Configurar ajustes do suplicante do 802.1X em um WAP125 ou em um WAP581

Objetivo

Um suplicante é um dos três papéis no padrão de IEEE do 802.1X. o 802.1X foi desenvolvido para fornecer a Segurança na camada 2 do modelo osi. Consiste nos seguintes componentes: Suplicante, autenticador, e Authentication Server. Um suplicante é o cliente ou o software que conectam a uma rede de modo que possa alcançar seus recursos. Precisa de fornecer credenciais ou Certificados para obter parte de um endereço IP de Um ou Mais Servidores Cisco ICM NT e para ser essa rede particular. Um suplicante não pode ter o acesso aos recursos de rede até que esteja autenticado.

Este artigo mostrar-lhe-á como configurar o Access point WAP125 ou WAP581 como um suplicante do 802.1X.

Nota: Para aprender como configurar credenciais do suplicante do 802.1X em seu interruptor, clique aqui.

Dispositivos aplicáveis

- WAP125
- WAP581

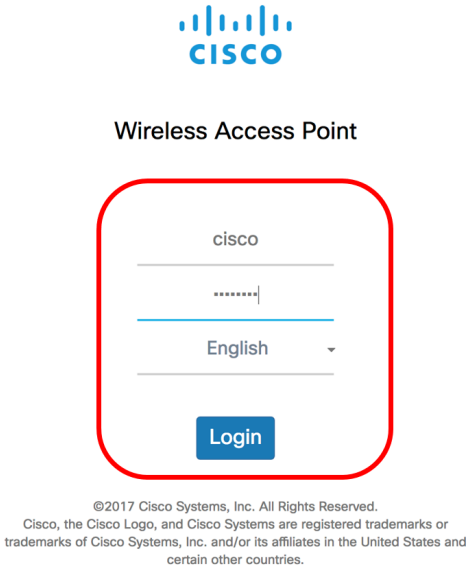
Versão de software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Configurar o suplicante do 802.1X

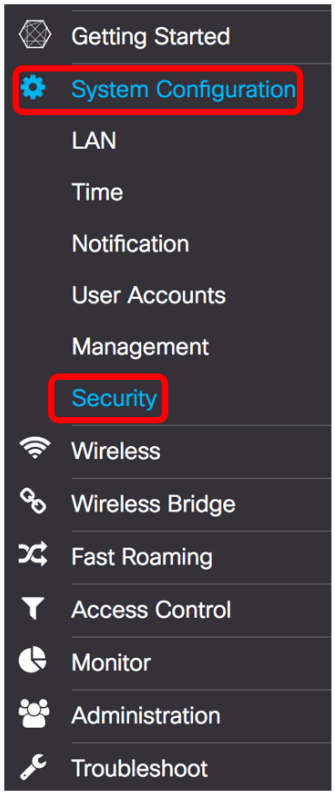
Configurar credenciais do suplicante

Etapa 1. Entre à utilidade com base na Web de seu WAP. O nome de usuário padrão e a senha são Cisco/Cisco.



Nota: Se você tem mudado a senha ou tem criado já uma conta nova, incorpore suas credenciais novas pelo contrário.

Etapa 2. Escolha o **> segurança da configuração de sistema**.

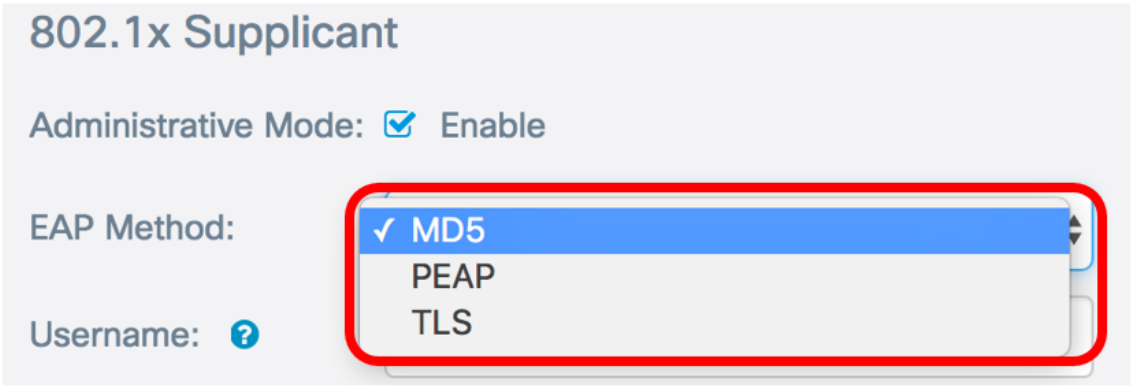


Etapa 3. Verifique a caixa de verificação da **possibilidade** para permitir o modo administrativo. Isto permite o WAP de atuar como o suplicante ao autenticador.

Etapa 4. Escolha o tipo apropriado de método do Extensible Authentication Protocol (EAP) que será usado para cifrar nomes de usuário e senha da lista de drop-down do *método de EAP*. As opções são:

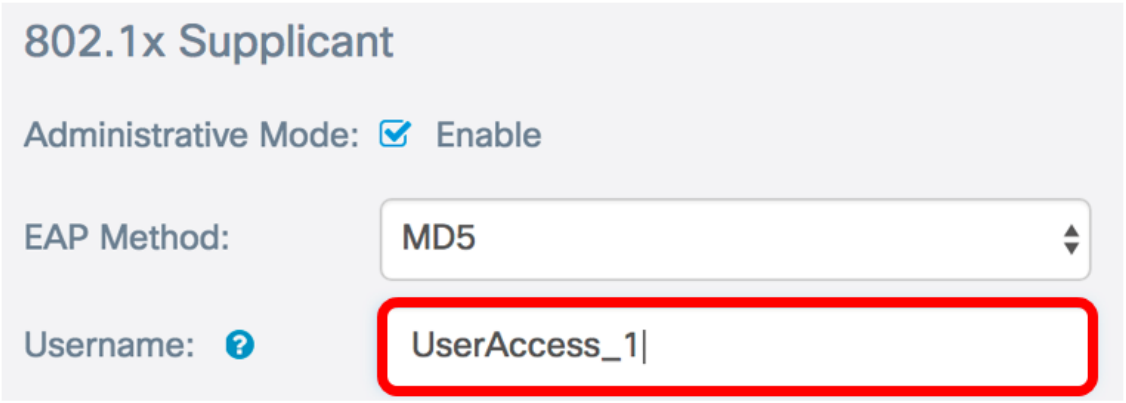
- MD5 — Usa o método de criptografia do 128-bit. O algoritmo MD5 usa um sistema criptográfico público para cifrar dados.
- PEAP — O protocolo extensible authentication protegido (PEAP) autentica clientes do Wireless LAN através dos Certificados digitais emitidos pelo server criando um túnel cifrado SSL/TLS entre o cliente e o Authentication Server.
- TLS — O Transport Layer Security (TLS) é um protocolo que forneça a Segurança e a integridade de dados para uma comunicação sobre o Internet. Assegura-se de que nenhuma terceira parte altere o mensagem original.

Nota: Neste exemplo, o MD5 é usado.

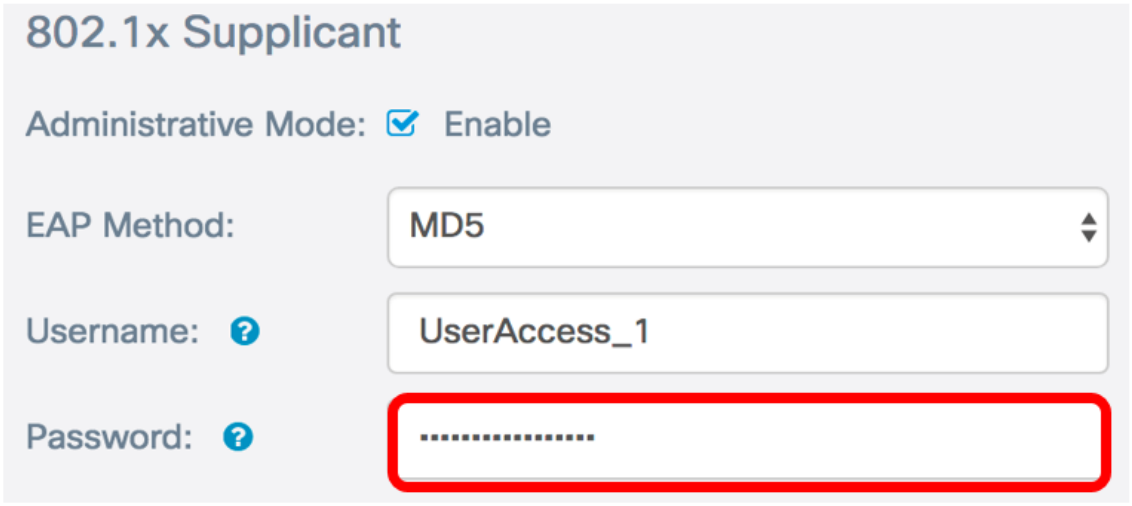


Etapa 5. Incorpore um username ao *campo de nome de usuário*. Este é o username que foi configurado no autenticador e é usado para responder ao autenticador do 802.1X. Pode ser um a 64 caráteres por muito tempo, pode incluir o uppercase e as letras minúsculas, os números, e os caracteres especiais exceto a cotação dobro - marcas.

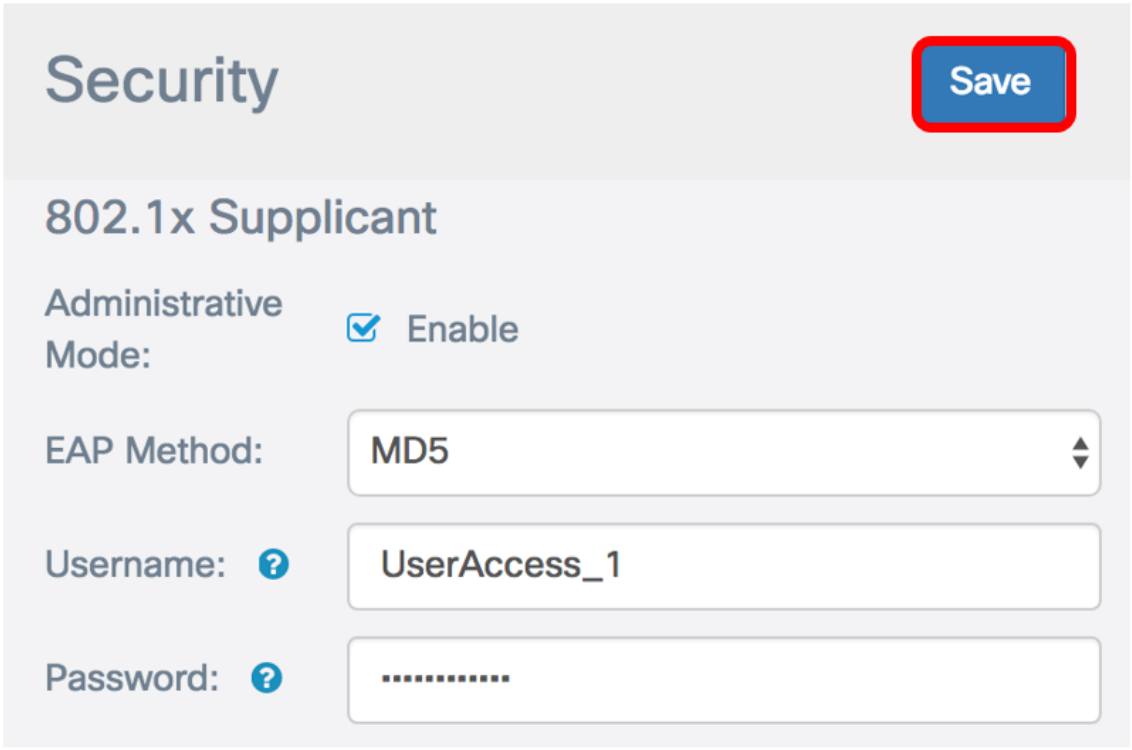
Nota: Neste exemplo, UserAccess_1 é usado.



Etapa 6. Incorpore uma senha associada com o username ao campo de *senha*. Esta senha MD5 é usada para responder ao autenticador do 802.1X. A senha pode ser um a 64 caráteres por muito tempo, pode incluir o uppercase e as letras minúsculas, os números, e os caracteres especiais exceto a cotação - marcas.



Etapa 7. Clique o **botão Save Button** para salvar os ajustes configurados.



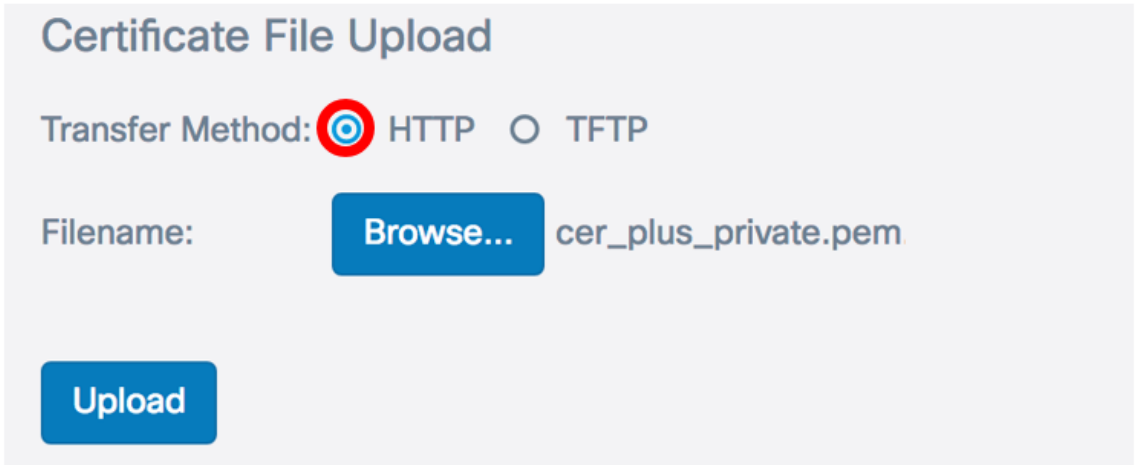
Você deve agora ter configurado ajustes do suplicante do 802.1X no WAP.

Transferência de arquivo pela rede do arquivo certificado

Etapa1. Do método de transferência, escolha um método que o WAP se use para obter o certificado SSL. O certificado SSL é digitalmente um certificado assinado por um Certificate Authority que permita que o navegador da Web tenha uma comunicação segura com o servidor de Web. As opções são:

- HTTP — O certificado é transferido arquivos pela rede com o protocolo hyper text transfer (HTTP) ou através do navegador.
- TFTP — O certificado é transferido arquivos pela rede através de um server do Trivial File Transfer Protocol (TFTP). Se isto é escolhido, salte a etapa 3. Você será exigido incorporar o nome de arquivo e o endereço TFTP.

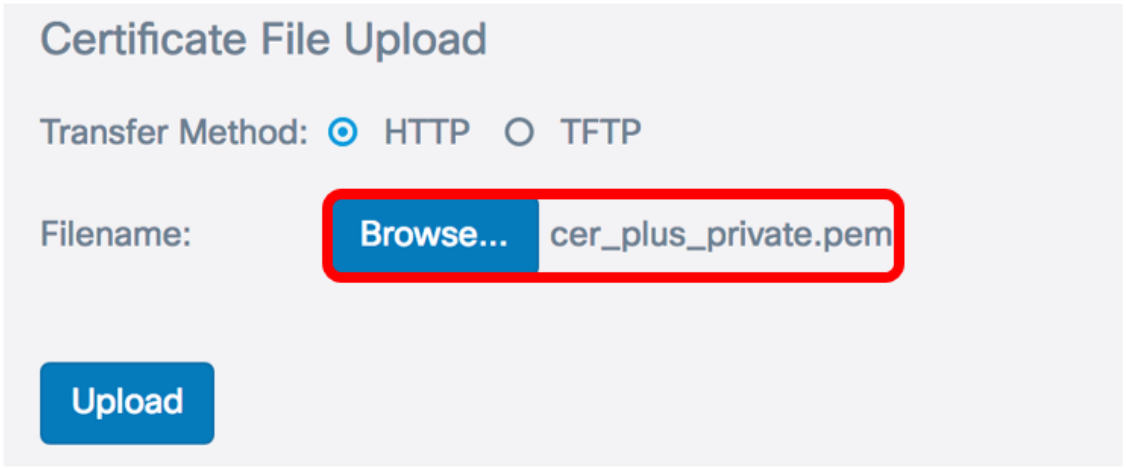
Nota: Neste exemplo, o HTTP é escolhido.



Método de transferência HTTP

Etapa 2. (opcional) se você escolheu o HTTP, clique **consulta…** e escolhe o certificado SSL.

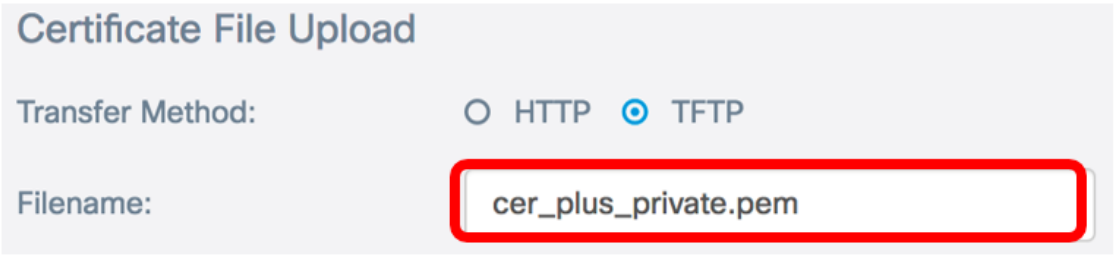
Nota: Neste exemplo, cer_plus_private.pem é usado.



Método de transferência de TFTP

Etapa 3. Se você escolheu o TFTP em etapa 1, dê entrada com o nome do arquivo no campo do nome de arquivo.

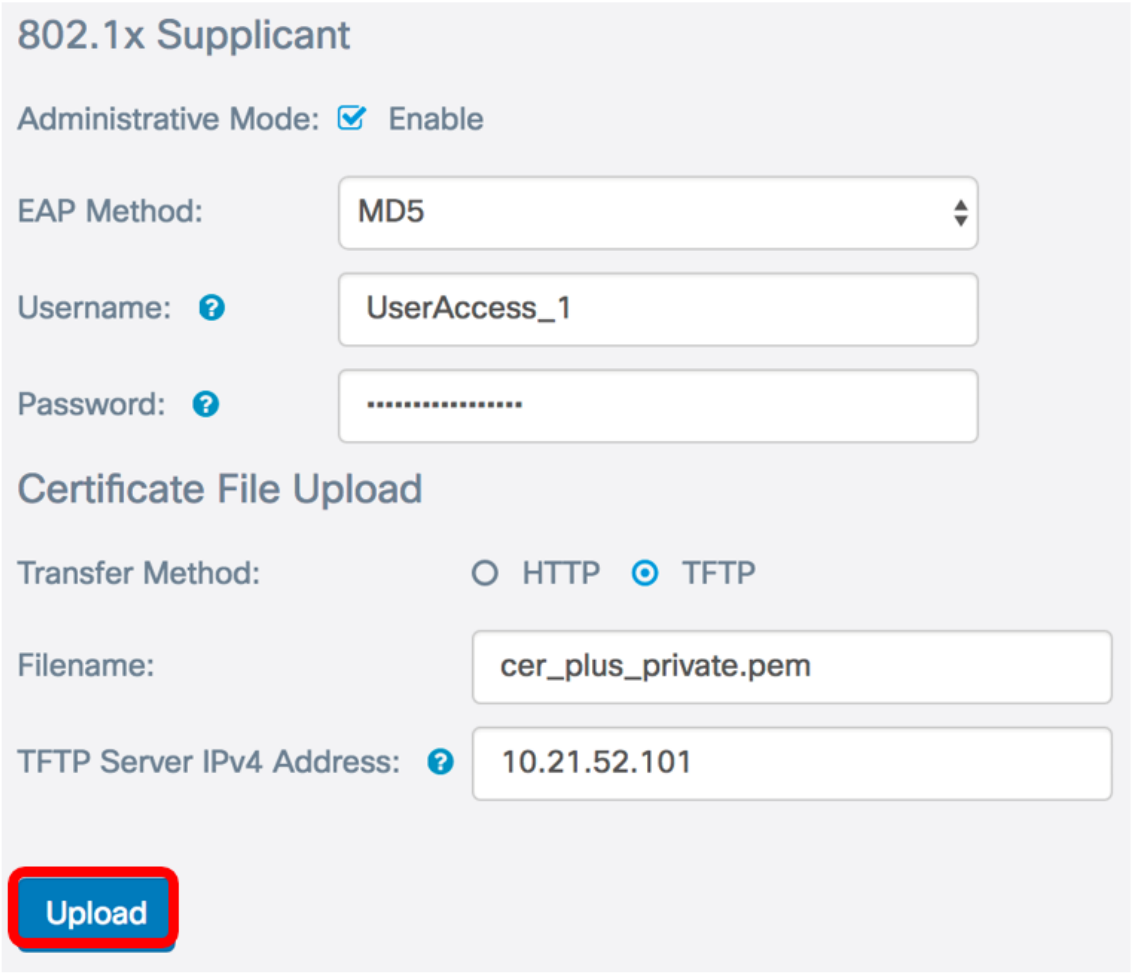
Nota: Neste exemplo, cer_plus_private.pem é usado.



Etapa 4. (opcional) se o TFTP é escolhido como o método de transferência, incorpora o endereço do IPv4 do servidor TFTP ao *campo de endereço do IPv4 do servidor TFTP*. Este é o trajeto que o WAP se usará para recuperar o certificado.

Nota: Neste exemplo, 10.21.52.101 é usado.

Etapa 5. **Transferência de arquivo pela rede do** clique.



Você deve agora com sucesso ter transferido arquivos pela rede um certificado no WAP.