

Configuración de 802.1X Supplicant Settings en un WAP125 o WAP581

Objetivo

Un solicitante es una de las tres funciones del estándar IEEE 802.1X. 802.1X se desarrolló para proporcionar seguridad en la capa 2 del modelo 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.

En este artículo se muestra cómo configurar el punto de acceso WAP125 o WAP581 como suplicante 802.1X.

Nota: Para saber cómo configurar las credenciales de suplicante 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

Configuración del suplicante 802.1X

Configurar las credenciales del solicitante

Paso 1. Inicie sesión en la utilidad basada en Web de su WAP. El nombre de usuario y la contraseña predeterminados son `cisco/cisco`.



Wireless Access Point

cisco

.....|

English

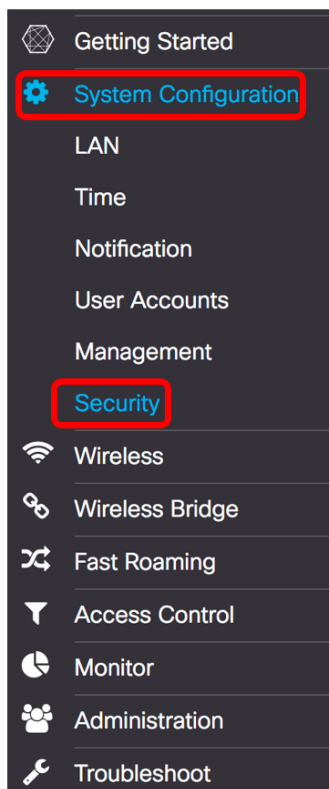
Login

©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.

Nota: Si ya ha cambiado la contraseña o ha creado una nueva cuenta, introduzca sus nuevas credenciales.

Paso 2. Elija **System Configuration > Security**.



Paso 3. Marque la casilla de verificación **Enable** para habilitar Administrative Mode. Esto permite que WAP actúe como suplicante del autenticador.

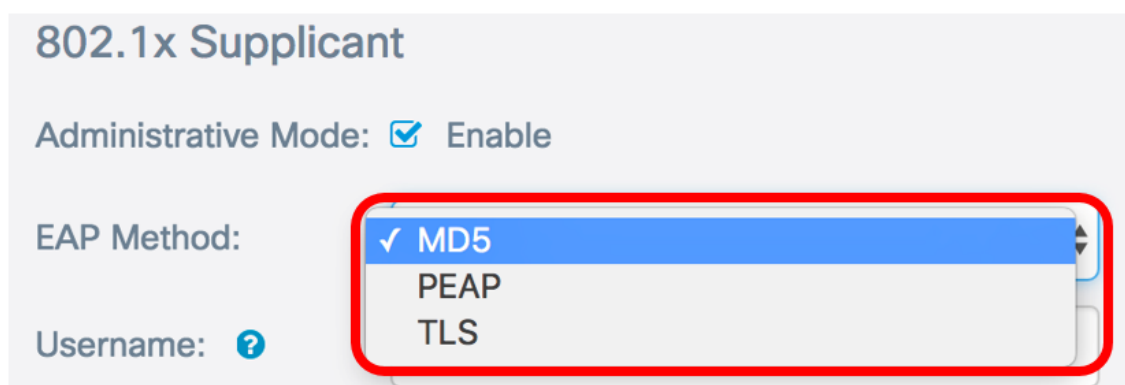
802.1x Supplicant

Administrative Mode:  Enable

Paso 4. Elija el tipo adecuado de método de protocolo de autenticación extensible (EAP) que se utilizará para cifrar nombres de usuario y contraseñas de la lista desplegable *Método EAP*. Las opciones son:

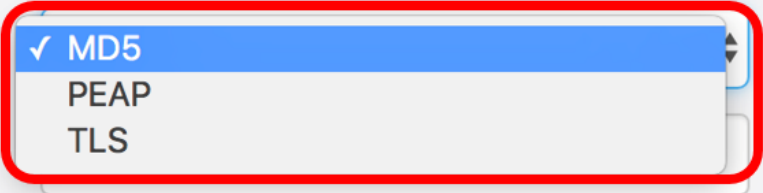
- MD5: utiliza el método de encriptación de 128 bits. El algoritmo MD5 utiliza un sistema criptográfico público para cifrar datos.
- PEAP: el protocolo de autenticación extensible protegido (PEAP) autentica a los clientes LAN inalámbricos mediante certificados digitales emitidos por el servidor mediante la creación de un túnel SSL/TLS cifrado entre el cliente y el servidor de autenticación.
- TLS: la seguridad de la capa de transporte (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.



802.1x Supplicant

Administrative Mode: Enable

EAP Method: 

Username: 

Paso 5. Ingrese un nombre de usuario en el campo *Nombre de usuario*. Este es el nombre de usuario que se ha configurado en Authenticator y se utiliza para responder al autenticador 802.1X. Puede tener entre uno y 64 caracteres, puede incluir letras mayúsculas y minúsculas, números y caracteres especiales, excepto comillas dobles.

Nota: En este ejemplo, se utiliza UserAccess_1.

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Paso 6. Introduzca una contraseña asociada al nombre de usuario en el campo *Contraseña*. Esta contraseña MD5 se utiliza para responder al autenticador 802.1X. La contraseña puede tener entre uno y 64 caracteres, puede incluir letras mayúsculas y minúsculas, números y caracteres especiales, excepto comillas.

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

Paso 7. Haga clic en el botón **Guardar** para guardar los parámetros configurados.

Security

Save

802.1x Supplicant

Administrative Mode: Enable

EAP Method: MD5

Username:

Password:

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

Carga de archivo de certificado

Paso 1. Desde el método de transferencia, elija un método que WAP utilizará para obtener el certificado SSL. 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. Las opciones son:

- HTTP: el certificado se carga a través del protocolo de transferencia de hipertexto (HTTP) o a través del explorador.
- TFTP: el certificado se carga a través de un servidor de protocolo de transferencia de archivos trivial (TFTP). Si selecciona esta opción, vaya directamente al [Paso 3](#). Se le pedirá que introduzca el nombre de archivo y la dirección TFTP.

Nota: En este ejemplo, se elige HTTP.

Certificate File Upload

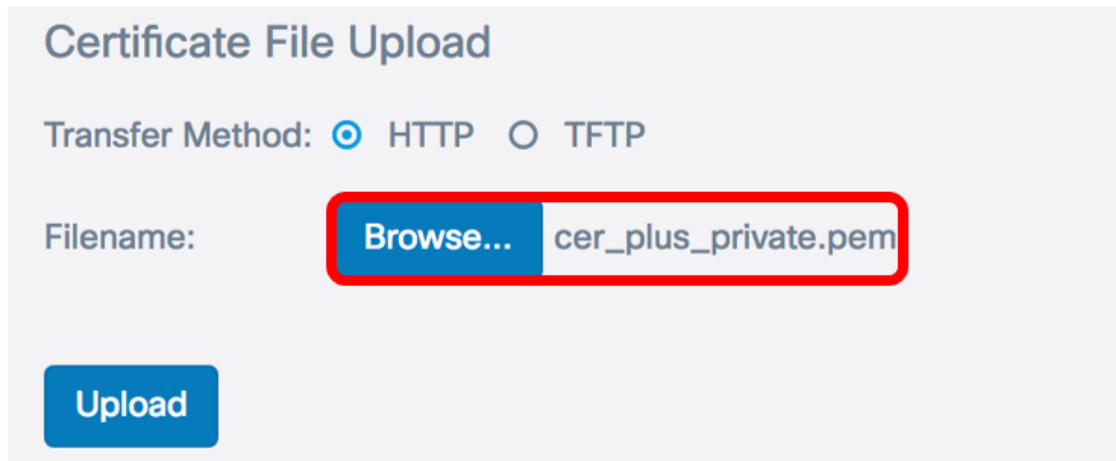
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

Método de transferencia HTTP

Paso 2. (Opcional) Si ha seleccionado HTTP, haga clic en **Examinar...** y elija el certificado SSL.

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



Certificate File Upload

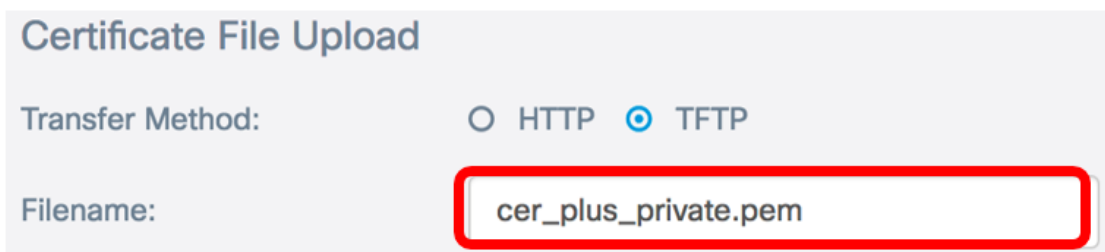
Transfer Method: HTTP TFTP

Filename: cer_plus_private.pem

Método de transferencia TFTP

Paso 3. Si ha elegido TFTP en el Paso 1, introduzca el nombre del archivo en el campo Nombre de archivo.

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



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

Paso 4. (Opcional) Si se elige TFTP como método de transferencia, ingrese la dirección IPv4 del servidor TFTP en el campo *TFTP Server IPv4 Address*. Ésta es la ruta que el WAP utilizará para recuperar el certificado.

Nota: En este ejemplo, se utiliza 10.21.52.101.



Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Paso 5. Haga clic en **Cargar**.

802.1x Supplicant

Administrative Mode: Enable

EAP Method:

Username:

Password:

Certificate File Upload

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

Ahora debería haber cargado correctamente un certificado en el WAP.