Configure 802.1X Supplicant Settings on a Wireless Access Point

Objective

The 802.1X standard was developed to provide security in Layer 2 of the Open System Interconnection (OSI) Model. It consists of the following components: Supplicant, Authenticator, and Authentication Server. A Supplicant is the client or software that connects to a network so that it can access its resources. It needs to provide credentials or certificates to obtain an IP address and be part of that particular network. A Supplicant cannot have access to the network resources until it has been authenticated.

Configuring 802.1X Supplicant settings on your Wireless Access Point (WAP) is useful to allow authorized devices behind your WAP to be part of the network and to access its resources. At the same time, it also adds a layer of security to the network.

This article will show you how to configure 802.1X Supplicant settings on your wireless access point.

Applicable Devices

- WAP100 Series
- WAP300 Series
- WAP500 Series

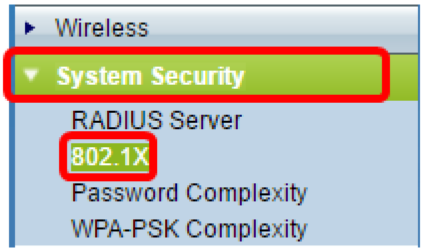
Software Version

- 1.0.1.2 – WAP150, WAP361
- 1.0.6.2 – WAP121, WAP321
- 1.0.2.2 – WAP131, WAP351
- 1.2.1.3 – WAP551, WAP561, WAP371
- 1.0.0.17 – WAP571, WAP571E

Configure 802.1X Supplicant Settings on a WAP

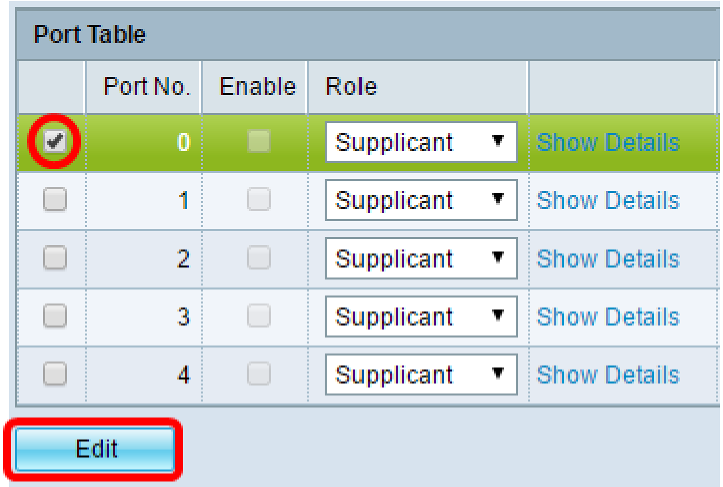
Step 1. Log in to the web-based utility of the access point and choose **System Security>802.1X**.

Note: The web-based utility menu may vary depending on the model of your WAP. The images below are taken from WAP361.



Note: If you are using other models of WAP, choose **System Security > 802.1X Supplicant** then skip to Step 3.

Step 2. Check the box of the Port number you wish to configure and then click **Edit**.

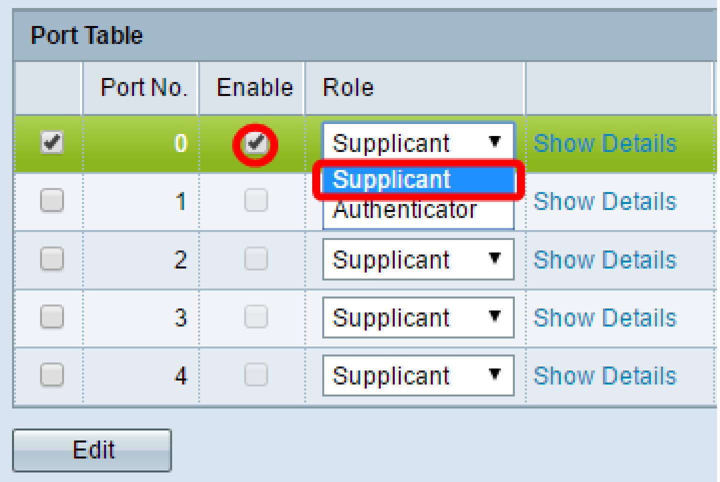


Port Table

	Port No.	Enable	Role	
☑	0	□	Supplicant ▼	Show Details
□	1	□	Supplicant ▼	Show Details
□	2	□	Supplicant ▼	Show Details
□	3	□	Supplicant ▼	Show Details
□	4	□	Supplicant ▼	Show Details

Step 3. Check the **Enable** check box and then choose **Supplicant** from the drop-down list. This is the default option.

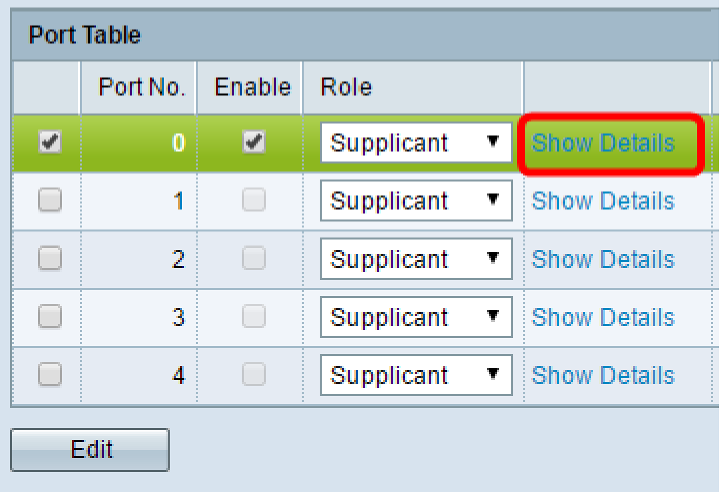
Note: For other models of WAP, check the **Enable** check box for the Administrative Mode then skip to Step 5.



Port Table

	Port No.	Enable	Role	
☑	0	☑	Supplicant ▼	Show Details
□	1	□		Show Details
□	2	□	Supplicant ▼	Show Details
□	3	□	Supplicant ▼	Show Details
□	4	□	Supplicant ▼	Show Details

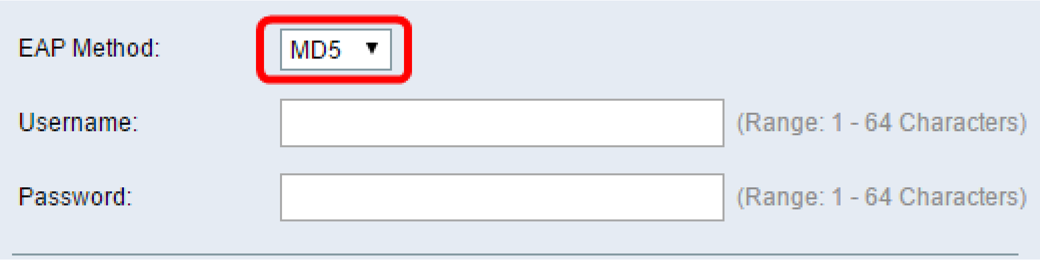
Step 4. Click on the **Show Details** link to enable you to edit the settings.



Port Table

	Port No.	Enable	Role	
☑	0	☑	Supplicant ▼	Show Details
□	1	□	Supplicant ▼	Show Details
□	2	□	Supplicant ▼	Show Details
□	3	□	Supplicant ▼	Show Details
□	4	□	Supplicant ▼	Show Details

Step 5. Choose the appropriate type of Extensible Authentication Protocol (EAP) Method from the EAP Method drop-down list.



EAP Method: MD5

Username: (Range: 1 - 64 Characters)

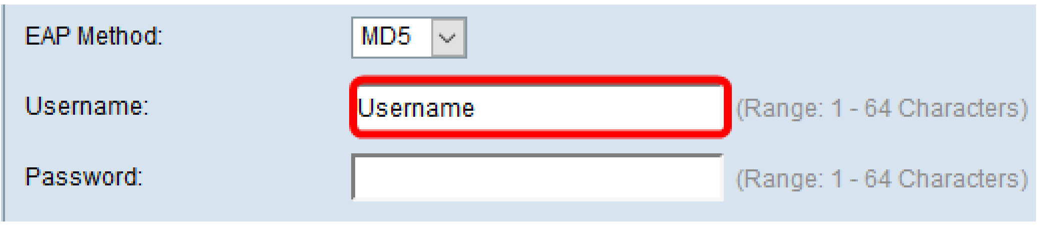
Password: (Range: 1 - 64 Characters)

The options are:

- MD5 — MD5 is an algorithm which is used to encrypt data of any size into 128 bit. The MD5 algorithm uses a public cryptosystem to encrypt data.
- PEAP — Protected Extensible Authentication Protocol (PEAP) authenticates wireless Local Area Network (LAN) clients through digital certificates issued by the server by creating an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) tunnel between the client and the authentication server.
- TLS — TLS is a protocol that provides security and data integrity for communication over the Internet. It ensures that no third party tampers with the original message.

Note: In this example, MD5 is used.

Step 6. Enter your preferred username in the *Username* field. This will be used when responding to an 802.1X Authenticator. It can be up to 64 characters long, may include uppercase and lowercase letters, numbers, and special characters except double quotation marks.

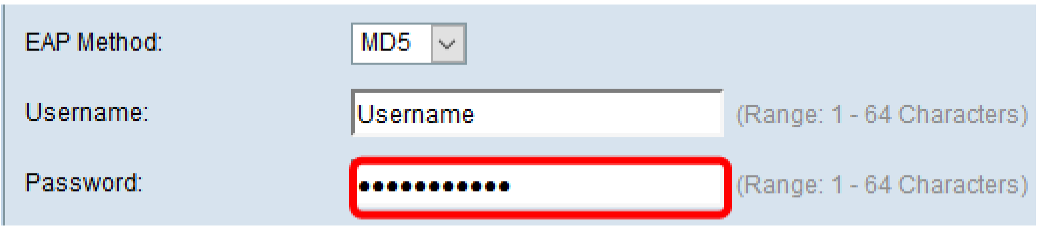


EAP Method: MD5

Username: Username (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Step 7. Enter your preferred password in the *Password* field. This MD5 password is used when responding to an 802.1X Authenticator. The password can be up to 64 characters long, may include uppercase and lowercase letters, numbers, and special characters except quotation marks.



EAP Method: MD5

Username: Username (Range: 1 - 64 Characters)

Password: ••••••••••• (Range: 1 - 64 Characters)

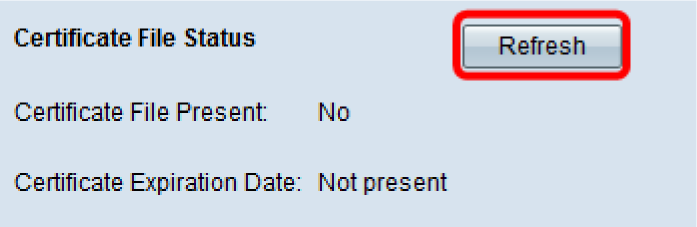
Step 8. Click the Save button.

You should now have configured the 802.1X Supplicant settings on your WAP.

View Certificate File Settings

The Certificate File Status area shows whether the certificate file is present or not. The SSL certificate is a digitally signed certificate by a certificate authority that allows the web browser to have a secure communication with the web server.

Step 1. To view the current status of the certificate file, click **Refresh**.



Certificate File Status

Certificate File Present: No

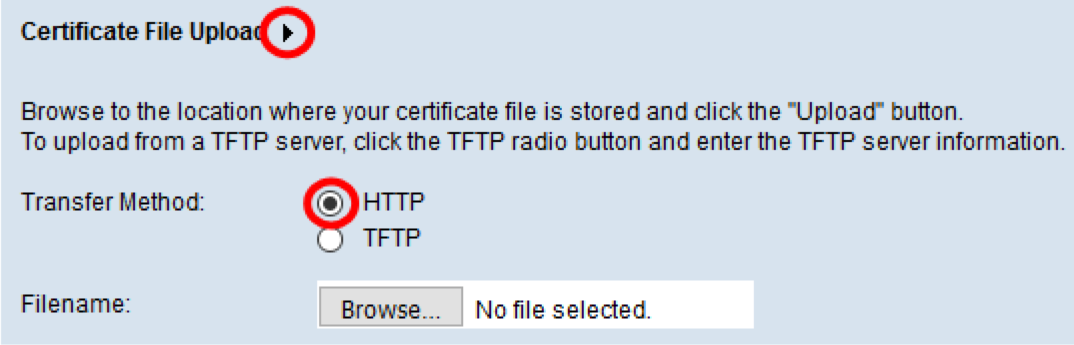
Certificate Expiration Date: Not present

The Certificate File Status area has the following fields:

- Certificate File Present – Displays whether the certificate file is present or not.
- Certificate Expiration Date – Displays the expiration date of the current certificate file.

Upload a Certificate File

Step 1. Click the arrow beside Certificate File Upload then choose the desired radio button from the Transfer Method.



Certificate File Upload

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: ● HTTP ○ TFTP

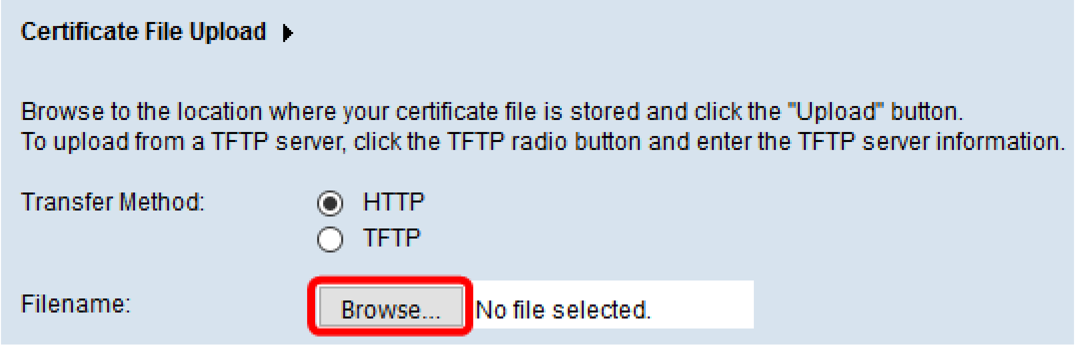
Filename: No file selected.

There are two transfer methods in uploading the file:

- Hypertext Transfer Protocol (HTTP)
- Trivial File Transfer Protocol (TFTP)

Note: In this example, HTTP is chosen.

Step 2. (Optional) If HTTP is chosen, click **Browse** to choose the certificate file from your computer then skip to Step 5.



Certificate File Upload

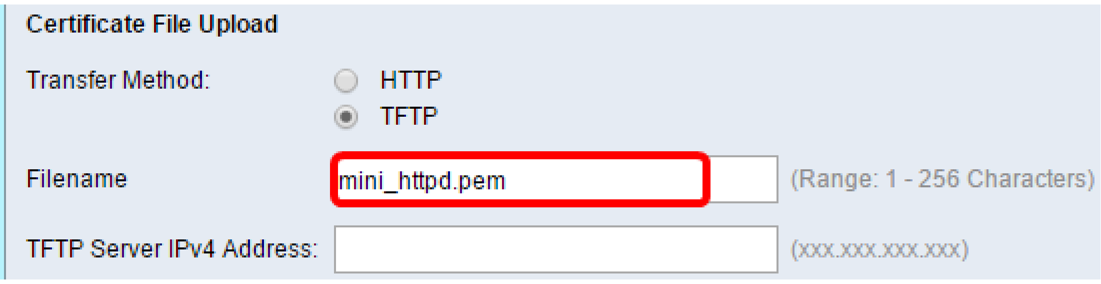
Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Transfer Method: ● HTTP ○ TFTP

Filename: No file selected.

Step 3. (Optional) If you chose TFTP in Step 1, enter the name of the certificate file in the *Filename* field. The TFTP server is used to automatically transfer boot files within devices and is very simple.

Note: In this example, *mini_httpd.pem* is used as the filename.



Certificate File Upload

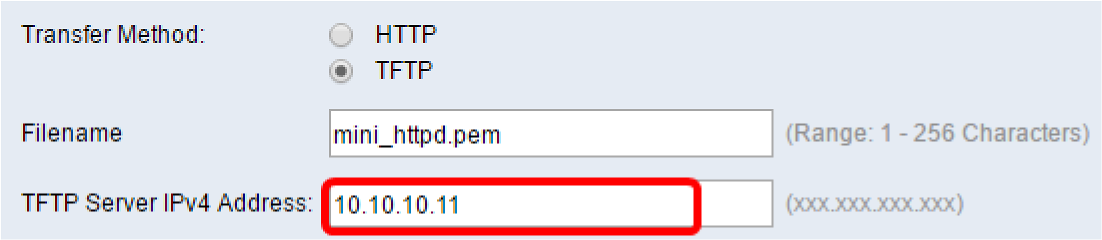
Transfer Method: ○ HTTP ● TFTP

Filename: mini_httpd.pem (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Step 4. Enter the IP address of the TFTP server in the *TFTP Server IPv4 Address* field.

Note: In this example, 10.10.10.11 is used as the TFTP Server IPv4 Address.

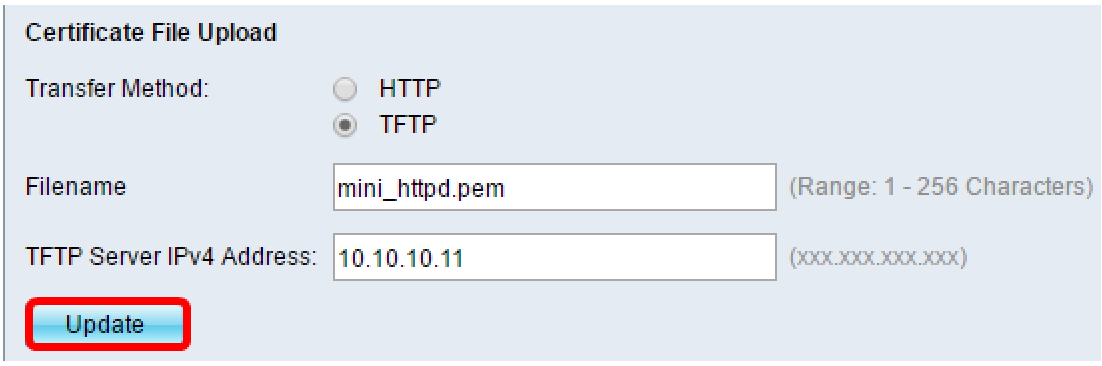


Transfer Method: ○ HTTP ● TFTP

Filename: mini_httpd.pem (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: 10.10.10.11 (xxx.xxx.xxx.xxx)

Step 5. Click **Update**.



Certificate File Upload

Transfer Method: ○ HTTP ● TFTP

Filename: mini_httpd.pem (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: 10.10.10.11 (xxx.xxx.xxx.xxx)

Note: If you are using other models of WAP, click **Upload**.

Step 6. Click the Save button to save your settings.

You should now have successfully uploaded a certificate file on your WAP.