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

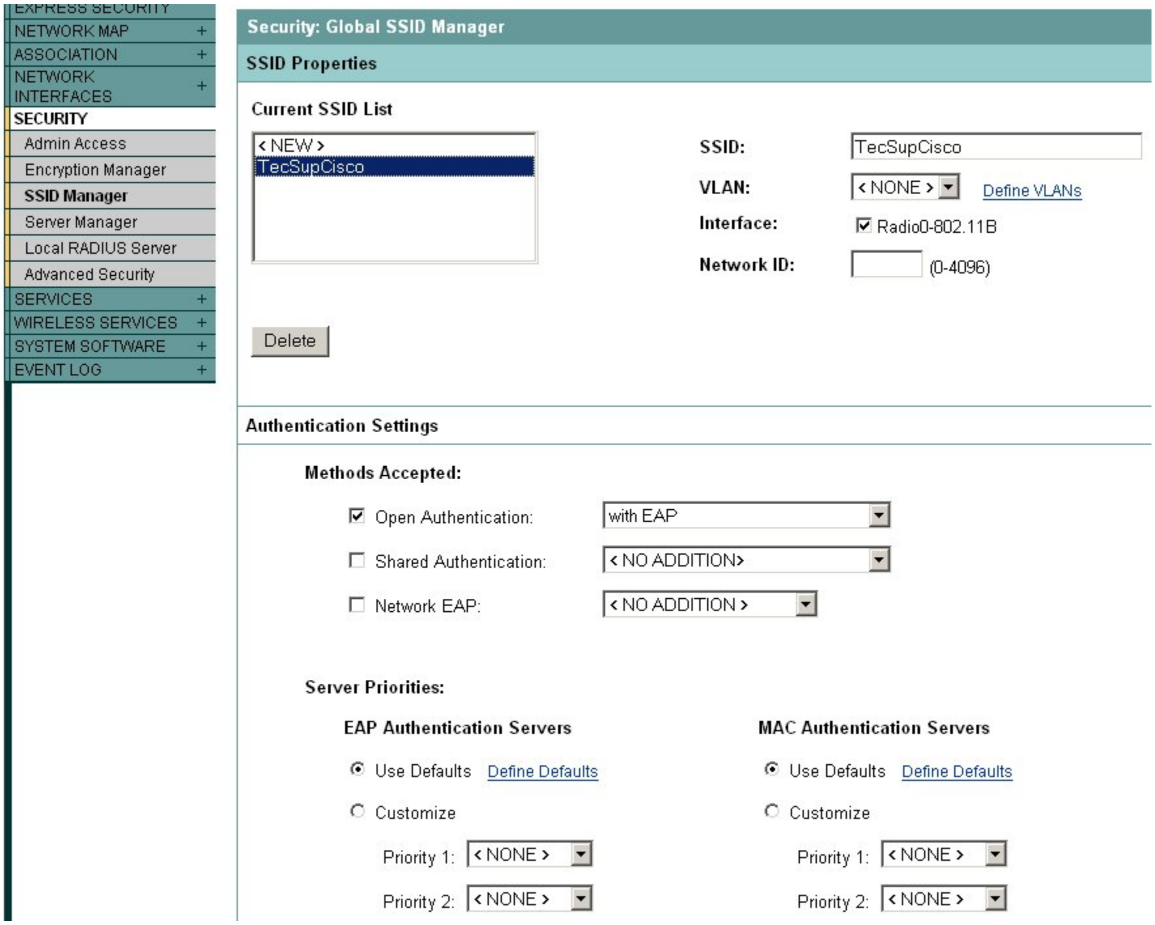
**Q.** What is EAP-TLS?

**A. E**xtensible **A**uthentication **P**rotocol- **T**ransport **L**evel **S**ecurity is an IEEE 802.1x EAP security method that uses digital certificates for mutual server and client authentication. EAP-TLS requires 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. Both the server and the client prove their identities via PKI (Public Key Infrastructure) cryptography passing X.509 digital certificates to each other. 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-TLS, which uses WEP encryption. Our second example will be WPA EAP-TLS, which uses TKIP encryption.

### Configure the Cisco 1200 AP for EAP-TLS 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:



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)

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 >

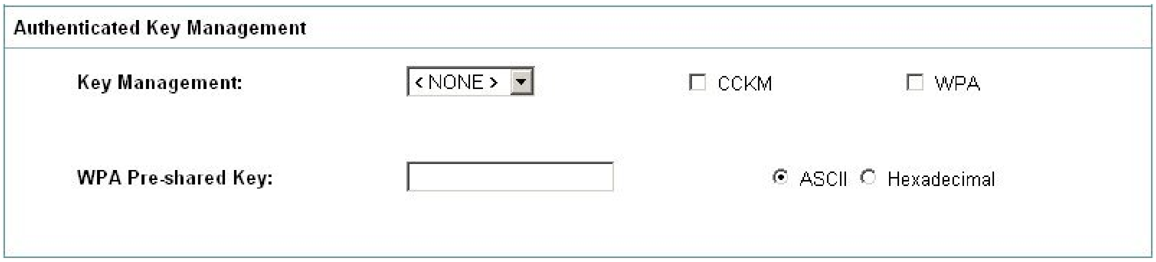
MAC Authentication Servers

● Use Defaults Define Defaults

○ Customize

Priority 1: < NONE >

Priority 2: < NONE >

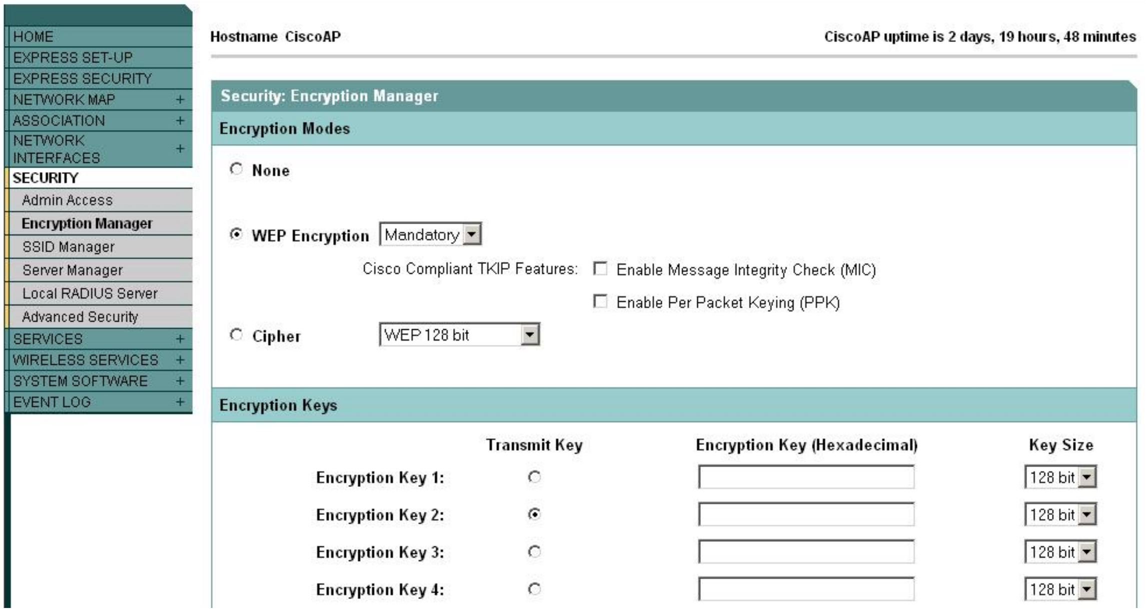


Authenticated Key Management

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)

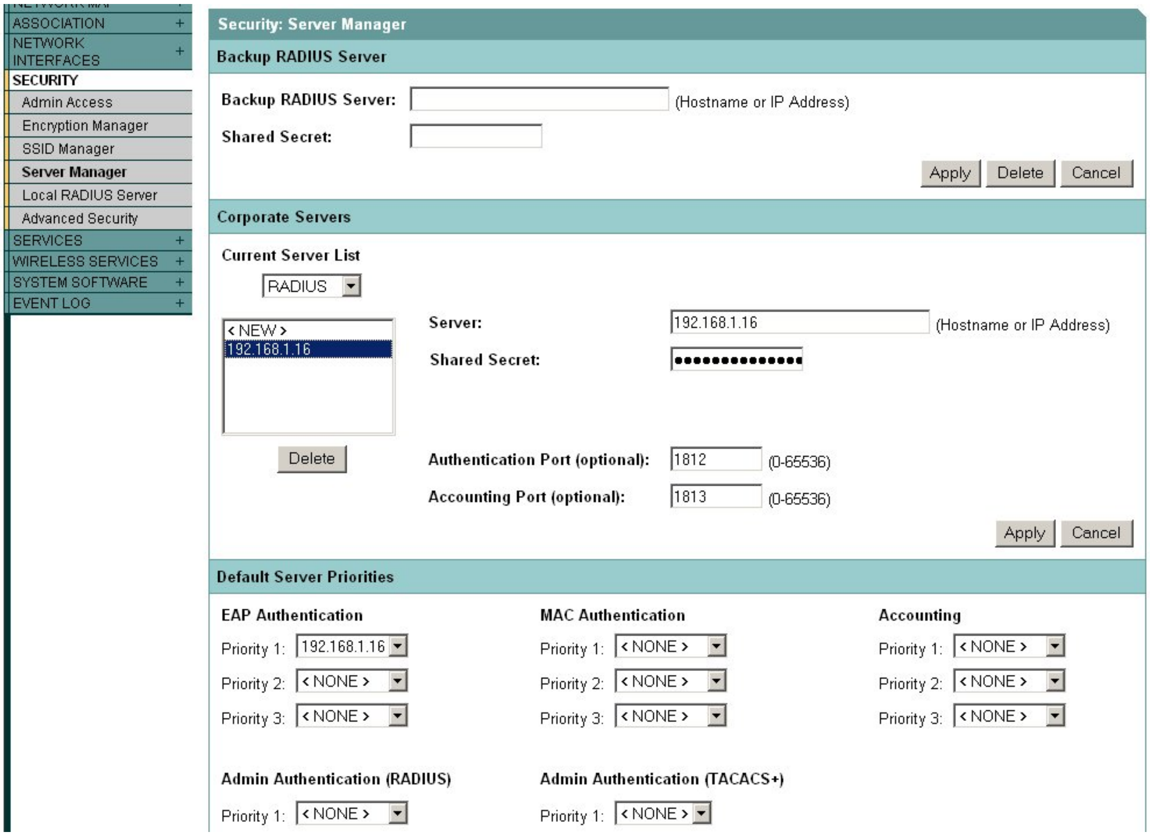
□ Enable Per Packet Keying (PPK)

○ Cipher: WEP 128 bit

Encryption Keys

| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|---|---|---|---|
| Encryption Key 1: | ○ | | 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 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

< NEW >
192.168.1.16

Server: 192.168.1.16 (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: 192.168.1.16 | 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 > |

## Configure the FreeRadius server for EAP-TLS 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
}
```

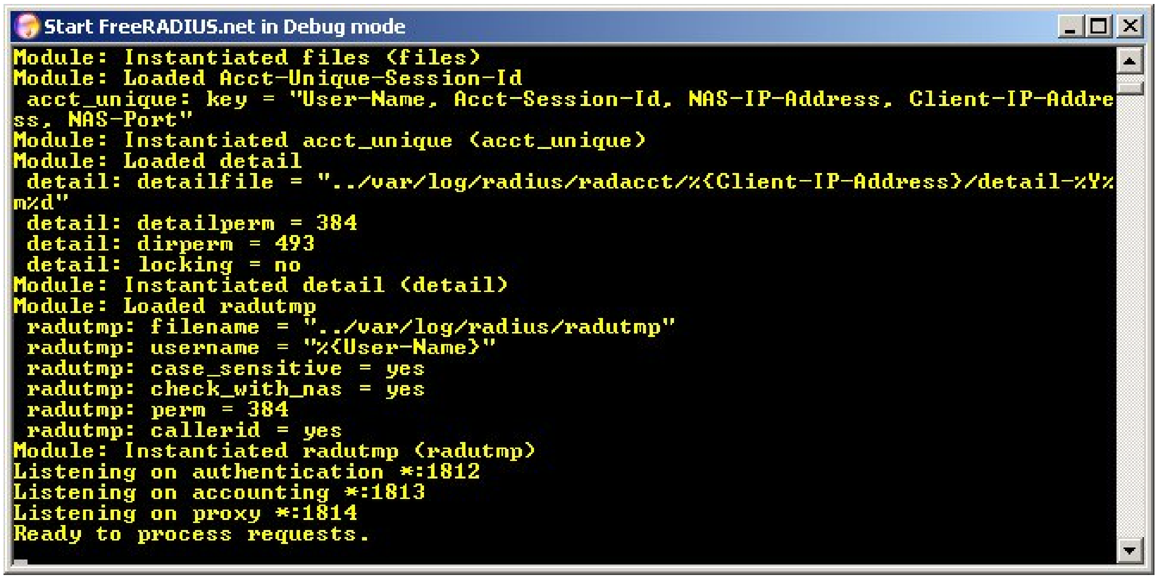
Save the file and open the Eap.conf file for editing. If necessary, edit the line that reads ‘default_eap_type’ to select the TLS protocol. Save the file if changes are made.

```
default_eap_type = tls
```

Next we will verify the user credentials that our printer will use to login to the network. Open the Users file. Verify that the user ‘FreeRADIUS.net-Client’ is uncommented as below. Save the file if changes are made.

```
# Test TLS Certificate based user
FreeRADIUS.net-Client User-zebra1 == "zebra1"
            Reply-Message = "Hello, %u"
```

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.



```
Module: Instantiated files (files)
Module: Loaded Acct-Unique-Session-Id
 acct_unique: key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-IP-Addre
ss, 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 the Zebra printer for EAP-TLS authentication.

To configure the Zebra printer for EAP-TLS authentication we must aquire and store the necessary certificate files on the printer, and configure the appropriate printer parameters to enable EAP-TLS authentication. For this example we will be using the demo certificates that are 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*

Three certificate files are required in order to successfully authenticate our printer using EAP-TLS (a root certificate from a certificate authority, a client certificate, and a client private key certificate). The certificates must be in PEM format. They need to have specific filenames, and must be stored in the printer's flash file system. Copy the following three files from the FreeRadius 'DemoCerts' folder and place them in a temporary folder. Rename the certificate files as shown below. The file names are not case sensitive.

**FreeRADIUS.net-Root.crt -> CacertSv.nrd**
**FreeRADIUS.net-Client.crt -> CertCln.nrd**
**FreeRADIUS.net-Client.pem -> privkey.nrd**

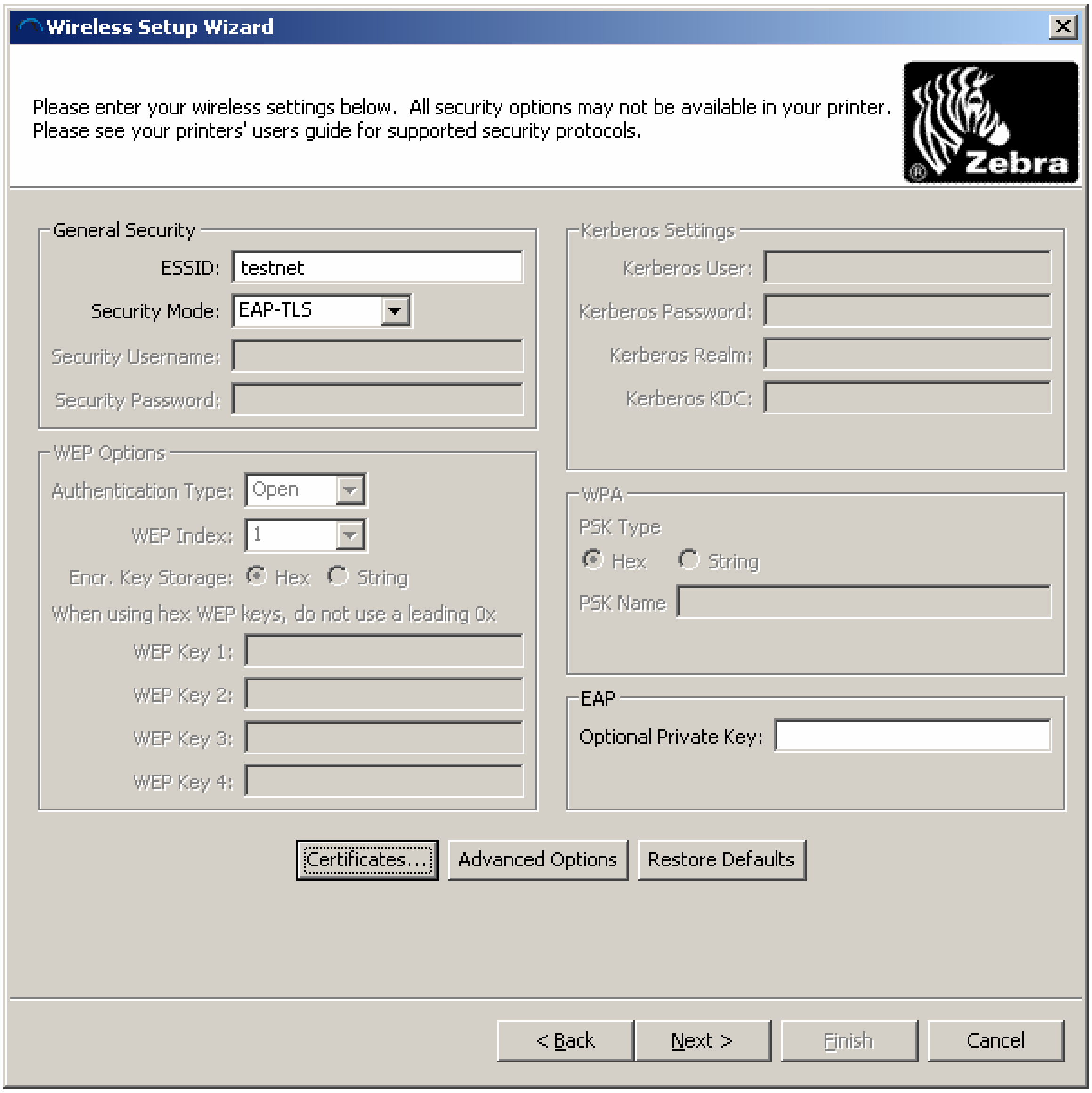
*Note: Certificate files are normally generated by a trusted 3rd-party Certificate Authority (CA). If you are using different certificate files the TLS section of the Eap.conf file will need to be edited to reference the appropriate files. Also, the root certificate file and client certificate files 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-TLS from the drop down list on Security Mode:



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: testnet

Security Mode: EAP-TLS

Security Username:

Security Password:

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

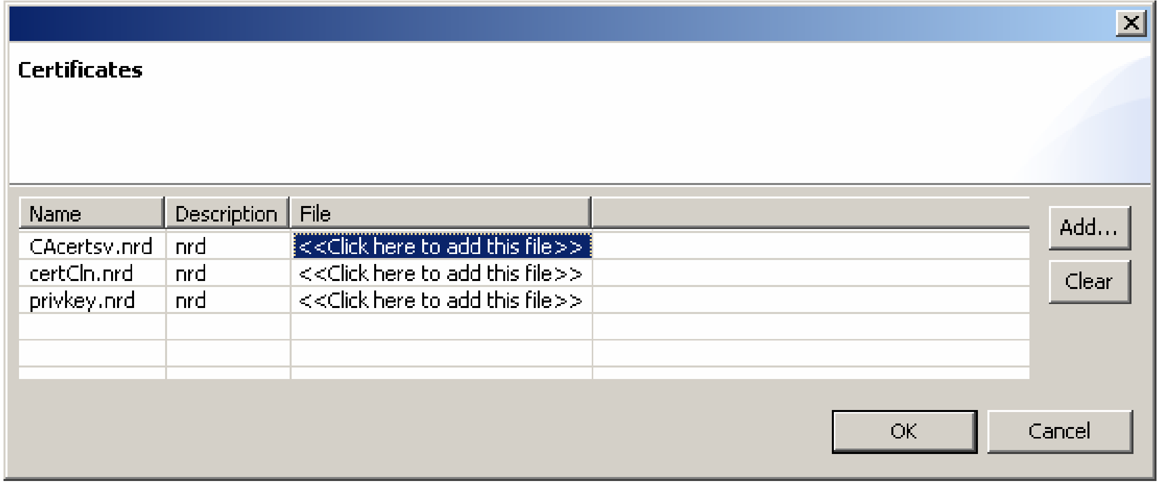
PSK Name

EAP

Optional Private Key:

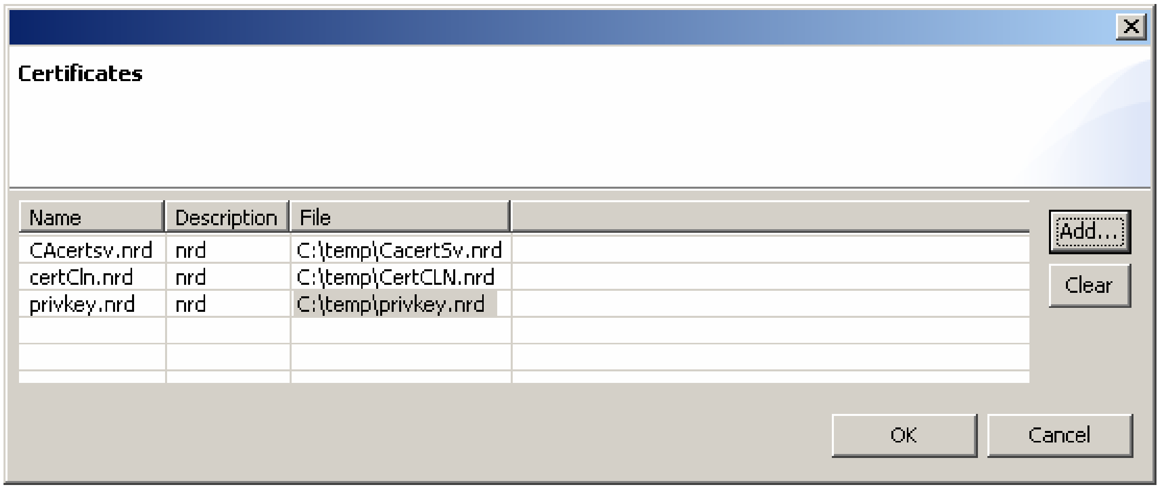
Next click **Certificates**:

Use the Add button to browse to the necessary Certificates:



Certificates

| Name | Description | File |
|---|---|---|
| CAcertsv.nrd | nrd | <<Click here to add this file>> |
| certCln.nrd | nrd | <<Click here to add this file>> |
| privkey.nrd | nrd | <<Click here to add this file>> |



| Name | Description | File |
|---|---|---|
| CAcertsv.nrd | nrd | C:\temp\CacertSv.nrd |
| certCln.nrd | nrd | C:\temp\CertCLN.nrd |
| privkey.nrd | nrd | C:\temp\privkey.nrd |

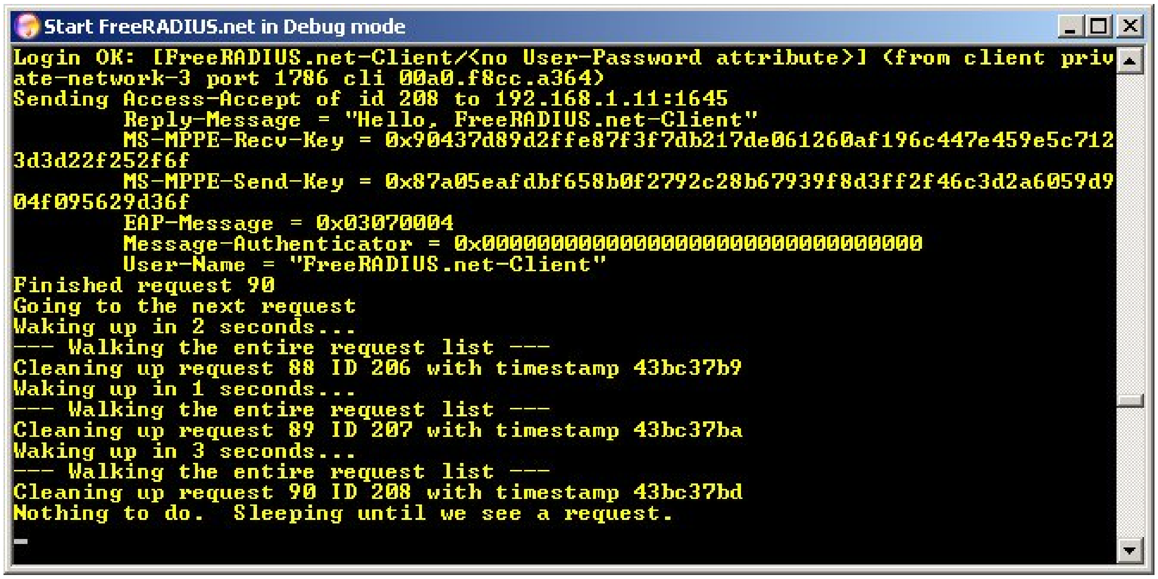
Click OK when finished.

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,,
^WKOFF,,,,
^WX04,


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

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



^FX: C:\temp\CertCLN.nrd will be downloaded as: certCln.nrd

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



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

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

^XZ
^XA
^JUS
^XZ
```

Click Finished to send the ZPL to the printer.

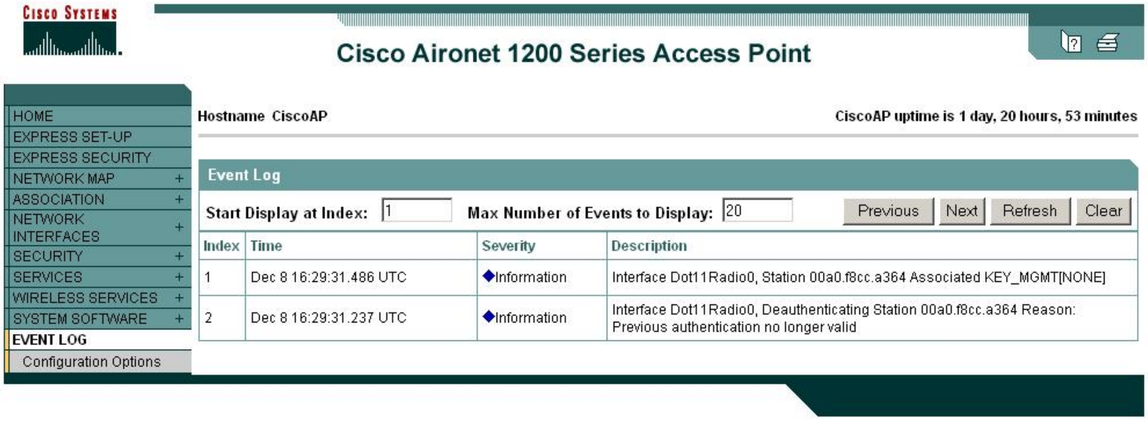
The following is an example of the FreeRadius log after a successful connection.



Start FreeRADIUS.net in Debug mode

```
Login OK: [FreeRADIUS.net-Client/<no User-Password attribute>] (from client priv
ate-network-3 port 1786 cli 00a0.f8cc.a364)
Sending Access-Accept of id 208 to 192.168.1.11:1645
        Reply-Message = "Hello, FreeRADIUS.net-Client"
        MS-MPPE-Recv-Key = 0x90437d89d2ffe87f3f7db217de061260af196c447e459e5c712
3d3d22f252f6f
        MS-MPPE-Send-Key = 0x87a05eafdbf658b0f2792c28b67939f8d3ff2f46c3d2a6059d9
04f095629d36f
        EAP-Message = 0x03070004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "FreeRADIUS.net-Client"
Finished request 90
Going to the next request
Waking up in 2 seconds...
--- Walking the entire request list ---
Cleaning up request 88 ID 206 with timestamp 43bc37b9
Waking up in 1 seconds...
--- Walking the entire request list ---
Cleaning up request 89 ID 207 with timestamp 43bc37ba
Waking up in 3 seconds...
--- Walking the entire request list ---
Cleaning up request 90 ID 208 with timestamp 43bc37bd
Nothing to do.  Sleeping until we see a request.
_
```

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

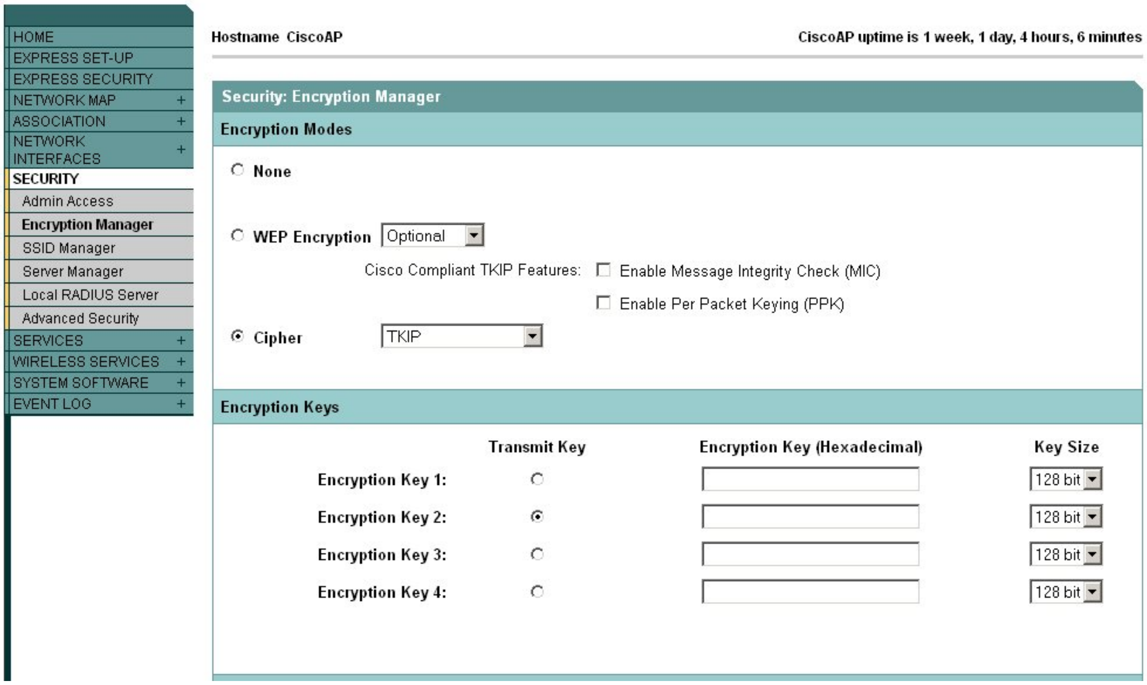
Start Display at Index: 1   Max Number of Events to Display: 20

| 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-TLS. 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-TLS except for the changes shown in the following two screenshots.

**Configure the Cisco 1200 AP for WPA EAP-TLS 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)

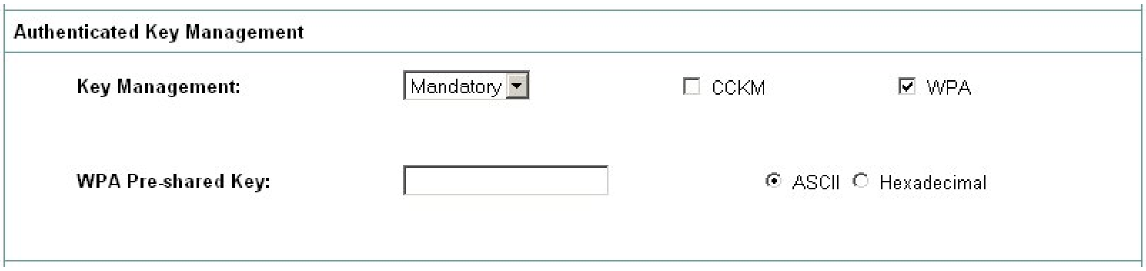
□ Enable Per Packet Keying (PPK)

● 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

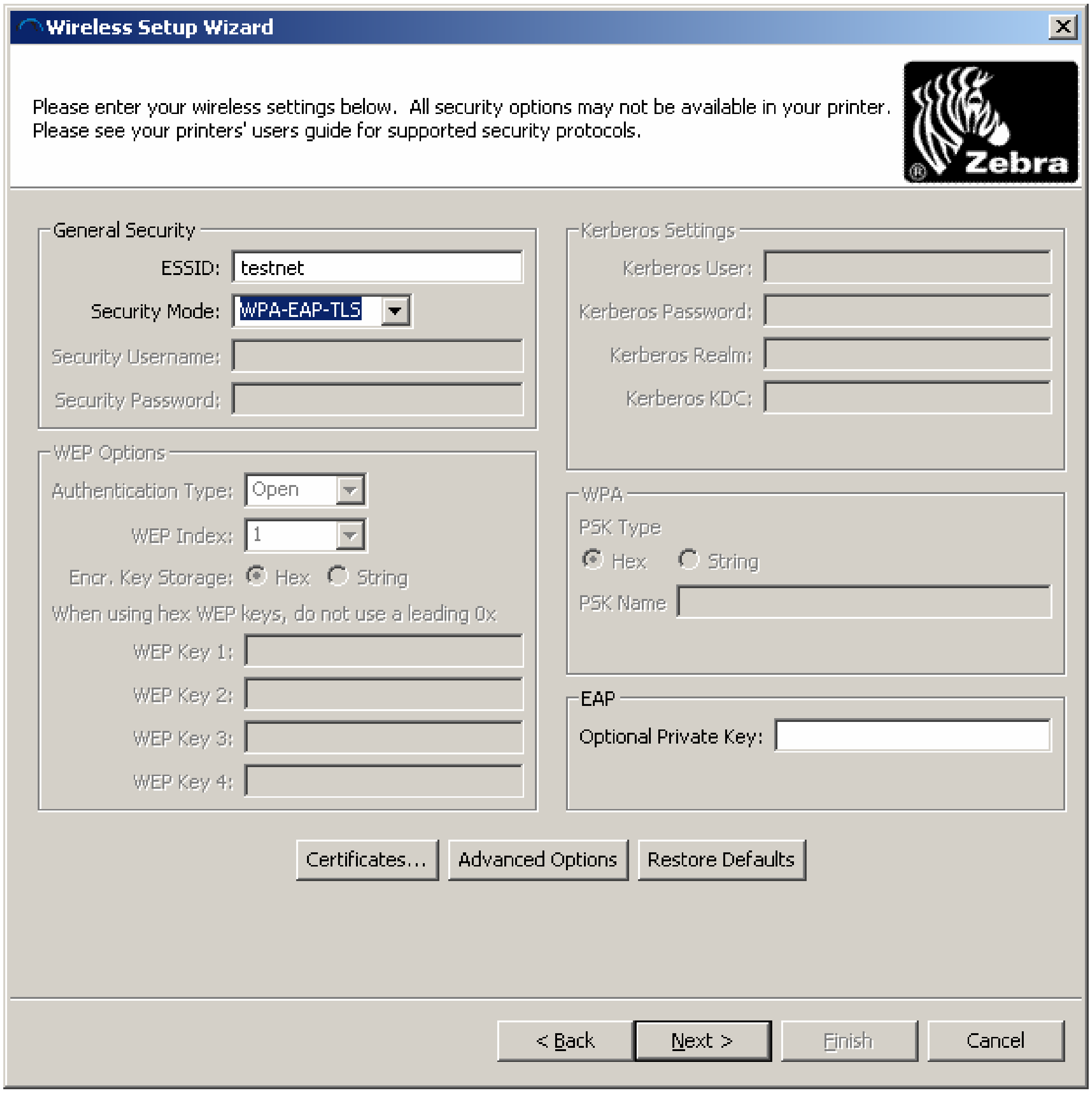
---

## Configure the Zebra printer for WPA EAP-TLS 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-TLS from the drop down list on Security Mode:



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: testnet

Security Mode: WPA-EAP-TLS

Security Username:

Security Password:

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

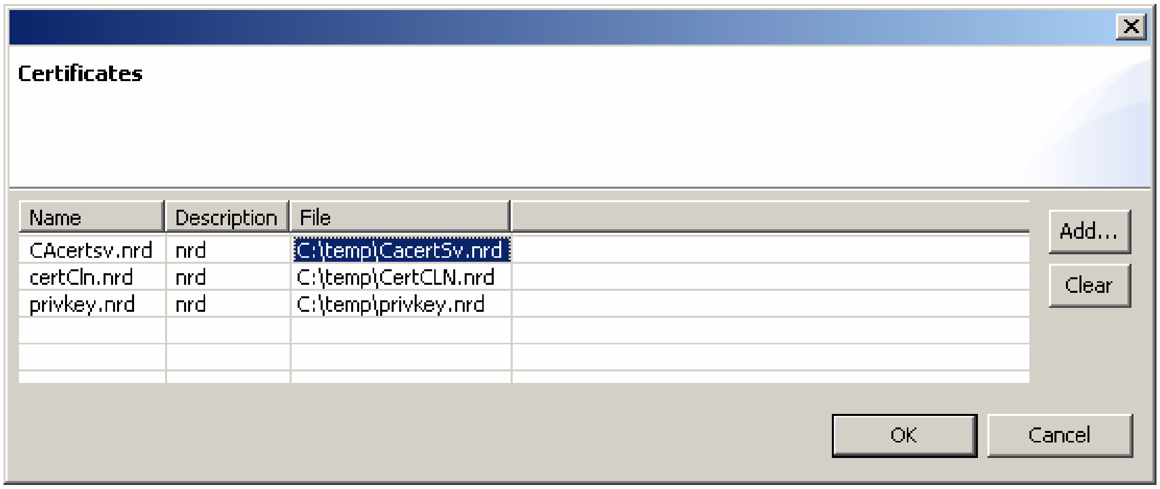
● Hex ○ String

PSK Name

EAP

Optional Private Key:

Add the Certificates:



**Certificates**

| Name | Description | File |
|---|---|---|
| CAcertsv.nrd | nrd | C:\temp\CacertSv.nrd |
| certCln.nrd | nrd | C:\temp\CertCLN.nrd |
| privkey.nrd | nrd | C:\temp\privkey.nrd |

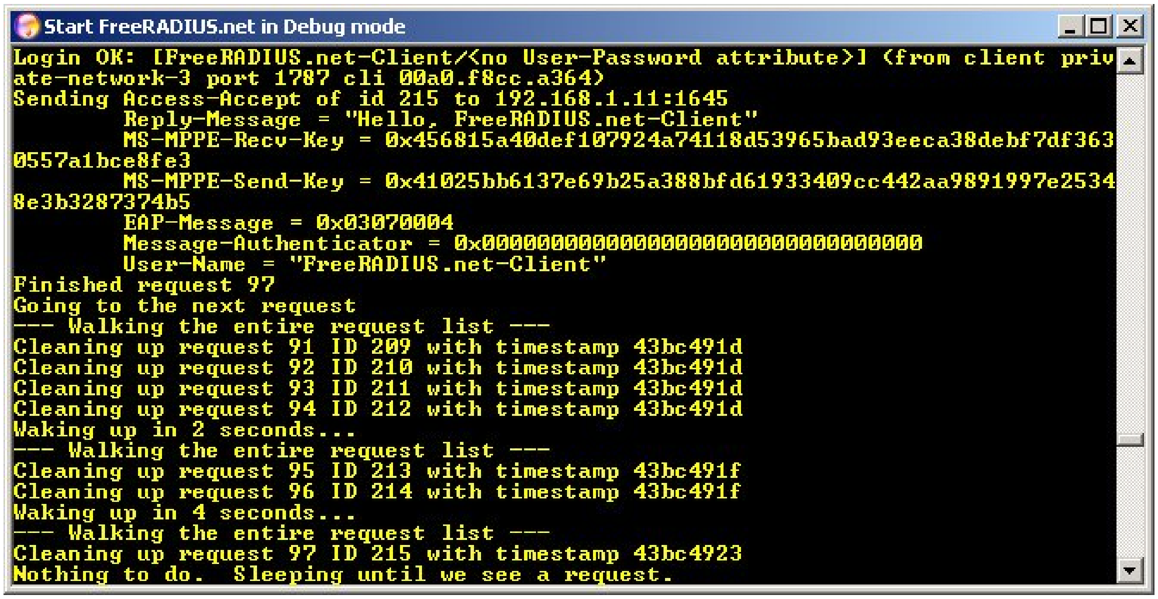
Click Next to view the ZPL:

```
^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,,
^WKOFF,,,,
^WX10,


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

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



^FX: C:\temp\CertCLN.nrd will be downloaded as: certCln.nrd

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



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

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

^XZ
^XA
^JUS
^XZ
```

Click Finished to send the ZPL to the printer.

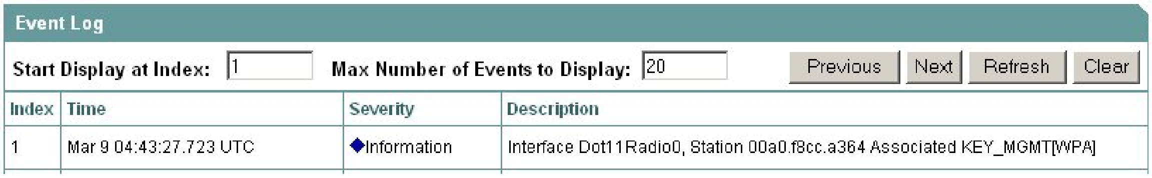
.

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



```
Login OK: [FreeRADIUS.net-Client/<no User-Password attribute>] (from client priv
ate-network-3 port 1787 cli 00a0.f8cc.a364)
Sending Access-Accept of id 215 to 192.168.1.11:1645
        Reply-Message = "Hello, FreeRADIUS.net-Client"
        MS-MPPE-Recv-Key = 0x456815a40def107924a74118d53965bad93eeca38debf7df363
0557a1bce8fe3
        MS-MPPE-Send-Key = 0x41025bb6137e69b25a388bfd61933409cc442aa9891997e2534
8e3b3287374b5
        EAP-Message = 0x03070004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "FreeRADIUS.net-Client"
Finished request 97
Going to the next request
--- Walking the entire request list ---
Cleaning up request 91 ID 209 with timestamp 43bc491d
Cleaning up request 92 ID 210 with timestamp 43bc491d
Cleaning up request 93 ID 211 with timestamp 43bc491d
Cleaning up request 94 ID 212 with timestamp 43bc491d
Waking up in 2 seconds...
--- Walking the entire request list ---
Cleaning up request 95 ID 213 with timestamp 43bc491f
Cleaning up request 96 ID 214 with timestamp 43bc491f
Waking up in 4 seconds...
--- Walking the entire request list ---
Cleaning up request 97 ID 215 with timestamp 43bc4923
Nothing to do.  Sleeping until we see a request.
```

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



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] |