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

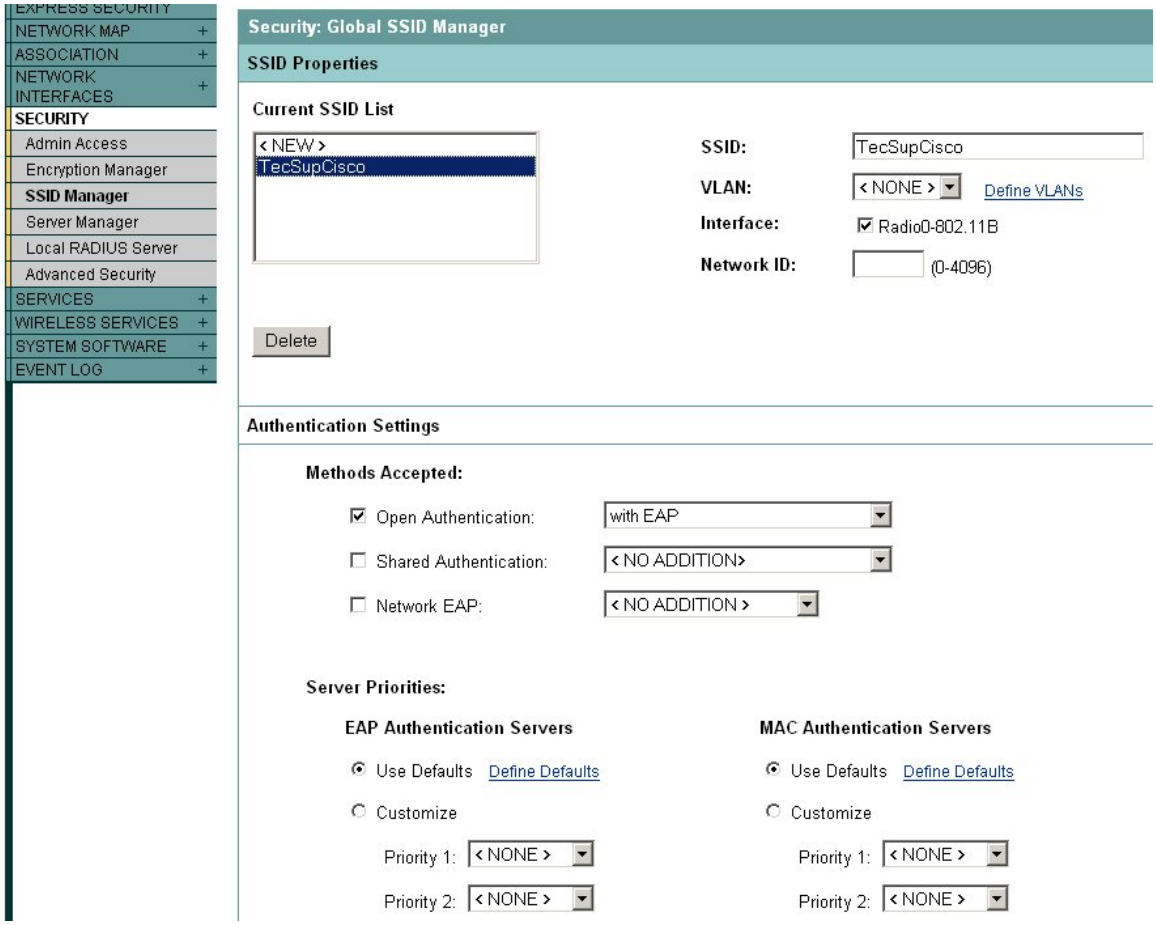
Q. What is EAP-TTLS?

A. Extensible **A**uthentication **P**rotocol- **T**unneled **T**ransport **L**evel **S**ecurity 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 (our Zebra mobile printer) by passing a digital certificate to the printer. A root certificate is stored on the printer which will be 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.

Our first example will be standard EAP-TTLS, which uses WEP encryption. Our second example will be WPA EAP-TTLS, which uses TKIP encryption. To begin, make sure that the printer model you wish to configure for EAP-TTLS has an SH3 microprocessor. You can determine this by performing a 2-key self test (power on the printer with the Feed button pressed, and release it once the self test starts printing). Verify that in the second part of the test in the Program section that the Software version begins with SH. If your printer does not show this information then you do not have an SH3 processor, which is a requirement for EAP-TTLS authentication on a Zebra mobile printer.

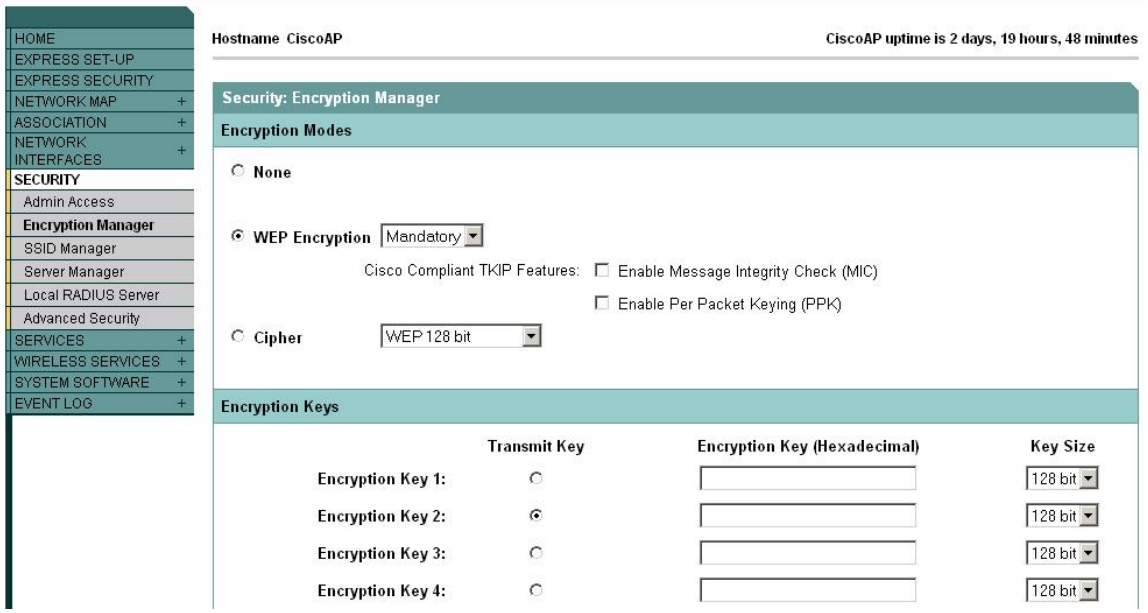
Configure the Cisco 1200 AP for EAP-TTLS authentication.

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

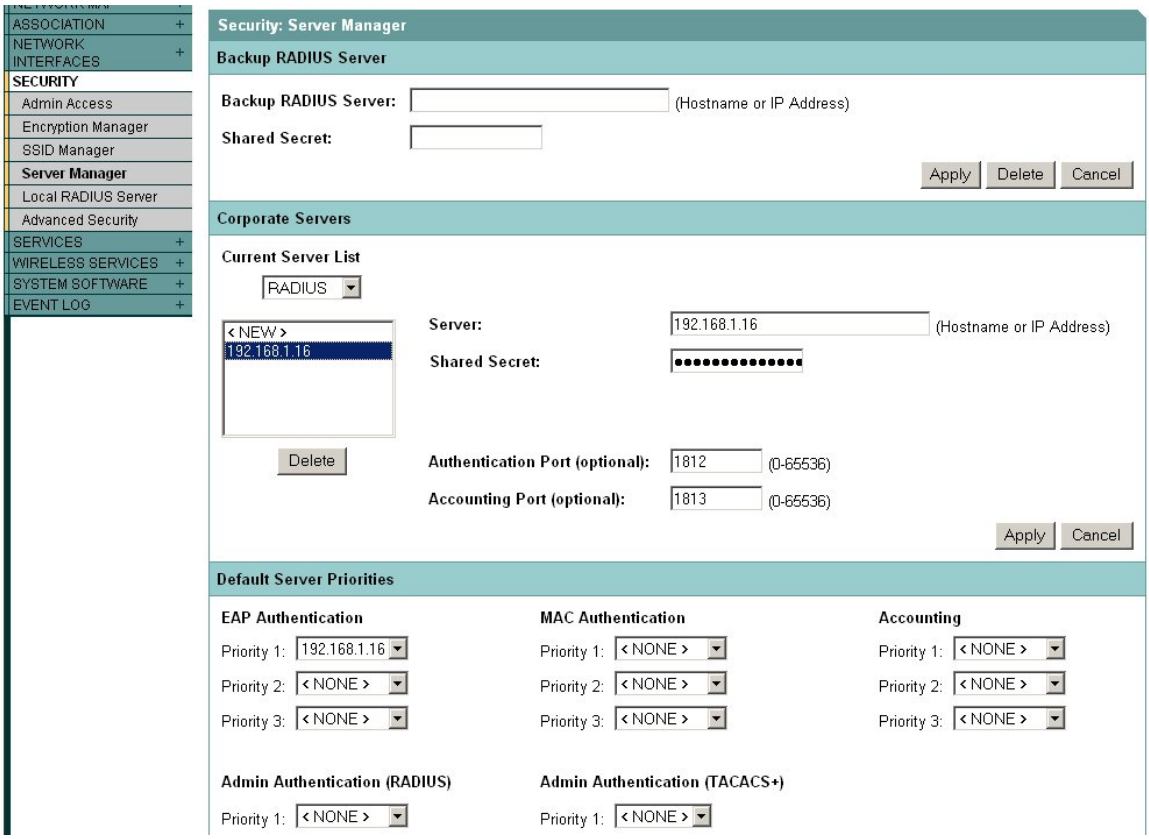

EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY
Admin Access
Encryption Manager
SSID Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +
Security: Global SSID Manager
SSID Properties
Current SSID List
< NEW >
TecSupCisco
SSID:
TecSupCisco
VLAN:
< NONE >
Define VLANs
Interface:
Radio0-802.11B
Network ID:
(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:



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 EAP-TTLS 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 TTLS protocol. Save the file if changes are made.

```
default_eap_type = ttls
```

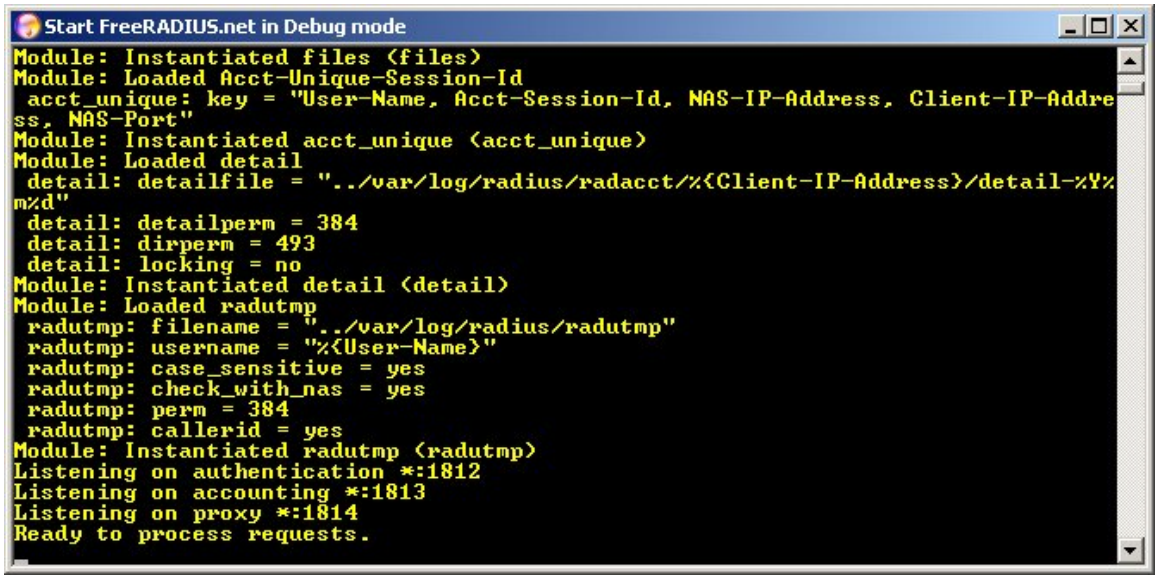
Open the Radiusd.conf file. Locate the PAP module and change the encryption_scheme to clear text as shown below. Save the file if changes are made.

```
#  DEFAULT: crypt
      pap {
            encryption_scheme = clear
      }
```

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 TTLS user 'ttls' as shown below. Save the file if changes are made.

```
# Test TTLS user
ttls Auth-Type := pap, 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 the Zebra printer for EAP-TTLS authentication.

To configure the Zebra printer for EAP-TTLS authentication we must aquire and store the necessary certificate file on the printer, and configure the appropriate printer parameters to enable EAP-TTLS authentication. For this example we will be using the demo certificate that is supplied with the Windows version of FreeRadius. Locate the 'DemoCerts' folder of your FreeRadius installation. At the time of this writing the default path and version is:

C:\Program Files\FreeRADIUS.net-1.0.2-r0.0.8\etc\raddb\certs\FreeRADIUS.net\DemoCerts

Only one certificate file is required in order to successfully authenticate our printer using EAP-TTLS (a root certificate from a certificate authority), and a user name and password that has also been properly configured in the RADIUS server (in this example the 'ttls' user that we setup previously). The certificate file must be in PEM format. It needs to have a specific filename, and must be stored in the printer's flash file system. Copy the following file from the FreeRadius 'DemoCerts' folder and place it in a temporary folder. Rename the certificate file as shown below. The file name is not case sensitive.

FreeRADIUS.net-Root.crt -> CacertSv.nrd

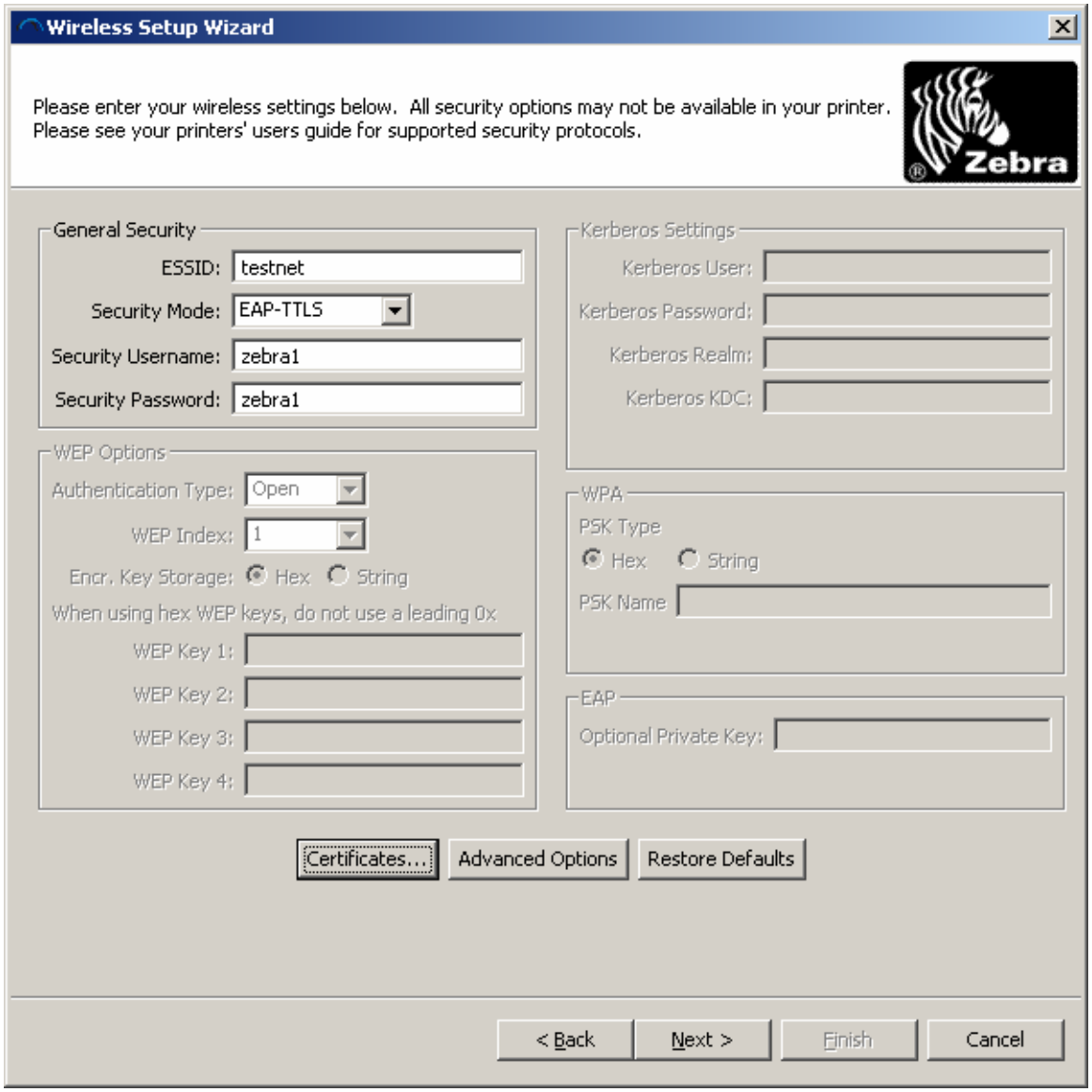
Note: Certificate files are normally generated by a trusted 3rd-party Certificate Authority (CA). If you are using different certificate files the TTLS section of the Eap.conf file will need to be edited to reference the appropriate files. Also, the root certificate file must be renamed as above and saved to the printer's file system.

Setting up the Print Server:

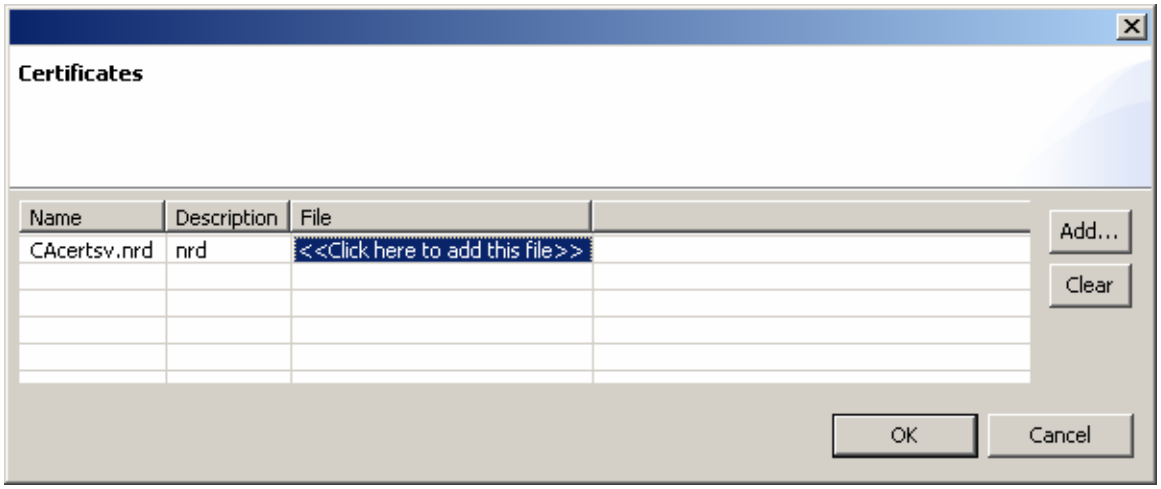
The Printer must have **firmware x.15.x** or higher.

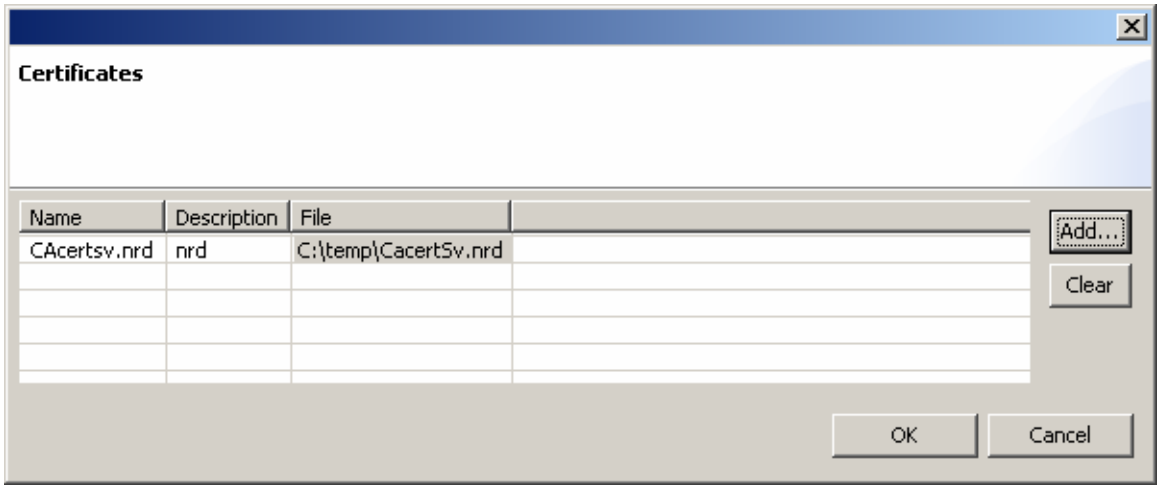
To configure the printer use **ZebraNet Bridge Enterprise** V1.2.1 or higher. From Tools, select the Wireless Setup Wizard.

Select **EAP-TTLS** from the security Mode drop down box:



Next click **Certificates** to add:



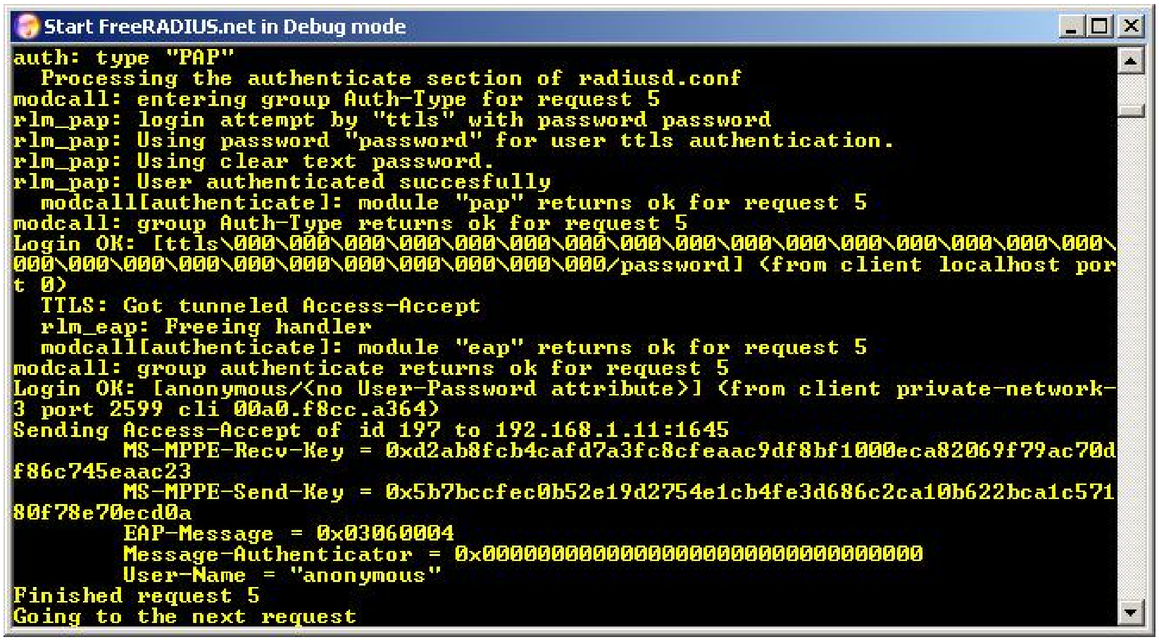


Click next to view the ZPL:

```
^XA
^WIP,10.17.50.71,255.255.255.0,10.17.50.1
^WAD,D
^WEOFF,1,O,H,,,,
^WP0,0
^WR,,,,100
^WStestnet,I,L
^NBS
^WLOFF,zebra1,zebra1
^WKOFF,,,,
^WX05,zebra1,zebra1


^FX: C:\temp\CacertSv.nrd will be downloaded as: CAcertsv.nrd

~DYE:CAcertsv.nrd,A,6,,ddfsaf

^XZ
^XA
^JUS
^XZ
```

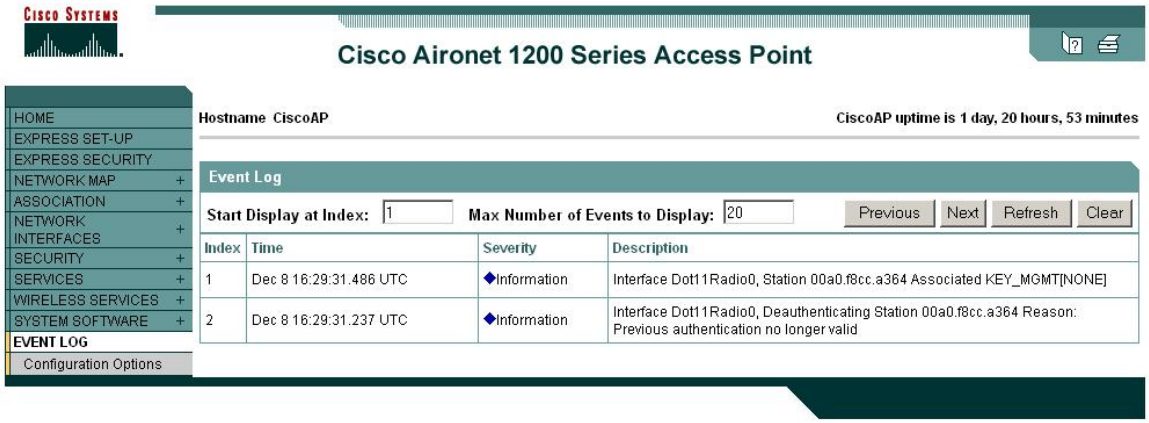
Click finish to send to the printer.

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



```
Start FreeRADIUS.net in Debug mode
auth: type "PAP"
  Processing the authenticate section of radiusd.conf
modcall: entering group Auth-Type for request 5
rlm_pap: login attempt by "ttls" with password password
rlm_pap: Using password "password" for user ttls authentication.
rlm_pap: Using clear text password.
rlm_pap: User authenticated succesfully
  modcall[authenticate]: module "pap" returns ok for request 5
modcall: group Auth-Type returns ok for request 5
Login OK: [ttls\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\
000\000\000\000\000\000\000\000\000\000\000/password] (from client localhost por
t 0)
  TTLS: Got tunneled Access-Accept
  rlm_eap: Freeing handler
  modcall[authenticate]: module "eap" returns ok for request 5
modcall: group authenticate returns ok for request 5
Login OK: [anonymous/<no User-Password attribute>] (from client private-network-
3 port 2599 cli 00a0.f8cc.a364)
Sending Access-Accept of id 197 to 192.168.1.11:1645
        MS-MPPE-Recv-Key = 0xd2ab8fcb4cafd7a3fc8cfeaac9df8bf1000eca82069f79ac70d
f86c745eaac23
        MS-MPPE-Send-Key = 0x5b7bccfec0b52e19d2754e1cb4fe3d686c2ca10b622bca1c571
80f78e70ecd0a
        EAP-Message = 0x03060004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "anonymous"
Finished request 5
Going to the next request
```

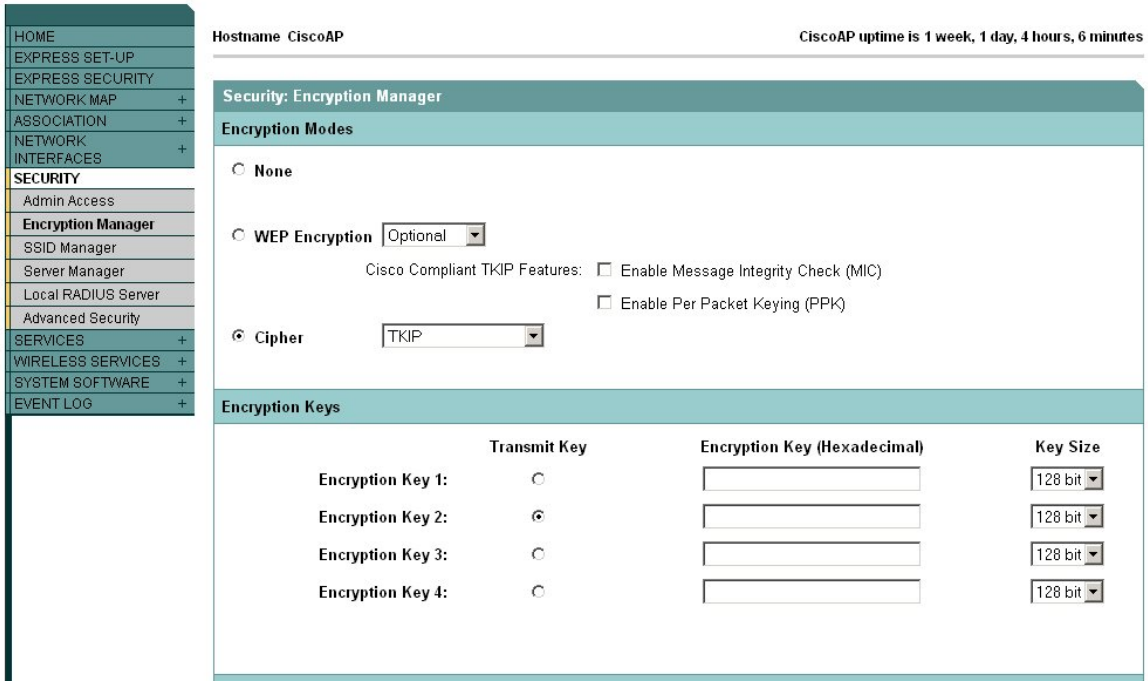
The access point's event log should also contain information regarding the printer's successful connection.



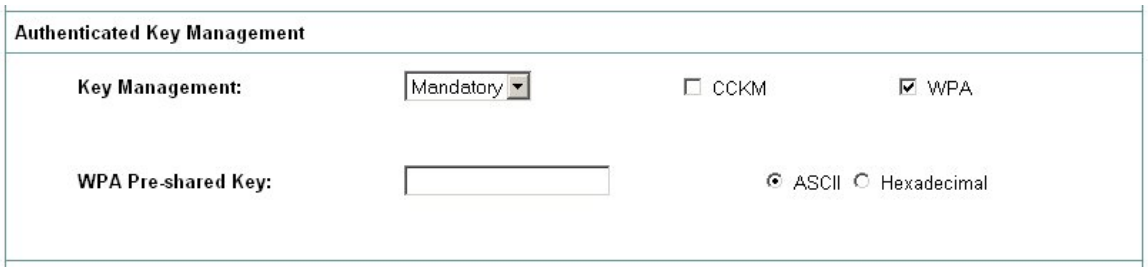
Next, we will modify the settings on the Cisco access point and the Zebra printer to use WPA EAP-TTLS. WPA increases security further by using TKIP (Temporal Key Integrity Protocol) as an encryption scheme instead of WEP. All the Cisco access point settings are the same as shown previously for standard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

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

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



In the SSID Manager configure WPA as shown below.

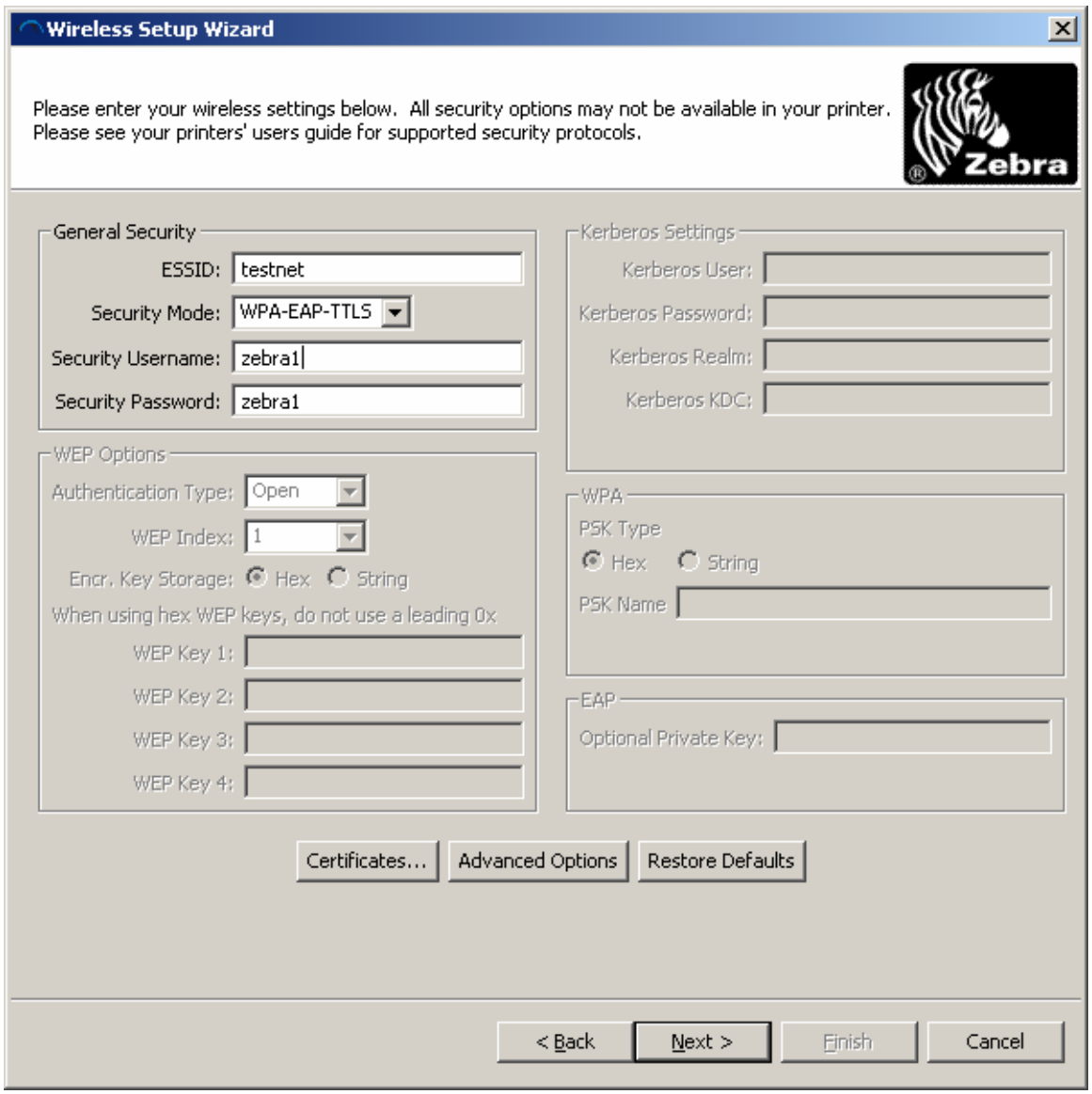


Configure the Zebra printer for WPA EAP-TTLS authentication.

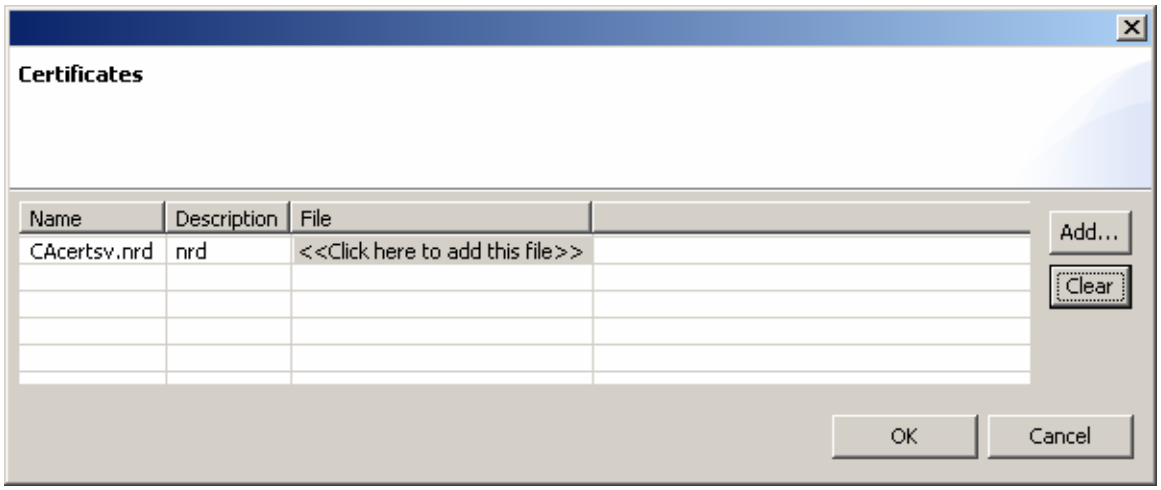
The Printer must have **firmware x.15.x** or higher.

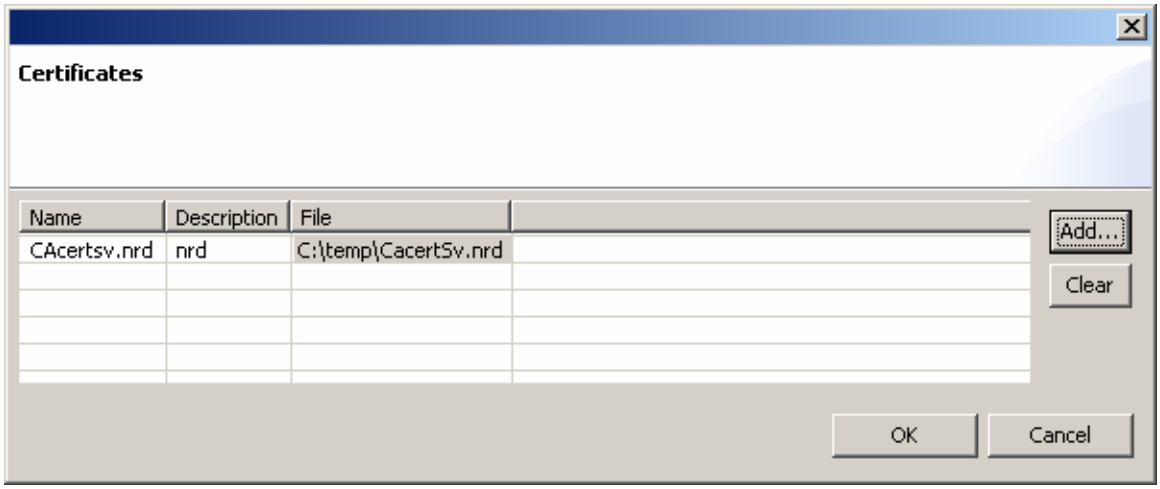
To configure the printer use **ZebraNet Bridge Enterprise** V1.2.1 or higher. From Tools, select the Wireless Setup Wizard.

Select **WPA-EAP-TTLS** from the security Mode drop down box:



Click Certificates to add:





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
^WStestnet,I,L
^NBS
^WLOFF,zebra1,zebra1
^WKOFF,,,,
^WX11,zebra1,zebra1

^FX: C:\temp\CacertSv.nrd will be downloaded as: CAcertsv.nrd

~DYE:CAcertsv.nrd,A,6,,ddfsaf

^XZ
^XA
^JUS
^XZ

Click finished to send ZPL to the printer.

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

Start FreeRADIUS.net in Debug mode

```
auth: type "PAP"
  Processing the authenticate section of radiusd.conf
modcall: entering group Auth-Type for request 11
rlm_pap: login attempt by "ttls" with password password
rlm_pap: Using password "password" for user ttls authentication.
rlm_pap: Using clear text password.
rlm_pap: User authenticated succesfully
  modcall[authenticate]: module "pap" returns ok for request 11
modcall: group Auth-Type returns ok for request 11
Login OK: [ttls\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\
000\000\000\000\000\000\000\000\000\000\000/password] (from client localhost por
t 0)
  TTLS: Got tunneled Access-Accept
  rlm_eap: Freeing handler
  modcall[authenticate]: module "eap" returns ok for request 11
modcall: group authenticate returns ok for request 11
Login OK: [anonymous/<no User-Password attribute>] (from client private-network-
3 port 2600 cli 00a0.f8cc.a364)
Sending Access-Accept of id 203 to 192.168.1.11:1645
        MS-MPPE-Recv-Key = 0x50ffcd730acc9420f58822d04f7f983b55dd5ecba4dc912aacc
a28dc73ae6d38
        MS-MPPE-Send-Key = 0xe1982c987fa4801a81ea64765db646ca85e11370203dcdcdb55
20b7038be273c
        EAP-Message = 0x03060004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "anonymous"
Finished request 11
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: 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]