

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

**Q.** What is PEAP?

**A.** Protected Extensible Authentication Protocol 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 (Remote Authentication Dial-In User Service) 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:

The image shows two screenshots of the Cisco 1200 AP configuration interface. The top screenshot displays the 'Security: Global SSID Manager' page. On the left is a navigation menu with categories like EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The 'SSID Manager' option is selected. The main area is titled 'Security: Global SSID Manager' and contains a 'Current SSID List' table with one entry 'TecSupCisco'. To the right of the table are fields for 'SSID' (TecSupCisco), 'VLAN' (< NONE >), 'Interface' (Radio0-802.11B), and 'Network ID' (0-4096). Below the table is a 'Delete' button. The bottom screenshot shows the 'Authentication Settings' page. It has sections for 'Methods Accepted' (Open Authentication with EAP, Shared Authentication, Network EAP), 'Server Priorities' (EAP and MAC Authentication Servers), and 'Authenticated Key Management' (Key Management, WPA Pre-shared Key).

**Security: Global SSID Manager**

**SSID Properties**

Current SSID List

< NEW >	SSID:	TecSupCisco
TecSupCisco	VLAN:	< NONE > <a href="#">Define VLANs</a>
	Interface:	<input checked="" type="checkbox"/> Radio0-802.11B
	Network ID:	<input type="text"/> (0-4096)

Delete

**Authentication Settings**

**Methods Accepted:**

Open Authentication: with EAP

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

**Server Priorities:**

**EAP Authentication Servers**

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

**MAC Authentication Servers**

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

**Authenticated Key Management**

**Key Management:** < NONE >  CCKM  WPA

**WPA Pre-shared Key:**   ASCII  Hexadecimal

In the Encryption Manager set WEP Encryption to Mandatory:

Hostname CiscoAP CiscoAP uptime is 2 days, 19 hours, 48 minutes

### Security: Encryption Manager

#### Encryption Modes

None  
 **WEP Encryption** Mandatory  
 Cisco Compliant TKIP Features:
  Enable Message Integrity Check (MIC)
  Enable Per Packet Keying (PPK)

Cipher WEP 128 bit

#### Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<span style="border: 1px solid black; padding: 2px;">128 bit</span>

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).

### Security: Server Manager

#### Backup RADIUS Server

Backup RADIUS Server:  (Hostname or IP Address)  
 Shared Secret:

#### Corporate Servers

Current Server List: RADIUS

Server	Shared Secret
<span style="border: 1px solid black; padding: 2px;">&lt;NEW&gt;</span>	
<span style="border: 1px solid black; padding: 2px;">192.168.1.16</span>	<input type="text"/>

Server:  (Hostname or IP Address)  
 Shared Secret:   
 Authentication Port (optional):  (0-65536)  
 Accounting Port (optional):  (0-65536)

#### Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: <span style="border: 1px solid black; padding: 2px;">192.168.1.16</span>	Priority 1: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>	Priority 1: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>
Priority 2: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>	Priority 2: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>	Priority 2: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>
Priority 3: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>	Priority 3: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>	Priority 3: <span style="border: 1px solid black; padding: 2px;">&lt;NONE&gt;</span>

Admin Authentication (RADIUS): Priority 1: <NONE>  
 Admin Authentication (TACACS+): Priority 1: <NONE>

## 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
}
```

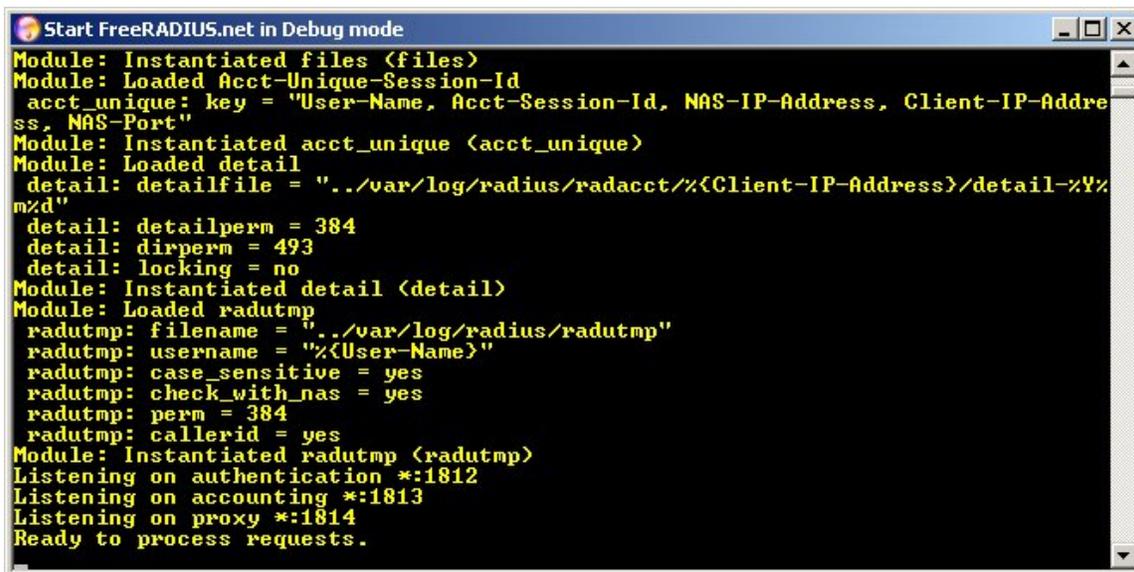
Save the file and open the Eap.conf file for editing. If necessary, edit the line that reads 'default\_eap\_type' to select the PEAP protocol. Save the file if changes are made.

```
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.



```
Start FreeRADIUS.net in Debug mode
Module: Instantiated files (files)
Module: Loaded Acct-Unique-Session-Id
acct_unique: key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-IP-Address, NAS-Port"
Module: Instantiated acct_unique (acct_unique)
Module: Loaded detail
detail: detailfile = "./var/log/radius/radacct/%{Client-IP-Address}/detail-%Y%m%d"
detail: detailperm = 384
detail: dirperm = 493
detail: locking = no
Module: Instantiated detail (detail)
Module: Loaded radutmp
radutmp: filename = "./var/log/radius/radutmp"
radutmp: username = "%{User-Name}"
radutmp: case_sensitive = yes
radutmp: check_with_nas = yes
radutmp: perm = 384
radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
Listening on authentication *:1812
Listening on accounting *:1813
Listening on proxy *:1814
Ready to process requests.
```

## 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 from the drop down list in Security Mode and set the user name and password used on the RADIUS server.

Please enter your wireless settings below. All security options may not be available in your printer. Please see your printers' users guide for supported security protocols.

**General Security**

ESSID: testnet

Security Mode: PEAP

Security Username: zebra1

Security Password: zebra1

**WEP Options**

Authentication Type: Open

WEP Index: 1

Encl. Key Storage:  Hex  String

When using hex WEP keys, do not use a leading 0x.

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

**Kerberos Settings**

Kerberos User:

Kerberos Password:

Kerberos Realm:

Kerberos KDC:

**WPA**

PSK Type

Hex  String

PSK Name:

**EAP**

Optional Private Key:

Certificates... Advanced Options Restore Defaults

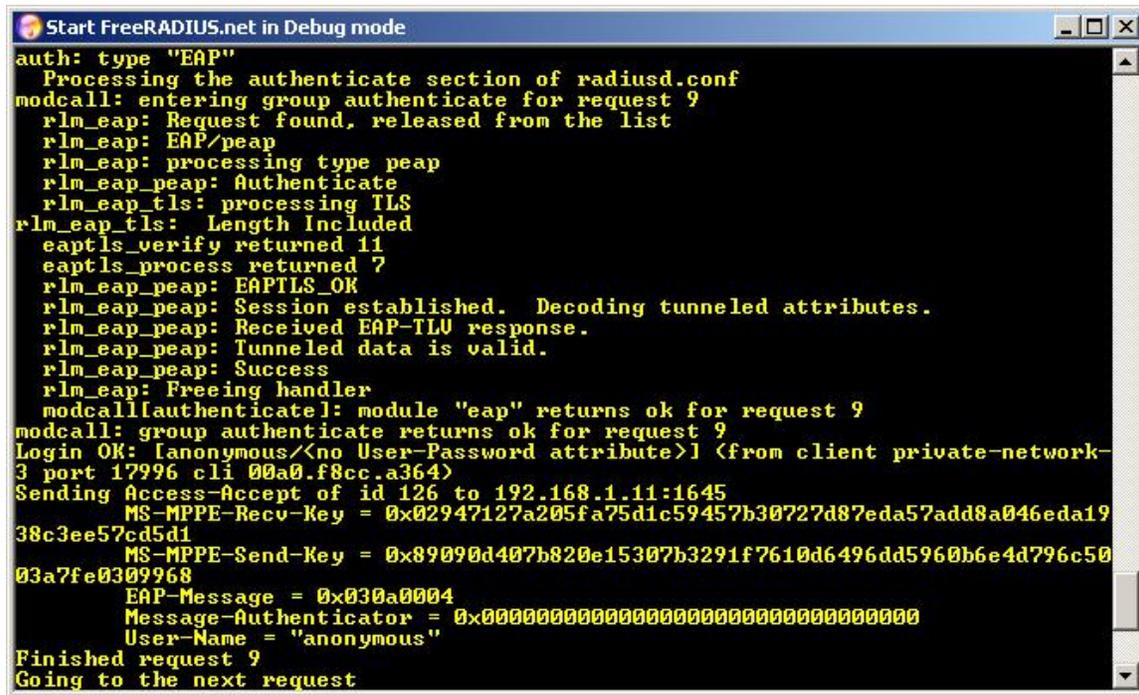
< Back Next > Finish Cancel

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,,,
^WPO,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.



```
Start FreeRADIUS.net in Debug mode
auth: type "EAP"
  Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 9
  rlm_eap: Request found, released from the list
  rlm_eap: EAP/peap
  rlm_eap: processing type peap
  rlm_eap_peap: Authenticate
  rlm_eap_tls: processing TLS
  rlm_eap_tls: Length Included
  eaptls_verify returned 11
  eaptls_process returned 7
  rlm_eap_peap: EAPTLS_OK
  rlm_eap_peap: Session established. Decoding tunneled attributes.
  rlm_eap_peap: Received EAP-TLV response.
  rlm_eap_peap: Tunneled data is valid.
  rlm_eap_peap: Success
  rlm_eap: Freeing handler
modcall[authenticate]: module "eap" returns ok for request 9
modcall: group authenticate returns ok for request 9
Login OK: [anonymous/<no User-Password attribute>] (from client private-network-3 port 17996 cli 00a0.f8cc.a364)
Sending Access-Accept of id 126 to 192.168.1.11:1645
  MS-MPPE-Recv-Key = 0x02947127a205fa75d1c59457b30727d87eda57add8a046eda1938c3ee57cd5d1
  MS-MPPE-Send-Key = 0x89090d407b820e15307b3291f7610d6496dd5960b6e4d796c5003a7fe0309968
  EAP-Message = 0x030a0004
  Message-Authenticator = 0x00000000000000000000000000000000
  User-Name = "anonymous"
Finished request 9
Going to the next request
```

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

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration interface. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "CiscoAP" and the uptime is "1 day, 20 hours, 53 minutes". The "Event Log" section is active, showing a table of events. The table has columns for Index, Time, Severity, and Description. Two events are listed:

Index	Time	Severity	Description
1	Dec 8 16:29:31.486 UTC	Information	Interface Dot11Radio0, Station 00a0.f8cc.a364 Associated KEY_MGMT[NONE]
2	Dec 8 16:29:31.237 UTC	Information	Interface Dot11Radio0, Deauthenticating Station 00a0.f8cc.a364 Reason: Previous authentication no longer valid

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.

The screenshot shows the "Security: Encryption Manager" configuration page. The hostname is "CiscoAP" and the uptime is "1 week, 1 day, 4 hours, 6 minutes". The "Encryption Modes" section is active, showing the following options:

- None
- WEP Encryption Optional
  - Cisco Compliant TKIP Features:
    - Enable Message Integrity Check (MIC)
    - Enable Per Packet Keying (PPK)
- Cipher TKIP

The "Encryption Keys" section is also visible, showing four keys with their respective Transmit Key status, Encryption Key (Hexadecimal) input fields, and Key Size (128 bit) dropdown menus.

In the SSID Manager configure WPA as shown below.

Authenticated Key Management			
<b>Key Management:</b>	<input type="text" value="Mandatory"/>	<input type="checkbox"/> CCKM	<input checked="" type="checkbox"/> WPA
<b>WPA Pre-shared Key:</b>	<input type="text"/>	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal	

### 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 from the drop down list in Security Mode and set the user name and password used on the RADIUS server.

**Wireless Setup Wizard**

Please enter your wireless settings below. All security options may not be available in your printer. Please see your printers' users guide for supported security protocols.



**General Security**

ESSID:

Security Mode:

Security Username:

Security Password:

**WEP Options**

Authentication Type:

WEP Index:

Encr. Key Storage:  Hex  String

When using hex WEP keys, do not use a leading 0x

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

**Kerberos Settings**

Kerberos User:

Kerberos Password:

Kerberos Realm:

Kerberos KDC:

**WPA**

PSK Type

Hex  String

PSK Name:

**EAP**

Optional Private Key:

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,,,
^WPO,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.

```

Start FreeRADIUS.net in Debug mode
auth: type "EAP"
Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 39
rlm_eap: Request found, released from the list
rlm_eap: EAP/peap
rlm_eap: processing type peap
rlm_eap_peap: Authenticate
rlm_eap_tls: processing TLS
rlm_eap_tls: Length Included
eaptls_verify returned 11
eaptls_process returned 7
rlm_eap_peap: EAPTLS_OK
rlm_eap_peap: Session established. Decoding tunneled attributes.
rlm_eap_peap: Received EAP-TLV response.
rlm_eap_peap: Tunneled data is valid.
rlm_eap_peap: Success
rlm_eap: Freeing handler
modcall[authenticate]: module "eap" returns ok for request 39
modcall: group authenticate returns ok for request 39
Login OK: [anonymous/<no User-Password attribute>] <from client private-network-3 port 17999 cli 00a0.f8cc.a364>
Sending Access-Accept of id 156 to 192.168.1.11:1645
MS-MPPE-Recv-Key = 0xd822c96d15bcb0808b74b2b0c28350f4cf2a23d8267931ed018c621a9f82c767
MS-MPPE-Send-Key = 0xd29193477efe6c4ba1c03e31629ca2a1b8ed5ecbd25b05bf3b84746cbf77f7ef
EAP-Message = 0x030a0004
Message-Authenticator = 0x00000000000000000000000000000000
User-Name = "anonymous"
Finished request 39
Going to the next request

```

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

Event Log			
Start Display at Index: <input type="text" value="1"/>		Max Number of Events to Display: <input type="text" value="20"/>	
		<input type="button" value="Previous"/>	<input type="button" value="Next"/>
		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>
Index	Time	Severity	Description
1	Mar 9 04:43:27.723 UTC	◆ Information	Interface Dot11Radio0, Station 00a0.f8cc.a364 Associated KEY_MGMT[WPA]