

Enabling EAP in Cisco Secure ACS

Follow these steps to include the Access Point as a Network Access Server (NAS) in Cisco Secure ACS:

1. Click **Network Configuratio**n on the ACS Main Menu.
2. Click the name of the Network Device Group (NDG), if applicable, to which the NAS is assigned.
3. Click **Add New Access Serve**r.
4. Type the name assigned to the access server in the **Network Access Server Hostname** box. Also include in this field any information for a Cisco Systems PIX Firewall.
   Note - This field does not appear if you are configuring an existing NAS.
5. Type the Access Point's IP address in the **Network Access Server IP address** box. Also enter information for a Cisco Systems PIX Firewall in this field.
6. Type the shared secret in the **Key** box. The TACACS+ or RADIUS NAS and Cisco Secure ACS use the shared secret to encrypt data. For correct operation, the identical key (case sensitive) must be configured on the Access Point's Authenticator Configuration page and in Cisco Secure ACS.
7. If you are using NDGs, go to the **Network Device Group** drop-down menu and click the name of the NDG to which the Access Point should belong, or click **Not Assigned** to have the Access Point be independent of NDGs.
   Note - To enable NDGs, click **Interface Configuration > Advanced Options > Network Device Group**s.
8. Click the network security protocol from the **Authenticate Using** list box. Select **RADIUS (Cisco Aironet**).
9. If you are using the TACACS+ security protocol, select **Single Connect TACACS+ NAS** to allow a stop record to be sent to the TACACS+ accounting log for each user connected through the Access Point.
   Note - If your connection is unreliable, do not use this feature.
10. Select the **Log Update/Watchdog Packets from this Access Server** option to allow accounting packets sent by the Access Point to be logged in the **Reports & Activit**y: **TACACS+ Accounting** or **RADIUS Accounting** reports.
11. Select the **Log RADIUS tunneling Packets from this Access Server** option to allow RADIUS tunneling accounting packets to be logged in the Reports & Activity: RADIUS Accounting reports.
12. To save your changes and apply them immediately, click the **Submit + Restart** button.
    Tips - To save your changes and apply them later, click **Submi**t. When you are ready to implement the changes, click **System Configuration > Service Control** and click **Restar**t.
    Note - Restarting the service clears the Logged-in User Report, refreshes the Max Sessions counter, and temporarily interrupts all Cisco Secure ACS services.

National Sales Office
2500 Port Malabar Blvd. NE
Palm Bay, FL 32905

800-628-3888 – V
321-724-4321 – V
321-723-2895 – F
sales@compsee.com

Corporate Headquarters
400 N. Main St.
Mt. Gilead, NC 27306

Enabling/Creating users in the Cisco Secure ACS

Users who need to have access to the network must be included in the Cisco Secure User Database or they must be in the Windows NT/2000 user database. Cisco Secure ACS is capable of user authentication by using either database. In order to create user account(s) on Windows NT/2000 network, contact your network administrator. Creating user in Cisco ACS requires the following steps:

1. Click the User Setup button from the main page of the Cisco ACS.
2. Create a new user by entering user name into the User: box and press Enter.
3. At minimum, User's real name and description must be entered on the new user setup page.
4. If authentication for this user is from Cisco Secure Database, then select that option from the drop down menu.
5. Type in Password and retype to confirm.
6. User will be in default user group unless a specific group is selected.
7. Next step is to select the proper method for assigning an IP address for this user.
8. Lastly, account limitations are set prior to completing user creation.
9. When finished, click the Submit button.

Enabling EAP in Client Adapter

AWCLEAP.EXE

Description	Sets the LEAP username and password	
Syntax	AWCLEAP [username|noname] password [-clear] [-d]	
Options	username	Sets a username
	-noname	Disables the username feature
	password	Sets a LEAP password
	-clear	Clears current username and password
	-d	Displays current settings
Standard Options (Default settings in brackets)	-p[IO base]	IO base address (hex) [300]
	-io#|-misa#|-isa#	IO type, #={8/16}
	-b [membase]	Memory base address (hex) [D000]
	-I [irq]	Interrupt request (decimal) [5]
	-s [slot]	Slot number (decimal) [0]
	-365	82365 card startup
	-pci	PCI card startup
	-nocheck	I/O access not tested on startup
Remarks	The card startup option (-365) is required to run this utility.	

Apex command line: awcleap –365 tst2000 pass123

National Sales Office
2500 Port Malabar Blvd. NE
Palm Bay, FL 32905

800-628-3888 – V
321-724-4321 – V
321-723-2895 – F
sales@compsee.com

Corporate Headquarters
400 N. Main St.
Mt. Gilead, NC 27306

Technical Assistance:
Users requiring Technical Assistance should contact Compsee Technical Support at **1-800-628-3888**. Technical questions can also be e-mailed to **sales@compsee.com**.

National Sales Office
2500 Port Malabar Blvd. NE
Palm Bay, FL 32905

800-628-3888 – V
321-724-4321 – V
321-723-2895 – F
sales@compsee.com

Corporate Headquarters
400 N. Main St.
Mt. Gilead, NC 27306