Configurar a autenticação EAP local no Catalyst 9800 WLC

Contents

Introdução

Este documento descreve a configuração de EAP Local em WLCs Catalyst 9800 (Wireless LAN Controllers).

Pré-requisitos

Requisitos

Este documento descreve a configuração do EAP Local (Extensible Authentication Protocol) nas WLCs do Catalyst 9800; isto é, a WLC é executada como servidor de autenticação RADIUS para os clientes sem fio.

Este documento pressupõe que você esteja familiarizado com a configuração básica de uma WLAN na WLC 9800 e se concentra somente na WLC que opera como servidor EAP Local para clientes sem fio.

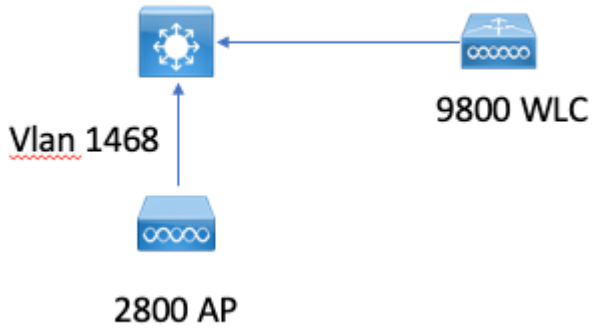
Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Catalyst 9800 na versão 16.12.1s

Configurar

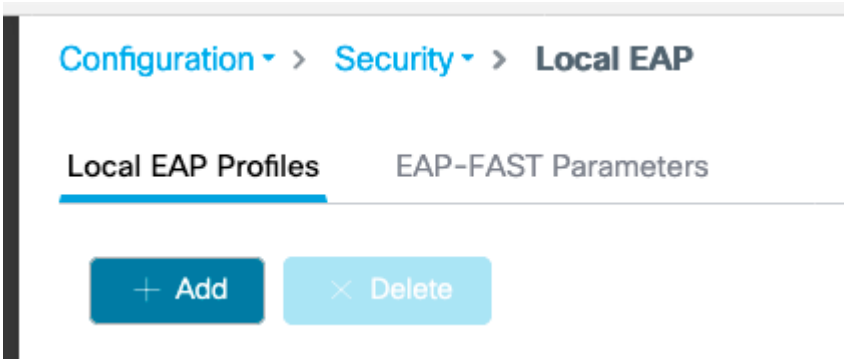
Diagrama de Rede



Configuração principal de EAP local

Etapa 1. Perfil EAP local

Vá para **Configuration > Security > Local EAP** na interface do usuário da Web do 9800.

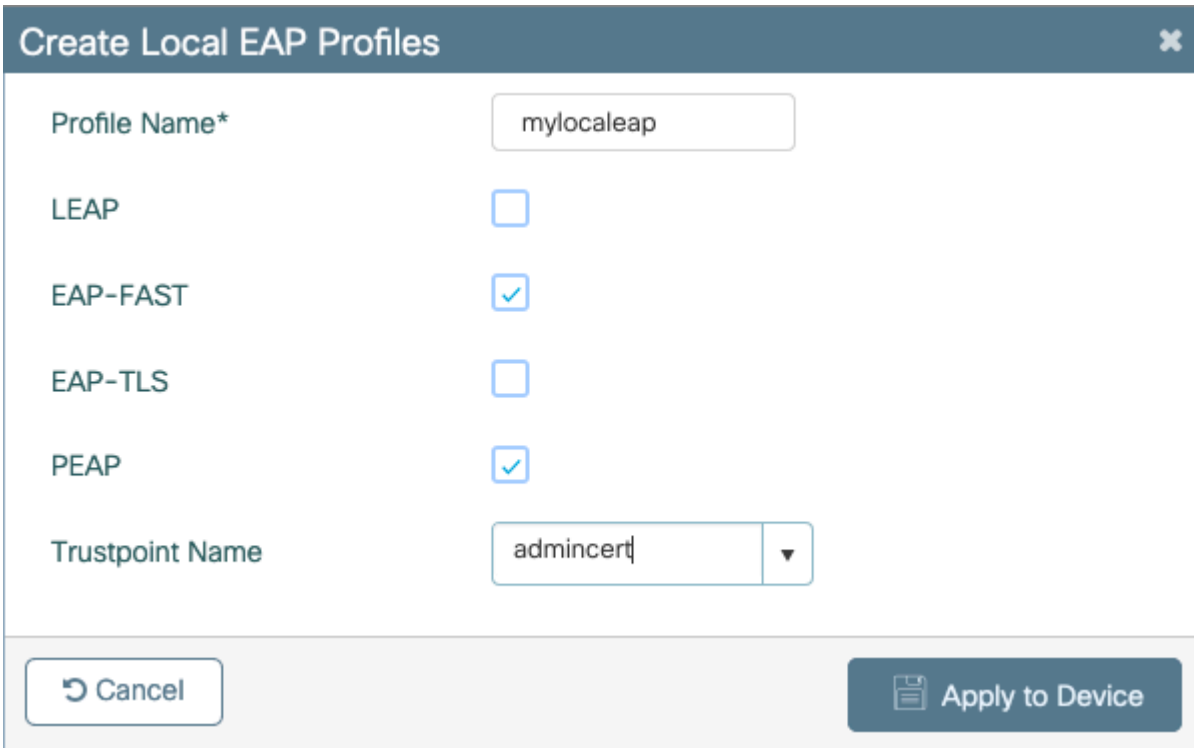


Selecione **Adicionar**

Digite um nome de perfil.

Não é aconselhável usar o LEAP devido à sua segurança fraca. Qualquer um dos outros três métodos EAP exige que você configure um ponto de confiança. Isso ocorre porque o 9800, que atua como autenticador, precisa enviar um certificado para que o cliente confie nele.

Os clientes não confiam no certificado padrão da WLC, portanto, você precisaria desativar a validação do certificado do servidor no lado do cliente (não recomendável) ou instalar um ponto de confiança de certificado na WLC 9800 em que o cliente confia (ou importá-lo manualmente no armazenamento de confiança do cliente).



CLI:

```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Etapa 2. método de autenticação AAA

Você precisa configurar um método AAA dot1x que aponte também localmente para usar o banco de dados local de usuários (mas você pode usar a pesquisa LDAP externa, por exemplo).

Vá para **Configuration> Security > AAA** e vá para a guia **AAA method list** para **Authentication**. Selecione **Adicionar.**

Escolha o tipo "dot1x" e o tipo de grupo local.

Etapa 3. Configurar um método de autorização AAA

Vá para a subguia **Autorização** e crie um novo método para o tipo **credential-download** e aponte-o para local.

Faça o mesmo para o tipo de autorização de **rede**

CLI:

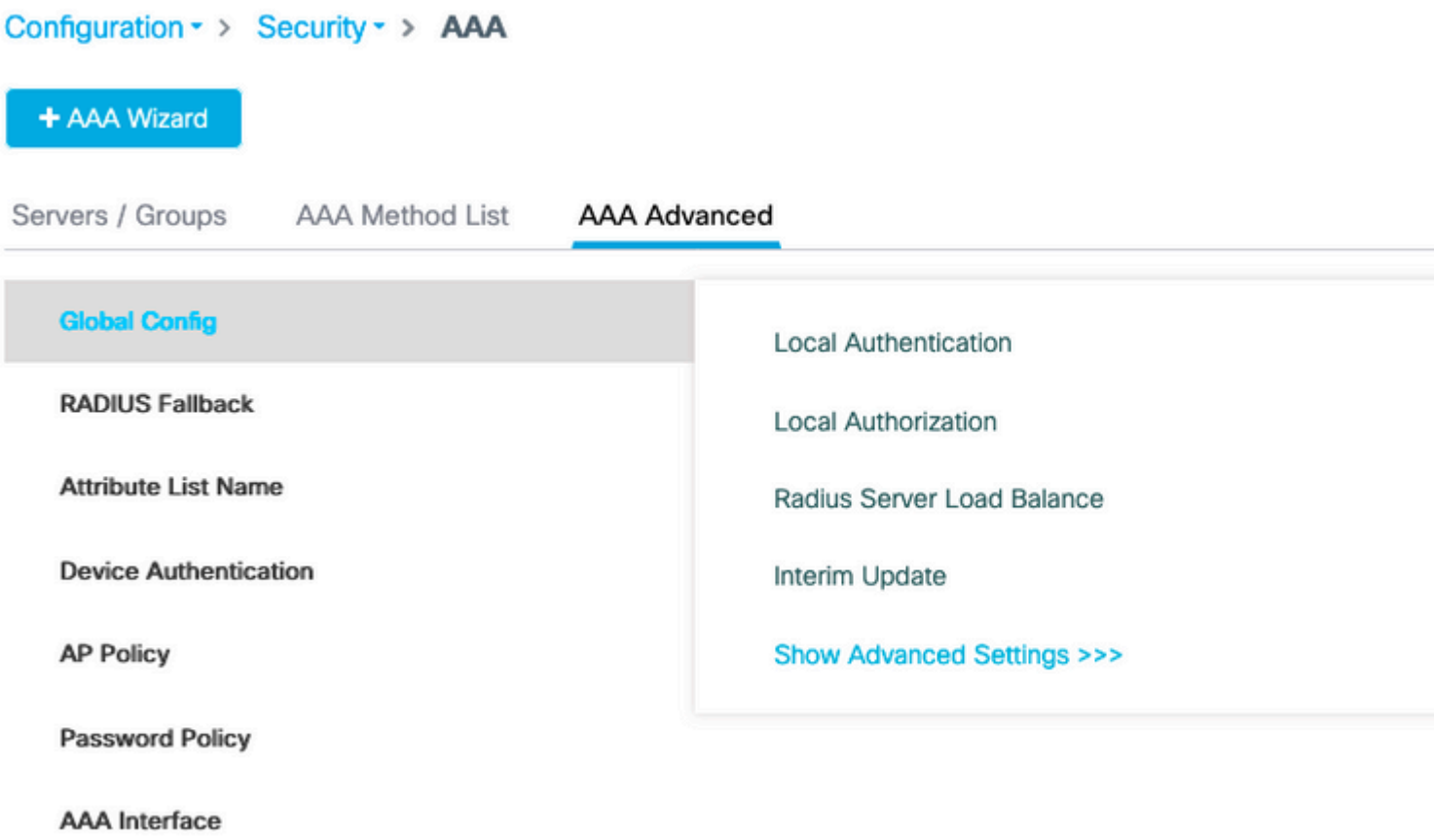
```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

Etapa 4. Configurar métodos locais avançados

Vá para a guia **AAA advanced**.

Defina a autenticação local e o método de autorização. Como esse exemplo usou o método "default" de download de credenciais e o método "Default" dot1x, você precisa definir o padrão para as caixas suspensas de autenticação local e autorização aqui.

Caso você tenha definido métodos nomeados, escolha "lista de métodos" no menu suspenso e outro campo permitirá que você insira o nome do método.



CLI:

```
aaa local authentication default authorization default
```

Etapa 5. Configurar uma WLAN

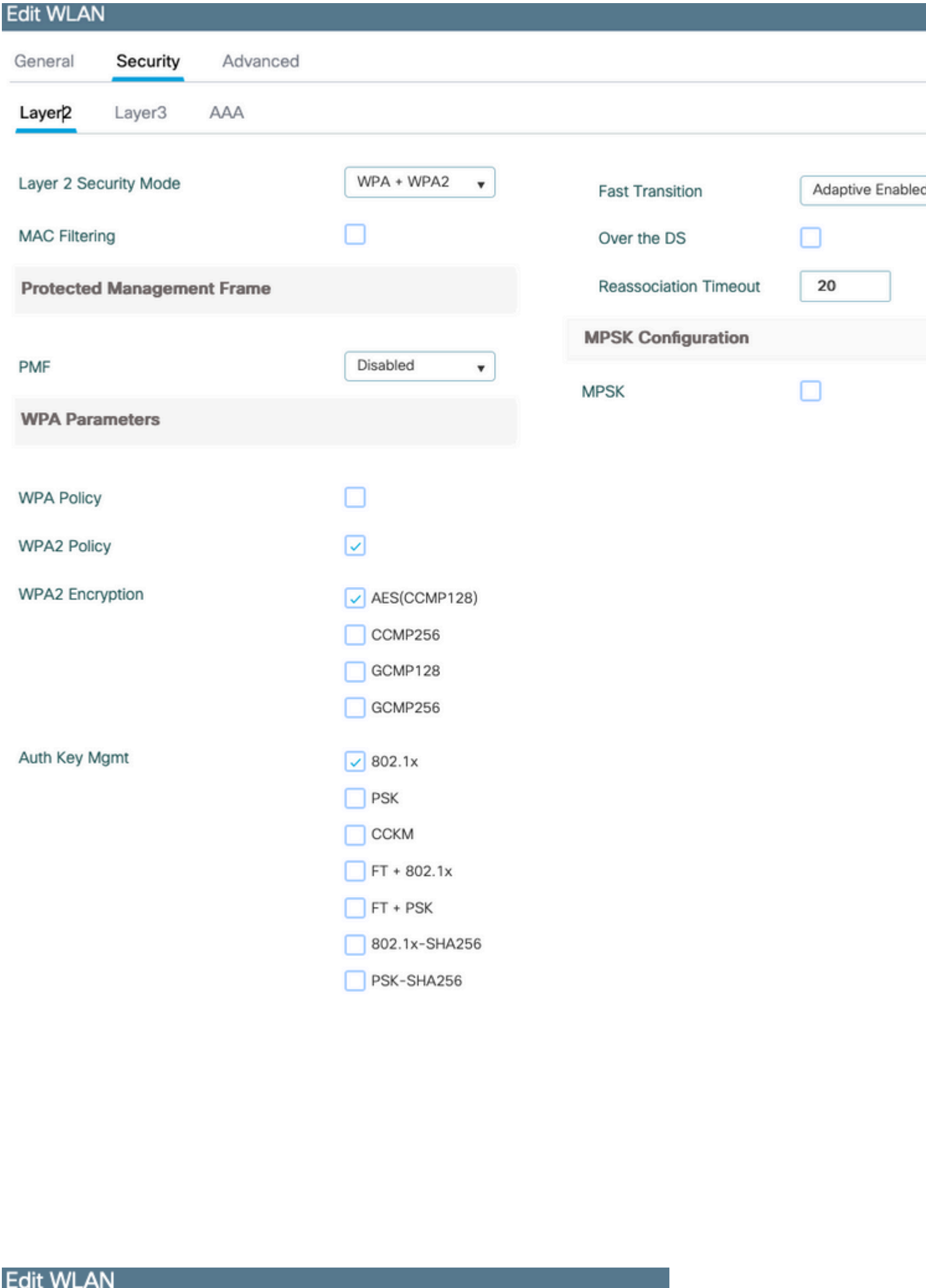
Você pode configurar sua WLAN para segurança 802.1x em relação ao perfil EAP local e ao método de autenticação AAA definidos na etapa anterior.

Vá para Configuration > Tags and Profiles > WLANs > + Add >

Forneça o SSID e o nome do perfil.

A segurança Dot1x é selecionada por padrão na Camada 2.

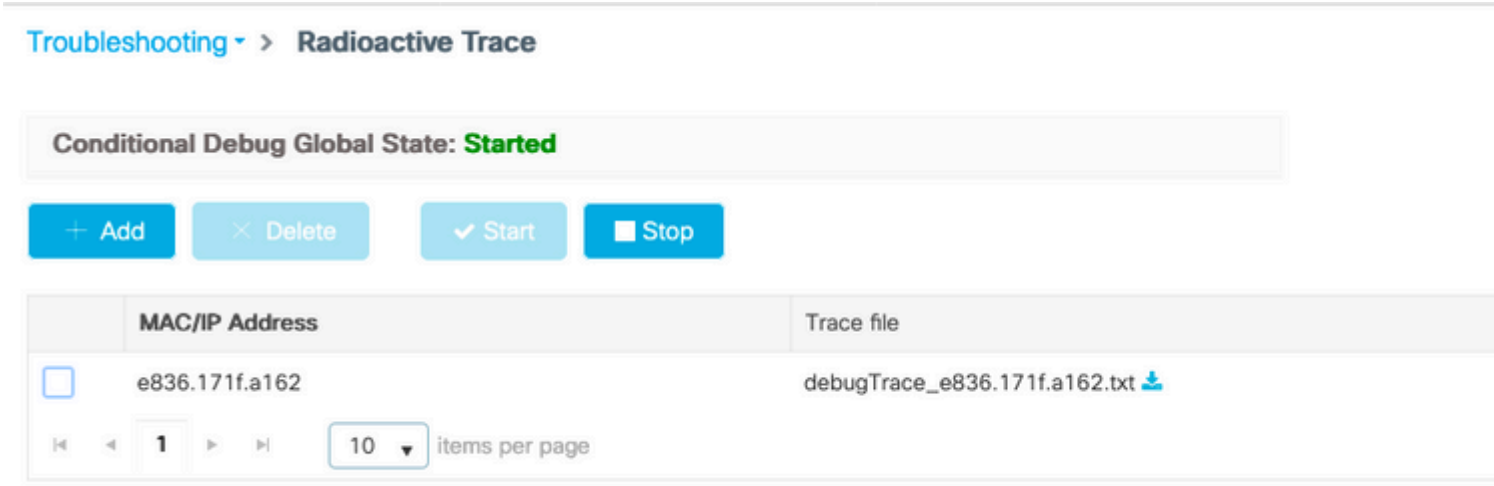
Em AAA, selecione Local EAP Authentication e escolha Local EAP profile e AAA Authentication list no menu suspenso.


Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Adaptive Enabled
Over the DS
Reassociation Timeout
20
MPSK Configuration
MPSK
Edit WLAN

16.12 e versões anteriores suportam apenas TLS 1.0 para autenticação de EAP local, o que pode causar problemas se o seu cliente suportar apenas TLS 1.2, como é cada vez mais a norma. O Cisco IOS® XE 17.1 e posterior suporta TLS 1.2 e TLS 1.0.

Para solucionar problemas de um cliente específico que tenha problemas de conexão, use o RadioActive Tracing. Vá para **Troubleshooting > RadioActive Trace** e adicione o endereço mac do cliente.

Selecione **Start** para ativar o rastreamento para esse cliente.



Depois que o problema for reproduzido, você poderá selecionar o botão **Generate** para produzir um arquivo que contenha a saída de depuração.

Exemplo de um cliente que não consegue se conectar devido a uma senha incorreta

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.785 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAPV
```

```
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sent
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rece
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: m
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAST
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rais
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication failed
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

Rastrear em caso de falha

É possível verificar a lista de eventos de falha para um determinado endereço mac com o comando trace-on-failure, mesmo quando nenhuma depuração está habilitada.

No próximo exemplo, o método AAA estava ausente no início (evento de inatividade do servidor AAA) e, em seguida, o cliente usou credenciais incorretas alguns minutos mais tarde.

O comando é **show logging trace-on-failure summary** na versão 16.12 e anterior e é **show logging profile wireless (filter mac <mac>) trace-on-failure** no **Cisco IOS® XE** 17.1 e posterior. Não há diferença técnica além do 17.1 e posterior, que permite filtrar o endereço mac do cliente.

```
Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 2 ...
sending cmd to chassis 1 ...
Collecting files on current[1] chassis.
# of files collected = 30
Collecting files on current[2] chassis.
# of files collected = 30
Collecting files from chassis 1.
Time                          UUID                 Log

----------------------------------------------------------------------------------------------------


2019/10/30 14:51:04.438     0x0      SANET_AUTHC_FAILURE - AAA Server Down username , audit session id 0
2019/10/30 14:58:04.424     0x0      e836.171f.a162 CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN pr
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.