

Configure 802.1X Supplicant Settings on a WAP125 or WAP581

Objective

A supplicant is one of the three roles in the 802.1X IEEE Standard. 802.1X was developed to provide security in Layer 2 of the 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.

This article will show you how to configure the WAP125 or WAP581 access point as an 802.1X Supplicant.

Note: To learn how to configure 802.1X Supplicant Credentials on your switch, click [here](#).

Applicable Devices

- WAP125
- WAP581

Software Version

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Configure the 802.1X Supplicant

Configure Supplicant Credentials

Step 1. Log in to the web-based utility of your WAP. The default username and password is cisco/cisco.



Wireless Access Point

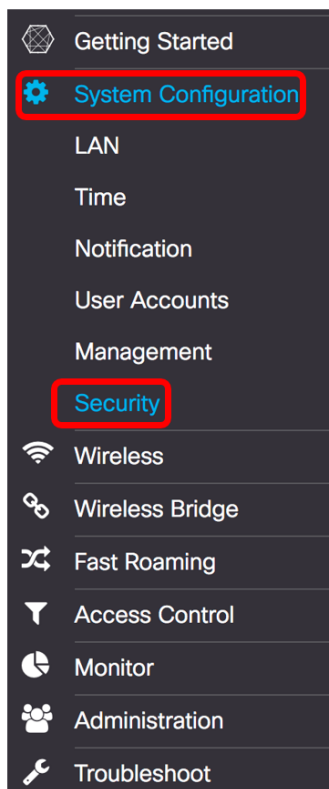
A login form for a Cisco Wireless Access Point. It features a red rounded rectangular border. Inside, there is a text input field containing 'cisco', a password input field with masked characters '*****', a language dropdown menu set to 'English', and a blue 'Login' button at the bottom.

©2017 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Note: If you already have changed the password or created a new account, enter your new credentials instead.

Step 2. Choose **System Configuration > Security**.



Step 3. Check the **Enable** check box to enable Administrative Mode. This enables the WAP to act as the supplicant to the authenticator.

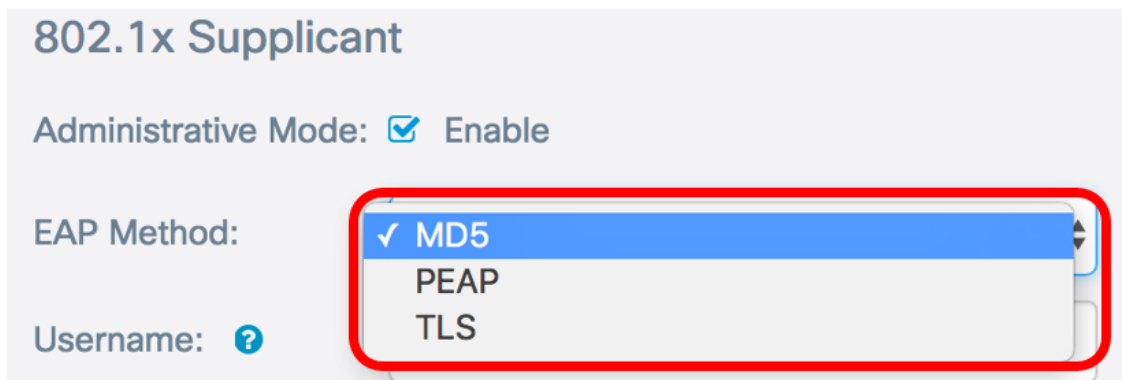
802.1x Supplicant

Administrative Mode:  Enable

Step 4. Choose the appropriate type of Extensible Authentication Protocol (EAP) Method that will be used to encrypt usernames and passwords from the *EAP Method* drop-down list. The options are:

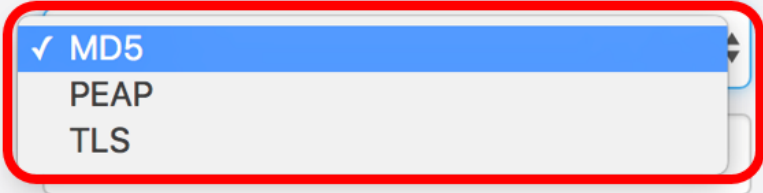
- MD5 — Uses 128-bit encryption method. The MD5 algorithm uses a public crypto-system to encrypt data.
- PEAP — Protected Extensible Authentication Protocol (PEAP) authenticates wireless LAN clients through digital certificates issued by the server by creating an encrypted SSL/TLS tunnel between the client and the authentication server.
- TLS — Transport Layer Security (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.



802.1x Supplicant

Administrative Mode: ☒ Enable

EAP Method: 

Username: 

Step 5. Enter a username in the *Username* field. This is the username that has been configured on the Authenticator and is used to respond to the 802.1X Authenticator. It can be one to 64 characters long, may include uppercase and lowercase letters, numbers, and special characters except double quotation marks.

Note: In this example, UserAccess_1 is used.

802.1x Supplicant

Administrative Mode: ☒ Enable

EAP Method: MD5

Username: ? UserAccess_1|

Step 6. Enter a password associated with the Username in the *Password* field. This MD5 password is used to respond to the 802.1X Authenticator. The password can be one to 64 characters long, may include uppercase and lowercase letters, numbers, and special characters except quotation marks.

802.1x Supplicant

Administrative Mode: ☒ Enable

EAP Method: MD5

Username: ? UserAccess_1

Password: ?

Step 7. Click the **Save** button to save the configured settings.

Security

Save

802.1x Supplicant

Administrative Mode:

☒ Enable

EAP Method:

MD5

Username: ?

UserAccess_1

Password: ?

.....

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

Certificate File Upload

Step 1. From the transfer method, choose a method which the WAP will use to obtain the SSL certificate. 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. The options are:

- HTTP — Certificate is uploaded through the Hyper Text Transfer Protocol (HTTP) or through the browser.
- TFTP — Certificate is uploaded through a Trivial File Transfer Protocol (TFTP) server. If this is chosen, skip to [Step 3](#). You will be required to enter the file name and the TFTP address.

Note: In this example, HTTP is chosen.

Certificate File Upload

Transfer Method: ☒ HTTP ☐ TFTP

Filename:

Browse...

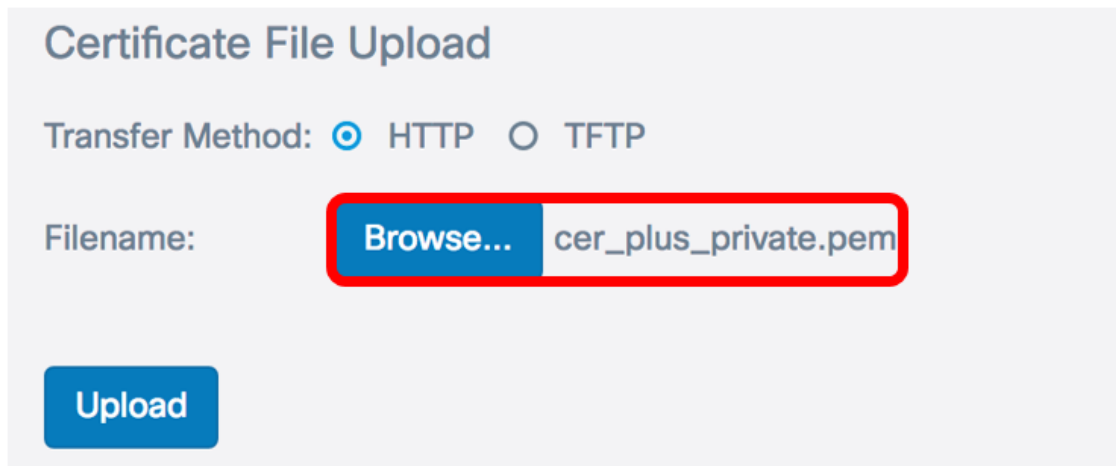
cer_plus_private.pem

Upload

HTTP Transfer Method

Step 2. (Optional) If you have chosen HTTP, click **Browse...** and choose the SSL Certificate.

Note: In this example, cer_plus_private.pem is used.



Certificate File Upload

Transfer Method: ☒ HTTP ☐ TFTP

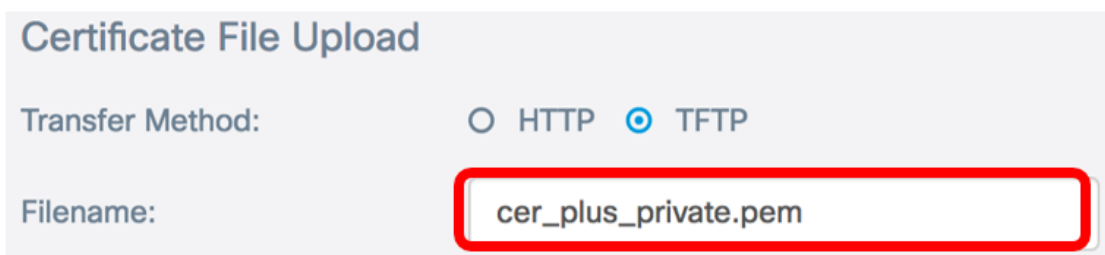
Filename: Browse... cer_plus_private.pem

Upload

TFTP Transfer Method

[Step 3](#). If you have chosen TFTP in Step 1, enter the name of the file in the Filename field.

Note: In this example, cer_plus_private.pem is used.



Certificate File Upload

Transfer Method: ☐ HTTP ☒ TFTP

Filename: cer_plus_private.pem

Step 4. (Optional) If TFTP is chosen as the transfer method, enter the IPv4 address of the TFTP server in the *TFTP Server IPv4 Address* field. This is the path which the WAP will use to retrieve the certificate.

Note: In this example, 10.21.52.101 is used.



Certificate File Upload

Transfer Method: ☐ HTTP ☒ TFTP

Filename: cer_plus_private.pem

TFTP Server IPv4 Address: ? 10.21.52.101

Step 5. Click **Upload**.

802.1x Supplicant

Administrative Mode: ☒ Enable

EAP Method:

Username:

Password:

Certificate File Upload

Transfer Method: ☐ HTTP ☒ TFTP

Filename:

TFTP Server IPv4 Address:

Upload

You should now have successfully uploaded a certificate on the WAP.