

Configuración de los parámetros del suplicante 802.1X en un punto de acceso inalámbrico

Objetivo

El estándar 802.1X se desarrolló para proporcionar seguridad en la capa 2 del modelo de interconexión de sistemas abiertos (OSI). Consta de los siguientes componentes: Supplicant, Authenticator y Authentication Server. Un suplicante es el cliente o software que se conecta a una red para que pueda acceder a sus recursos. Necesita proporcionar credenciales o certificados para obtener una dirección IP y ser parte de esa red en particular. Un solicitante no puede tener acceso a los recursos de red hasta que se haya autenticado.

La configuración de los parámetros de suplicante 802.1X en el punto de acceso inalámbrico (WAP) es útil para permitir que los dispositivos autorizados detrás de su WAP formen parte de la red y accedan a sus recursos. Al mismo tiempo, también agrega una capa de seguridad a la red.

En este artículo se explica cómo configurar los parámetros del suplicante 802.1X en el punto de acceso inalámbrico.

Dispositivos aplicables

- Serie WAP100
- Serie WAP300
- Serie WAP500

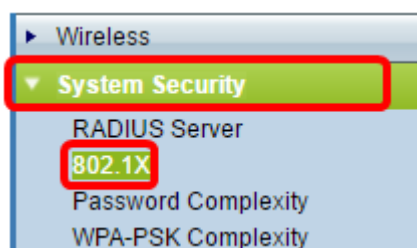
Versión del software

- 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

Configuración de los parámetros del suplicante 802.1X en un WAP

Paso 1. Inicie sesión en la utilidad basada en web del punto de acceso y elija **Seguridad del sistema > 802.1X**.

Nota: El menú de la utilidad basada en Web puede variar en función del modelo de su WAP. Las imágenes siguientes se han tomado del dispositivo WAP361.



Nota: Si utiliza otros modelos de WAP, elija **System Security > 802.1X Supplicant** y luego vaya al [Paso 3](#).

Paso 2. Marque la casilla del número de puerto que desea configurar y luego haga clic en **Editar**.

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Paso 3. Marque la casilla de verificación **Enable** y luego elija **Supplicant** en la lista desplegable. Esta es la opción predeterminada.

Nota: Para otros modelos de WAP, marque la casilla de verificación **Enable** para Administrative Mode y luego vaya al [Paso 5](#).

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant Authenticator	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Paso 4. Haga clic en el enlace **Mostrar detalles** para poder editar los parámetros.

Port Table				
	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

Paso 5. Elija el tipo adecuado de método de protocolo de autenticación extensible (EAP) en la lista desplegable Método EAP.

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Las opciones son:

- MD5 — MD5 es un algoritmo que se utiliza para cifrar datos de cualquier tamaño en 128 bits. El algoritmo MD5 utiliza un criptosistema público para cifrar datos.
- PEAP: el protocolo de autenticación extensible protegido (PEAP) autentica a los clientes de red de área local (LAN) inalámbrica mediante certificados digitales emitidos por el servidor mediante la creación de un túnel de capa de conexión segura (SSL) o seguridad de la capa de transporte (TLS) cifrado entre el cliente y el servidor de autenticación.
- TLS: TLS es un protocolo que proporciona seguridad e integridad de datos para la comunicación a través de Internet. Garantiza que ningún tercero altere el mensaje original.

Nota: En este ejemplo, se utiliza MD5.

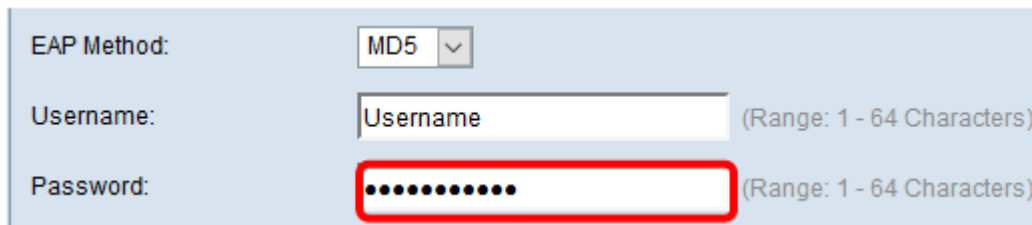
Paso 6. Ingrese su nombre de usuario preferido en el campo *Username*. Esto se utilizará al responder a un autenticador 802.1X. Puede tener hasta 64 caracteres, puede incluir letras mayúsculas y minúsculas, números y caracteres especiales, excepto comillas dobles.

EAP Method:

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

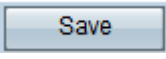
Paso 7. Introduzca la contraseña que prefiera en el campo *Password* (Contraseña). Esta contraseña MD5 se utiliza cuando se responde a un autenticador 802.1X. La contraseña puede tener hasta 64 caracteres, puede incluir letras mayúsculas y minúsculas, números y caracteres especiales, excepto comillas.



EAP Method: MD5

Username: Username (Range: 1 - 64 Characters)

Password: [Redacted] (Range: 1 - 64 Characters)

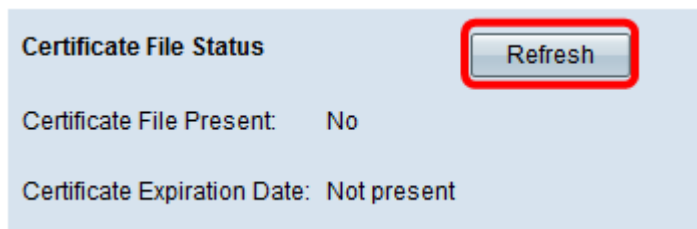
Paso 8. Haga clic en el  botón.

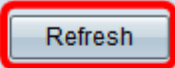
Ahora debería haber configurado la configuración del suplicante 802.1X en su WAP.

Ver configuración de archivo de certificado

El área Estado del archivo de certificado muestra si el archivo de certificado está presente o no. El certificado SSL es un certificado firmado digitalmente por una autoridad certificadora que permite al navegador web tener una comunicación segura con el servidor web.

Paso 1. Para ver el estado actual del archivo de certificado, haga clic en **Actualizar**.



Certificate File Status 

Certificate File Present: No

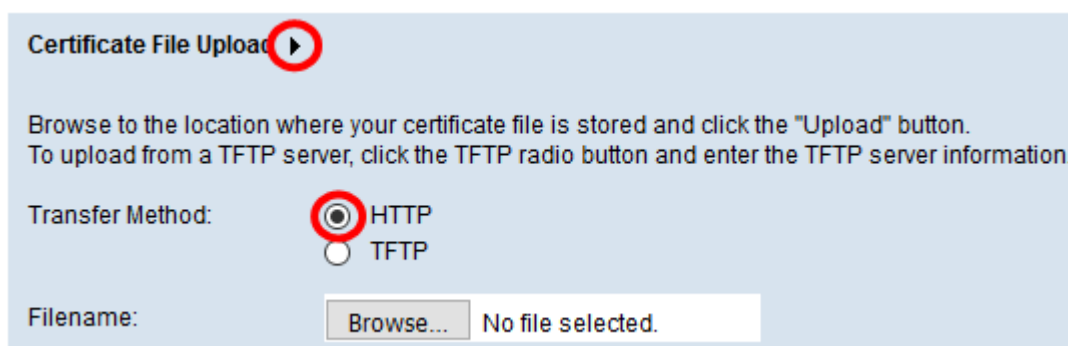
Certificate Expiration Date: Not present


El área Estado del archivo de certificado tiene los siguientes campos:

- Archivo de certificado presente: muestra si el archivo de certificado está presente o no.
- Fecha de vencimiento del certificado: muestra la fecha de vencimiento del archivo de certificado actual.

Cargar un archivo de certificado

Paso 1. Haga clic en la flecha situada junto a Cargar archivo de certificado y, a continuación, seleccione el botón de opción deseado del Método de transferencia.



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.

Hay dos métodos de transferencia para cargar el archivo:

- HTTP (Hypertext Transfer Protocol)
- Protocolo trivial de transferencia de archivos (TFTP)

Nota: En este ejemplo, se elige HTTP.

Paso 2. (Opcional) Si se elige HTTP, haga clic en **Examinar** para elegir el archivo de certificado de su equipo y, a continuación, vaya directamente al [Paso 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.

Paso 3. (Opcional) Si eligió TFTP en el Paso 1, ingrese el nombre del archivo de certificado en el campo *Nombre de archivo*. El servidor TFTP se utiliza para transferir automáticamente archivos de inicio dentro de los dispositivos y es muy simple.

Nota: En este ejemplo, *mini_httpd.pem* se utiliza como nombre de archivo.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

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

Paso 4. Ingrese la dirección IP del servidor TFTP en el campo *TFTP Server IPv4 Address*.

Nota: En este ejemplo, 10.10.10.11 se utiliza como dirección IPv4 del servidor TFTP.

Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

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

Paso 5. Haga clic en Update (Actualizar).

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename (Range: 1 - 256 Characters)

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

Nota: Si utiliza otros modelos de WAP, haga clic en **Cargar**.

Paso 6. Haga clic en el  botón para guardar los parámetros.

Ahora debería haber cargado correctamente un archivo de certificado en su WAP.