EZCAST.COM

WIFI ENTERPRISE INTRODUCTION AND SETUP

By EZCast

Table of Contents

ABSTRACT

Technology is changing our life! With the advancement of IoT technologies in recent years, many devices now demand network connectivity for control and communication. As a result, smartphones have become more popular, and the prices have become cheaper. Nowadays, everyone owns at least one device; even some children own a smartphone. Can you imagine that just a few decades ago, you could only use a public telephone or home phone to have a call with friends?

Traditionally, laptops and computers can connect to the internet via wired or wireless connections. A wired connection uses the Ethernet cable plugged into an ADSL router to access the internet, while wireless connections use a wireless router. Moreover, mobile devices and smart-home devices usually use wireless or 4G/5G network connections. Therefore, the wired connection has become inconvenient to use.

Although the internet makes our lives more convenient, it is also imperative to keep our data secure. We upload a large quantity of information on the internet, including personal and financial data. Protecting our information on the internet has become a crucial issue. In this article, we will cover security during wireless connections and the steps to connect to Wi-Fi enterprise.

WHAT IS WIRELESS NETWORK SECURITY?

Wireless network security is primarily concerned with preventing unwanted and harmful access to a wireless network. It is typically provided by wireless devices (usually a wireless router/switch) that by default encrypt and secure all wireless traffic. Even if the security of the wireless network is breached, the hacker will not be able to see the content of the traffic/packets in transit. Furthermore, wireless intrusion detection and prevention systems defend a wireless network by notifying the administrator in the event of a security breach. Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA) are two common algorithms and standards for ensuring wireless network security (WPA) (TechoPedia, 2022).

HOW DO UNSECURED WI-FI NETWORKS RISKS EMERGE?

When wireless devices in a network are in an "open" state or unsecured, they're accessible to any device within the Wi-Fi range, such as a computer or smartphone. Users and organizations may face risks if they use unsecured or open networks. Cybercriminals can capture personal information and steal identities from internet-connected devices, increase the risk of data leakage of financial and other business information, listen in on conversations, and more.

HOW TO MINIMIZE THE RISKS TO YOUR WIRELESS NETWORK?

There are several methods to diminish the risks of getting your wireless network compromised. In this article, we will go in-depth on the concept of Encryption for it is one of the safest methods. By encrypting your wireless data, you prevent anyone who may be able to access your network from viewing it. Multiple encryption protocols are available to protect your data. WPA, WPA2, and WPA3 encrypt information sent between wireless routers and wireless devices. WPA3 is currently the strongest encryption. Although WPA and WPA2 are still available, it is preferable to use equipment that specifically supports WPA3, since the other protocols may expose your network to exploitation (CISA, 2010)

However other methods include:

- Changing Default Passwords
- Access Restriction
- Protection of your Service Set Identifier (SSID)
- Firewall Installation
- Antivirus software maintenance
- Connection using a Virtual Private Network (VPN)

ENCRYPTION

Wi-Fi networks and devices can be protected using security protocols with encryption. In digital communications, encryption encodes data and only allows authorized recipients to decode it. Encrypting information transferred over your network scrambles it. Other people will be unable to observe what you're doing or obtain your personal information (Consumer FTC, 2021).

Several encryption standards are in use today, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). Whereas, newer access points and Wi-Fi routers provide wireless security through built-in wireless encryption protocols (CISCO, 2022).

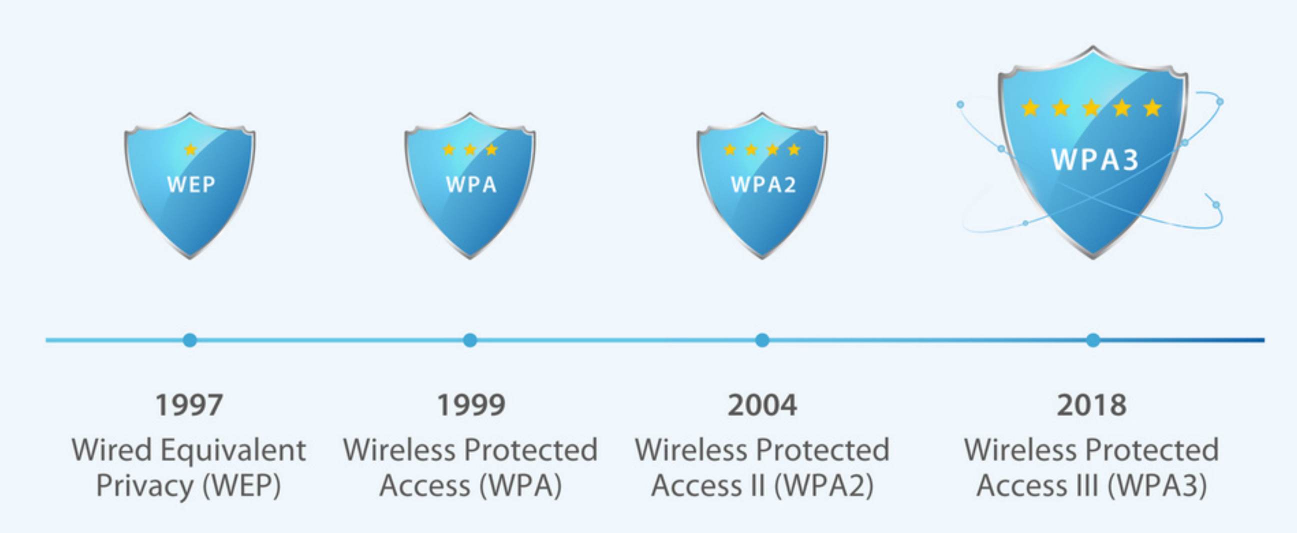
Wireless transmition can be used in a variaty of scenarios in the modern era.

WIRELESS CONNECT ENCRYPTION PROTOCOL EVOLUTION (Part 1)

There are different wireless connections. The basic one is browsing the internet using a wireless connection with no encryption. In this scenario, it is like going naked and walking down the street. You cannot defend yourself, and you are exposed to the public. As you can imagine, it is very unsafe. To avoid the insecurity issues, the Wi-Fi Alliance* announced the following protocols in chronological order: WEP (Wired Equivalent Privacy)**, WPA (Wi-Fi Protected Access), WPA2, and WPA3***. The WEP was an outdated security protocol for wireless networks; it became a standard in 1997 and was deprecated in 2003. Since the WEP protocol used a low quantity of initial vector bits combined with a key to generate encryption data, if attackers collected the encryption data, they could break the key easily. Therefore, WEP became very insecure to use. After the WEP protocol, the Wi-Fi Alliance drafted and ratified the IEEE 802.11i standard, but many old wireless routers couldn't be certified and fully compatible with the IEEE 802.11i standard, so they released a transition version called WPA, which supports partial IEEE 802.11i standard and compatible with old network adapters, and wireless routers. Now WPA2 is fully compatible with the 802.11i standard and uses more complex algorithms to protect data. In 2018, the Wi-Fi Alliance drafted WPA3, with the purpose to replace WPA2, with a longer length of the encryption key and more complexity of encryption algorithms. For now, most devices fully support WPA and WPA2, and other devices support the new WPA3 protocol.

So we can have a list for wifi connection protocols, and more security from top to down:

- No encryption
- WEP
- WPA
- WPA2
- WPA3


WEP
WPA
WPA2
WPA3
1997
Wired Equivalent Privacy (WEP)
1999
Wireless Protected Access (WPA)
2004
Wireless Protected Access II (WPA2)
2018
Wireless Protected Access III (WPA3)

▼CONTINUED

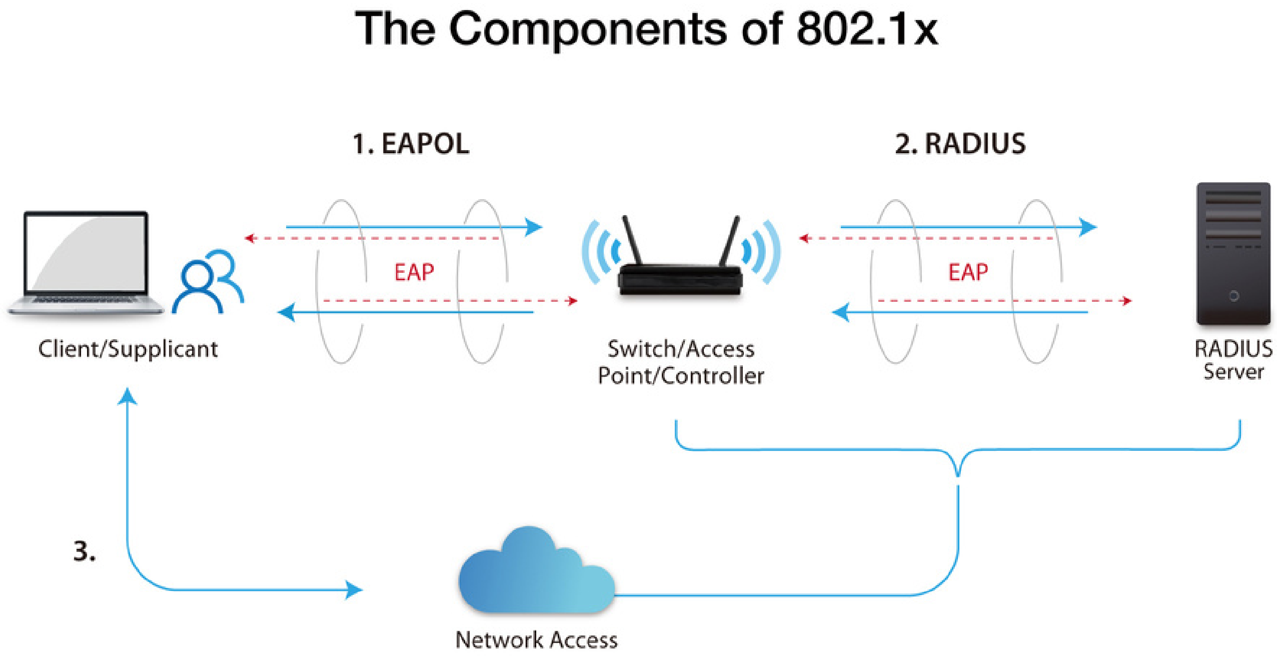
* https://www.wi-fi.org/

** https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

*** https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

WIRELESS CONNECT ENCRYPTION PROTOCOL EVOLUTION (Part 2)

We can divide the WPA security protocol series into two target users. The first one is for personal use. In this scenario, you can use a pre-shared key (PSK) to encrypt data, called WPA/WPA2-Personal, or WPA/WPA2-PSK for short. Managing a shared password is easy and fast for situations where few people are involved. But when there is an enormous mass of people or a big office environment, a common password cannot afford the challenges. Besides, it is very hard to manage in this case. As a result, there is another type of WPA security protocol called WPA/WPA2-Enterprise, it is made for non-personal use. Without a shared password, combined with the EAPOL (EAP over Lan) and an authentication server, WPA/WPA2-Enterprise can build an 802.1X* environment (See Figure x).



The components of 802.1X architecture

▼CONTINUED

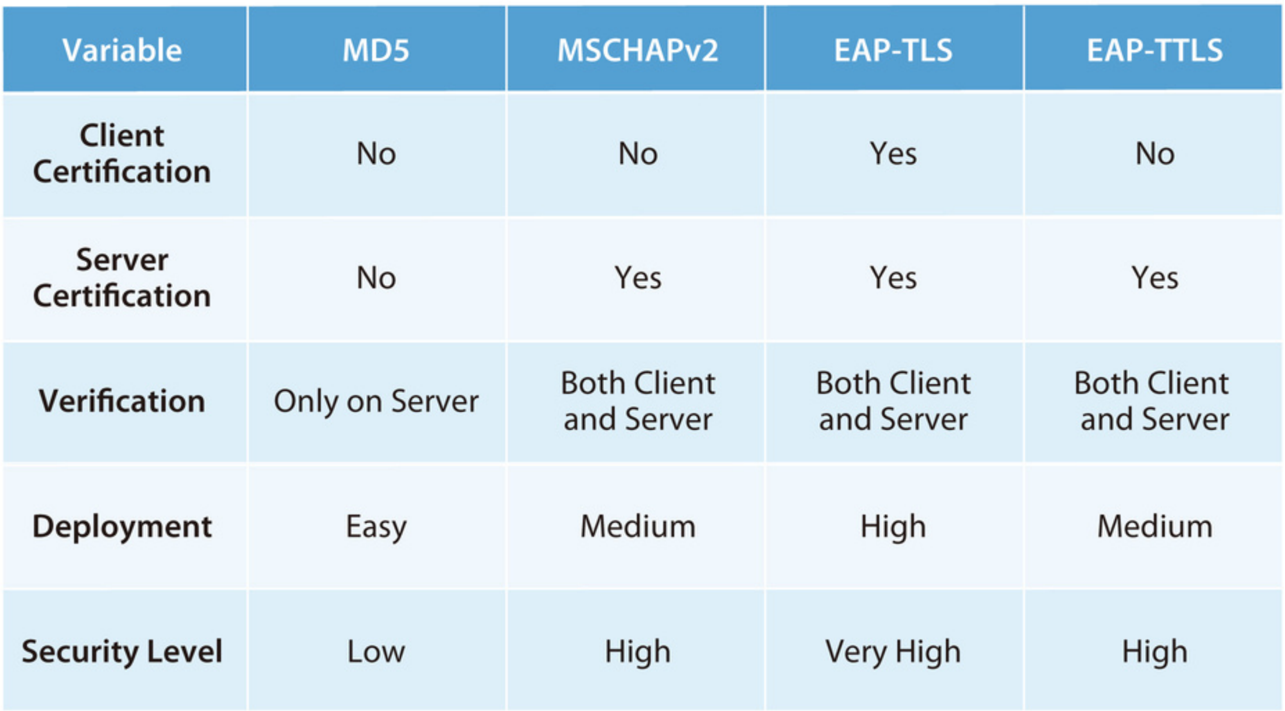
* https://en.wikipedia.org/wiki/IEEE_802.1X

WIRELESS CONNECT ENCRYPTION PROTOCOL EVOLUTION (Part 3)

We can configure the EAP with several types*. Some of the commonly used ones are:

- **EAP-MD5**
  - A weak method that uses the md5 function to check the server only. Md5 encryption is easy to crack. Hence, this method is no longer recommended.
  - It is deprecated in Windows Vista.
- **PEAPv0/EAP-MSCHAPv2**
  - Uses MS-CHAPv2 format to authenticate
- **EAP-TLS**
  - It uses a public-key infrastructure to set up the environment. It also needs root, service, and client certification for server and client. Therefore, it is hard to deploy, but it's the safest type.
- **EAP-TTLS**
  - Extension of EAP-TLS type, but the client only owns the CA certification to verify the server and build a security tunnel between client and server.
- **Others**

Here is a quick overview:



Variable	MD5	MSCHAPv2	EAP-TLS	EAP-TTLS
Client Certification	No	No	Yes	No
Server Certification	No	Yes	Yes	Yes
Verification	Only on Server	Both Client and Server	Both Client and Server	Both Client and Server
Deployment	Easy	Medium	High	Medium
Security Level	Low	High	Very High	High

For EZCast products, we support **PEAPv0/EAP-MSCHAPv2**, **EAP-TLS**, **EAP-TTLS**.

Later in this article, we'll discuss how to set up WPA/WPA2-Enterprise authentication with our product.

* https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

BASIC WPA/WP2-ENTERPRISE ENVIRONMENT SETUP TUTORIAL (Part 1)

Now we will introduce how to build a WPA/WPA2-Enterprise ready environment on Ubuntu 20.04 LTS. First, download and install Ubuntu 20.04 LTS from Ubuntu official webpage, and you can choose a server or desktop edition. After that, install the free radius package in the system.

```
#apt update
#apt install freeradius
```

To allow the client to connect to the free radius server, add the following content into /etc/freeradius/3.0/client.conf file.

```
client For-Test {
        ipaddr     = 192.168.1.0/24
        secret     = test123
}
```

The parameter IPAddr sets the IPs, which the radius server allows to connect and recognize the client group name. Please remember the secret word, you can use it for wireless router authentication to a radius server.

To build the certifications, go to /etc/freeradius/3.0/certs/directory, change ca.cnf, server.cnf, and client.cnf files for your environment. Check the default setting is ok for quickly building and test environment. If you change the password of the private key, please don't forget it. You will need it later. Then, run the following command to generate certifications for the free radius server and client.

```
#make all
```

Now, we have the files to configure the EAP environment.
Back to /etc/freeradius/3.0/directory. Change the mods-available/eap file. Then, replace the following line:

```
private_key_password = whatever
private_key_file = ${certdir}/server.pem
certificate_file = ${certdir}/server.pem
ca_file = ${certdir}/ca.pem
dh_file = ${certdir}/dh
```

▼CONTINUED

BASIC WPA/WP2-ENTERPRISE ENVIRONMENT SETUP TUTORIAL (Part 2)

Finally, we add some users for the test. Edit the /etc/freeradius/3.0/users file, uncomment user bob section,

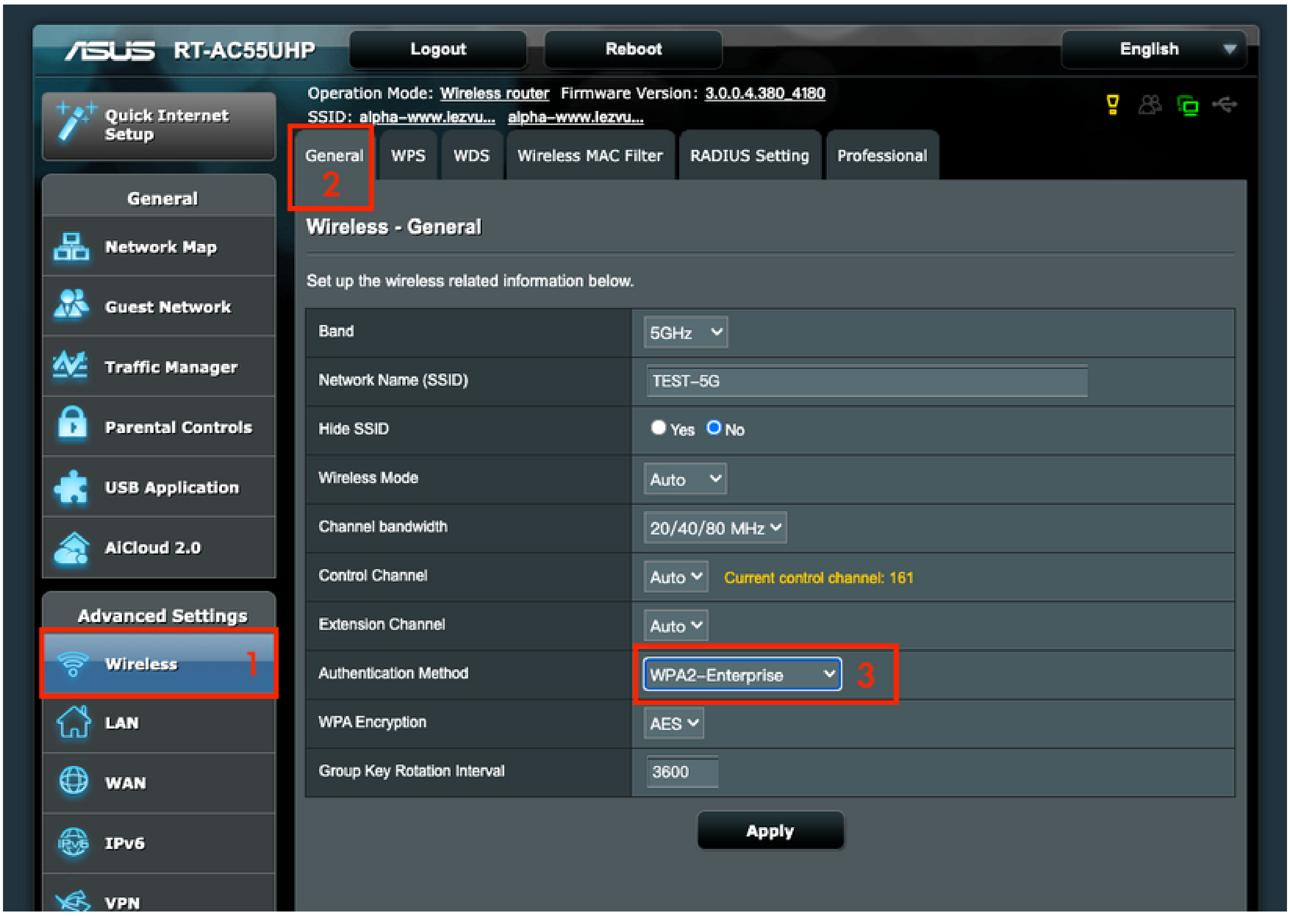
```
bob    Cleartext-Password := "hello"
       Reply-Message := "Hello, %{User-Name}"
```

When all the above is done, restart the service and let's try it.

```
#systemctl restart freeradius
```

We use ASUS RT-AC55UHP for the test environment.
Change to the Wireless - General setting page, choose WPA2-Enterprise method,
and then replace the radius server information in the RADIUS Setting page.

Finally, just reboot the wireless router, and all the settings are done.



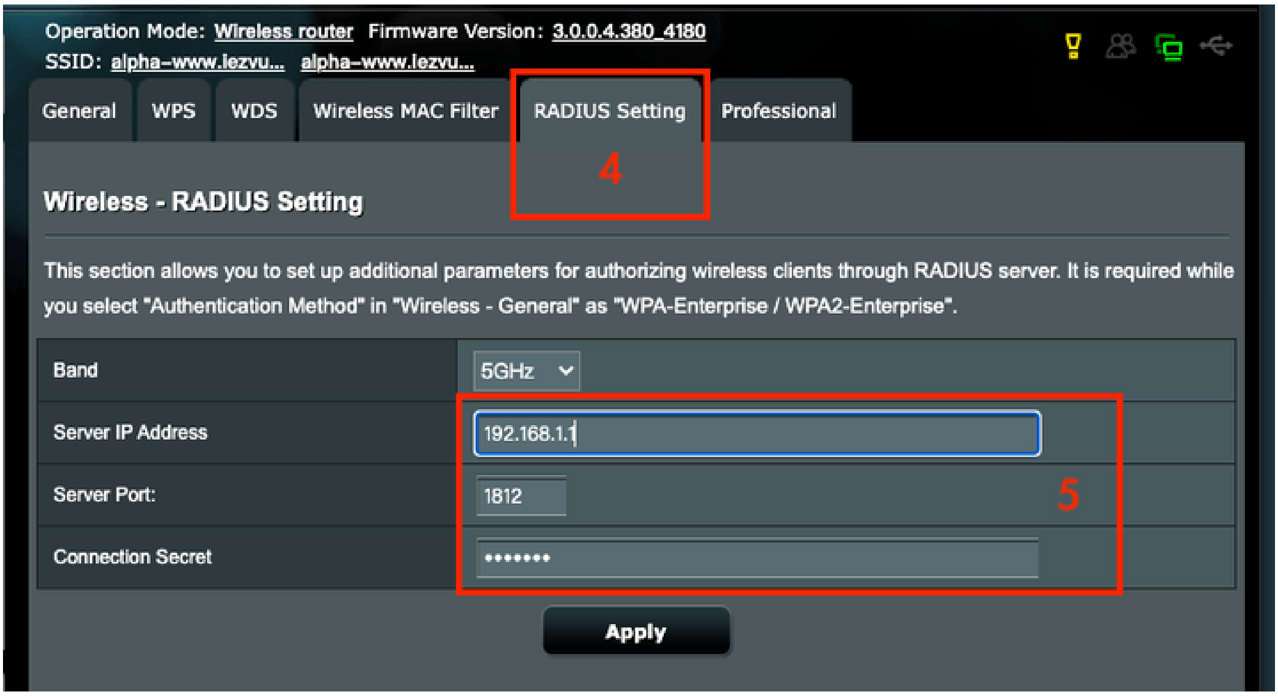
Operation Mode: Wireless router Firmware Version: 3.0.0.4.380_4180
SSID: alpha-www.lezvu... alpha-www.lezvu...

Wireless - General

Set up the wireless related information below.

Band	5GHz
Network Name (SSID)	TEST-5G
Hide SSID	○ Yes ● No
Wireless Mode	Auto
Channel bandwidth	20/40/80 MHz
Control Channel	Auto Current control channel: 161
Extension Channel	Auto
Authentication Method	WPA2-Enterprise
WPA Encryption	AES
Group Key Rotation Interval	3600

▼CONTINUED



Operation Mode: Wireless router Firmware Version: 3.0.0.4.380_4180
SSID: alpha-www.lezvu... alpha-www.lezvu...

Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".

Band	5GHz
Server IP Address	192.168.1.1
Server Port:	1812
Connection Secret	•••••••

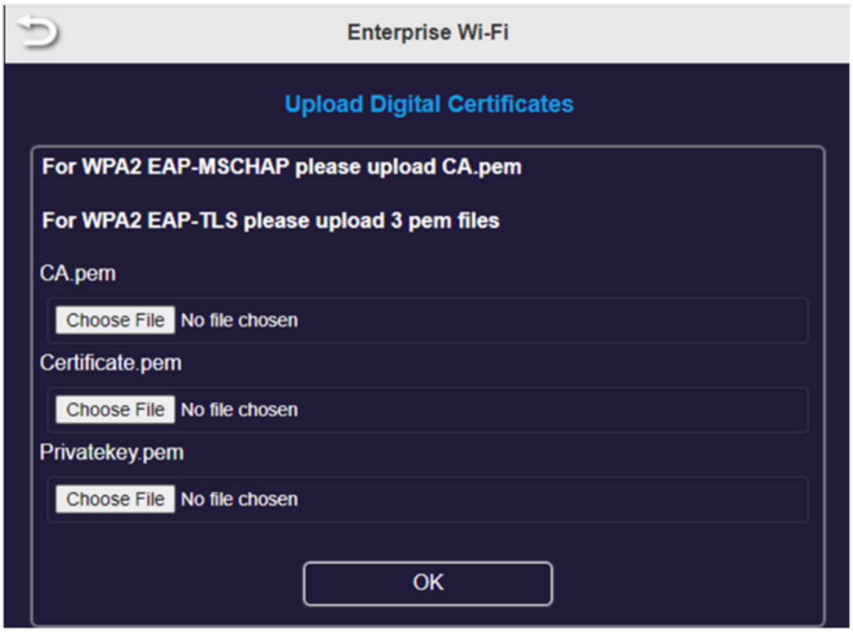
You also can verify the connection log by /var/log/freeradius/radius.log.

```
Tue Feb 22 09:29:48 2022 : Auth: (97) Login OK: [bob] (from client For-Test port 0 via TLS tunnel)
Tue Feb 22 09:29:48 2022 : Auth: (98) Login OK: [bob] (from client For-Test port 0 cli XX-XX-XX-XX-XX-XX)
Tue Feb 22 09:31:30 2022 : Auth: (107) Login OK: [user@example.org] (from client For-Test port 0 cli XX-XX-XX-XX-XX-XX)
```

HOW TO USE WI-FI ENTERPRISE IN PRO2 SERIES (Part 1)

Users can enter the EZCast pro web setting page to connect to an Enterprise AP.
Before connecting to an Enterprise AP, you need to upload related certification files in EZCast pro products.

EZCast pro support 3 EAP types: PEAP / PEAP2(MSCHARPv2) / TLS.



Enterprise Wi-Fi

Upload Digital Certificates

For WPA2 EAP-MSCHAP please upload CA.pem

For WPA2 EAP-TLS please upload 3 pem files

CA.pem

Choose File No file chosen

Certificate.pem

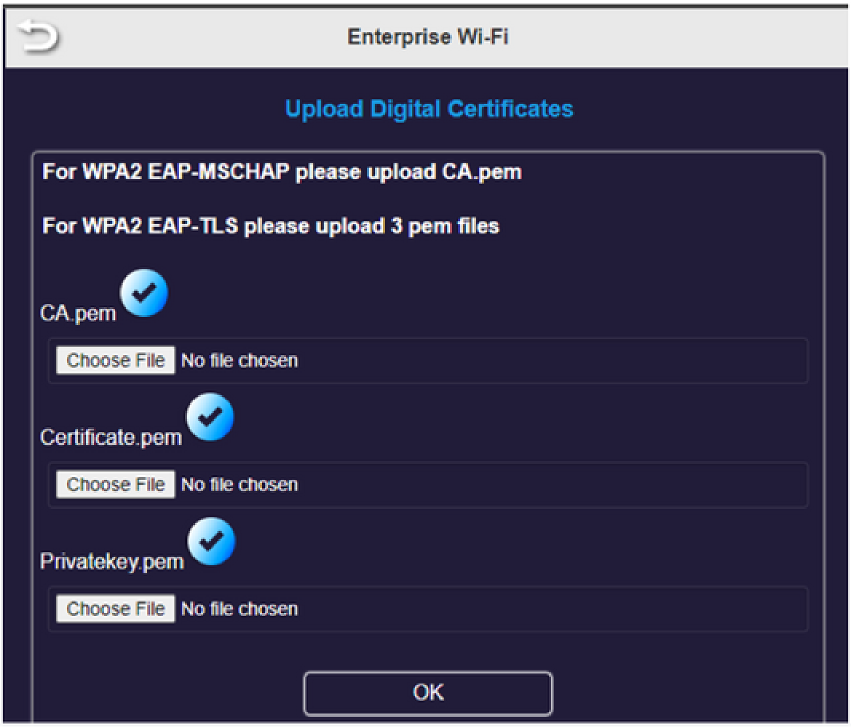
Choose File No file chosen

Privatekey.pem

Choose File No file chosen

OK

After uploading completely, you can find the tick icon beside the columns.



Enterprise Wi-Fi

Upload Digital Certificates

For WPA2 EAP-MSCHAP please upload CA.pem

For WPA2 EAP-TLS please upload 3 pem files

CA.pem ✓

Choose File No file chosen

Certificate.pem ✓

Choose File No file chosen

Privatekey.pem ✓

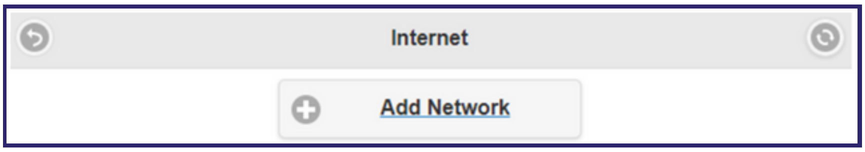
Choose File No file chosen

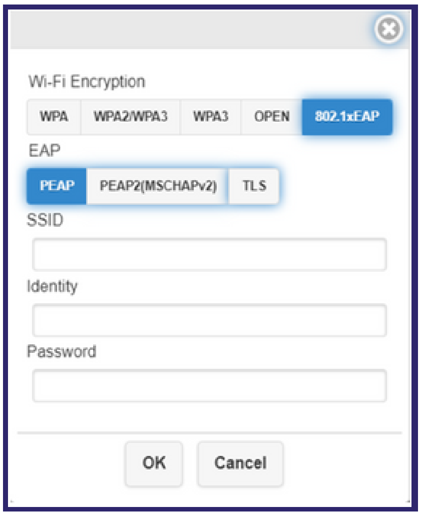
OK

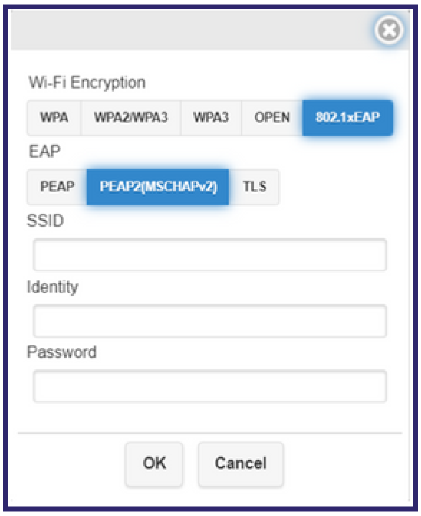
▼CONTINUED

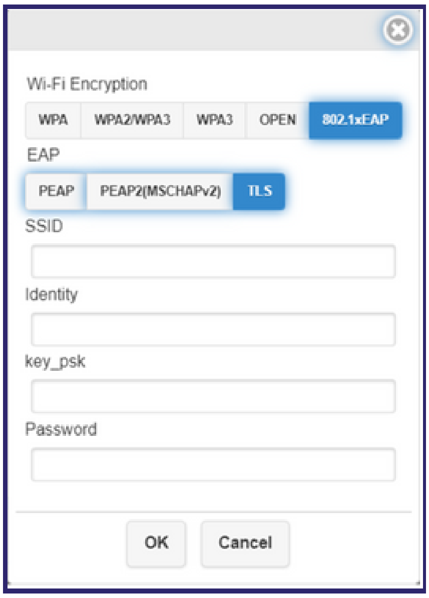
HOW TO USE WI-FI ENTERPRISE IN PRO2 SERIES (Part 2)

Now, you can select or add an enterprise AP from Wi-Fi list scan page.









WHY IS WI-FI ENTERPRISE IMPORTANT?

Today, almost everyone owns one or more Internet-connected devices. As the number of these devices increases, it is imperative that a security strategy be implemented to minimize the potential for exploitation. Criminal Organizations may utilize Internet-connected devices to collect personal data, steal identities, compromise financial data, and surreptitiously spy on people. The risks of an unsecured wireless network are the same whether it's a residential or business network. The following are some of the dangers:

- Piggybacking
- Evil Twin Attacks
- Unauthorized Computer Access
- Wireless Sniffing
- Wardriving
- Shoulder Surfing
- Theft of Mobile Devices

This type of behavior can be avoided by taking a few precautions in the configuration and use of your equipment. By encrypting your wireless data, anyone who has access to your network won't be able to see your information (CISA, 2010). Using “Wi-Fi Enterprise” mode provides the security required for wireless networks in business environments. Although it sounds complicated to set up, it allows individual and centralized management of access to Wi-Fi networks. It is important to note that when clients try to connect to the network; they need to provide their login credentials. Also, note that WPA-Enterprise/Enterprise should only be used when connecting to a server for client authentication.

EXCELLENT PROTECTION FOR YOUR BUSINESS WITH EZCAST PRO

With our wireless display solutions, IT administrators can configure device settings according to their organization's security measures. EZCast Pro displays support Encrypted data transmission. Using this can validate the identity of other devices, secure connections between your display and other servers, ensure data integrity, and encrypt data to prevent snooping.

Third party software can contain security risks for your IT infrastructure. Besides, our EZCast Pro solutions are hardware-based, so no installations are necessary.

REFERENCES

CISA. (2010, March 11). *Security Tip (ST05-003)*. Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/uscert/ncas/tips/ST05-003#:~:text=Encrypting%20your%20wireless%20data%20prevents,wireless%20routers%20and%20wireless%20devices

CISCO. (2022). *What Is Wi-Fi Security?* Retrieved from CISCO: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html

Consumer FTC. (2021, May). *Federal Trade Comission Consumer Advice*. Retrieved from How To Secure Your Home Wi-Fi Network: https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network

TechoPedia. (2022). *Wireless Network Security*.
.