Entender e configurar o cache AAA para TLS no 9800 WLC

Contents

Introdução

Este documento descreve como entender e configurar o cache AAA em Cisco Catalyst 9800 Wireless LAN Controllers (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos de autenticação AAA, incluindo protocolos RADIUS e EAP
- Fluxos de trabalho de operação e configuração da controladora Wireless LAN (WLC)
- Métodos de autenticação e gerenciamento de certificados 802.1X
- Infraestrutura básica de chave pública (PKI) e processos de assinatura de certificado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador de LAN sem fio Cisco Catalyst 9800 Series
- Software versão 17.18.1 ou posterior (recurso de cache AAA suportado nesta versão)
- Cisco Identity Services Engine (ISE) como servidor AAA/RADIUS
- Dispositivos de acesso à rede compatíveis com 802.1X, EAP-TLS, EAP-PEAP, MAB e iPSK

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.

Informações de Apoio

Os métodos de autenticação, como 802.1X, dependem da comunicação com um servidor de autenticação externo (como um servidor RADIUS). Quando a controladora Wireless LAN (WLC) não consegue alcançar o servidor ou quando o servidor não está disponível, os clientes sem fio não conseguem se conectar ao SSID, levando a interrupções no serviço. A WLC bloqueia o tráfego do cliente até que a autenticação tenha êxito.

A partir da versão 17.18.1, o recurso de cache AAA permite que o Catalyst 9800 WLC autentique clientes sem fio, mesmo que o servidor AAA se torne indisponível usando entradas de autenticação em cache. Isso reduz significativamente a interrupção do serviço durante interrupções do servidor AAA e mantém a conectividade perfeita do cliente.

O mecanismo de cache AAA é suportado quando os Access Points estão operando no modo local ou no modo FlexConnect (autenticação central).

Funcionalidade de cache AAA no Cisco Catalyst 9800 WLC:

- Autenticação inicial (quando o servidor AAA estiver acessível): A WLC encaminha a solicitação de autenticação do cliente para o servidor AAA configurado usando RADIUS. Quando o servidor retorna Access-Accept, a WLC armazena os detalhes de autenticação do cliente localmente em seu cache AAA.
- Reconexão do cliente (quando o servidor AAA não pode ser alcançado): Se um cliente se reconectar antes que sua entrada em cache expire, a WLC consultará seu cache AAA local. Se existirem dados armazenados em cache válidos, o acesso à rede será concedido sem entrar em contato com o servidor AAA.
- Suporte a failover: Se o servidor AAA estiver inacessível devido a problemas ou falhas na rede, a WLC continuará a autenticar os clientes usando dados em cache, garantindo que os usuários autenticados anteriormente mantenham acesso ininterrupto.
- Tempo de vida e expiração do cache: As entradas no cache AAA são temporárias e configuráveis. A duração padrão do cache é de 24 horas; definir o temporizador como 0 faz com que as entradas nunca expirem. Se um cliente se reconecta após a expiração de sua entrada de cache, a WLC tenta acessar o servidor AAA para autenticação.

```
VK-WLC#show aaa cache group VK-SRV-GRP all
----------------------------------------------------------------
 IOSD AAA Auth Cache entries:

 Entries in Profile dB VK-SRV-GRP for exact match:
No entries found in Profile dB
----------------------------------------------------------------

  SMD AAA Auth Cache Entries:

 Total number of Cache entries is 0

 WNCD AAA Auth Cache entries:

MAC ADDR:                       C4E9.0A00.B1B0
Profile Name:                   VK-CACHE
User Name:                      vk@wireless.com
Timeout:                        28800
Created Timestamp :             09/18/25 15:28:54 UTC
Server IP Address:              10.106.37.159
```

Os tipos de autenticação suportados para o cache AAA incluem:

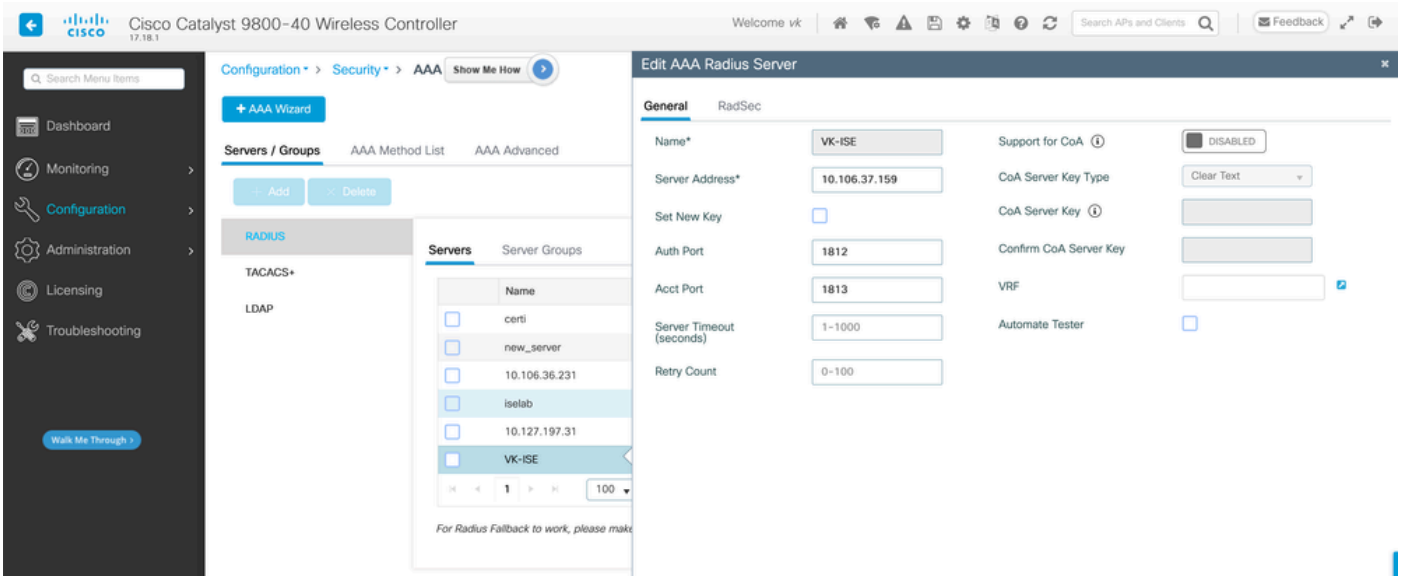
- EAP-TLS
- EAP-PEAP com MSCHAPv2
- MAC Authentication Bypass (MAB), MAB+PSK e MAB+802.1x/iPSK

Configurar

Passo 1: Adicionar servidor AAA no WLC

Comece adicionando seu servidor AAA (RADIUS) ao Wireless LAN Controller. Isso pode ser feito por meio da GUI ou da CLI.

Método GUI: Navegue para Configuration > Security > AAA e adicione seu servidor.



Método CLI:

```
radius server VK-ISE
 address ipv4 10.106.37.159 auth-port 1812 acct-port 1813
 key Cisco123
```

Este comando cria uma entrada de servidor RADIUS chamada VK-ISE com o endereço IP, a porta de autenticação, a porta de relatório e a chave compartilhada especificados.

Passo 2: Criar perfil de cache AAA (somente CLI)

Crie um perfil de cache AAA para definir o comportamento do cache. Esta etapa é somente CLI.

```
aaa cache profile VK-CACHE all
```

Esse comando cria um perfil de cache chamado VK-CACHE e habilita o cache para todos os tipos de autenticação suportados.

Passo 3: Criar grupo de servidores e mapear o servidor RADIUS e o perfil de cache (somente CLI)

Crie um grupo de servidores RADIUS, associe o servidor AAA, configure a expiração do cache e mapeie perfis de autorização/autenticação.

```
aaa group server radius VK-SRV-GRP
 server name VK-ISE
 cache expiry 8
 cache authorization profile VK-CACHE
 cache authentication profile VK-CACHE
 deadtime 5
radius-server dead-criteria time 5 tries 5
```

Este conjunto de comandos:

- Cria um grupo de servidores chamado VK-SRV-GRP
- Associa o servidor VK-ISE
- Define a expiração do cache para 8 horas
- Mapeia perfis de autorização e autenticação para VK-CACHE
- Define o tempo limite para servidores inacessíveis como 5 minutos e critérios inativos para lógica de repetição

Passo 4: Criar métodos de autenticação e autorização

Defina listas de métodos para autenticação e autorização, especificando o uso do grupo de servidores e do cache.

```
aaa authentication dot1x default group VK-SRV-GRP cache VK-SRV-GRP
aaa authorization network default group VK-SRV-GRP cache VK-SRV-GRP
aaa local authentication default
authorization default
aaa authorization credential-download default cache VK-SRV-GRP
```

Esses comandos configuram listas de métodos padrão para autenticação 802.1X e autorização de rede, priorizando o cache e o grupo de servidores.

Se você quiser que o WLC verifique o cache primeiro antes de tentar o servidor RADIUS (para uma autenticação mais rápida se o usuário já estiver em cache), use:

```
aaa authentication dot1x default cache VK-SRV-GRP group VK-SRV-GRP
aaa authorization network default cache VK-SRV-GRP group VK-SRV-GRP
```

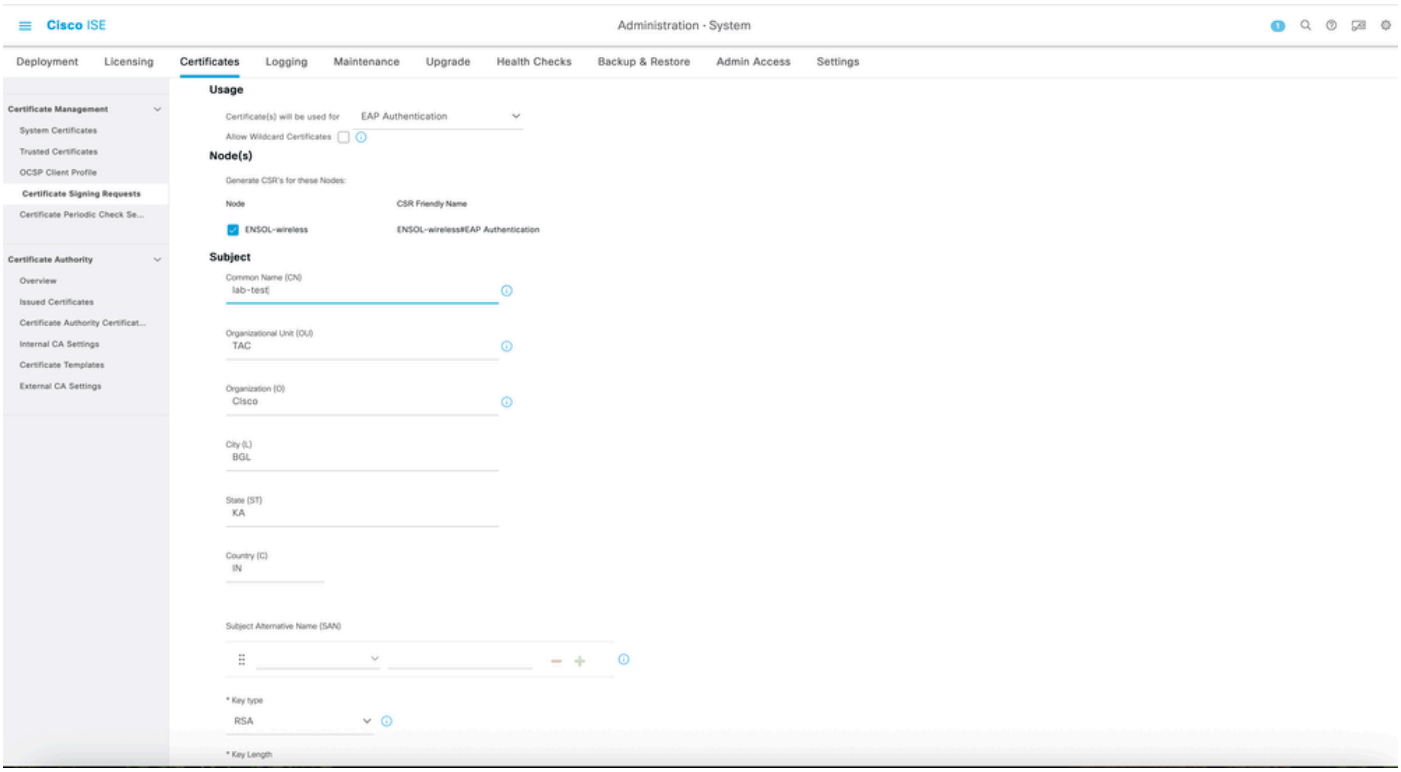
Com essas listas de métodos, a WLC consulta o cache primeiro, entrando em contato com o servidor somente se o usuário não for encontrado no cache, resultando em uma autenticação mais rápida para clientes em cache.

Passo 5: Configurar autenticação TLS (Configuração de certificado)

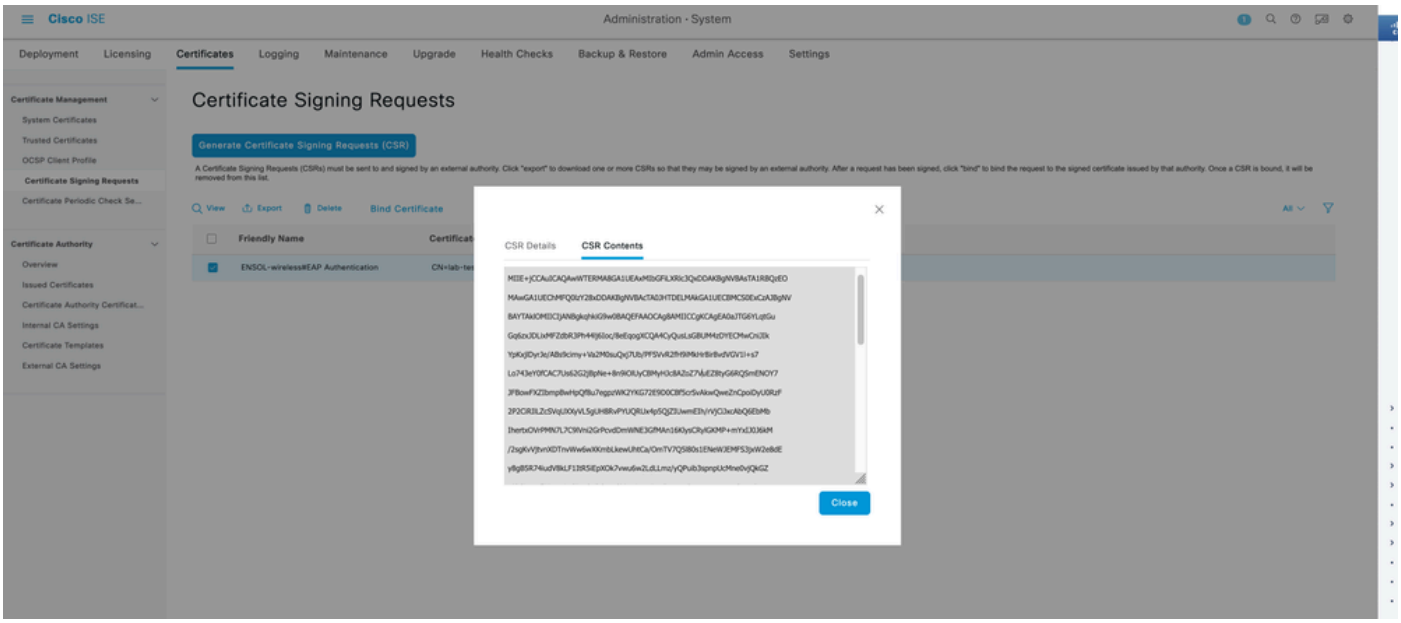
Para a autenticação EAP-TLS, o servidor WLC e AAA exigem certificados de servidor assinados por uma CA (Autoridade de Certificação).

No Cisco ISE (servidor AAA):

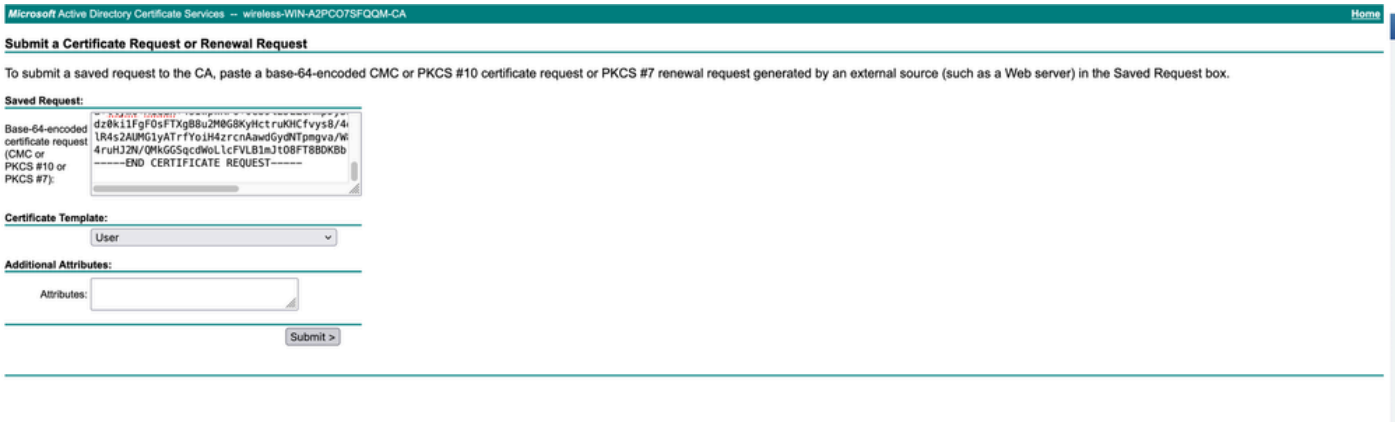
- Gere uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado) via Certificados > Gerenciamento de certificado > Solicitações de assinatura de certificado



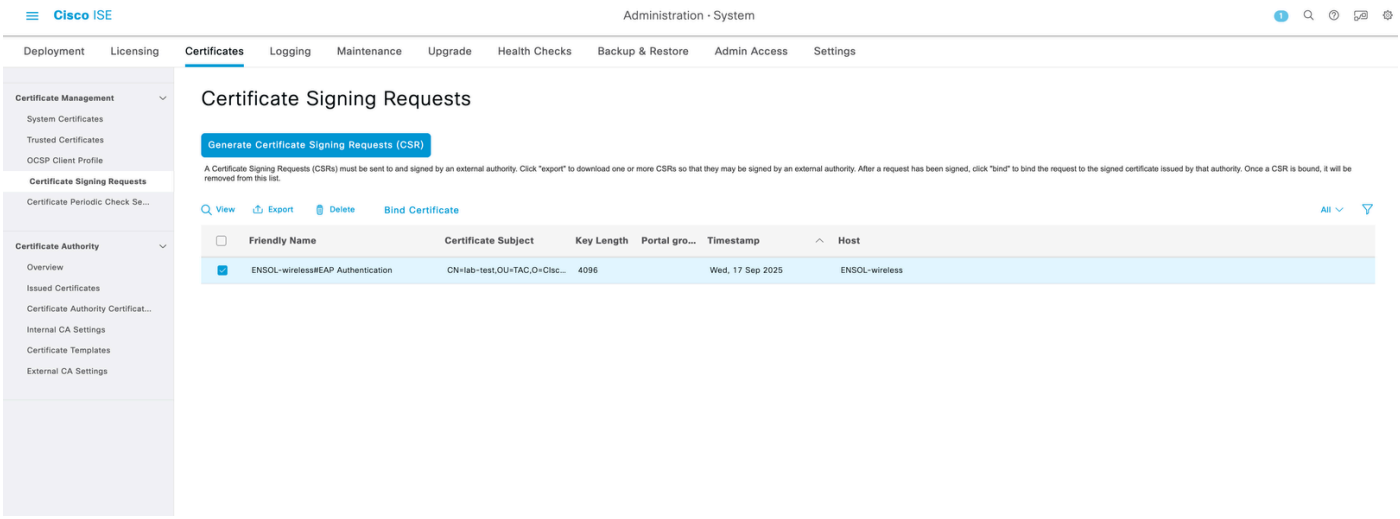
- Copie o conteúdo de CSR e assine-o pela sua CA

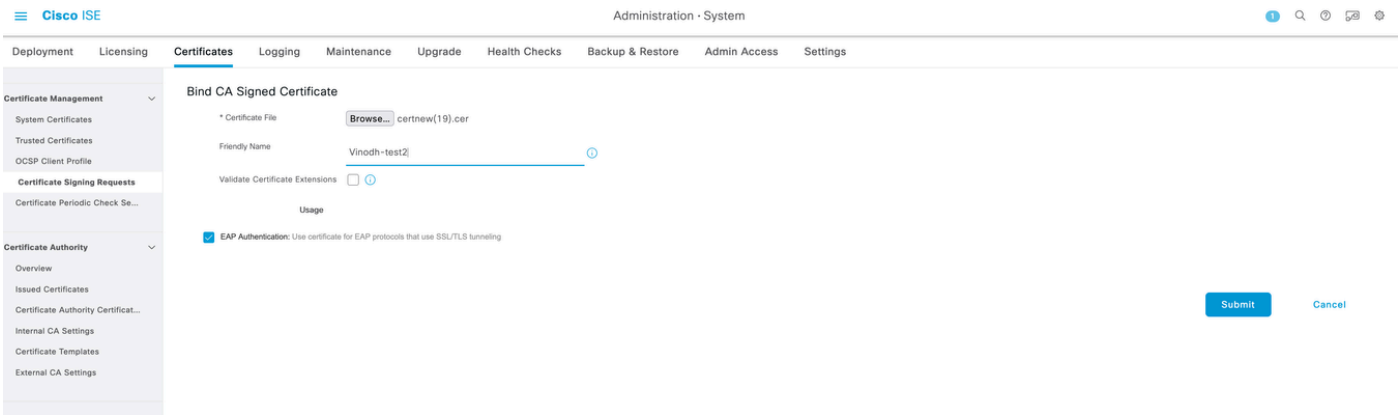


- Faça o download do certificado assinado (no formato .cer ou .pem)

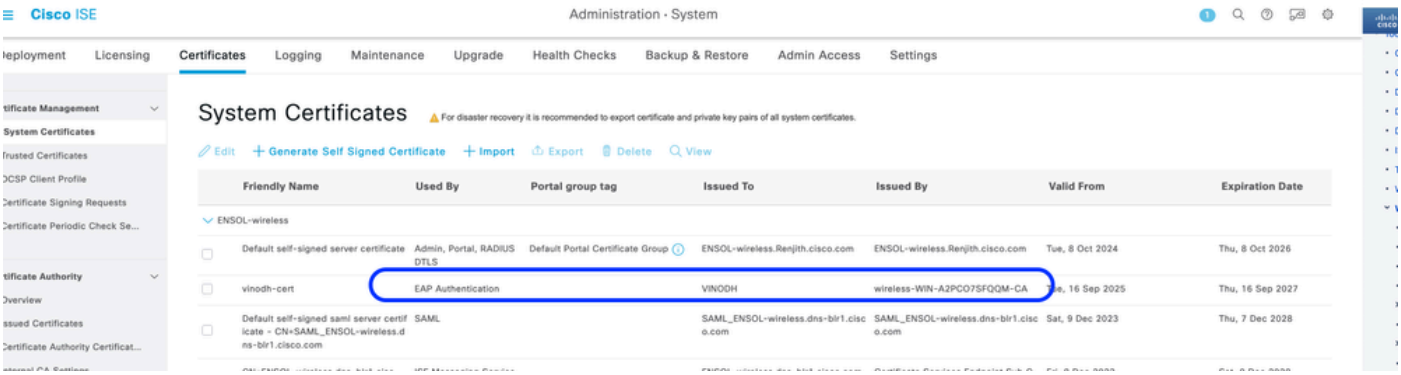


- Vincule o certificado no ISE navegando até o arquivo de certificado assinado e clicando em "Enviar"



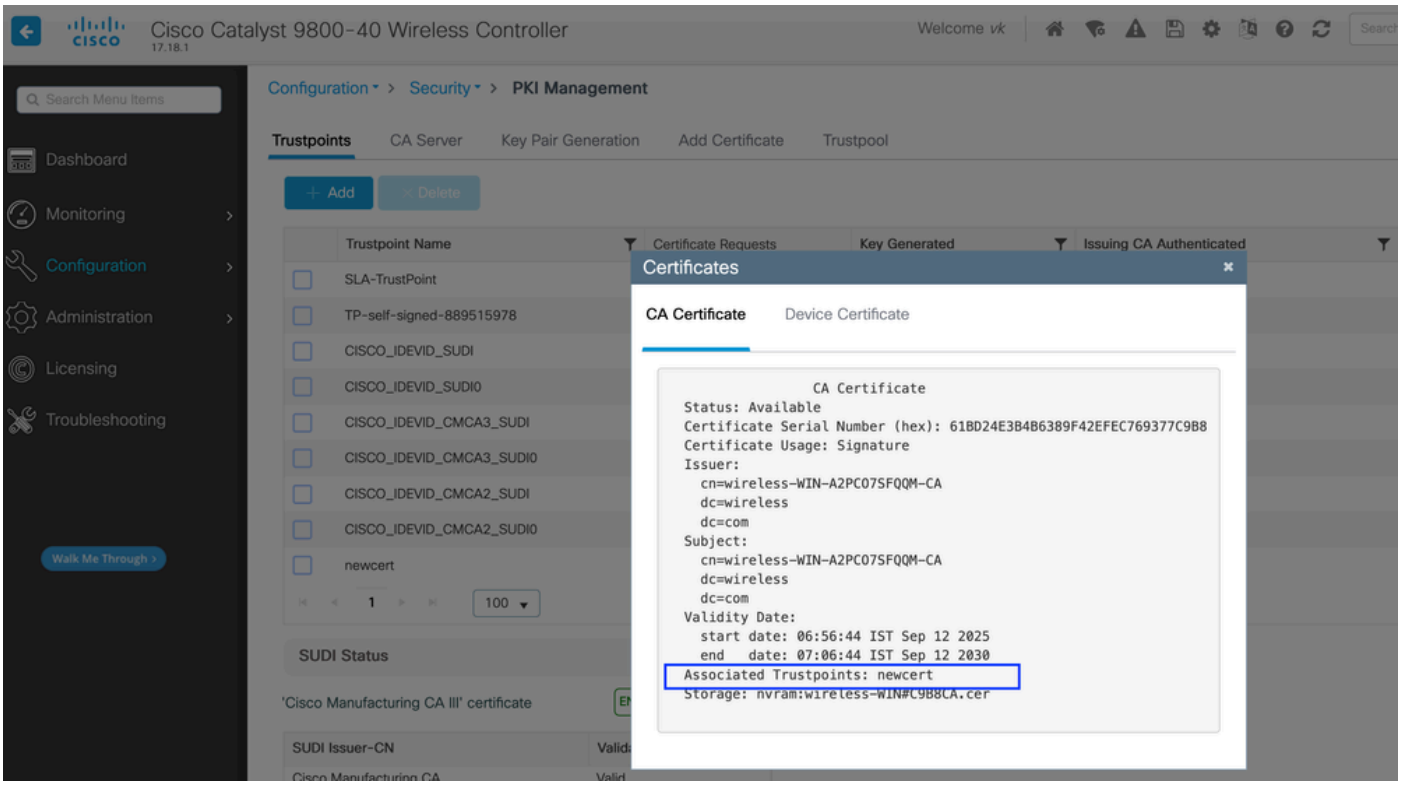


- Verifique se o certificado assinado está refletido no certificado do sistema para autenticação EAP



No Cisco Catalyst 9800 WLC:

- Gerar um CSR no WLC
- Obter a assinatura do CSR pela mesma CA usada para o ISE
- Carregar o certificado assinado para o WLC



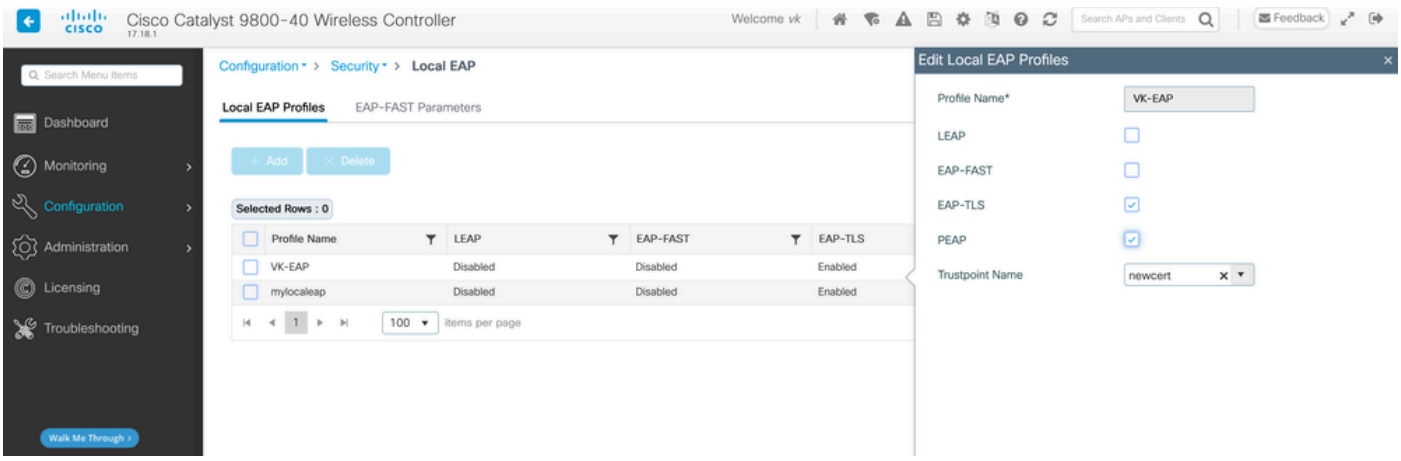
Passo 6: Criar perfil EAP local e mapear ponto de confiança

Crie um perfil EAP local e mapeie o ponto de confiança para a autenticação EAP-TLS.

```
eap profile VK-EAP
 method tls
 pki-trustpoint newcert
```

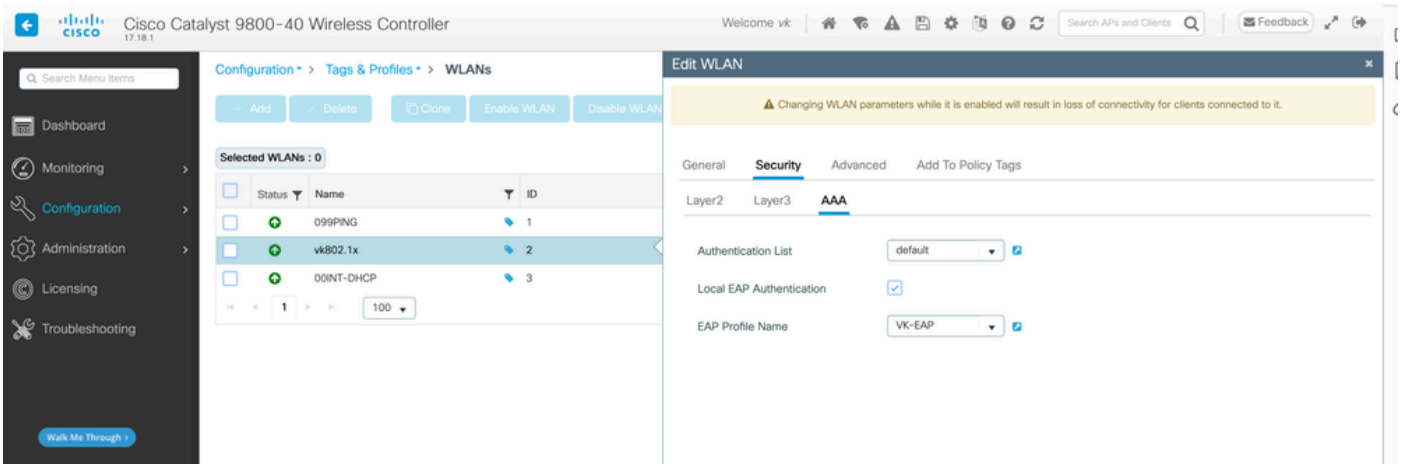
Esse comando cria um perfil EAP chamado VK-EAP usando EAP-TLS e mapeia o ponto de confiança para o certificado chamado newcert.

Método GUI: Navegue até Configuration > Security > Local EAP e crie o perfil EAP.



Passo 7: Aplicar lista de métodos e perfil EAP ao SSID

Configure seu SSID para usar a autenticação criada e o perfil EAP.



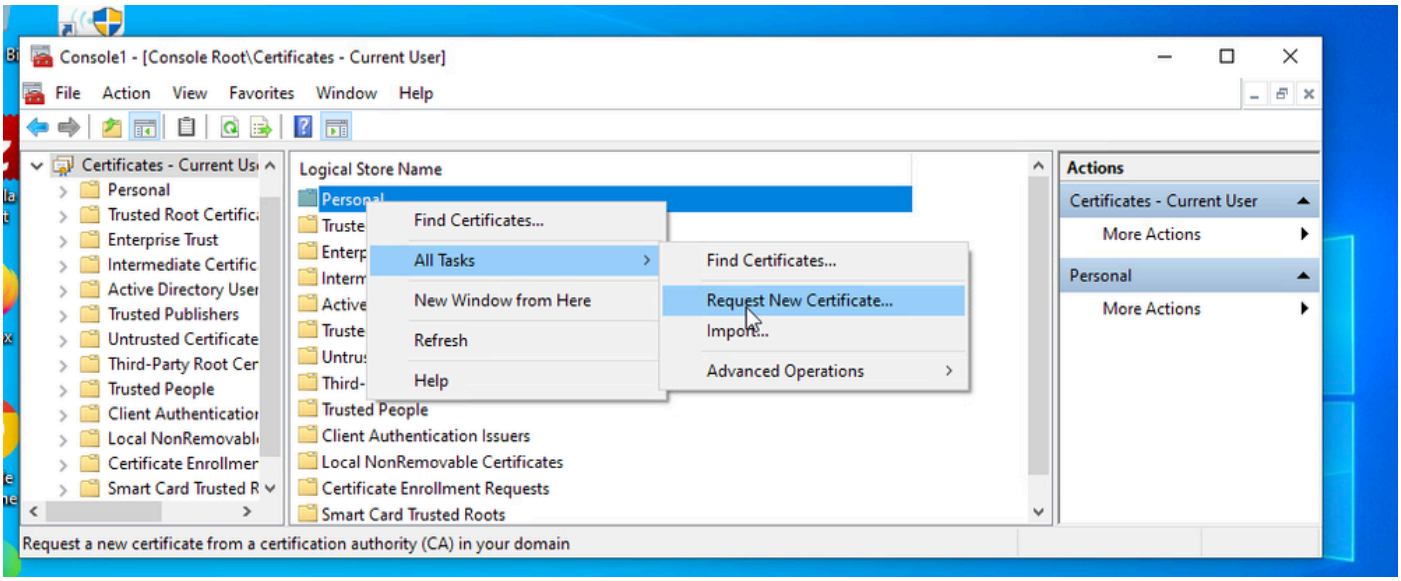

```
wlan vk802.1x 2 vk802.1x
 local-auth VK-EAP
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list default
 no shutdown
```

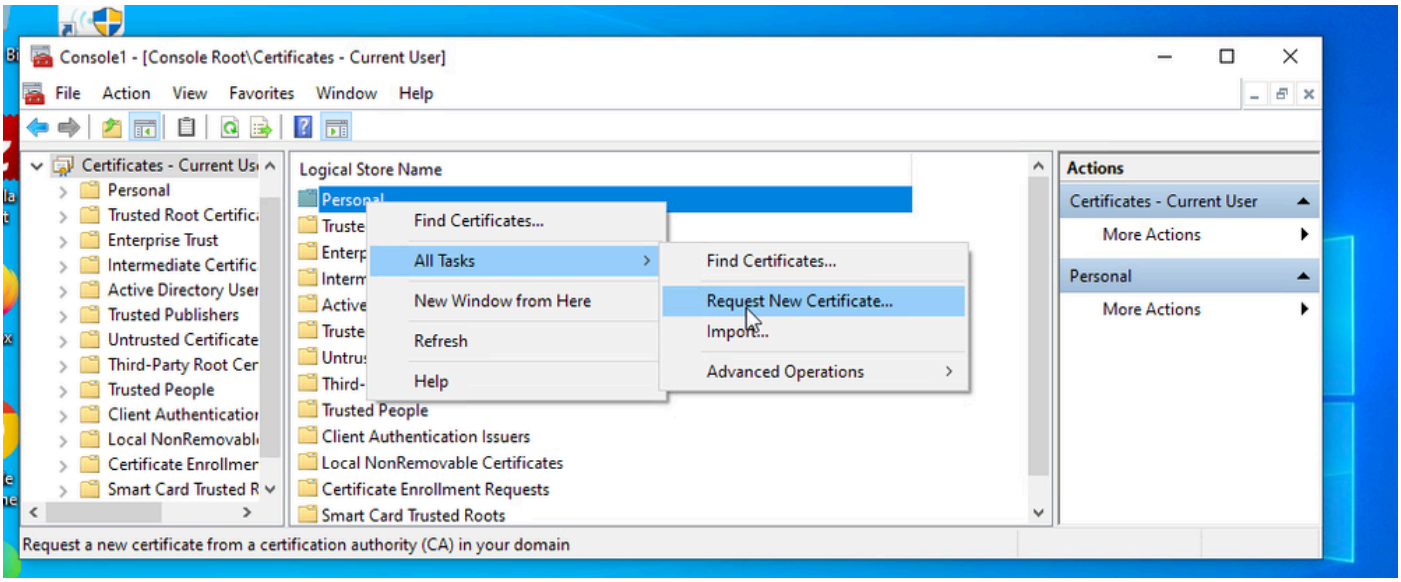
Esta configuração:

- Cria SSID vk802.1x com WLAN ID 2
- Habilita a autenticação local com o perfil VK-EAP
- Aplica políticas de rádio para faixas de 2,4 GHz e 5 GHz
- Aplica a autenticação 802.1X usando a lista de métodos padrão
- Ativa o SSID (sem desligamento)

Passo 8: Implantação de certificado do usuário em clientes sem fio

Certifique-se de que os clientes sem fio tenham o certificado de usuário necessário para a autenticação. Para ambientes de laboratório, um dispositivo associado a um domínio do Ative Diretory (AD) pode receber o certificado via MMC (Microsoft Management Console). Há outros métodos para distribuir certificados, dependendo do seu ambiente.





Verificar

Você pode verificar as entradas de cache AAA na WLC 9800 usando comandos CLI. Observe que para as WLCs do Catalyst 9800, as entradas de cache são listadas em "WNCD AAA Auth Cache entries", não em "SMD AAA Auth Cache entries".

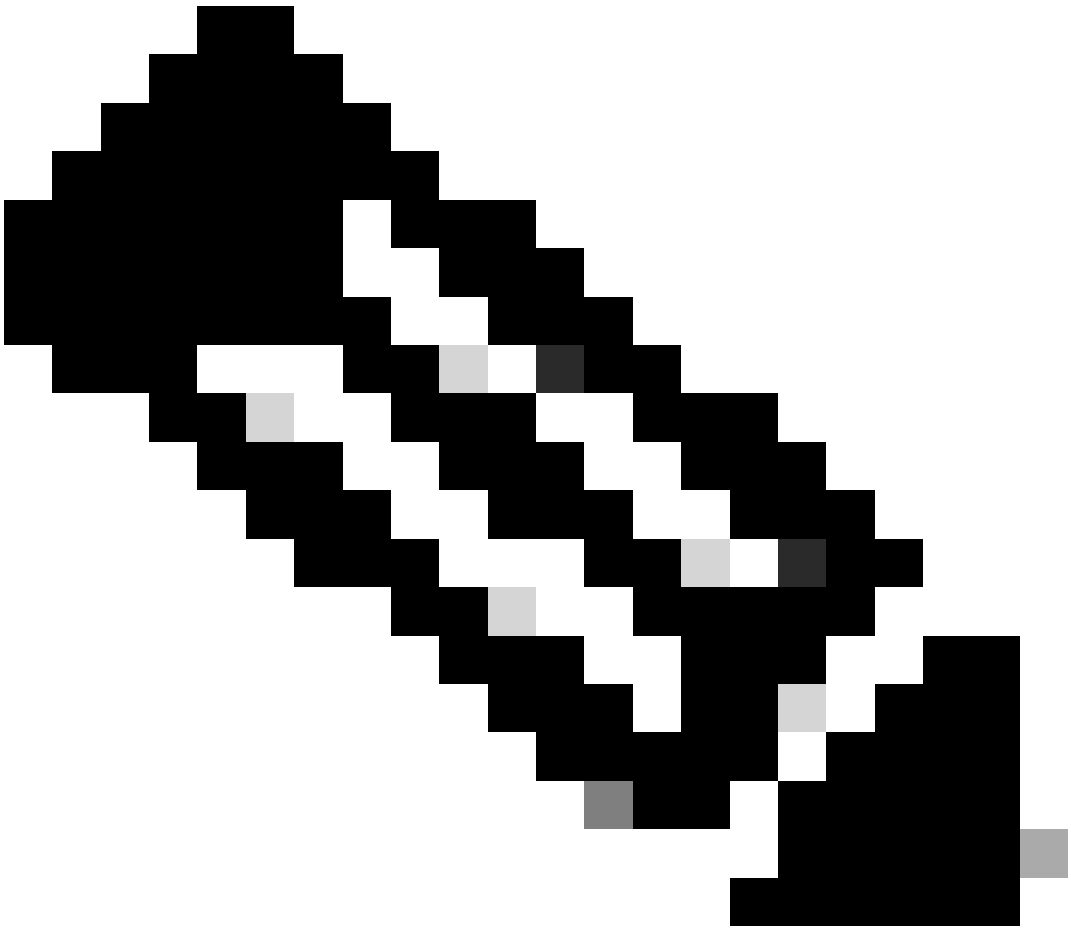
```
show aaa cache group <Server Group> all
```

Esse comando exibe as entradas de cache AAA atuais armazenadas no WLC. Saída de exemplo:

```
WNCD AAA Auth Cache entries
---------------------------
Client MAC: 00:11:22:33:44:55
SSID: vk802.1x
User: user@domain.com
```

```
Cache Expiry: 8h
Auth Method: EAP-TLS
...
```

Verifique se os clientes podem se reconectar e se são autenticados através do cache AAA quando o servidor AAA não está disponível.



Note: Para a autenticação PEAP , o projeto atual requer o retorno de pares Cisco AV que contenham o nome de usuário e o hash de credencial para cada usuário durante a autenticação pelo servidor Radius.

cisco-av-pair = AS-Username=testuser

cisco-av-pair = AS-Credential-Hash=F2E787D376CBF6D6DD3600132E9C215D

Cada usuário deve ser configurado com os atributos do par AV no RADIUS.

A senha ou AS-Credential-Hash deve estar no formato NT-hash

(https://codebeautify.org/ntlm-hash-generator).

Troubleshooting

A identificação e solução de problemas de autenticação e cache AAA envolve várias etapas:

Passo 1: Verificar Entradas de Cache AAA

```
show aaa cache group <Server Group> all
```

Verifique se as entradas esperadas do cliente estão presentes no cache.

Passo 2: Validar a Instalação de Certificados e Pontos Confiáveis

```
show crypto pki trustpoints
show crypto pki certificates
```

Certifique-se de que os certificados estejam corretamente instalados e mapeados para os pontos de confiança apropriados para a autenticação EAP-TLS.

Passo 3: Confirmar listas de métodos de autenticação

```
show running-config | include aaa authentication
show running-config | include aaa authorization
```

Valide se as listas de métodos fazem referência ao grupo de servidores e aos perfis de cache corretos.

Passo 5: Verificar rastreamento interno de RA

<#root>

```
2025/09/18 13:02:37.069850424 {wncd_x_R0-0}{2}: [radius] [16292]: (ERR): RADIUS/DECODE: No response fro
2025/09/18 13:02:37.069850966 {wncd_x_R0-0}{2}: [radius] [16292]: (ERR): RADIUS/DECODE: Case error(no r
2025/09/18 13:02:37.069853220 {wncd_x_R0-0}{2}: [aaa-sg-ref] [16292]: (debug): AAA/SG: Server group wra
2025/09/18 13:02:37.069853836 {wncd_x_R0-0}{2}: [aaa-sg-ref] [16292]: (debug): AAA/SG: Server group ref
2025/09/18 13:02:37.069855784 {wncd_x_R0-0}{2}: [aaa-sg-cache] [16292]: (debug): AAA/AUTHEN/CACHE: Don'
2025/09/18 13:02:37.069856826 {wncd_x_R0-0}{2}: [aaa-svr] [16292]: (debug): AAA SRV(00000000): protocol
2025/09/18 13:02:37.069860954 {wncd_x_R0-0}{2}: [aaa-authen] [16292]: (debug): MAC address in AAA reque
```

2025/09/18 13:02:37.069864992 {wncd_x_R0-0}{2}: [aaa-svr] [16292]: (debug): AAA SRV(00000000): Authen me

2025/09/18 13:02:37.069868198 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Add message event
2025/09/18 13:02:37.069875634 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Evmgr message even
2025/09/18 13:02:37.069876688 {wncd_x_R0-0}{2}: [wncd_0] [16292]: (debug): Sanet eventQ: AAA_CACHE_EVEN

2025/09/18 13:02:37.069887794 {wncd_x_R0-0}{2}: [aaa-prof] [16292]: (debug): AAA/PROFILE/DB: Find - Four
2025/09/18 13:02:37.069955264 {wncd_x_R0-0}{2}: [aaa-sg-cache] [16292]: (debug): AAA/AUTHEN/CACHE(00000

this indiates that cache/local auth is being used

2025/09/18 13:02:37.070019998 {wncd_x_R0-0}{2}: [wncd_0] [16292]: (debug): AAA Local EAP(1419) Sending
2025/09/18 13:02:37.070022944 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Add message event

2025/09/18 13:02:37.070025886 {wncd_x_R0-0}{2}: [aaa-sg-cache] [16292]: (debug): AAA/AUTHEN/CACHE(00000

2025/09/18 13:02:37.070028162 {wncd_x_R0-0}{2}: [ewlc-infra-evmgr] [16292]: (debug): Evmgr message even

Referências:

[17.18 Guia de configuração de software]

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.