

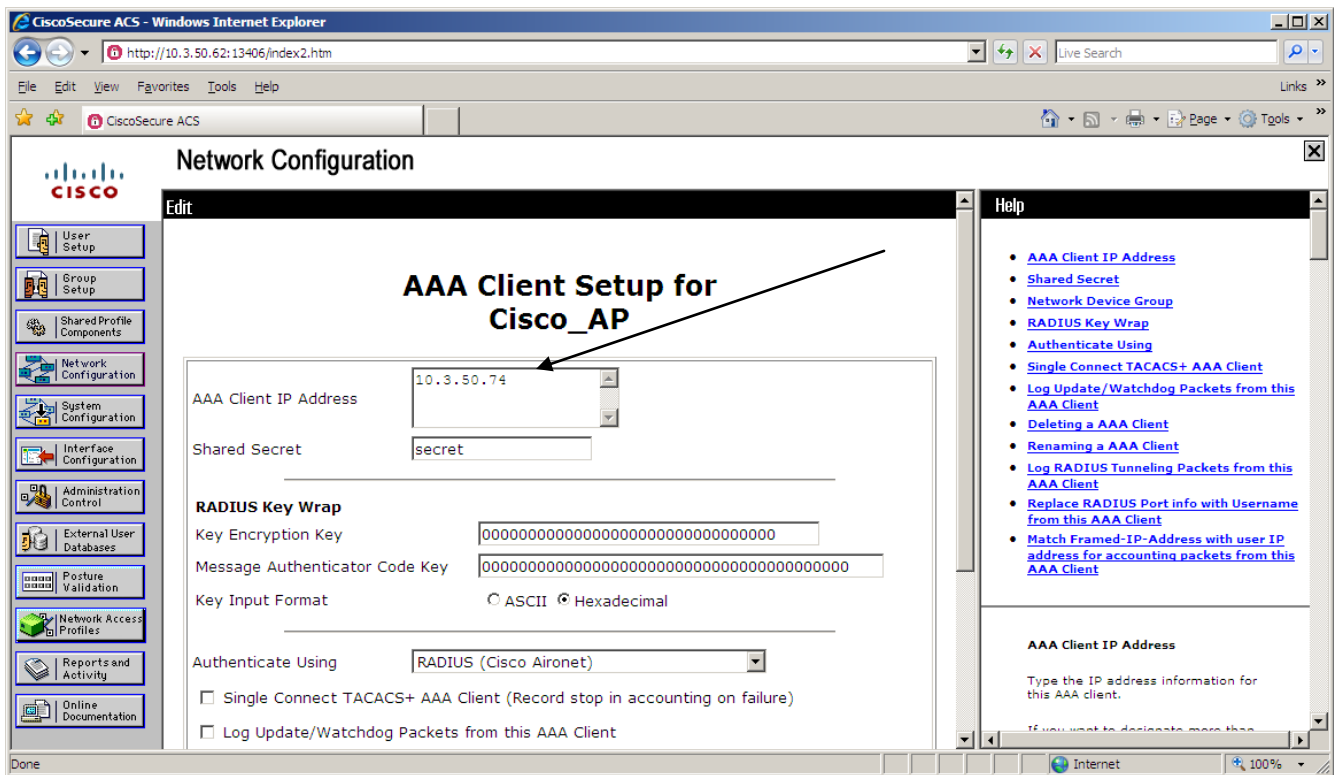
Zebra Setup Utility, Zebra Mobile Printer, Cisco ACS, Cisco Access Point, LEAP and WPA-LEAP

This section of the document illustrates the Cisco ACS radius server and how LEAP and WPA-LEAP was configured on this server.

This document is meant as an illustration only. Questions on the setup of ACS should be directed to Cisco. It should be Cisco that is used to determine if the illustration below is appropriate for your environment.

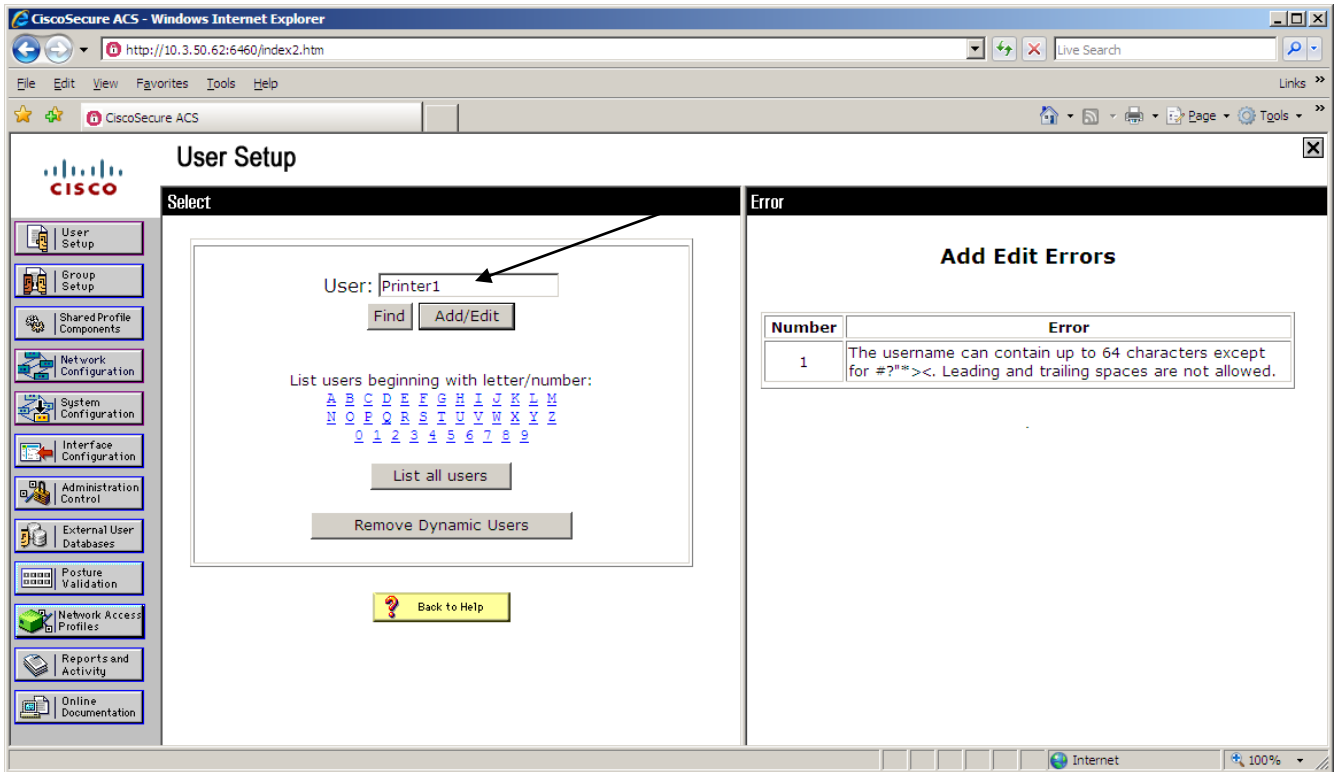
It is important to note that the setup on the ACS server did not differ when using WPA-LEAP or LEAP.

The first series of screenshots shows how a Radius client is added to ACS. In the screenshot below a Cisco Access Point with the IP address of 10.3.50.74 is added. The ACS server needs to have a client in the clients table to ensure that authentication requests are only being received from valid clients.

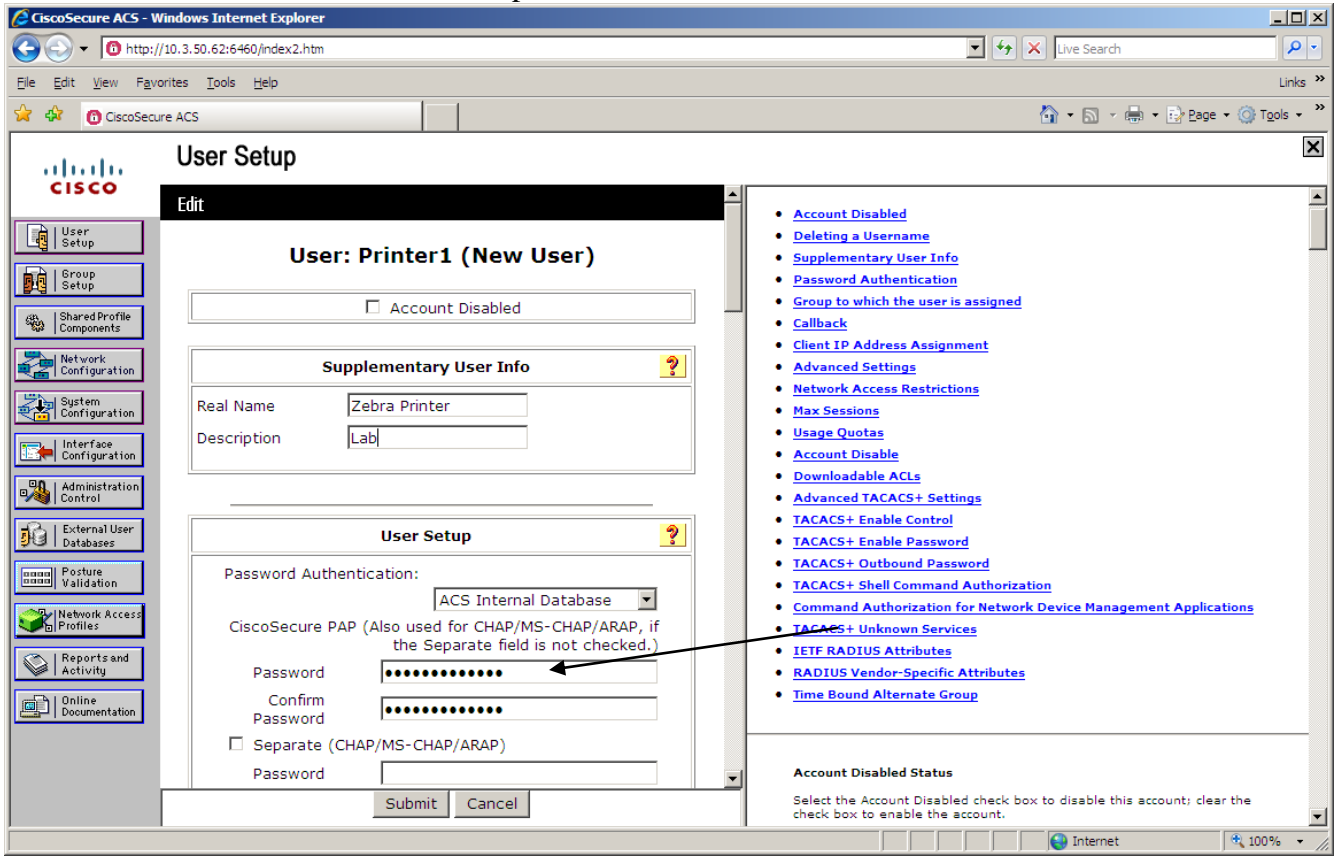


A secret key is entered on the ACS server. This secret key needs to match the secret key on the radius client (in this example the Cisco Access Point).

A username is entered for the printer and a password for the printer is also added. In this example the username is Printer1.



The screenshot below shows where the password is added.



In the system configuration on the ACS server, I have illustrated in the screenshot below that LEAP is enabled.

The screenshot shows the CiscoSecure ACS System Configuration interface. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and includes sections for EAP-FAST, EAP-TLS, LEAP, and EAP-MD5. A red arrow points from the "Reports and Activity" option in the sidebar to the "Reports and Activity" section in the main content area.

EAP-FAST
[EAP-FAST Configuration](#)

EAP-TLS
 Allow EAP-TLS
 Select one or more of the following options:
 Certificate SAN comparison
 Certificate CN comparison
 Certificate Binary comparison
 EAP-TLS session timeout (minutes):

Select one of the following options for setting username during authentication:
 Use Outer Identity
 Use CN as Identity
 Use SAN as Identity

LEAP
 Allow LEAP (For Aironet only)

EAP-MD5
 Allow EAP-MD5

AP EAP request timeout (seconds):

EAP Configuration

EAP is a flexible request-response protocol for exchanging information (RFC 2284). EAP is layered on top of UDP, 802.1x or RADIUS and supports multiple authentication methods.

[\[Back to Top\]](#)

PEAP

PEAP is the outer layer protocol for the secure transport of EAP messages.

Note: PEAP is a certificate-based authentication and can occur only after you have completed the required Certificate Setup page.

- **Allow EAP-MSCHAPv2** — Use to enable EAP-MSCHAPv2 authentication. Enable this protocol for any network devices such as Microsoft AD, and the ACS Internal Database.
- **Allow EAP-GTC** — Use to enable EAP-GTC with RADIUS. Enable this protocol for any network devices such as Microsoft AD, and the ACS Internal Database.

The screenshots below show how a successful authentication for LEAP or WPA-LEAP appears on the ACS server.

The screenshot shows the CiscoSecure ACS Reports and Activity page. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "Reports and Activity" and includes a "Reports" section with a list of reports: TACACS+ Accounting, TACACS+ Administration, RADIUS Accounting, VoIP Accounting, Passed Authentications, Failed Attempts, Logged-in Users, Disabled Accounts, ACS Backup And Restores, Administration Audit, User Password Changes, ACS Service Monitoring, and Entitlement Reports. The "Passed Authentications active.csv" report is selected, and a table of authentication events is displayed. A red arrow points from the "Reports and Activity" option in the sidebar to the "Reports and Activity" section in the main content area.

Passed Authentications active.csv Refresh Download

Regular Expression Start Date & Time End Date & Time Rows per Page

Apply Filter Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name	PEAP/EAP-FAST-Clear-Name	Access Device	Network Device Group
03/22/2011	07:59:32	Authen OK	Printer1	Default Group	0019.7013.9f6a	340	10.3.50.74	(Default)	17	LEAP	..	Cisco_AP	..

This section of the document illustrates a Cisco Access Point

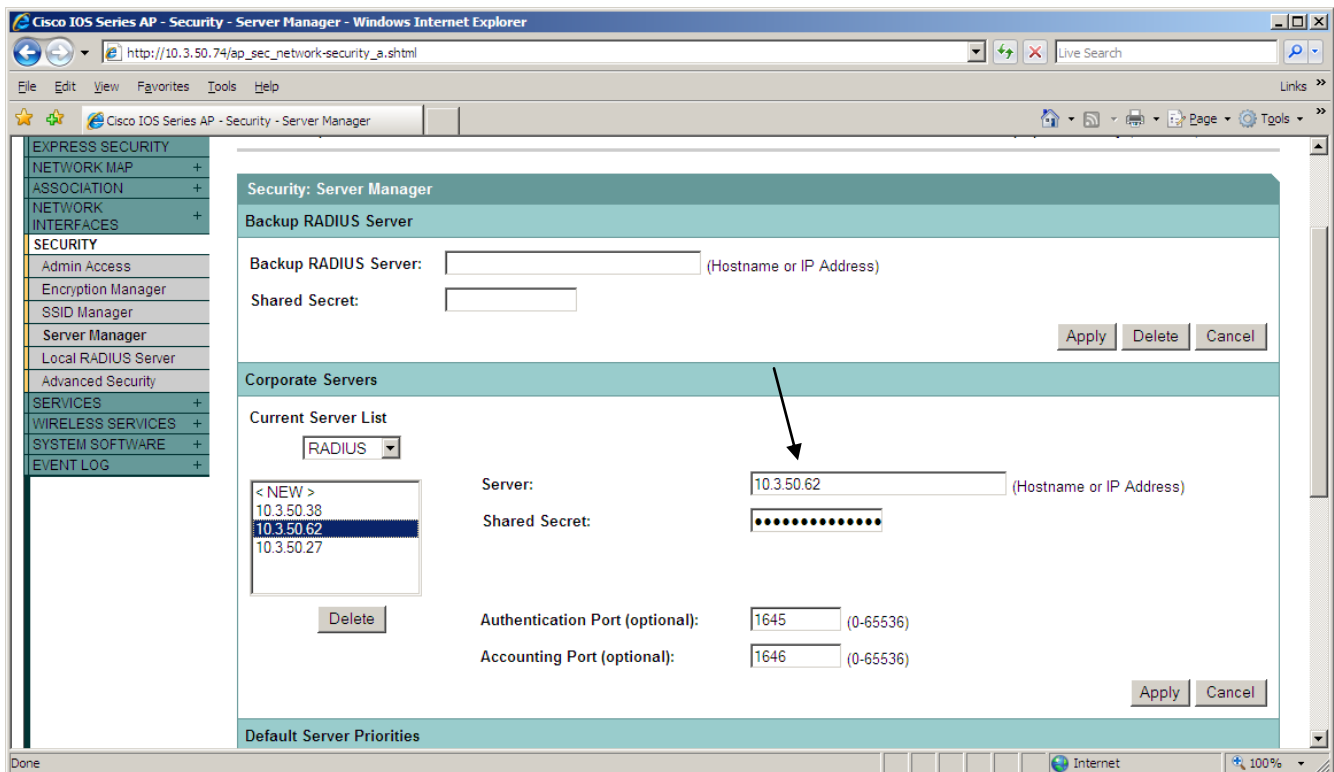
This document is meant as an illustration only. Questions on the setup of your Cisco Access Point should be directed to Cisco. It should be Cisco that is used to determine if the illustration below is

appropriate for your environment

This illustration shows how the Cisco Access Point was configured for LEAP initially and then WPA-LEAP.

With LEAP or WPA-LEAP the authentication request is forwarded to a Radius server. The following screenshots illustrate how a radius server can be added.

The example below shows an entry of a radius server with an IP address of 10.3.50.62 and utilizing the port number of 1645. 1645 and 1812 are common port numbers used with the RADIUS protocol. A secret key is also entered. This secret key needs to match the secret key that is entered on the RADIUS server.



The first step illustrated here is how an ESSID is created. It also illustrates some of the configuration on the access point for LEAP.

In this example the ESSID is "Zebra_LEAP" Please note that ESSID's are case sensitive.

Security: Global SSID manager

SSID Properties

Current SSID List

- < NEW >
- Zebra_FAST
- Zebra_LEAP**

SSID: Zebra_LEAP

VLAN: < NONE > [Define VLANs](#)

Backup 1:

Backup 2:

Backup 3:

Interface: Radio0-802.11G

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

- Open Authentication: < NO ADDITION >
- Shared Authentication: < NO ADDITION >
- Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

- Use Defaults [Define Defaults](#)
- Customize

Priority 1: 10.3.50.62

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

- Use Defaults [Define Defaults](#)
- Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Address of ACS server

The screenshot below shows additional screenshots that were used to configure **LEAP**

Cisco IOS Series AP - Security - Encryption Manager - Windows Internet Explorer

http://10.3.50.74/ap_sec_ap-key-security.shtml

File Edit View Favorites Tools Help

Cisco IOS Series AP - Security - Encryption Manager

CISCO

Cisco Aironet 1200 Series Access Point

ap uptime is 2 weeks, 3 days, 17 hours, 31 minutes

Hostname ap

Security: Encryption Manager

Encryption Modes

None
 WEP Encryption **Mandatory**
 Cipher **AES CCMP + TKIP**

Cisco Compliant TKIP Features:
 Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Global Properties

Broadcast Key Rotation Interval:

Disable Rotation
 Enable Rotation with Interval: **DISABLED** (10-10000000 sec)

Done

Internet 100%

The screenshots below show views on the Access Point of a successful LEAP connection.

Cisco IOS Series AP - Association - Windows Internet Explorer

http://10.3.50.74/ap_assoc.shtml

File Edit View Favorites Tools Help

Cisco IOS Series AP - Association

Cisco Aironet 1200 Series Access Point

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
Activity Timeout
NETWORK INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG

Hostname ap ap uptime is 2 weeks, 3 days, 17 hours, 44 minutes

Association

Clients: 1 Repeater: 0

View: Client Repeater Apply

Radio0-802.11G

SSID Zebra_LEAP :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	NONE	10.3.50.113	0019.7013.9f6a	EAP-Associated	self	none

Refresh

Close Window Copyright (c) 1992-2008 by Cisco Systems, Inc.

Done Internet 100%

Cisco Aironet 1200 Series Access Point

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION
Activity Timeout
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

STATISTICS PING/LINK TEST

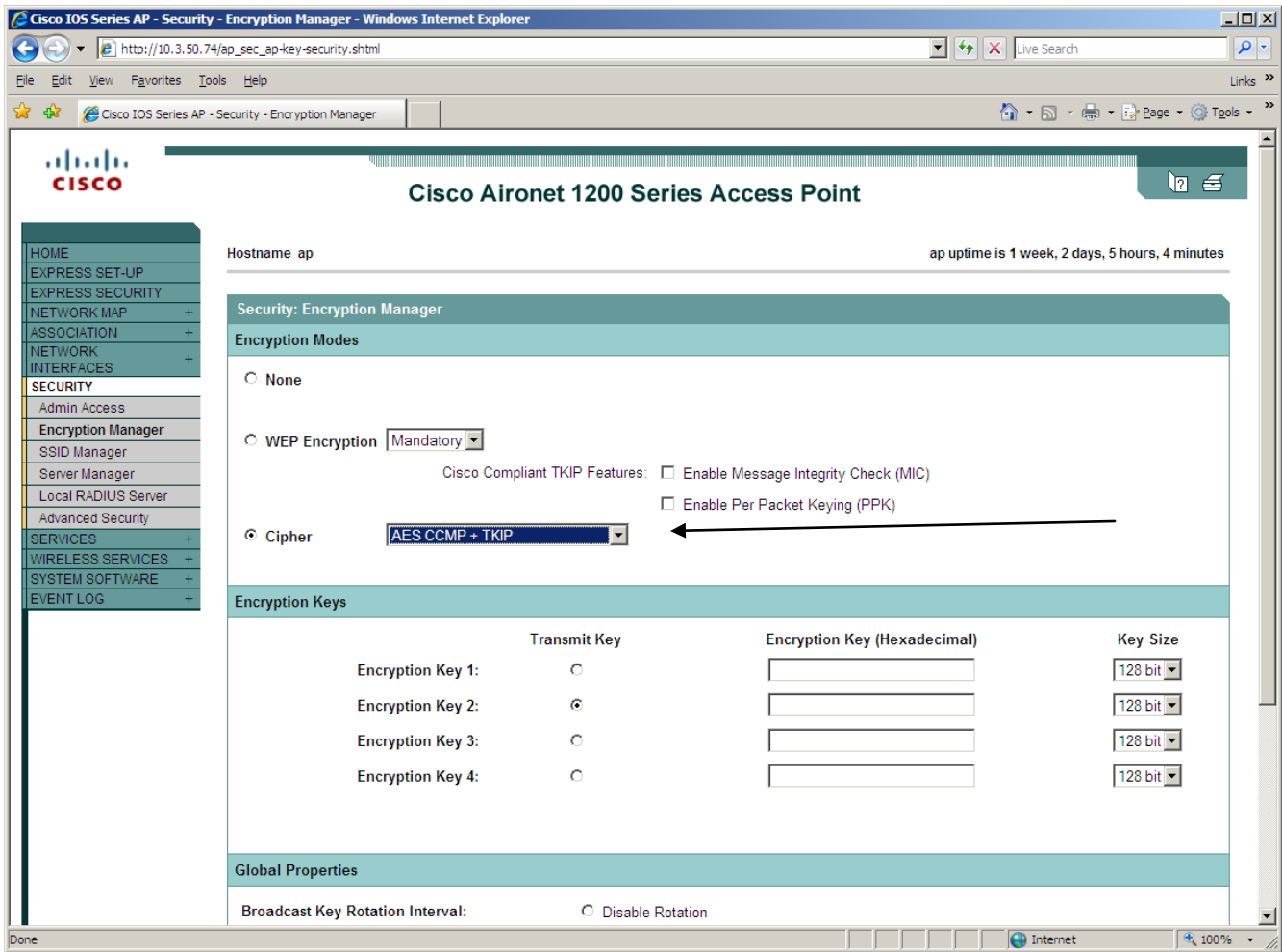
Hostname ap ap uptime is 2 weeks, 3 days, 17 hours, 42 minutes

Association: Station View-Client

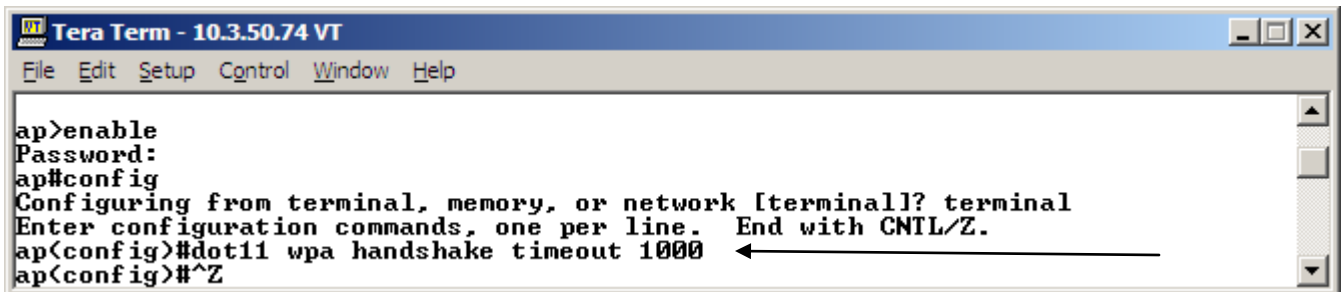
Station Information and Status

MAC Address	0019.7013.9f6a	Name	NONE
IP Address	10.3.50.113	Class	unknown
Device	unknown	Software Version	NONE
CCX Version	NONE		
State	EAP-Associated	Parent	self
SSID		VLAN	
Hops To Infrastructure	1	Communication Over Interface	Radio0-802.11G
Clients Associated	0	Repeaters Associated	0
Key Mgmt type	NONE	Encryption	WEP
Current Rate (Mb/sec)	54.0	Capability	ShortHdr ShortSlot
Supported Rates(Mb/sec)	1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0		
Voice Rates(Mb/sec)	disabled	Association Id	85
Signal Strength (dBm)	-70	Connected For (sec)	8
Signal to Noise (dBm)	22	Activity TimeOut (sec)	56
Power-save	Off	Last Activity (sec)	4
Apsd DE AC(s)	NONE	Posture Token	
Session TimeOut (sec)	0	Reauthenticate In (sec)	Never
Receive/Transmit Statistics			
Total Packets Input	9	Total Packets Output	16

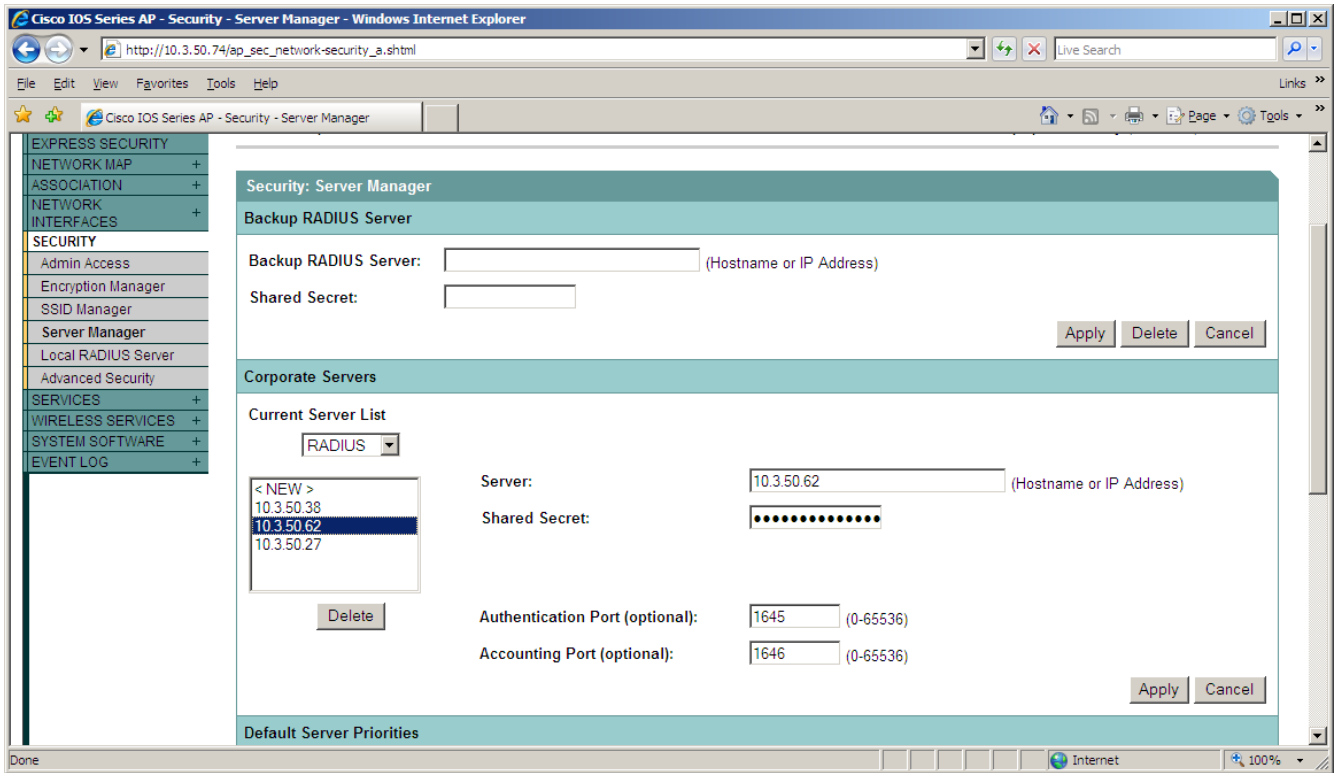
The next screenshots show how the Cisco Access Point was set for **WPA-LEAP**. In this example that I have enabled both wpa and wpa2 as shown below.



In this illustration, I have set the wpa handshake timeout to a value of 1000



With WPA-LEAP, the authentication is often done by an external radius server. In this example I have entered the ip address for the radius server as shown below.



In this illustration, I have chosen both TKIP and AES CCMP

Cisco IOS Series AP - Security - Encryption Manager - Windows Internet Explorer

http://10.3.50.74/ap_sec_ap-key-security.shtml

File Edit View Favorites Tools Help

Cisco IOS Series AP - Security - Encryption Manager

CISCO

Cisco Aironet 1200 Series Access Point

ap uptime is 1 hour, 35 minutes

Hostname ap

Security: Encryption Manager

Encryption Modes

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

Encryption Keys

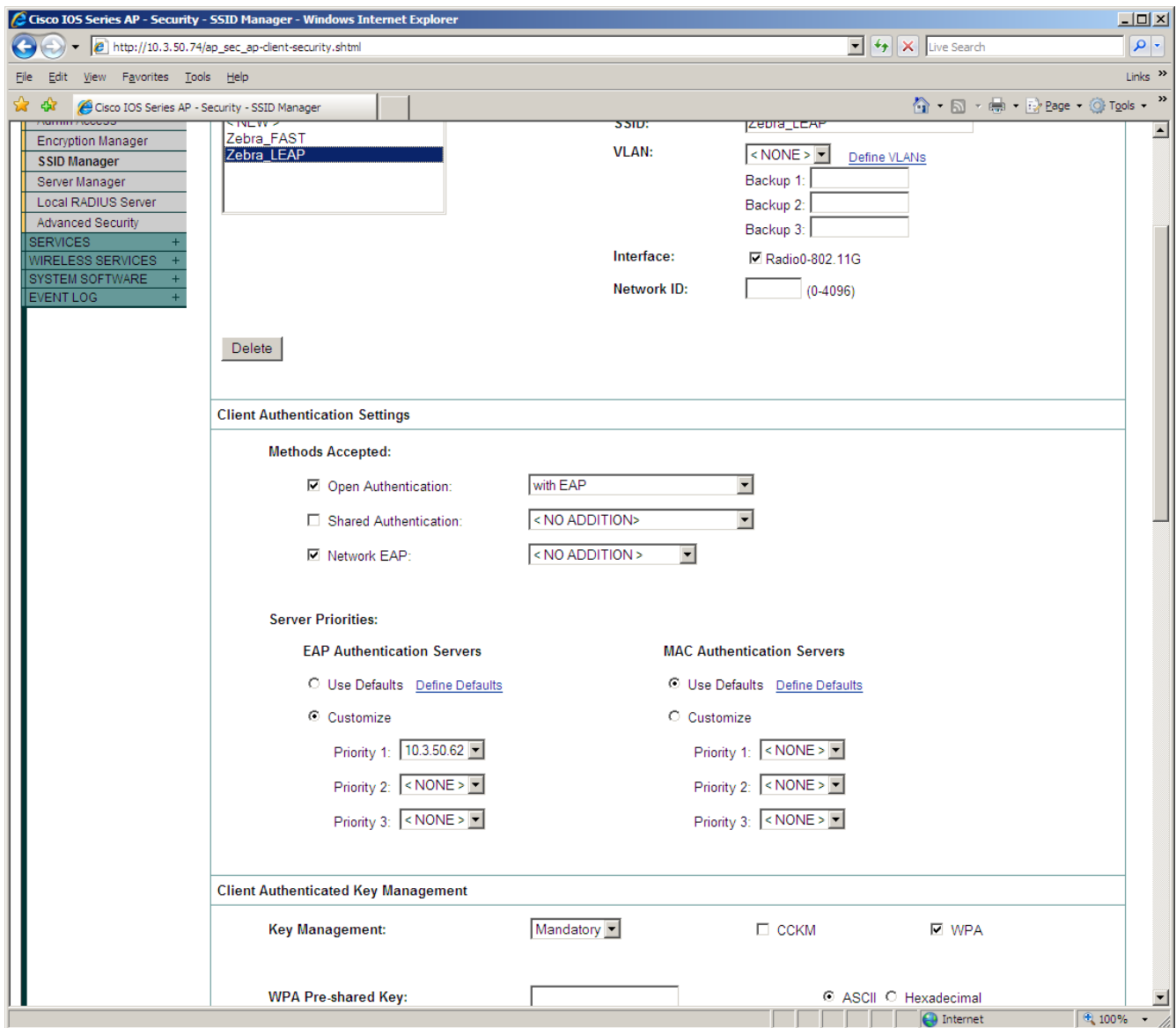
	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>

Global Properties

Broadcast Key Rotation Interval: Disable Rotation
 Enable Rotation with Interval: (10-10000000 sec)

Done

Internet 100%



Below is an example of what the Cisco Access point shows for a successful WPA-LEAP authentication.



Cisco Aironet 1200 Series Access Point



STATISTICS PING/LINK TEST

Hostname ap ap uptime is 7 minutes

Association: Station View- Client






Station Information and Status			
MAC Address	0019.7013.9f6a	Name	NONE
IP Address	10.3.50.93	Class	unknown
Device	unknown	Software Version	NONE
CCX Version	NONE	Parent	self
State	EAP-Associated	VLAN	
SSID		Communication Over Interface	Radio0-802.11G
Hops To Infrastructure	1	Repeaters Associated	0
Clients Associated	0	Encryption	AES-CCMP
Key Mgmt type	WPAv2	Capability	ShortHdr ShortSlot
Current Rate (Mb/sec)	54.0	Supported Rates(Mb/sec)	1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0
Voice Rates(Mb/sec)	disabled	Association Id	20
Signal Strength (dBm)	-66	Connected For (sec)	6
Signal to Noise (dBm)	26	Activity TimeOut (sec)	60
Power-save	Off	Last Activity (sec)	0
Apsd DE AC(s)	NONE	Posture Token	
Session TimeOut (sec)	0	Reauthenticate In (sec)	Never

This section of the document illustrates how to configure the printer for LEAP and will continue by illustrating how to configure the printer for WPA-LEAP. The illustration will use the **Zebra Setup Utility** as the method for configuring the printer.

Zebra Setup Utilities







Printers

The list below displays installed printers. To configure a printer, select it and choose one of the configuration options below.

 ZDesigner QL 420/QL 420 Plus (Copy 1) USB005	 ZDesigner QL 420/QL 420 Plus (Copy 2) USB006
 ZDesigner QLn320 USB001	 ZDesigner RW 220 USB003
 ZDesigner RW 420 USB002	





Printer Configuration

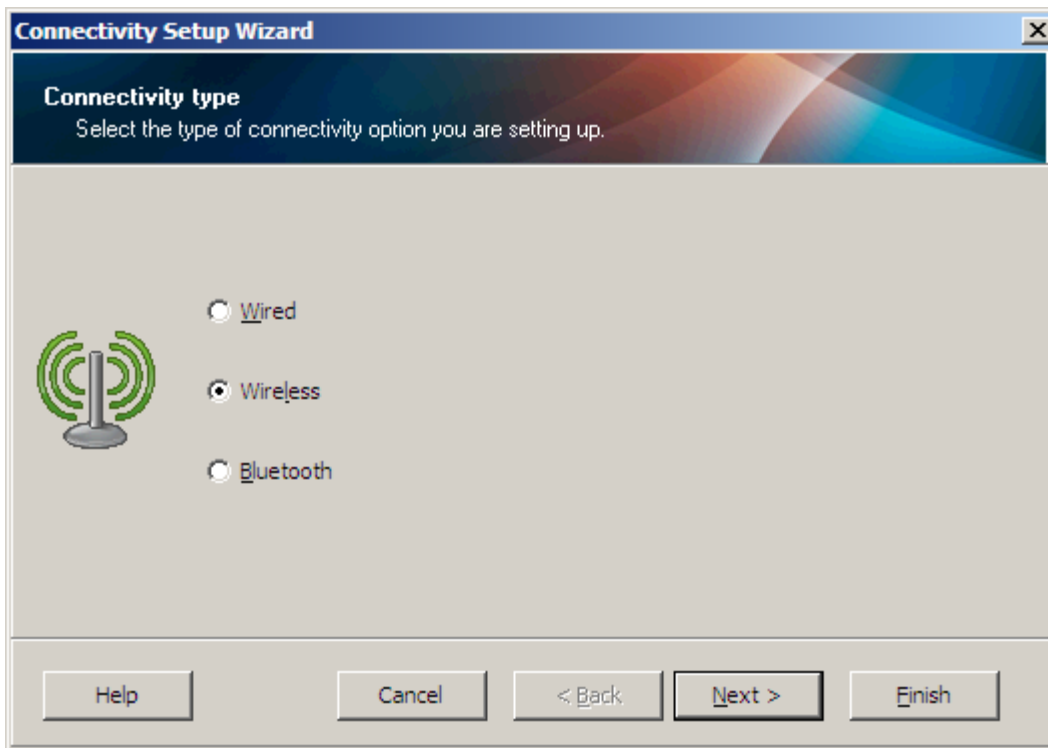
Configure the selected printer

 Configure Printer Settings	 Download Fonts and Graphics
 Configure Print Quality	 Open Printer Tools
 Configure Printer Connectivity	 Open Communication With Printer

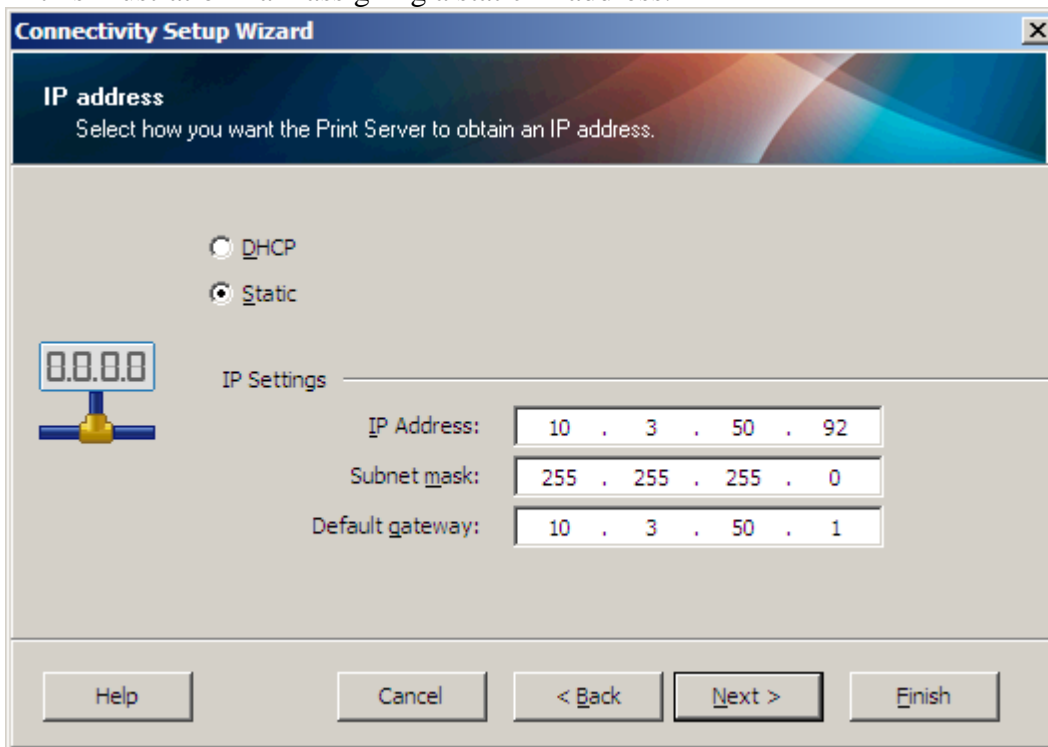
General Operations

Perform the following application operations

 Help	 About	 Options	 Close
--	---	---	---



In this illustration I am assigning a static IP address.



The screenshot below shows the security mode LEAP.

Connectivity Setup Wizard

Wireless settings.
Define wireless settings.

Please enter your wireless settings below. Settings for selected security mode will be configured on the following page.

LEAP

ESSID: Zebra_LEAP

Security mode: LEAP

Security username: Printer1

Security password: passworD12345

All security options may not be available in your printer. Please refer to the Wireless Print Server and Wireless Plus Print Server User Guide for supported security protocols.

Help Cancel < Back Next > Finish

The screenshot below shows the security mode WPA-LEAP

Connectivity Setup Wizard

Wireless settings.
Define wireless settings.

Please enter your wireless settings below. Settings for selected security mode will be configured on the following page.

WPA-LEAP

ESSID: Zebra_LEAP

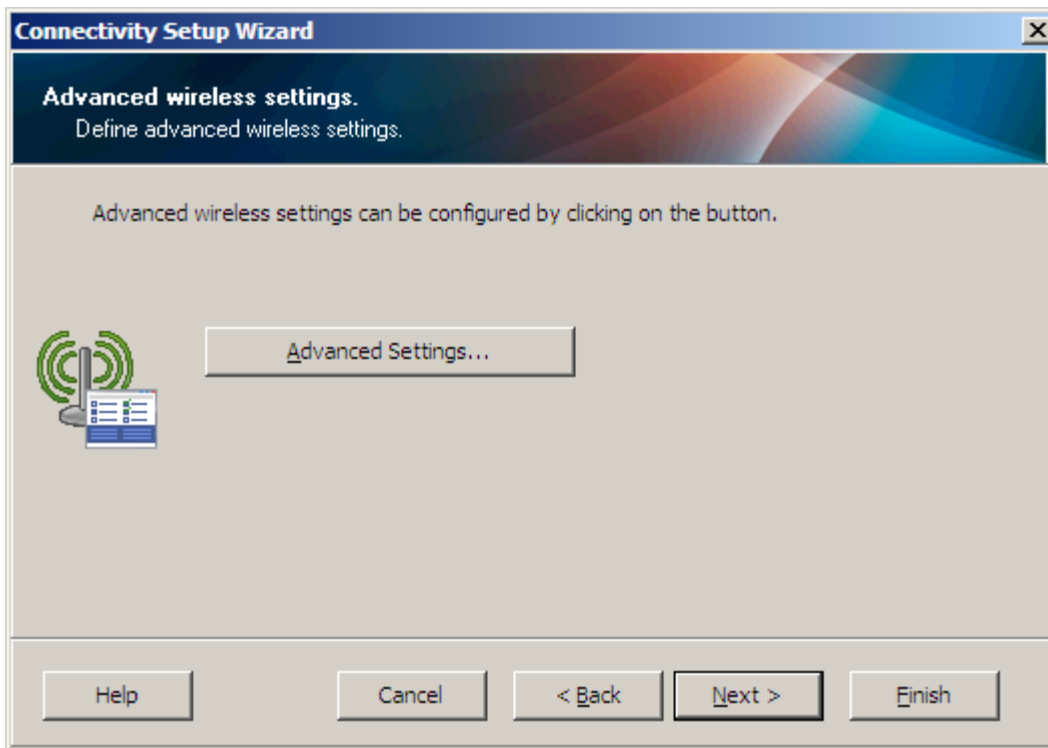
Security mode: WPA-LEAP/WPA2-LEAP

Security username: Printer1

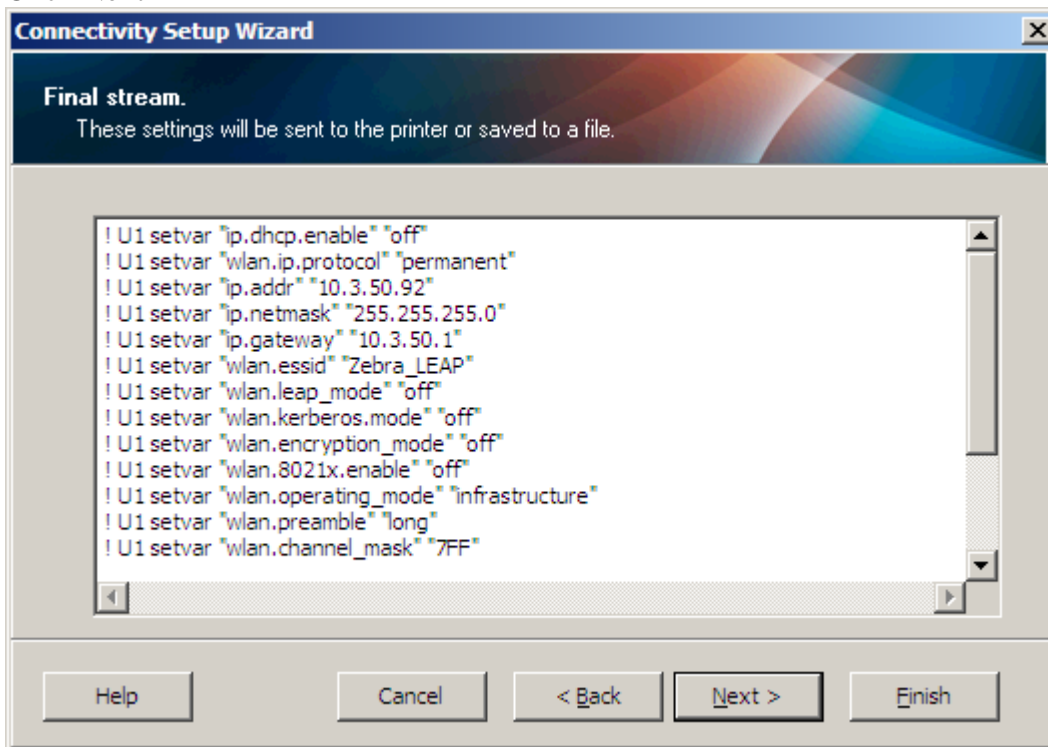
Security password: passworD12345

All security options may not be available in your printer. Please refer to the Wireless Print Server and Wireless Plus Print Server User Guide for supported security protocols.

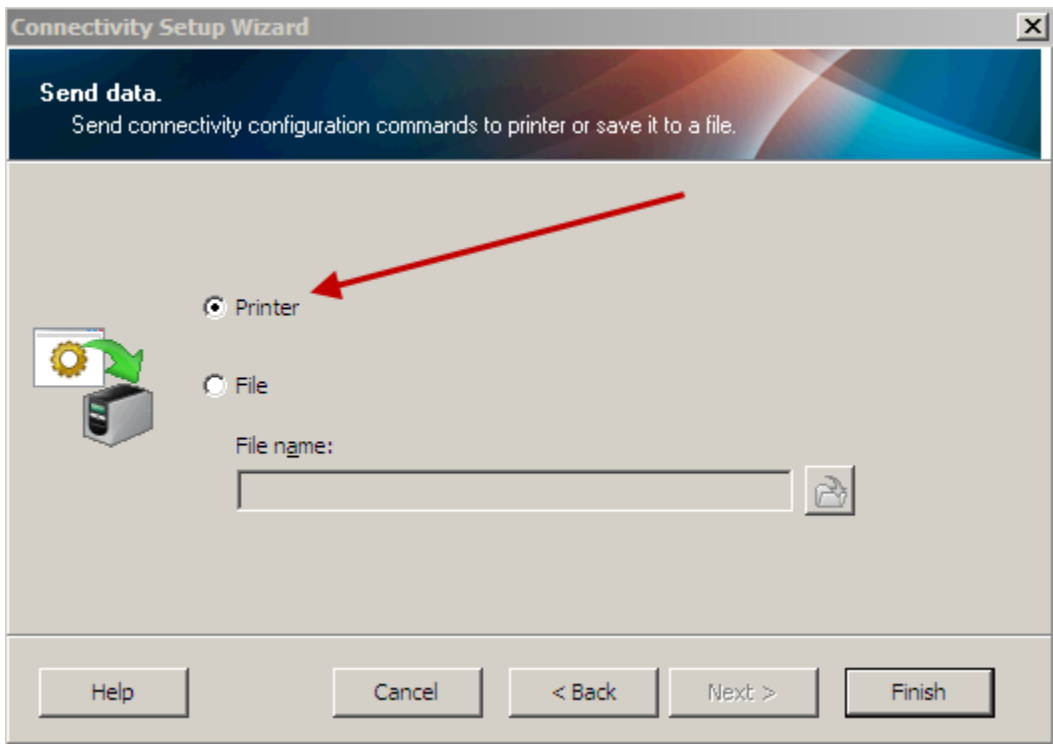
Help Cancel < Back Next > Finish



Click Next



Click Next



The data will now be sent to the printer and the printer will reboot.