Using EAP-FAST and WPA EAP-FAST Authentication Security on a Wireless Zebra Tabletop Printer

Q. What is EAP-FAST?

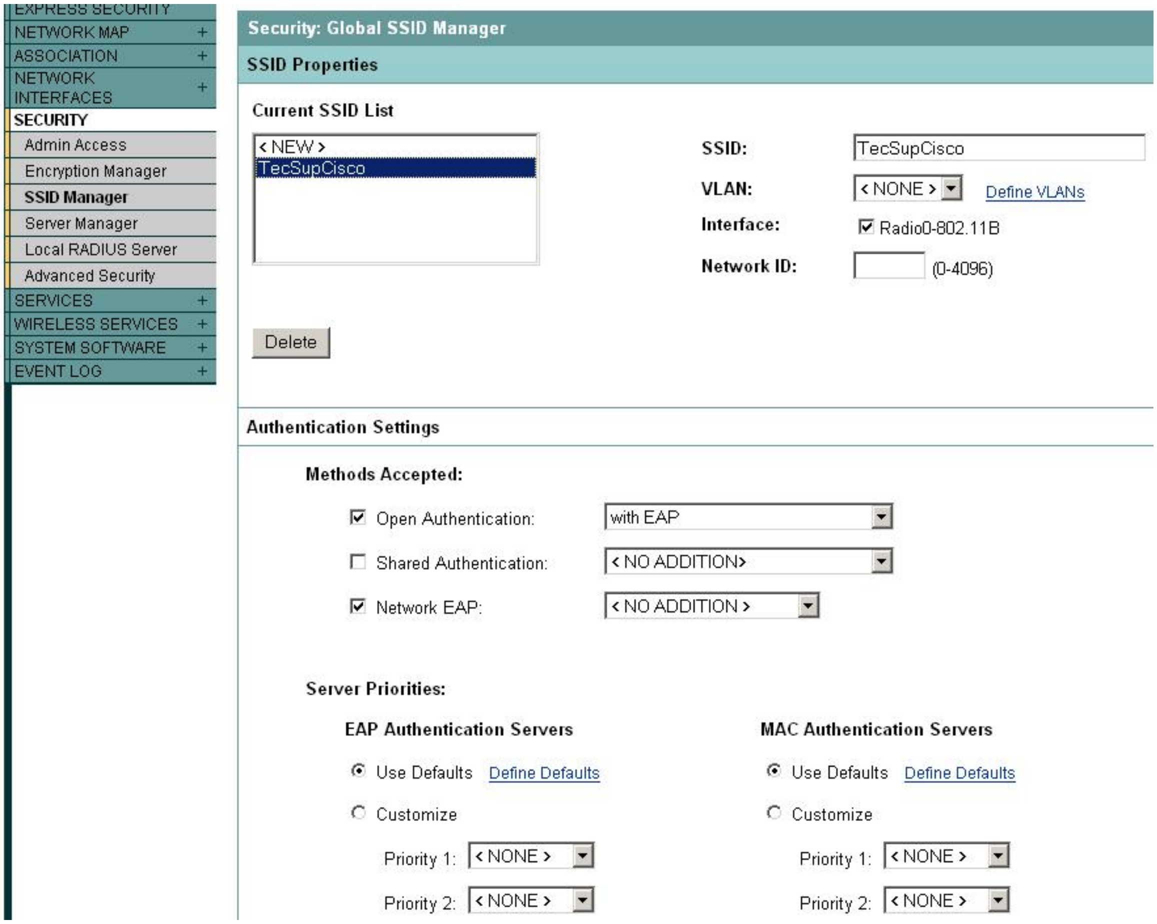
A. **E**xtensible **A**uthentication **P**rotocol-**F**lexible **A**uthentication via **S**ecure **T**unneling is an IEEE 802.1X EAP type developed by Cisco Systems®. It is a wireless security protocol that does not require an advanced password policy or digital certificates. This authentication protocol requires a specially formatted file called a PAC (**P**rotected **A**ccess **C**redential) file to be stored on the client requiring wireless access to the network. The PAC file contains an initial pre-shared key that is also known by the authentication server. PAC keys may be continuously updated once the client has been authenticated. This EAP method has an option called “auto-provisioning”, which allows a client to originally receive a PAC file wirelessly from the authentication server, but this method is less secure, and is <u>not</u> support by the Zebra mobile printer.

EAP-FAST is implemented using a RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) server to authenticate a user (our Zebra mobile printer) before allowing wireless access onto the network. In this example we will be using a Cisco Aironet 1200 access point, which has the built-in ability to act as a local RADIUS server for EAP-FAST authentication. The access point will also perform its regular duty as the EAP authenticator, transferring the data between the printer and the RADIUS server. The firmware level on the Cisco access point used for this test was 12.3(7)JA. Earlier firmware versions may not support local EAP-FAST authentication.

Our first example will be standard EAP-FAST, which uses WEP encryption. Our second example will be WPA EAP-FAST, which uses TKIP encryption.

Configure the Cisco 1200 AP for EAP-FAST authentication.

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



Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
TecSupCisco

SSID: TecSupCisco

VLAN: < NONE >

Interface: ☑ Radio0-802.11B

Network ID: (0-4096)

Authentication Settings

Methods Accepted:

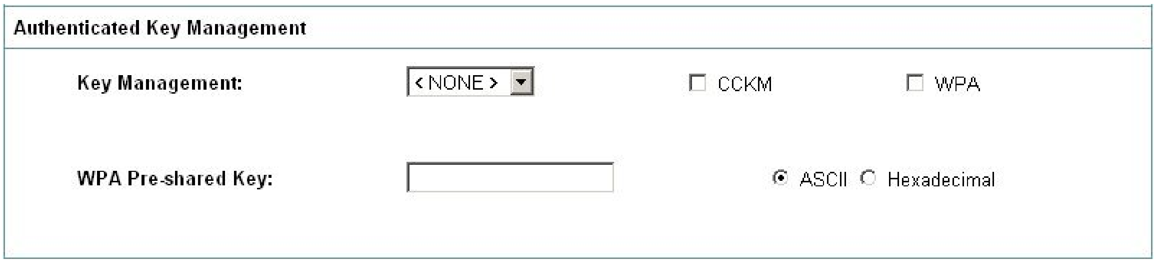
☑ Open Authentication: with EAP

□ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers	**MAC Authentication Servers**
● Use Defaults	● Use Defaults
○ Customize	○ Customize
Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >

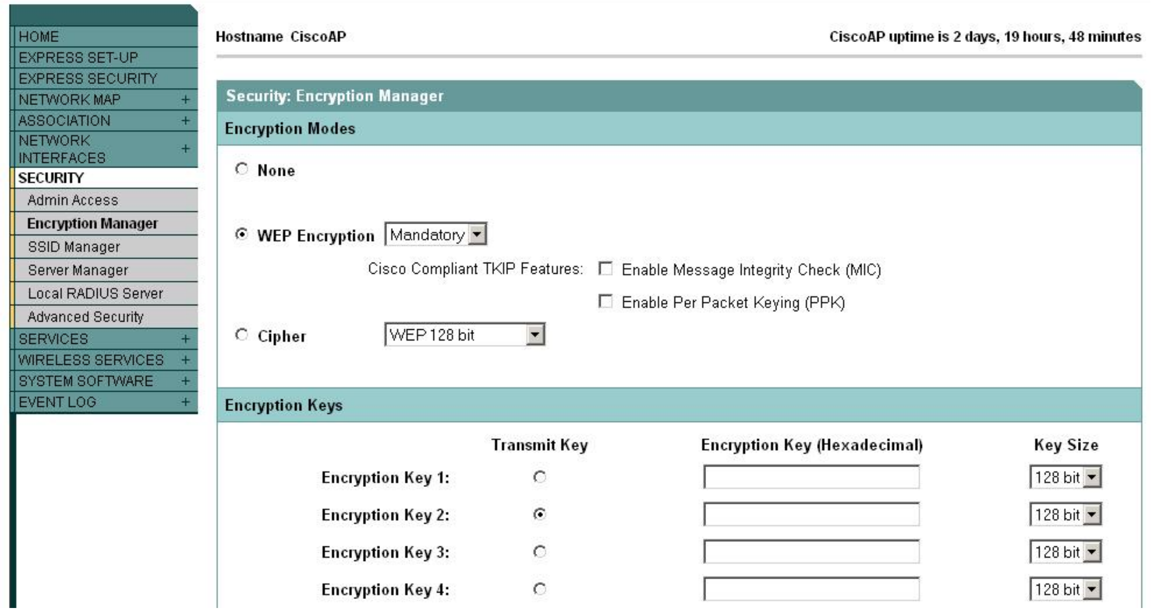


Authenticated Key Management

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)

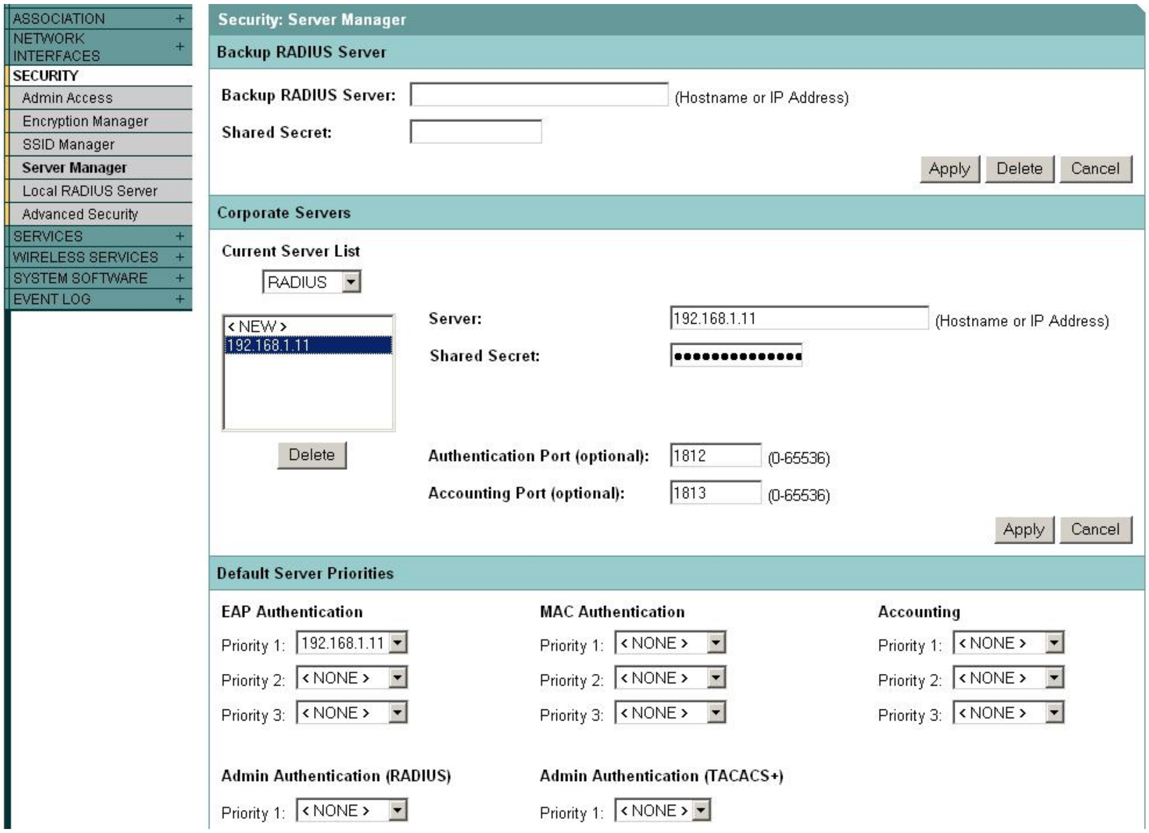
□ Enable Per Packet Keying (PPK)

○ Cipher: WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	○		128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

Next, configure a RADIUS server entry in the Server Manager. Select the IP address for the access point since it will serve as the local RADIUS authentication server, and enter its shared secret. The Cisco access point RADIUS Server listens on TCP ports 1812 and 1813. Select the access point’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

< NEW >
192.168.1.11

Server: 192.168.1.11 (Hostname or IP Address)

Shared Secret: •••••••••••••••

Authentication Port (optional): 1812 (0-65536)

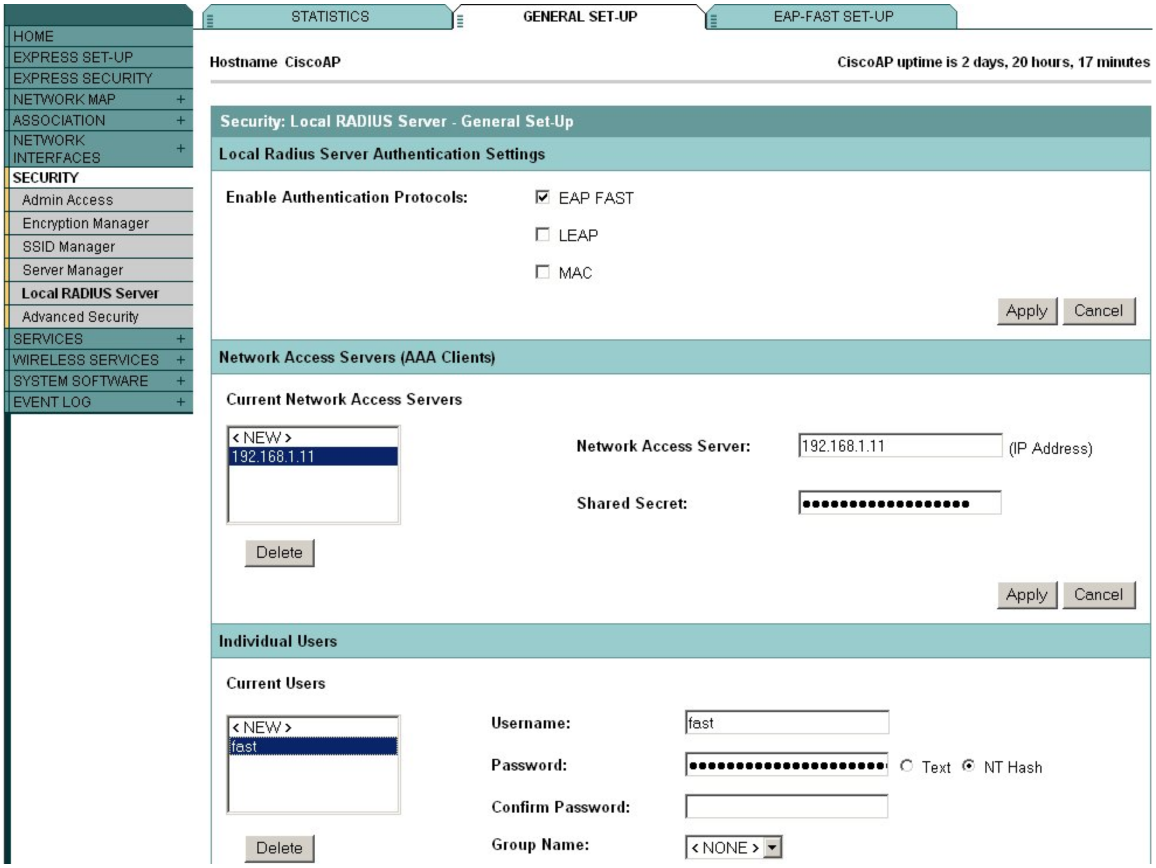
Accounting Port (optional): 1813 (0-65536)

Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: 192.168.1.11	Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >	Priority 3: < NONE >

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

In the Local RADIUS Server section click the General Set-Up tab. Check EAP FAST protocol in the Local Radius Server Authentication Settings section. Enter the IP address of the access point in the Network Access Servers section and enter the server's shared secret. In the Individual Users section click the Text button and ensure that a username and password are entered for the user that the printer will use to log onto the network.



Hostname CiscoAP

CiscoAP uptime is 2 days, 20 hours, 17 minutes

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols: ☑ EAP FAST ☐ LEAP ☐ MAC

Network Access Servers (AAA Clients)

Current Network Access Servers: < NEW > / 192.168.1.11

Network Access Server: 192.168.1.11 (IP Address)

Shared Secret: ••••••••••••••••••

Individual Users

Current Users: < NEW > / fast

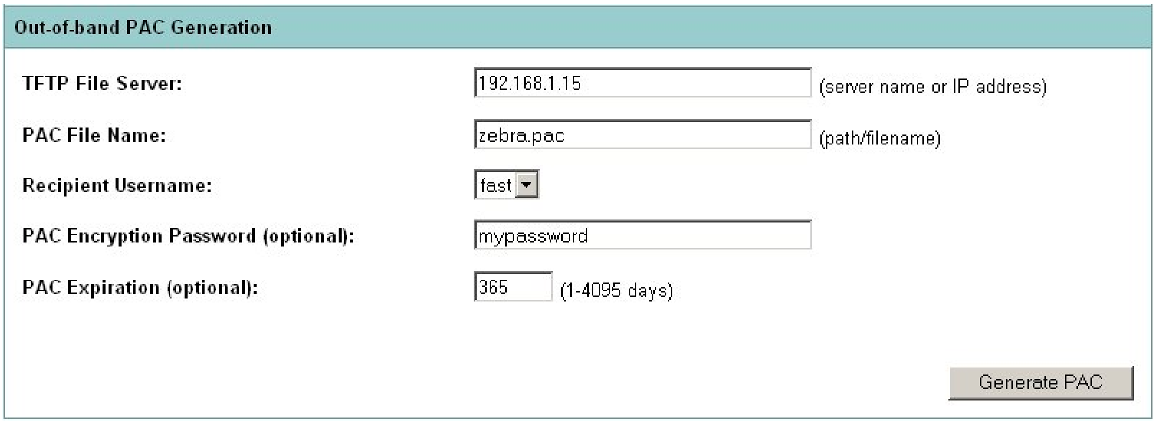
Username: fast

Password: ••••••••••••••••••••••• ○ Text ● NT Hash

Confirm Password:

Group Name: < NONE >

Next, click the EAP-FAST Setup tab to generate the PAC file. The Cisco access point PAC generator requires that a TFTP server be running to receive the file. Enter the IP address of the server. The printer PAC file **must** be named zebra.pac. Enter the username and password that the printer will log on as, and enter an expiration period for the PAC file. Click Generate PAC. Retrieve the file from your FTP server for storage on the printer. *NOTE: The PAC file is encrypted and cannot be viewed with a text editor.*



Out-of-band PAC Generation

TFTP File Server: 192.168.1.15 (server name or IP address)

PAC File Name: zebra.pac (path/filename)

Recipient Username: fast

PAC Encryption Password (optional): mypassword

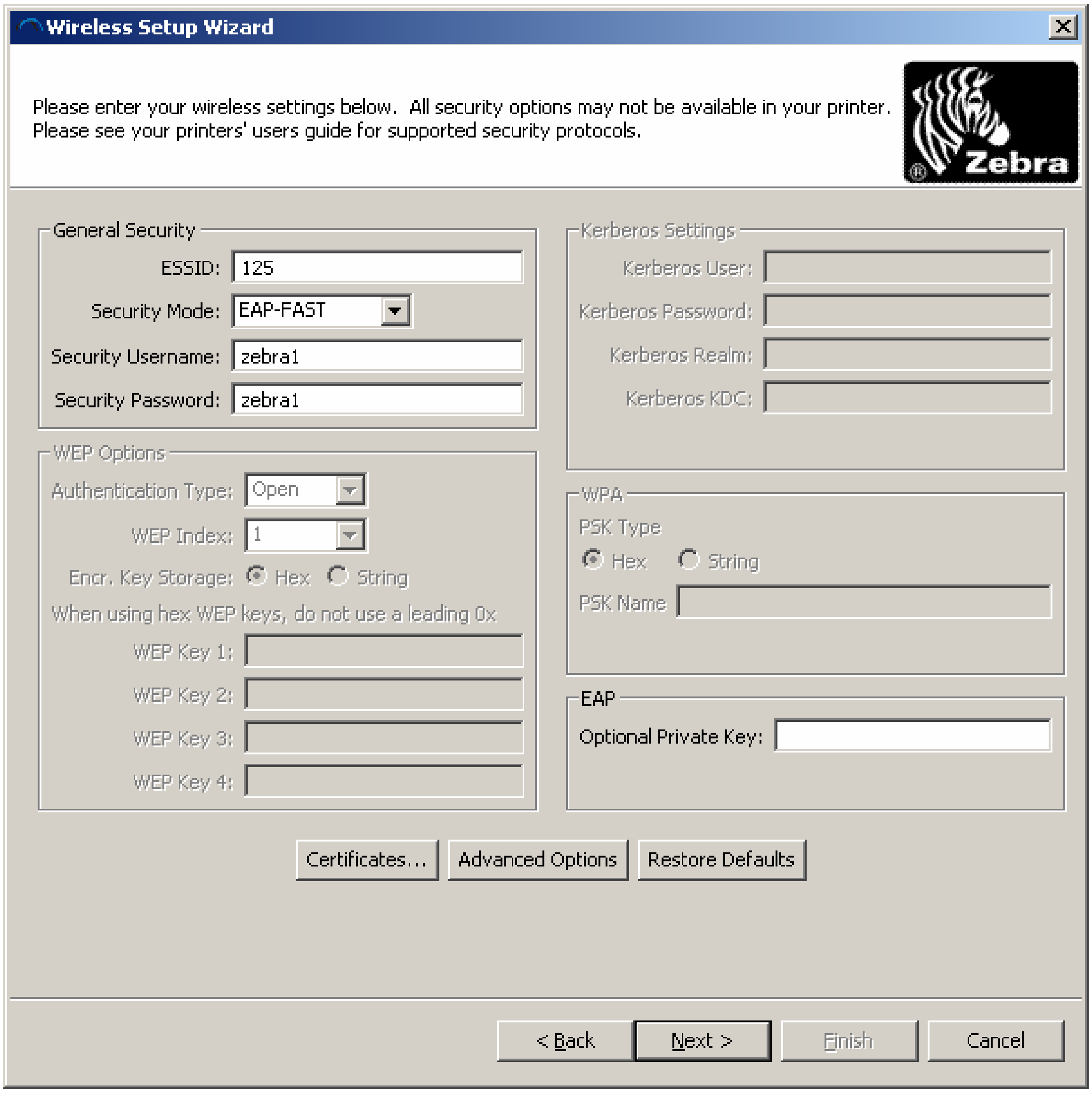
PAC Expiration (optional): 365 (1-4095 days)

Configure the Zebra printer for EAP-FAST 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 EAP-FAST from the Securities drop down box and enter the login info for 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: 125

Security Mode: EAP-FAST

Security Username: zebra1

Security Password: zebra1

WEP Options

Authentication Type: Open

WEP Index: 1

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

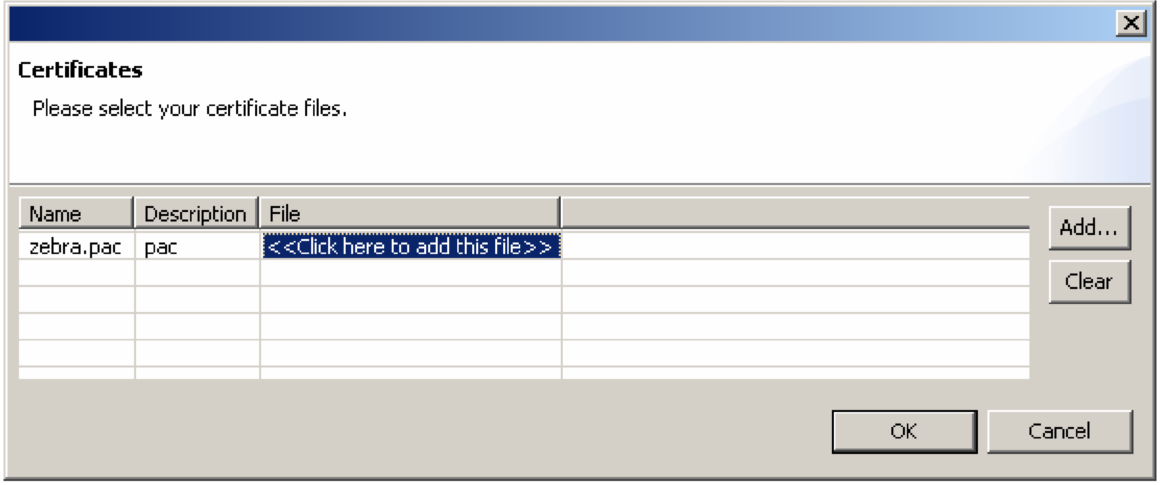
PSK Name

EAP

Optional Private Key:

Next click the **Certificates** button:

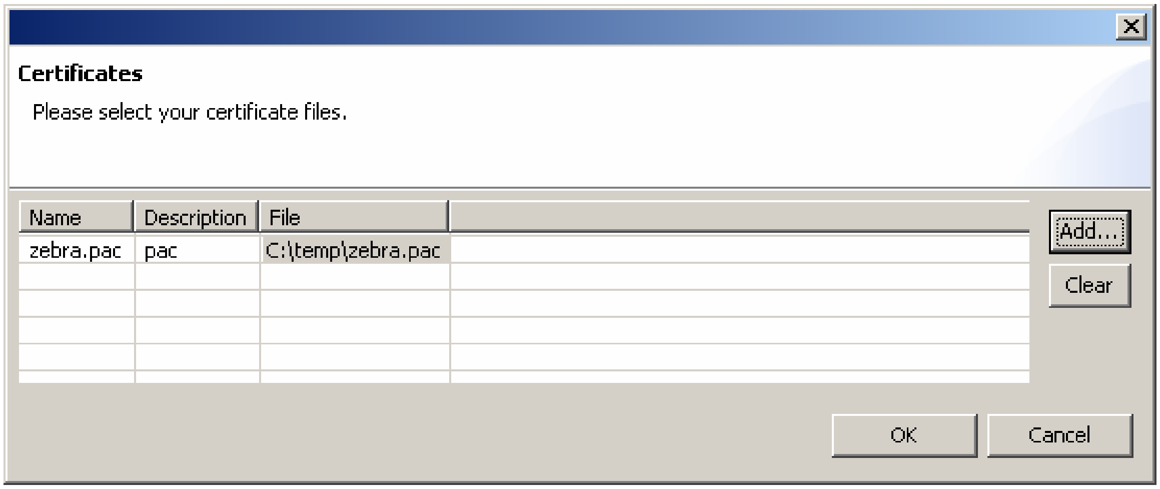
Click **Add** to browse to the zebra.pac file.



Certificates

Please select your certificate files.

Name	Description	File
zebra.pac	pac	<<Click here to add this file>>



Certificates

Please select your certificate files.

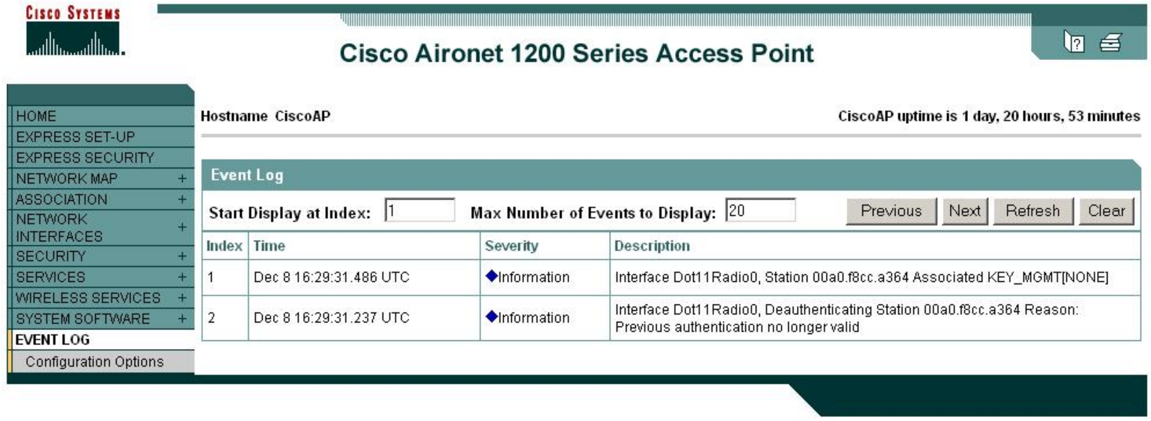
Name	Description	File
zebra.pac	pac	C:\temp\zebra.pac

Click next to view the ZPL:

```
^XA
^WIP,10.17.50.71,255.255.255.0,10.17.50.1
^WAD,D
^WEOFF,1,O,H,,,,
^WP0,0
^WR,,,,100
^WS125,I,L
^NBS
^WLOFF,zebra1 ,zebra1
^WKOFF,,,,
^WX06,zebra1 ,zebra1,


^FX: C:\temp\zebra.pac will be downloaded as: zebra.pac

~DYE:zebra.pac,B,8,,dsfsddsf

^XZ
^XA
^JUS
```

^XZ
Click Finish to send the ZPL to your printer.

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



Hostname CiscoAP

CiscoAP uptime is 1 day, 20 hours, 53 minutes

Event Log

Start Display at Index: 1

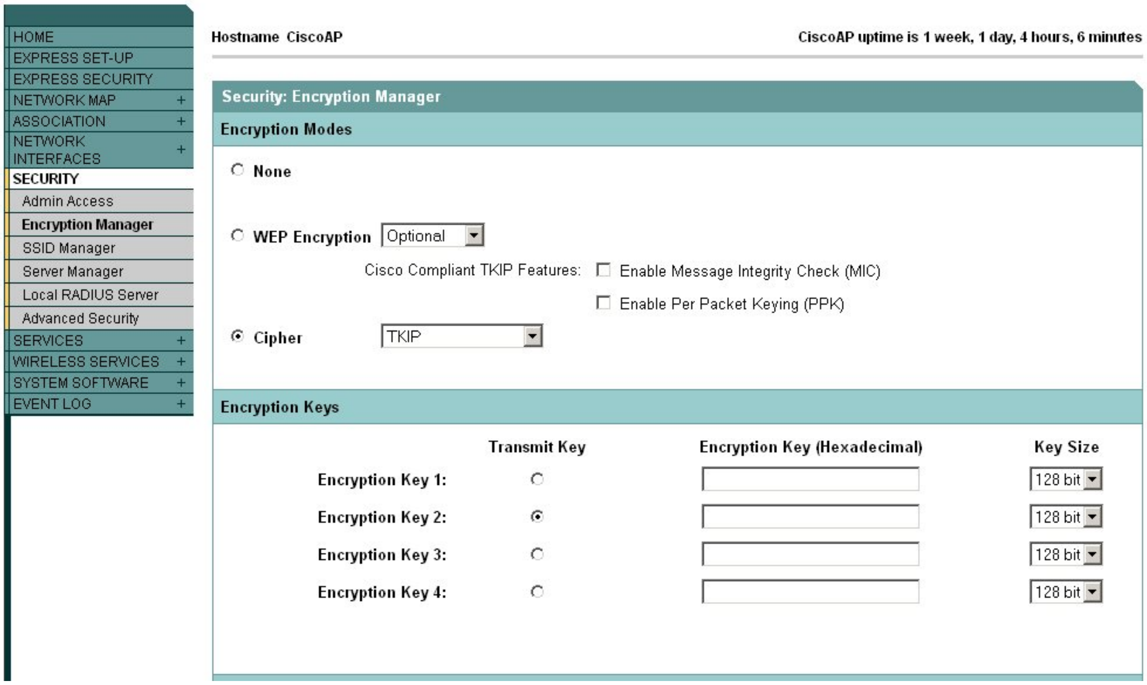
Max Number of Events to Display: 20

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 EAP-FAST. 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 EAP-FAST except for the changes shown in the following two screenshots.

Configure the Cisco 1200 AP for WPA EAP-FAST authentication.

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



Hostname CiscoAP

CiscoAP uptime is 1 week, 1 day, 4 hours, 6 minutes

Security: Encryption Manager

Encryption Modes

○ None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)

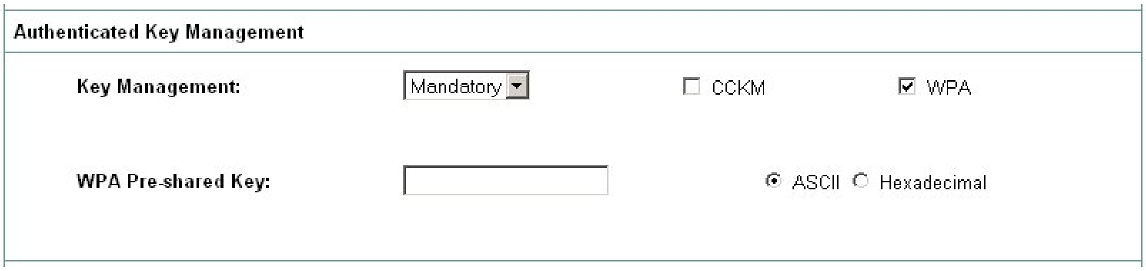
□ Enable Per Packet Keying (PPK)

● Cipher TKIP

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	○		128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

In the SSID Manager configure WPA as shown below.



Authenticated Key Management

Key Management: Mandatory ☐ CCKM ☑ WPA

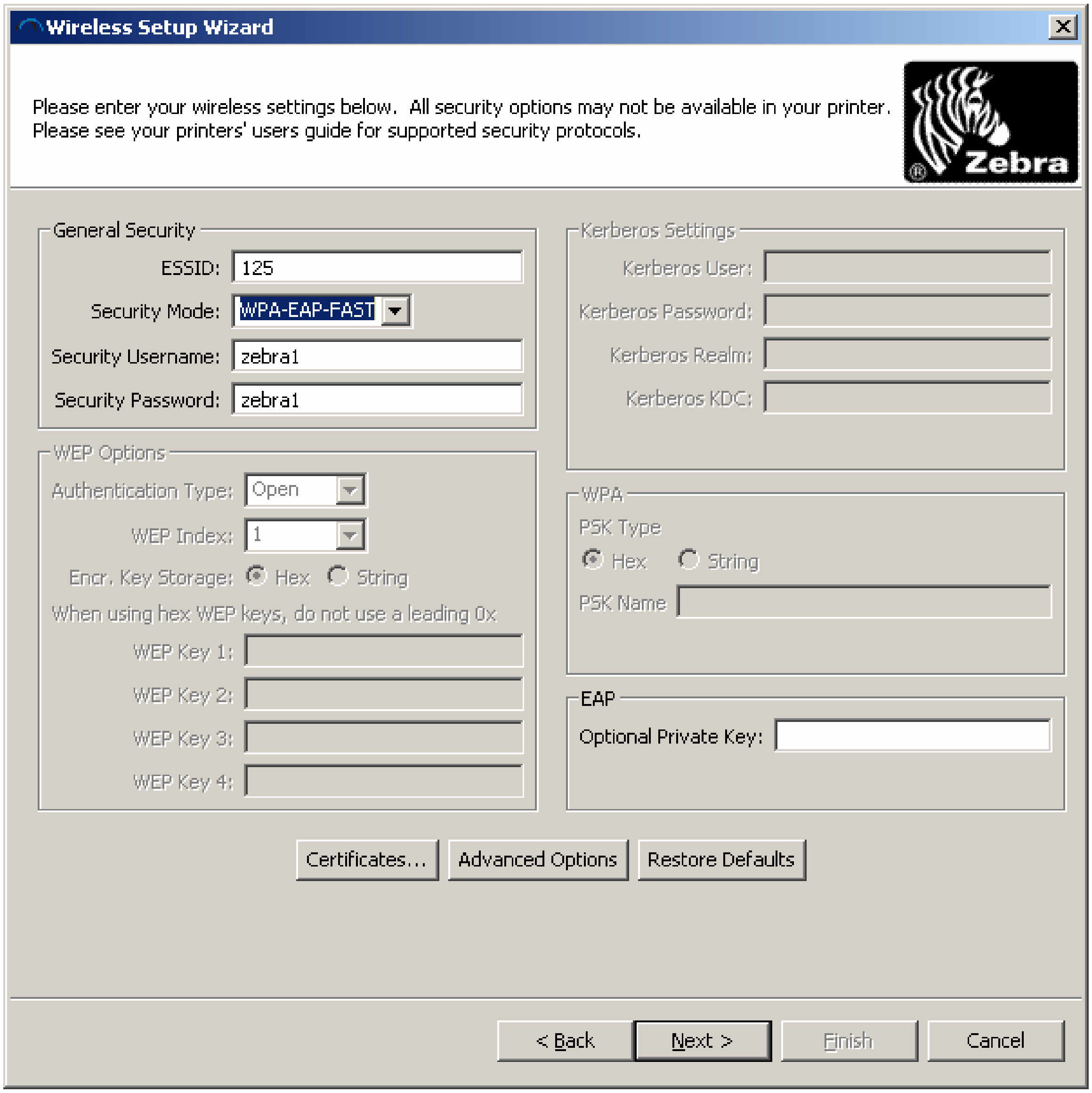
WPA Pre-shared Key: ● ASCII ○ Hexadecimal

Configure the Zebra printer for WPA EAP-FAST 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-EAP-FAST from the Securities drop down box and enter the login info for 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: 125

Security Mode: WPA-EAP-FAST

Security Username: zebra1

Security Password: zebra1

WEP Options

Authentication Type: Open

WEP Index: 1

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

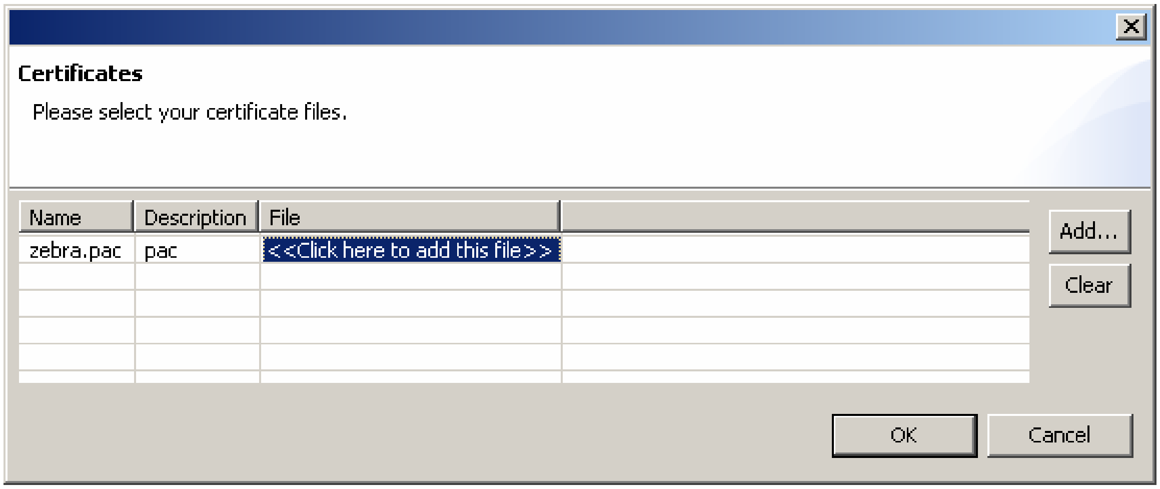
● Hex ○ String

PSK Name

EAP

Optional Private Key:

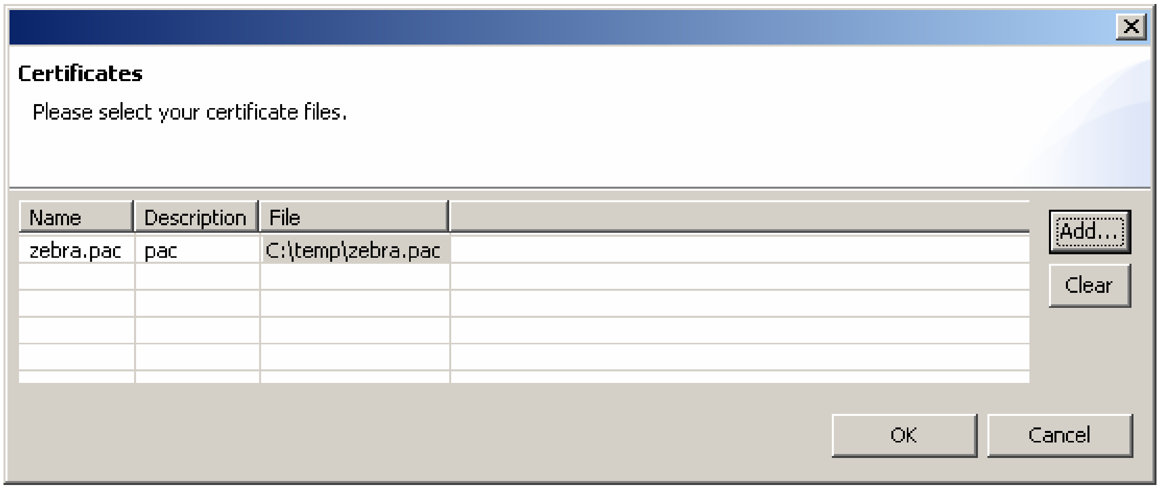
Click **Add** to browse to the zebra.pac file.



Certificates

Please select your certificate files.

Name	Description	File
zebra.pac	pac	<<Click here to add this file>>



Certificates

Please select your certificate files.

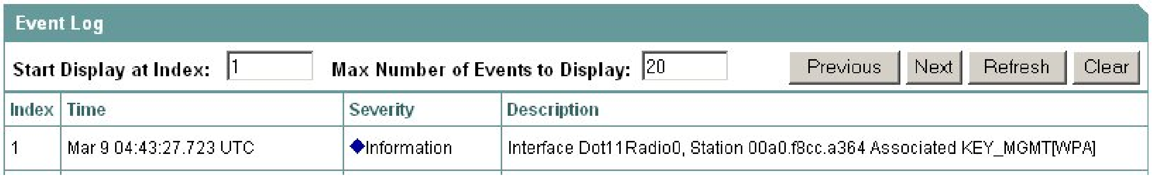
Name	Description	File
zebra.pac	pac	C:\temp\zebra.pac

Click Next to view ZPL:

```
^XA
^WIP,10.17.50.71,255.255.255.0,10.17.50.71
^WAD,D
^WEOFF,1,O,H,,,,
^WP0,0
^WR,,,,100
^WStestnet,I,L
^NBS
^WLOFF,zebra1,zebra1
^WKOFF,,,,
^WX12,zebra1,zebra1,


^FX: C:\temp\zebra.pac will be downloaded as: zebra.pac

~DYE:zebra.pac,B,8,,dsfsddsf

^XZ
^XA
^JUS
```

Click Finish to send ZPL to printer.

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



Event Log

Start Display at Index: 1 Max Number of Events to Display: 20

Index	Time	Severity	Description
1	Mar 9 04:43:27.723 UTC	◆Information	Interface Dot11Radio0, Station 00a0.f8cc.a364 Associated KEY_MGMT[WPA]