Using PEAP and WPA PEAP Authentication Security on a Zebra Wireless Tabletop Printer

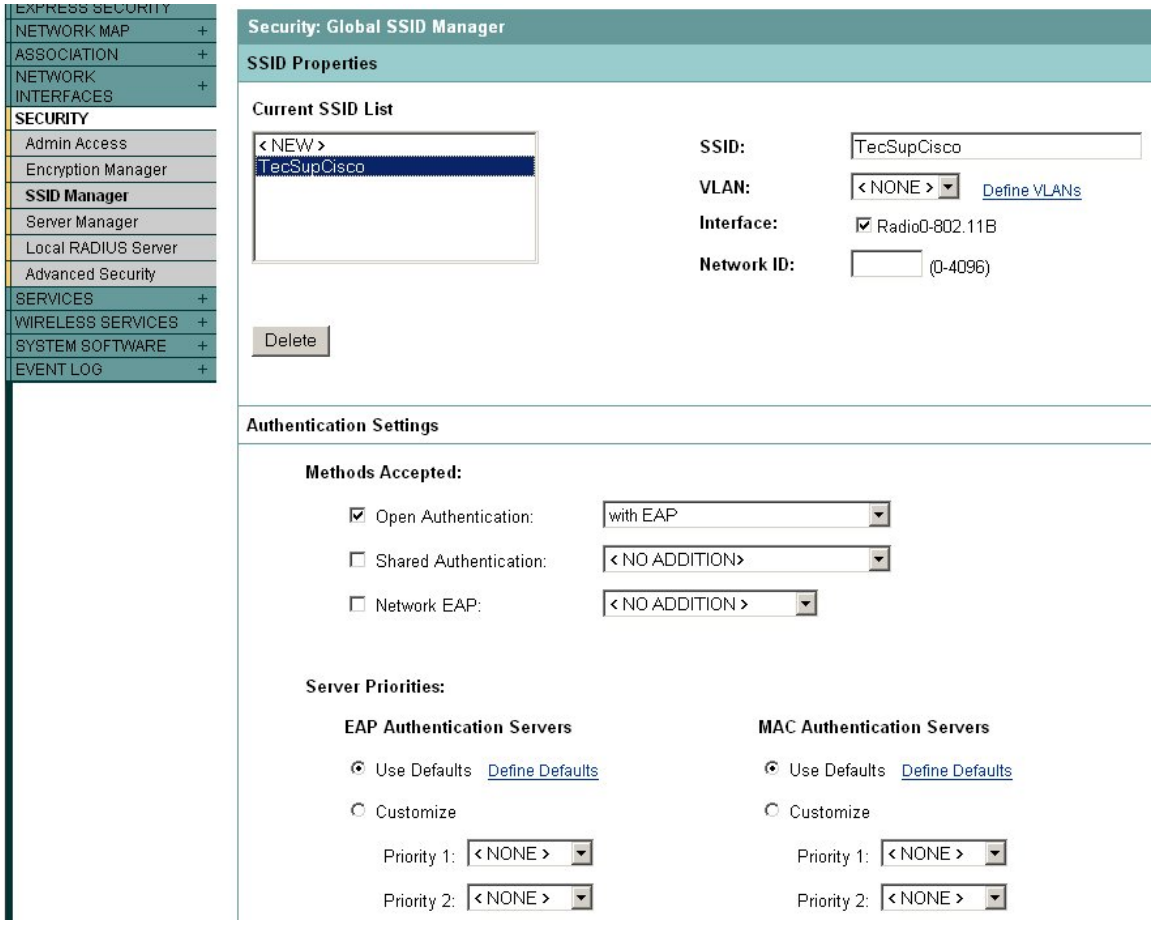
Q. What is PEAP?
A. Protected **E**xtensible **A**uthentication **P**rotocol is an IEEE 802.1x EAP security method that uses an initial TLS handshake to authenticate a server to a client using PKI (Public Key Infrastructure) cryptography X.509 digital certificates. Using the secure tunnel established by the TLS handshake, a RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) server is used to authenticate a client using legacy username and password authentication before allowing wireless access onto the network. The server proves its identity to the client by passing a digital certificate to the printer. An **optional** root certificate can be stored on the client which is used to help prove the identity of the server. The printer authenticates to the server by sending its username and password inside the secure TLS tunnel. Encryption keys are then generated securing all communications traffic between the wireless client and the network. In this example we will be using a Cisco Aironet 1200 access point (the EAP authenticator), and a Windows version of the popular FreeRadius authentication server. The firmware level on the Cisco access point used for this test was 12.3(7)JA. Information on FreeRadius appears later in this document. The version of PEAP supported in the TLS tunnel is the Microsoft implementation of MS-CHAPv2.

Note: Zebra Desktop and Tabletop Printers currently do not support the use of the optional root Certificate being stored on the printers with PEAP.

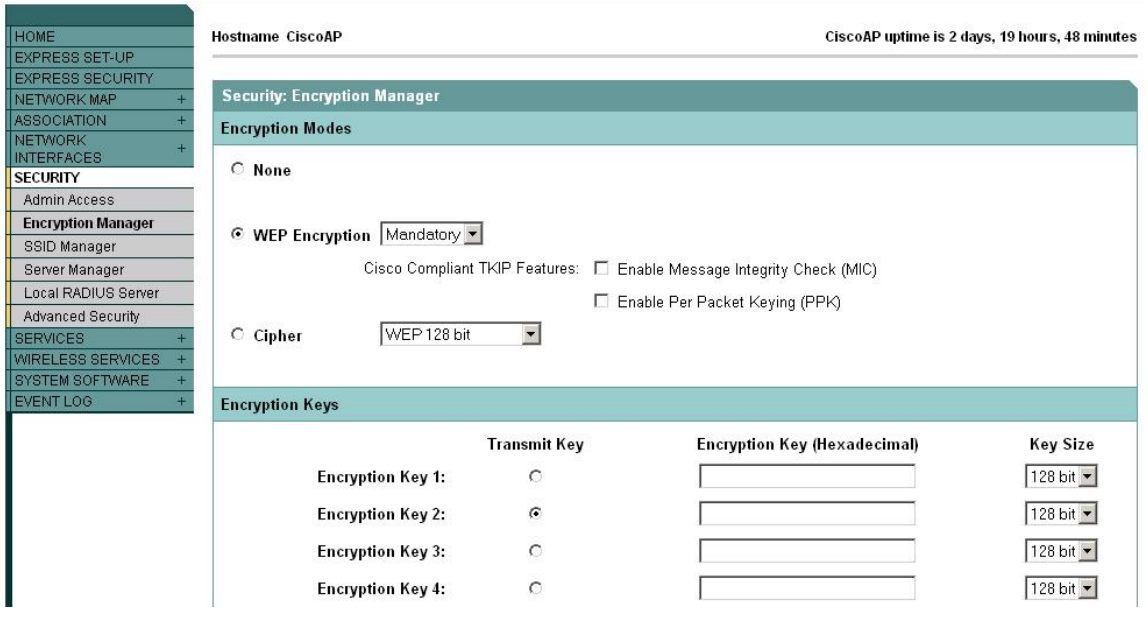
Our first example will be standard PEAP, which uses WEP encryption. Our second example will be WPA PEAP, which uses TKIP encryption.

Configure the Cisco 1200 AP for PEAP authentication.

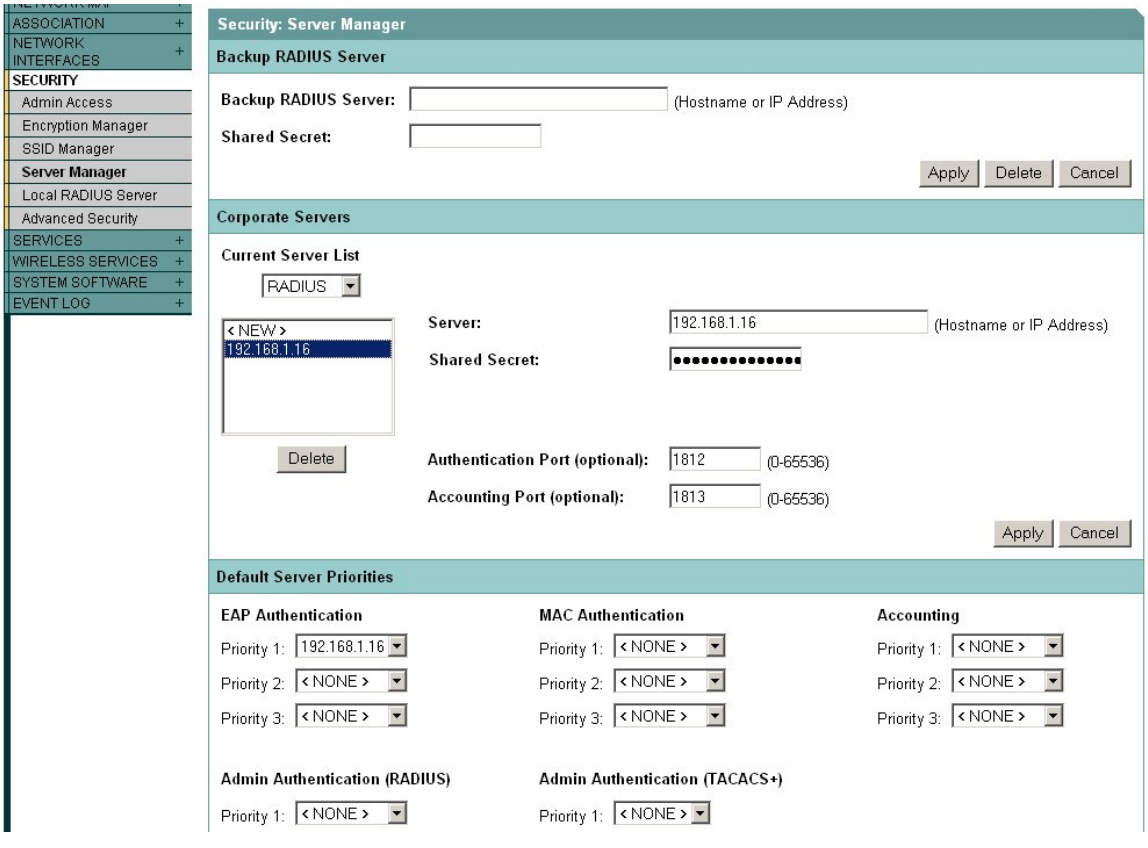
In the SSID Manager select your SSID, set Open Authentication with EAP, and no Key Management as shown in the following two screen shots:



In the Encryption Manager set WEP Encryption to Mandatory:



Next, configure a RADIUS server entry in the Server Manager. Select the IP address for your RADIUS server and enter its shared secret (we will edit the shared secret on the RADIUS server in the next step). By default the FreeRadius server listens on TCP ports 1812 and 1813. Select the RADIUS server's IP address in the Default Server Priorities (EAP Authentication section).



Configure the FreeRadius server for PEAP authentication.

The FreeRadius server is available under the GNU General Public License (GPL), and is freely downloadable from the internet. For our example we will be using a Windows build of the server that can be downloaded from the FreeRadius.net website (http://www.freeradius.net). To install this version of the FreeRadius server you will need a computer system running Windows XP.

Download and install the server. In the FreeRadius.net group click the 'Edit Clients.conf' icon. At the bottom of the file add the following lines to create our test network. This will allow for a range of access points that must also be configured with this same shared secret.

```
      client 192.168.1.0/24 {
  secret = password
  shortname = private-network-3
 }
```

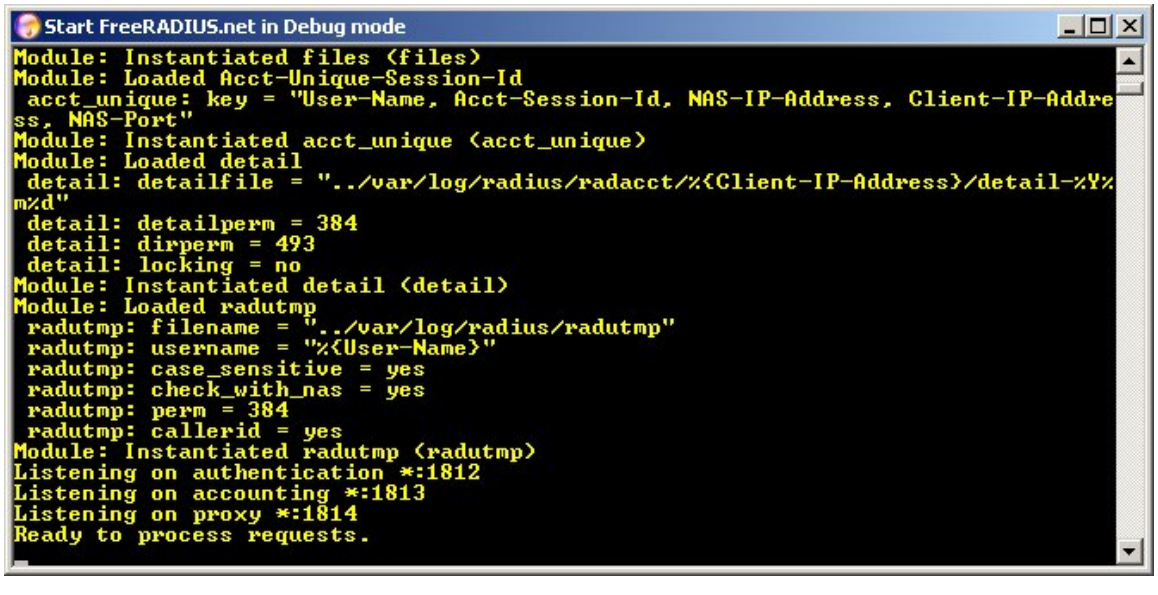
Save the file and open the Eap.conf file for editing. If necessary, edit the line that reads 'default_eap_type' to select the PEAP protocol. Save the file if changes are made.

```
      default_eap_type = peap
```

Next we will create user credentials that our printer will use to login to the network. Open the Users file. Just below the user 'FreeRADIUS.net-Client' add a PEAP user 'peap' as shown below. Save the file if changes are made.

```
      # Test PEAP user
      peap Auth-Type := eap, User-zebra1 == "zebra1"
  Service-Type = Login-User
```

The RADIUS server should now be configured correctly. Start the server in debug mode by selecting the appropriate icon. Once the server is initialized it will be ready to process requests and authenticate users.

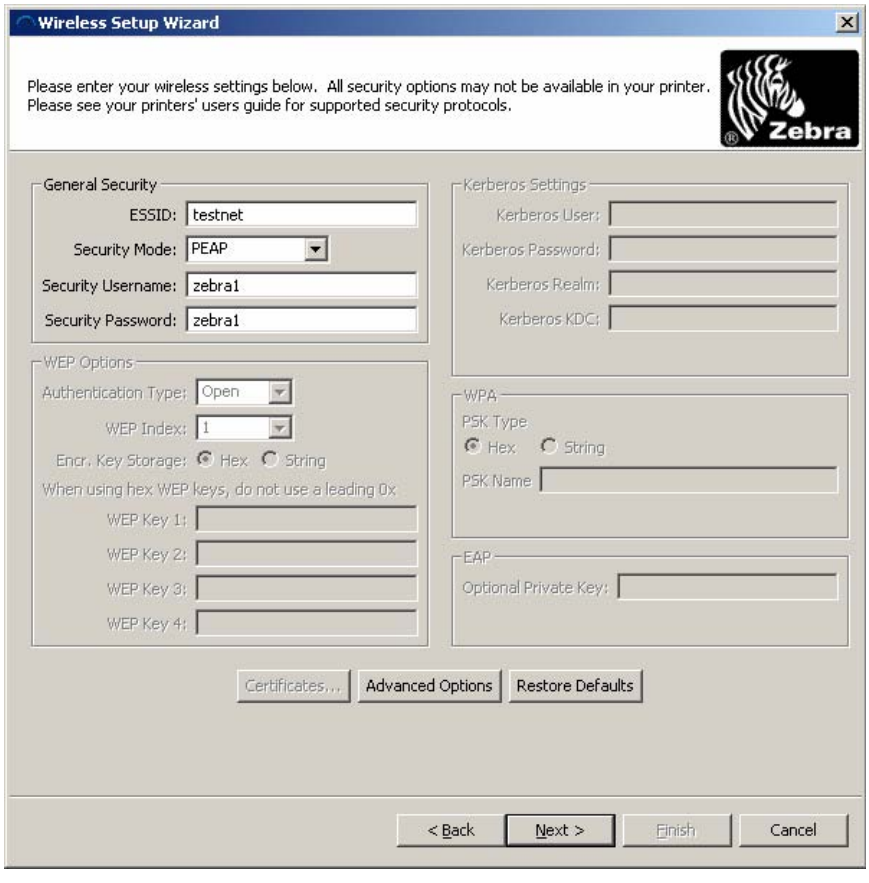


Configure Printer for PEAP authentication.

The Printer must have **firmware x.15.x** or higher.

To configure the printer use **ZebraNet Bridge Enterprise** V1.2.1 or higher. From Tools, select the Wireless Setup Wizard.

Select PEAP form the drop down list in Security Mode and set the user name and password used on the RADIUS server.

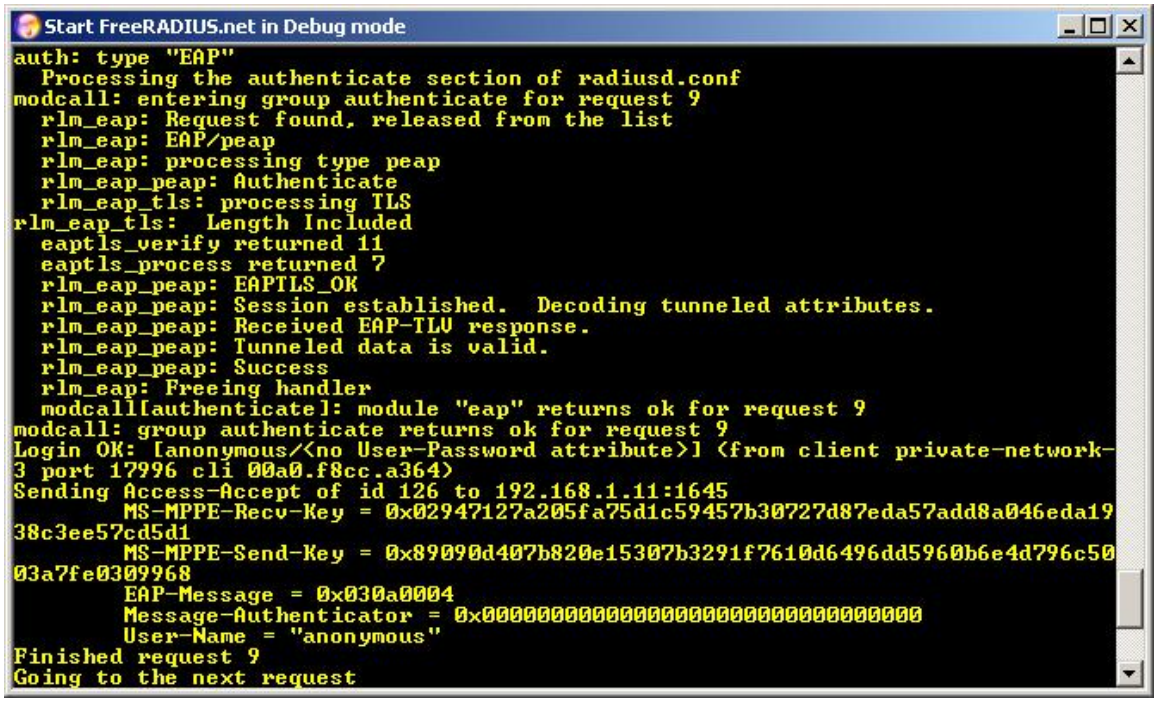


Click next to view the ZPL:

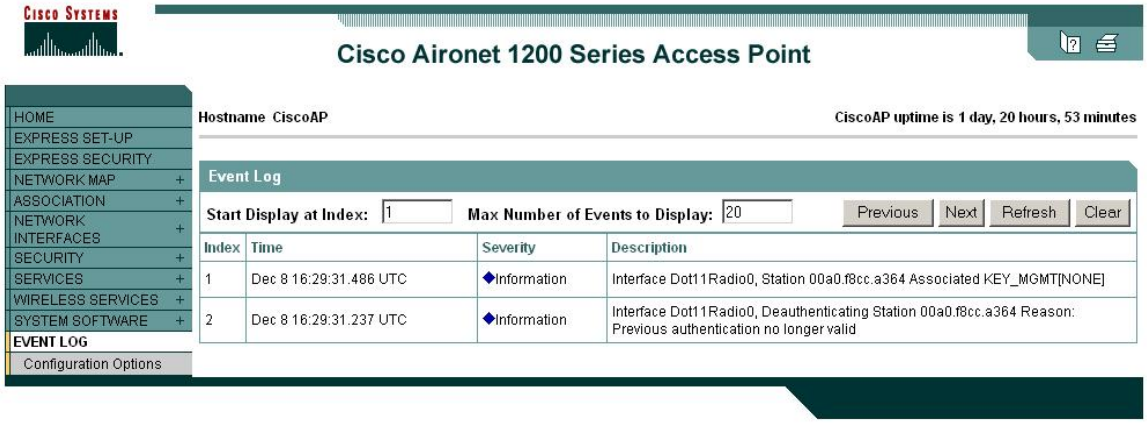
^XA
^WIP,10.17.50.91,255.255.255.0,10.17.50.1
^WAD,D
^WEOFF,1,O,H,,,,
^WP0,0
^WR,,,,100
^WStestnet,I,L
^NBS
^WLOFF,zebra1,zebra1
^WKOFF,,,,
^WX07,zebra1,zebra1
^XZ
^XA
^JUS
^XZ

Click Next to send ZPL to the printer.

The following is an example of the Free Radius log after a successful connection.



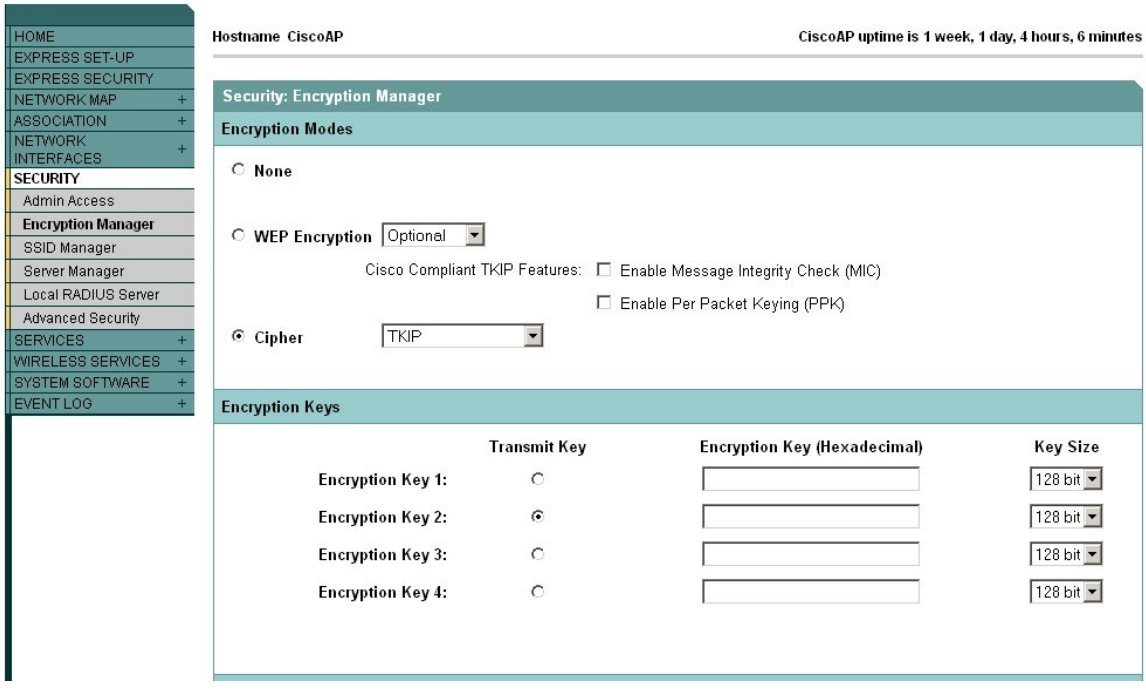
The access point's event log should also contain information regarding the printer's successful connection.



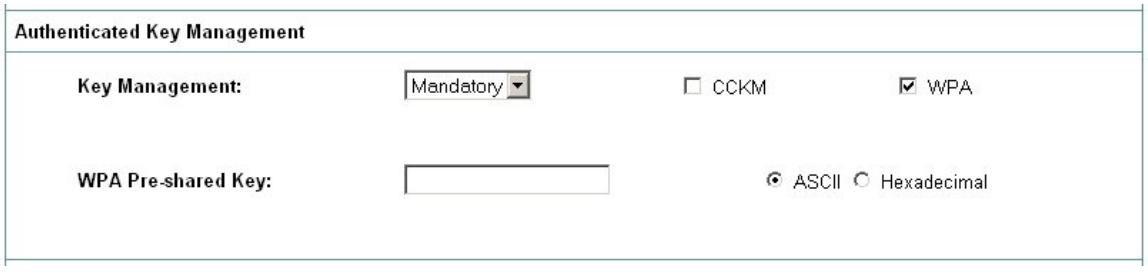
Next, we will modify the settings on the Cisco access point and the Zebra mobile printer to use WPA PEAP. WPA increases security further by using TKIP (Temporal Key Integrity Protocol) as an encryption scheme instead of WEP. All the Cisco access point settings are the same as shown previously for standard PEAP except for the changes shown in the following two screenshots.

Configure the Cisco 1200 AP for WPA PEAP authentication.

In the Encryption Manager click Cipher, and select TKIP from the dropdown box.



In the SSID Manager configure WPA as shown below.

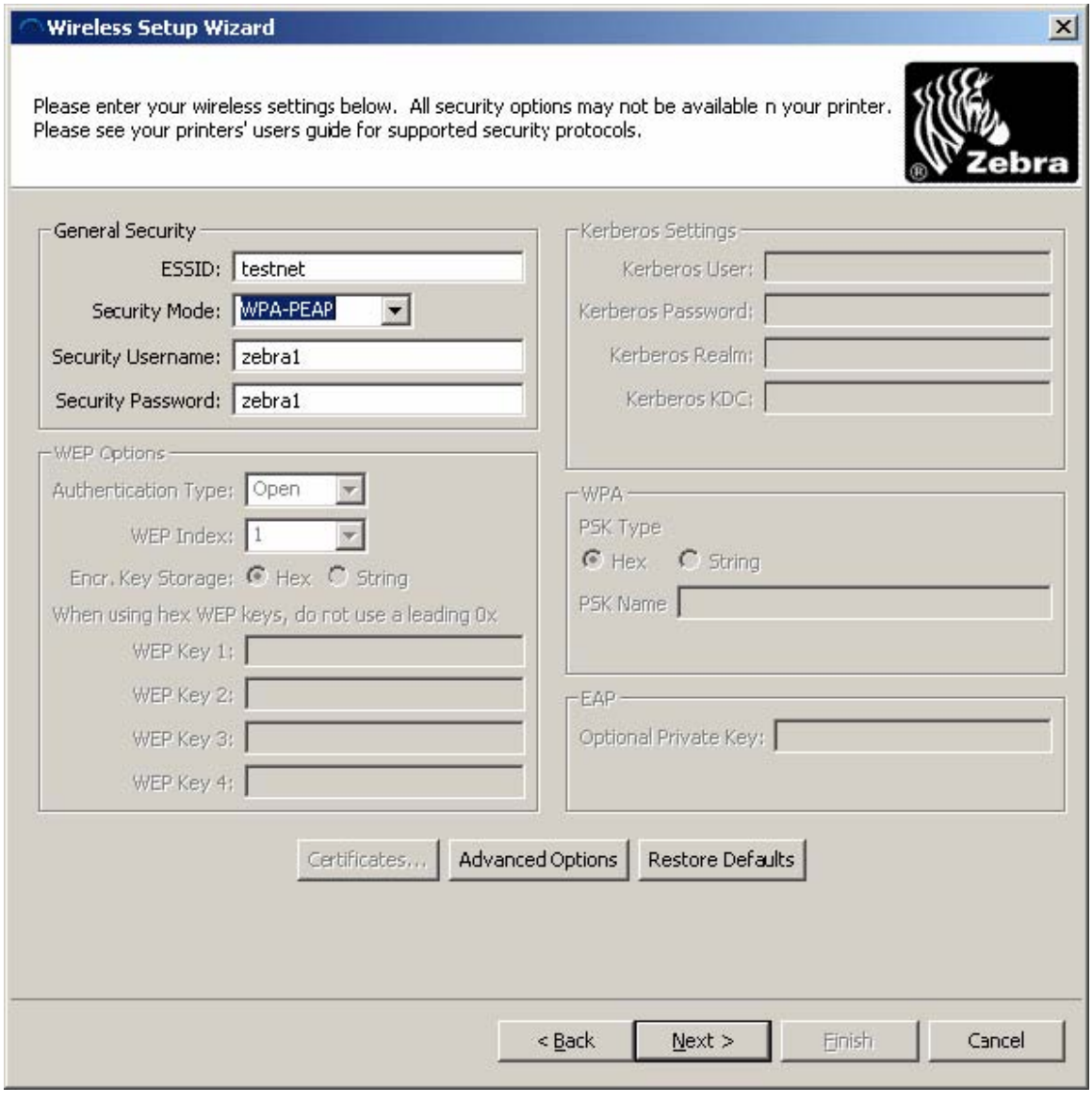


Configure the ZebraNet Printer for WPA PEAP authentication.

The Printer must have **firmware x.15.x** or higher.

To configure the printer use **ZebraNet Bridge Enterprise** V1.2.1 or higher. From Tools, select the Wireless Setup Wizard.

Select WPA-PEAP form the drop down list in Security Mode and set the user name and password used on the RADIUS server.

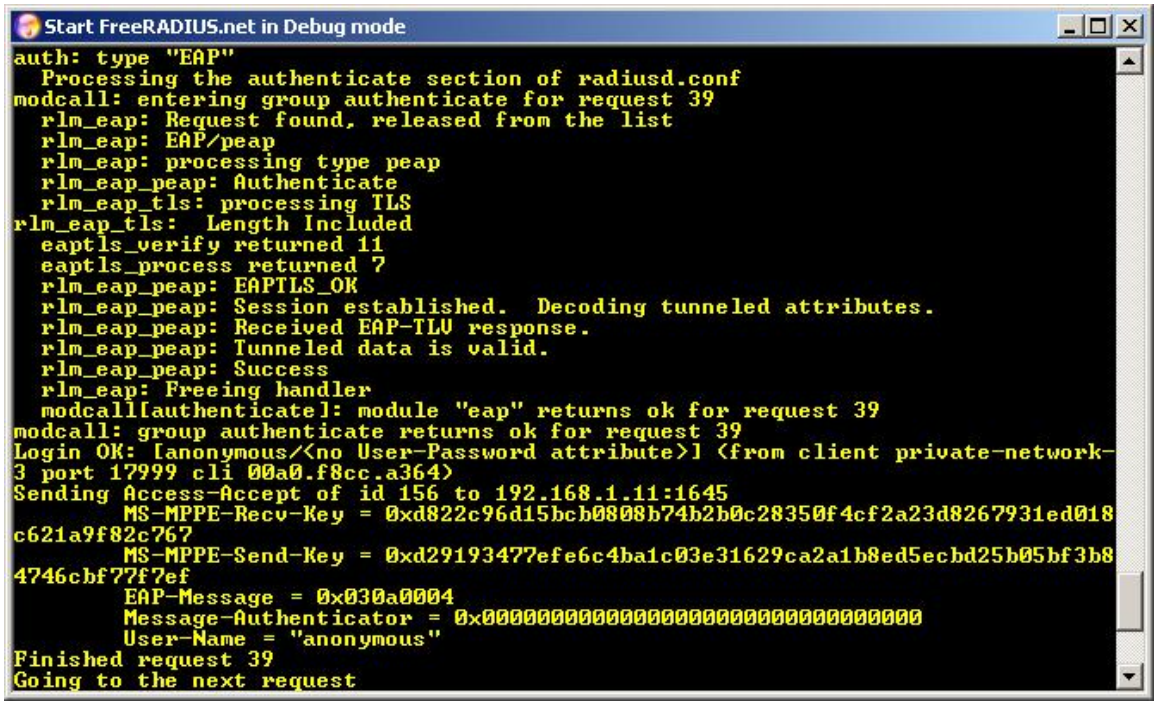


Click next to view the ZPL:

```
^XA
^WIP,10.17.50.91,255.255.255.0,10.17.50.1
^WAD,D
^WEOFF,1,O,H,,,,
^WP0,0
^WR,,,,100
^WStestnet,I,L
^NBS
^WLOFF,zebra1,zebra1
^WKOFF,,,,
^WX13,zebra1,zebra1
^XZ
^XA
^JUS
^XZ
```

Click Finish to sent the ZPL to the printer.

The following is an example of the Free Radius log after a successful WPA connection.



The access point's event log should also contain information regarding the printer's successful connection.