Configure las configuraciones del supplicant del 802.1x en un WAP125 o un WAP581

Objetivo

Un supplicant es uno de los tres papeles en la norma IEEE del 802.1x. el 802.1x fue desarrollado para proporcionar la Seguridad en la capa 2 del modelo de OSI. Consiste en los componentes siguientes: Supplicant, authenticator, y servidor de autenticación. Un supplicant es el cliente o el software que conectan con una red de modo que pueda acceder sus recursos. Necesita proporcionar las credenciales o los Certificados para obtener una dirección IP y para ser la parte de que red determinada. Un supplicant no puede tener acceso a los recursos de red hasta que se haya autenticado.

Este artículo le mostrará cómo configurar el Punto de acceso WAP125 o WAP581 como supplicant del 802.1x.

Nota: Para aprender cómo configurar las credenciales del supplicant del 802.1x en su Switch, haga clic aquí.

Dispositivos aplicables

- WAP125
- WAP581

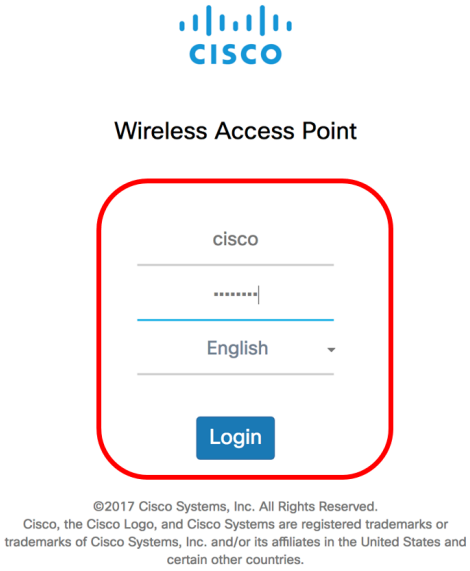
Versión del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Configure el supplicant del 802.1x

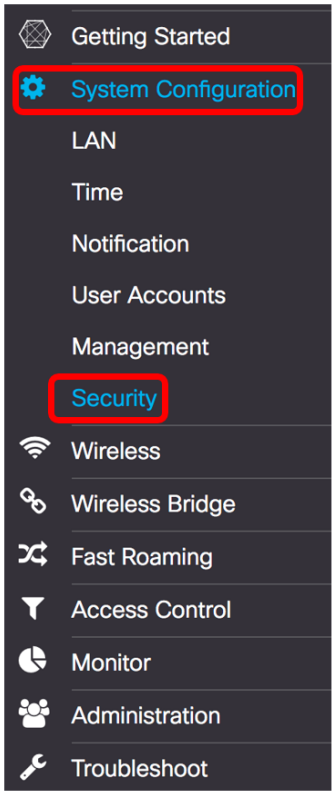
Configure las credenciales del supplicant

Paso 1. Inicie sesión a la utilidad basada en web de su WAP. El nombre de usuario predeterminado y la contraseña es Cisco/Cisco.



Nota: Si usted ha cambiado la contraseña o ha creado ya una nueva cuenta, ingrese sus nuevas credenciales en lugar de otro.

Paso 2. Elija el **> Security (Seguridad) de la configuración del sistema**.

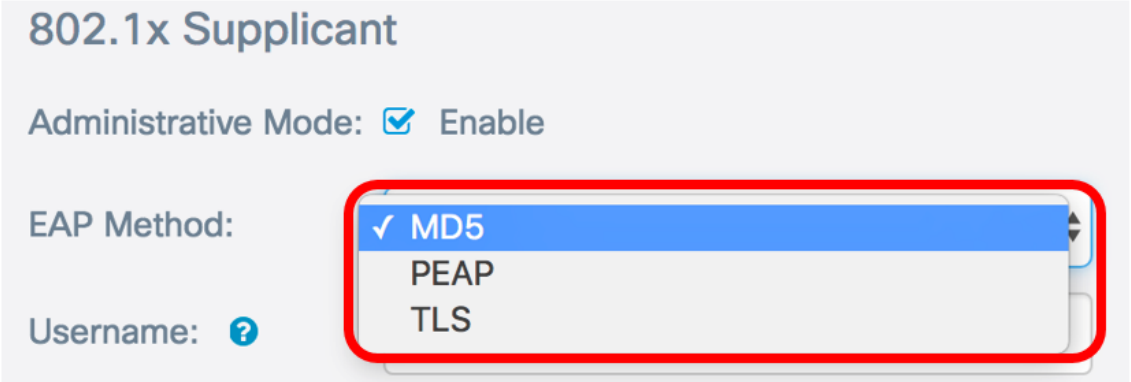


Paso 3. Marque la casilla de verificación del **permiso** para habilitar al modo administrativo. Esto permite al WAP para actuar como el supplicant al authenticator.

Paso 4. Elija el tipo apropiado de método del Protocolo de Autenticación Extensible (EAP) que será utilizado para cifrar los nombres de usuario y contraseña de la lista desplegable del *método EAP*. Las opciones son:

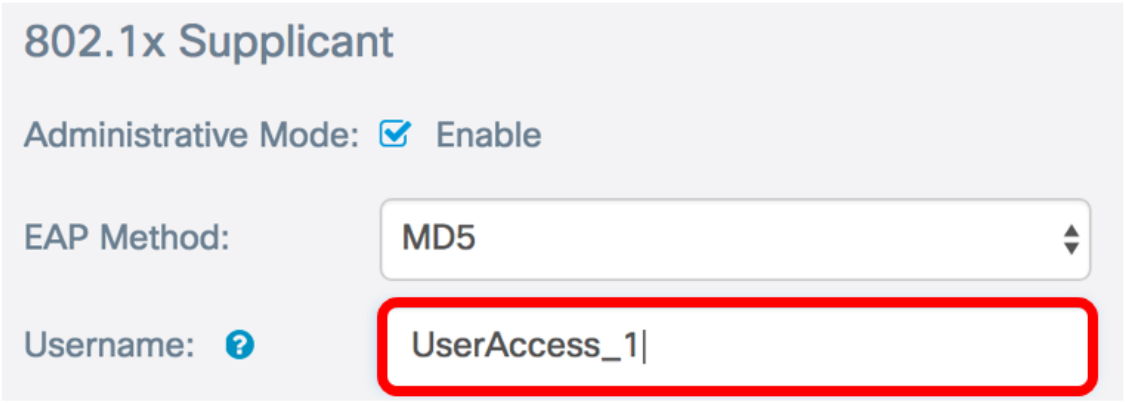
- MD5 — Utiliza el método de encripción del 128-bit. El algoritmo MD5 utiliza un sistema criptográfico público para cifrar los datos.
- PEAP — El protocolo extensible authentication protegido (PEAP) autentica a los clientes del Wireless LAN a través de los Certificados digitales publicados por el servidor creando un túnel cifrado SSL/TLS entre el cliente y el servidor de autenticación.
- TLS — Transport Layer Security (TLS) es un protocolo que proporciona la Seguridad y la integridad de los datos para la comunicación sobre Internet. Se asegura de que ningún otro vendedor trate de forzar con el mensaje original.

Nota: En este ejemplo, se utiliza el MD5.

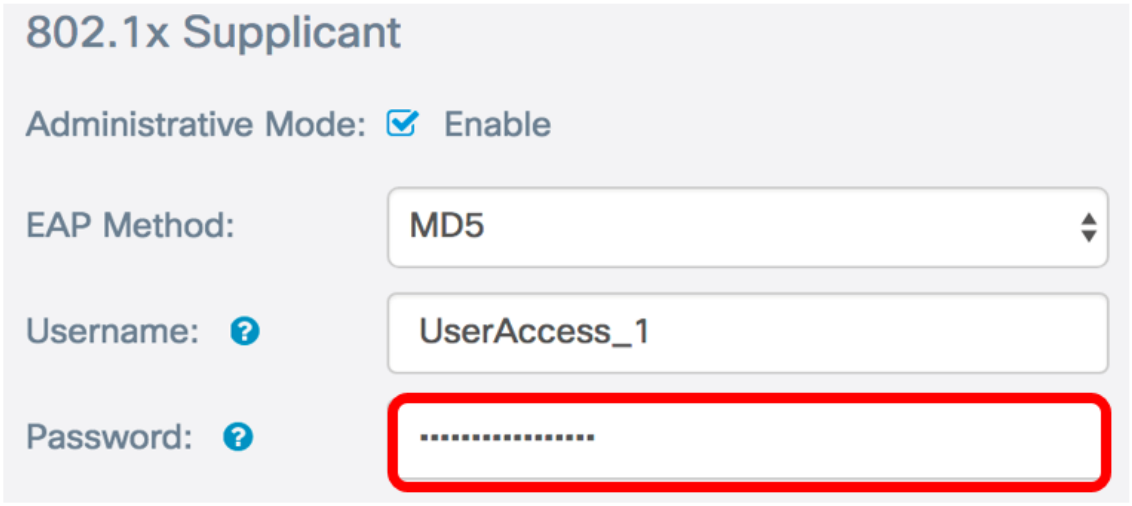


Paso 5. Ingrese un nombre de usuario en el *campo de nombre de usuario*. Éste es el nombre de usuario que se ha configurado en el authenticator y se utiliza para responder al authenticator del 802.1x. Puede ser un a 64 caracteres de largo, puede incluir el mayúscula y las letras minúsculas, los números, y los caracteres especiales excepto las comillas dobles.

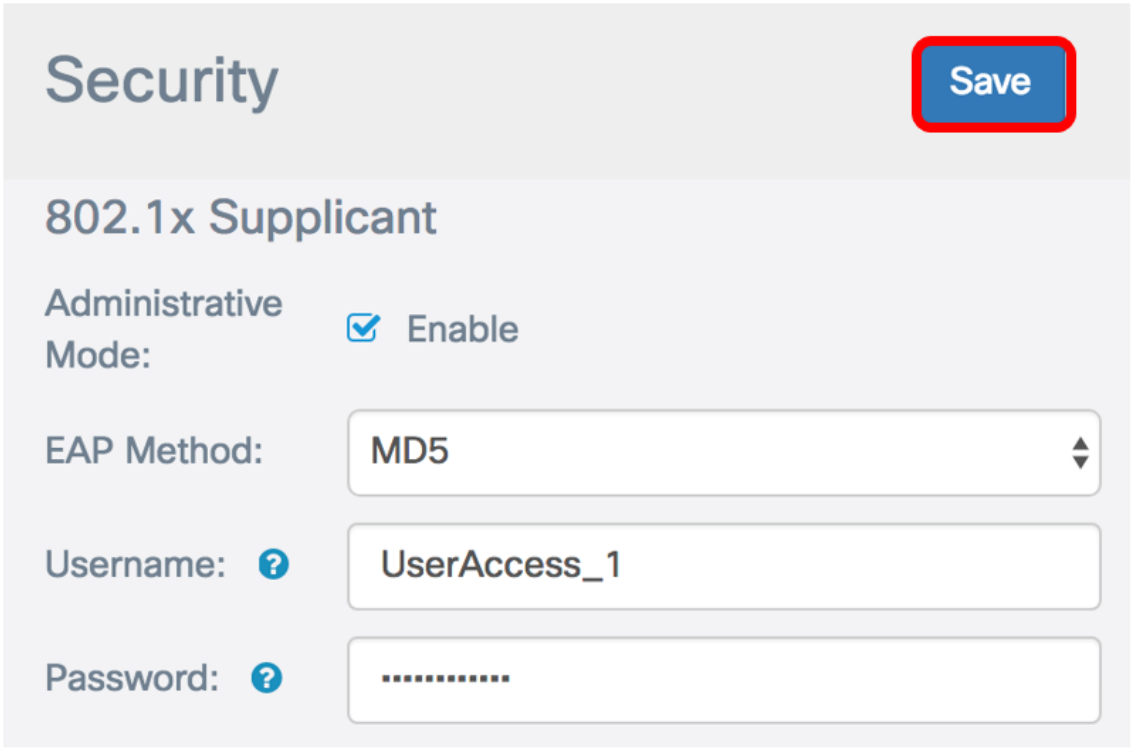
Nota: En este ejemplo, se utiliza UserAccess_1.



Paso 6. Ingrese una contraseña asociada al nombre de usuario en el campo de *contraseña*. Esta contraseña MD5 se utiliza para responder al authenticator del 802.1x. La contraseña puede ser un a 64 caracteres de largo, puede incluir el mayúscula y las letras minúsculas, los números, y los caracteres especiales excepto las comillas.



Paso 7. Haga clic el **botón Save Button** para salvar las configuraciones configuradas.



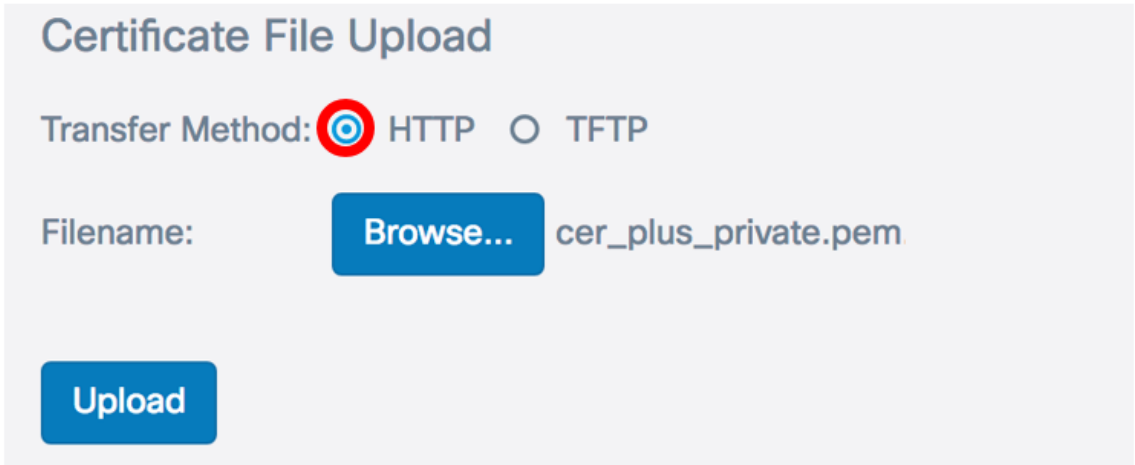
Usted debe ahora haber configurado las configuraciones del supplicant del 802.1x en el WAP.

Carga del archivo de certificado

Paso 1. Del método de la transferencia, elija un método que el WAP utilice para obtener el certificado SSL. El certificado SSL es un certificado firmado digitalmente por un Certificate Authority que permite que el buscador Web tenga una comunicación segura con el servidor Web. Las opciones son:

- HTTP — El certificado está cargado con el protocolo hyper text transfer (HTTP) o a través del navegador.
- TFTP — El certificado está cargado a través de un servidor del Trivial File Transfer Protocol (TFTP). Si se elige esto, salte al paso 3. Le requerirán ingresar el nombre del archivo y el direccionamiento TFTP.

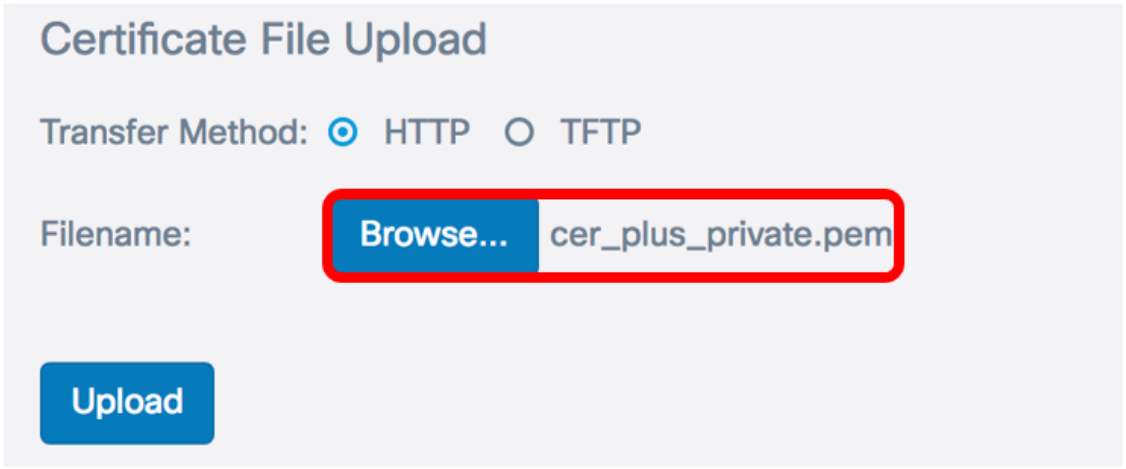
Nota: En este ejemplo, se elige el HTTP.



Método de la transferencia HTTP

El paso 2. (opcional) si usted ha elegido el HTTP, tecleo **hojea…** y elige el certificado SSL.

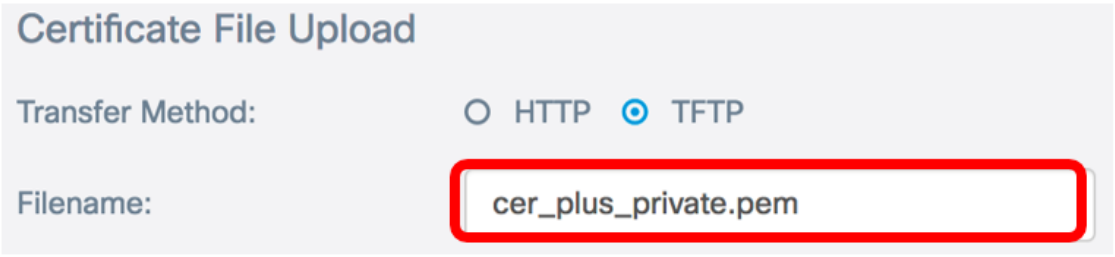
Nota: En este ejemplo, se utiliza cer_plus_private.pem.



Método de la transferencia TFTP

Paso 3. Si usted ha elegido el TFTP en el paso 1, ingrese el nombre del archivo en el campo del nombre de fichero.

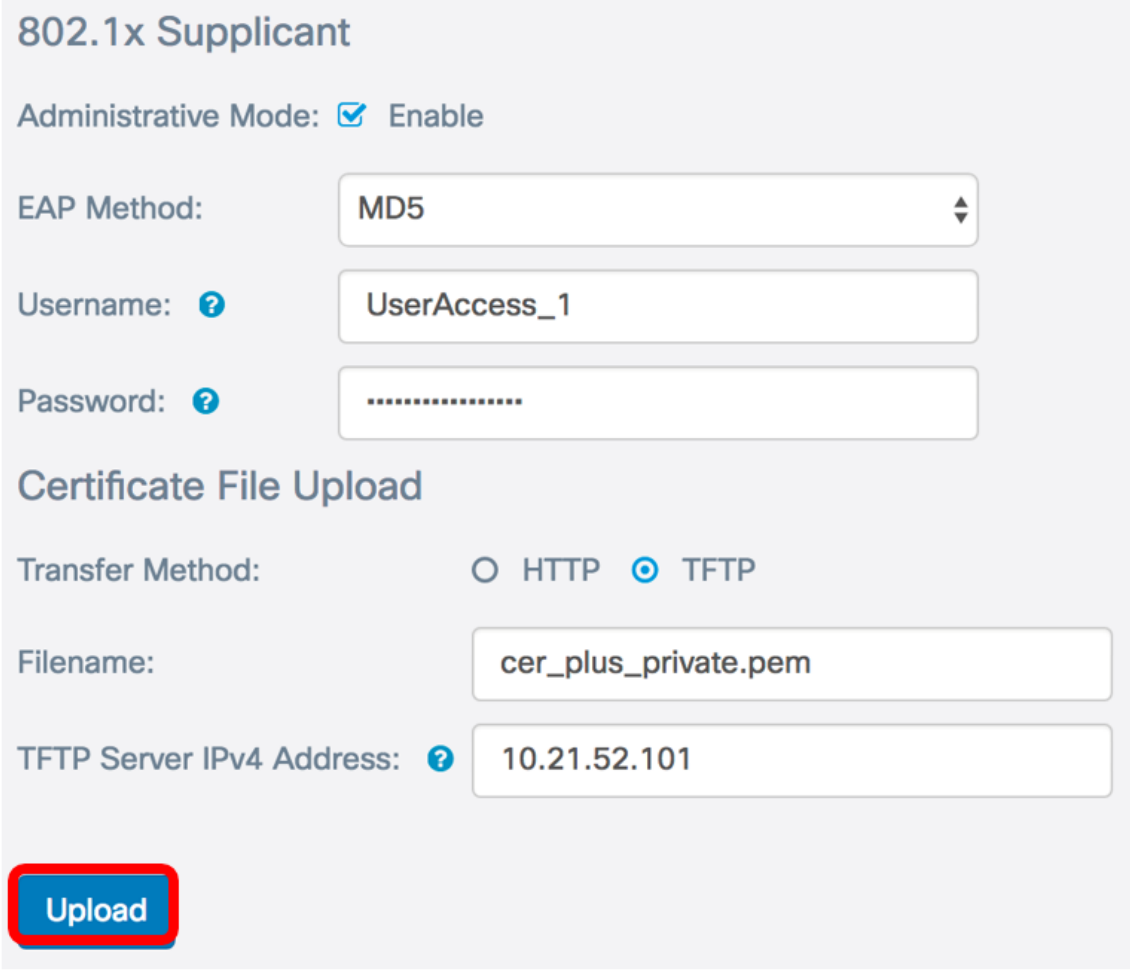
Nota: En este ejemplo, se utiliza cer_plus_private.pem.



El paso 4. (opcional) si el TFTP se elige como el método de la transferencia, ingresa el direccionamiento del IPv4 del servidor TFTP en el *campo de dirección del IPv4 del servidor TFTP* . Ésta es la trayectoria que el WAP utilizará para extraer el certificado.

Nota: En este ejemplo, se utiliza 10.21.52.101.

Paso 5. **Carga del** tecleo.



Usted debe ahora haber cargado con éxito un certificado en el WAP.