

Configurar Verificar e Solucionar Problemas de Web Auth em Falha de Filtro Mac

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar parâmetros da Web](#)

[Configurar Perfil de Política](#)

[Configurar o perfil da WLAN](#)

[Defina as configurações de AAA:](#)

[Configuração do ISE:](#)

[Verificar](#)

[Configuração do controlador](#)

[Estado da política do cliente no controlador](#)

[Troubleshooting](#)

[Coleta de traços radioativos](#)

[Capturas de pacotes incorporados:](#)

[Artigo relacionado](#)

Introdução

Este documento descreve como Configurar, Solucionar Problemas e Verificar a Autenticação da Web Local no recurso "Falha do Filtro Mac" usando o ISE para autenticação externa.

Pré-requisitos

Configurar o ISE para autenticação MAC

Credenciais de usuário válidas configuradas no ISE/Active Directory

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

Entendimento básico para navegar pela interface do usuário da Web do controlador

Configuração de Política, perfil de WLAN e Marcas de Política

Configuração da política de serviço no ISE

Componentes Utilizados

9800 WLC versão 17.12.2

AP AXI C9120

9300 switch

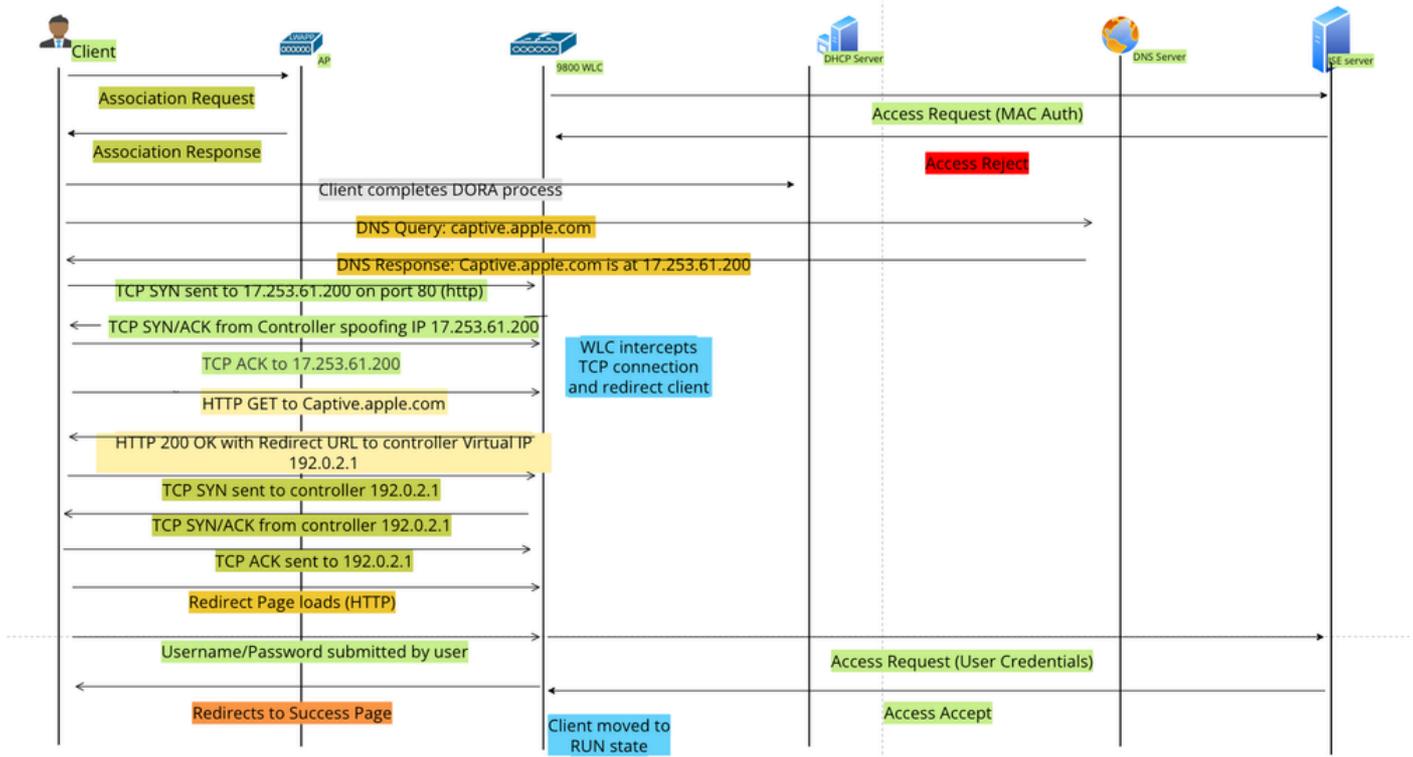
Versão do ISE 3.1.0.518

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

O recurso Web Auth "On Mac Failure Filter" serve como um mecanismo de retorno em ambientes WLAN que usam tanto a Autenticação MAC quanto a Autenticação da Web.

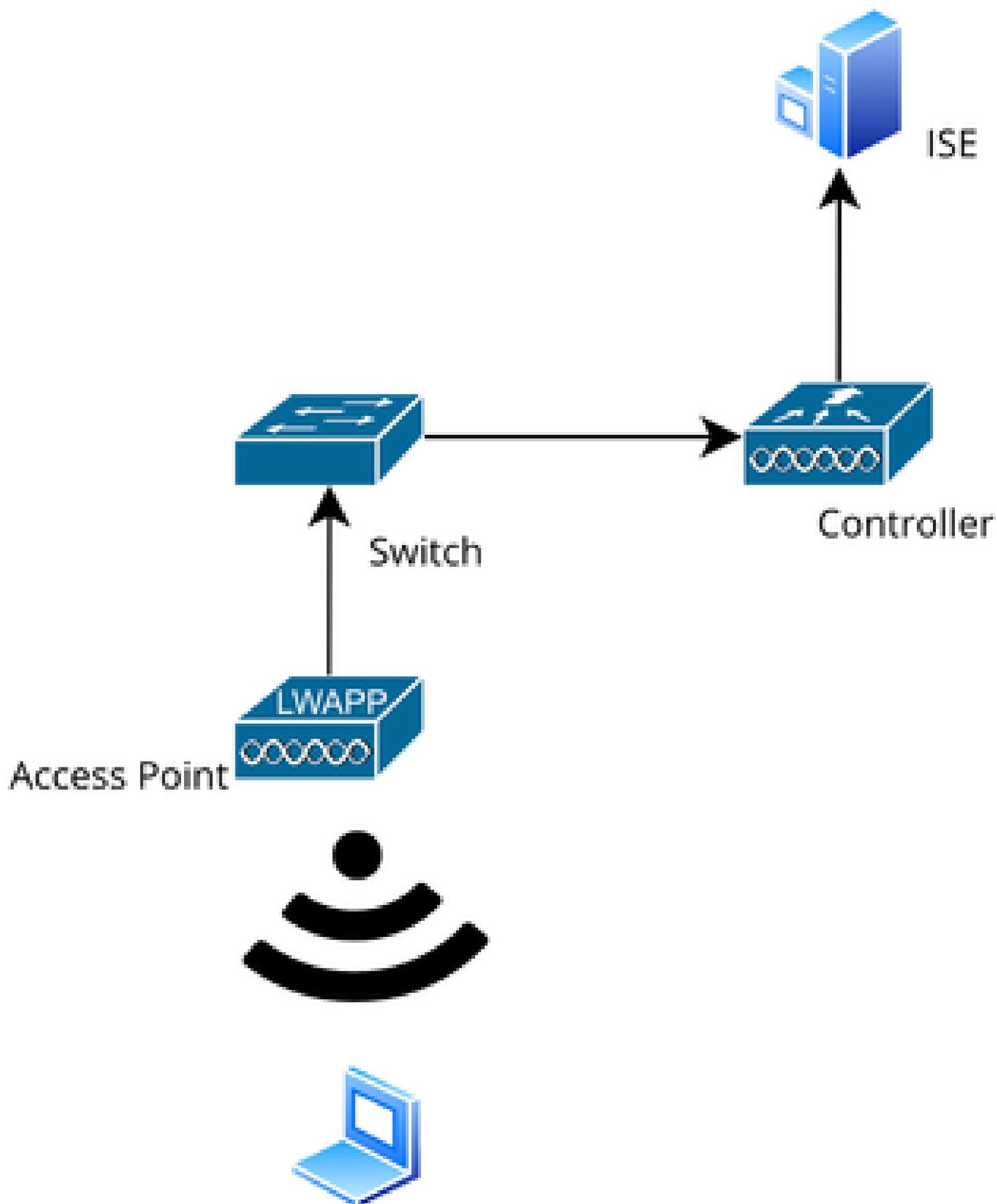
- Mecanismo de Fallback: quando um cliente tenta se conectar a uma WLAN com um Filtro MAC contra um servidor RADIUS externo (ISE) ou servidor local e não consegue se autenticar, este recurso inicia automaticamente uma Autenticação da Web de Camada 3.
- Autenticação Bem-sucedida: Se um cliente se autenticar com êxito através do Filtro MAC, a Autenticação da Web será ignorada, permitindo que o cliente se conecte diretamente à WLAN.
- Evitar Desassociações: esse recurso ajuda a evitar desassociações que podem ocorrer devido a falhas de autenticação do filtro MAC.



Fluxo de Autenticação da Web

Configurar

Diagrama de Rede



Topologia de rede

Configurações

Configurar parâmetros da Web

Navegue para Configuration > Security > Web Auth e selecione o mapa de parâmetros Global

Verifique a configuração de IP virtual e ponto confiável do Mapa de parâmetros globais. Todos os perfis de parâmetro de autenticação da Web personalizados herdam a configuração de IP virtual e de ponto confiável do Mapa de parâmetros globais.

Edit Web Auth Parameter

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3... ▼
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth ▼	Virtual IPv6 Address	xxxxxx
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>		
Sleeping Client Status	<input type="checkbox"/>		

Banner Configuration

Perfil de Parâmetro de Autenticação da Web Global

Etapa 1: selecione "Adicionar" para criar um mapa de parâmetros de autenticação da Web personalizado. Insira o nome do perfil e escolha Digitar como "Webauth".

Configuration > Security > Web Auth

+ Add Delete

Parameter Map Name

global

Create Web Auth Parameter

Parameter-map Name*	Web-Filter
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth ▼

Close Apply to Device

Se seus clientes também estiverem obtendo um endereço IPv6, você também deverá adicionar um endereço IPv6 virtual no mapa de parâmetros. Use um IP no intervalo de documentação 2001:db8::/32

Se seus clientes obtiveram um endereço IPv6, há uma boa chance de eles tentarem obter o redirecionamento de autenticação da Web HTTP em V6 e não em V4, por isso você precisa que o IPv6 Virtual também seja definido.

Configuração de CLI:

```
parameter-map type webauth Web-Filter  
type webauth
```

Configurar Perfil de Política

Etapa 1: Criar um Perfil de Política

Navegue até Configuração > Marcas e perfis > Política. Selecione Adicionar. Na guia Geral, especifique um nome para o perfil e ative a alternância de status.

Configuration > Tags & Profiles > Policy

+ Add Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility Advanced

Name* Web-Filter-Policy

Description Enter Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Perfil da política

Etapa 2:

Na guia Access Policies (Políticas de acesso), escolha a VLAN do cliente na lista suspensa da seção VLAN.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select ⓘ

VLAN

VLAN/VLAN Group VLAN2074 ⓘ

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select ⓘ

IPv6 ACL Search or Select ⓘ

URL Filters ⓘ

Pre Auth Search or Select ⓘ

Post Auth Search or Select ⓘ

Guia Política de acesso

Configuração de CLI:

```
wireless profile policy Web-Filter-Policy  
vlan VLAN2074  
no shutdown
```

Configurar o perfil da WLAN

Etapa 1: Navegue até Configuration > Tags and Profiles > WLANs. Selecione "Adicionar" para criar um novo perfil. Defina um nome de perfil e um nome SSID e ative o campo de status.

Configuration > Tags & Profiles > WLANs

+ Add × Delete Clone Enable WLAN Disable WLAN

Add WLAN

General Security Advanced

Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz

Status ENABLED ⓘ

- ✖ WPA3 Enabled
- ✔ Dot11ax Enabled

5 GHz

Status ENABLED

2.4 GHz

Status ENABLED

802.11b/g Policy 802.11b/g ▼

Perfil da WLAN

Etapa 2: Na guia Segurança, ative a caixa de seleção "Filtragem de Mac" e configure o servidor RADIUS na lista de autorização (ISE ou servidor local). Essa configuração utiliza o ISE para Autenticação Mac e Autenticação Web.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2

WPA2 + WPA3

WPA3

Static WEP

None

MAC Filtering

Authorization List*

network

OWE Transition Mode

Lobby Admin Access

Fast Transition

Status

Disabled

Over the DS

Reassociation Timeout *

20

Segurança da camada 2 da WLAN

Etapa 3: Navegue até Segurança > Camada 3. Ative a Política da Web e associe-a ao perfil do Mapa de Parâmetros de Autenticação da Web. Marque a caixa de seleção "On Mac Filter Failure" (Falha no filtro no Mac) e escolha o servidor RADIUS no menu suspenso Authentication list (Lista de autenticação).

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map

Web-Filter

Authentication List

ISE-List

For Local Login Method List to work, please make sure

<< Hide

On MAC Filter Failure

Splash Web Redirect

DISABLED

Preauthentication ACL

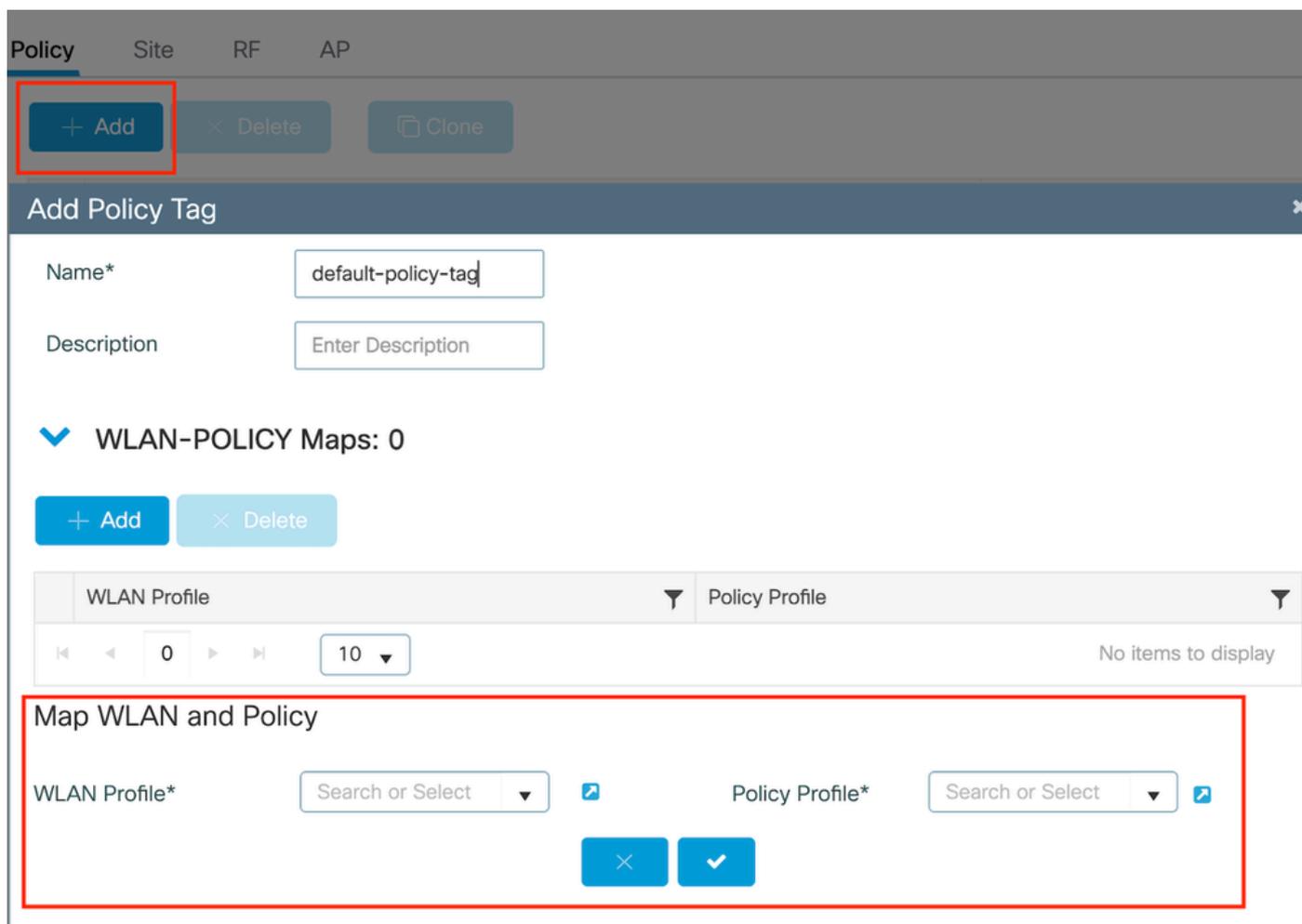
Guia de segurança da camada 3 da WLAN

Configuração de CLI

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
mac-filtering network
radio policy dot11 24ghz
radio policy dot11 5ghz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list ISE-List
security web-auth on-macfilter-failure
security web-auth parameter-map Web-Filter
no shutdown
```

Etapa 4: Configurar tags de política, Criar perfil de WLAN e Mapeamento de perfil de política

Navegue até Configuração > Marcas e perfis > Marcas > Política. Clique em "Adicionar" para definir um nome para a tag de política. Em WLAN-Policy Maps, selecione "Add" (Adicionar) para mapear o perfil WLAN e Policy criado anteriormente.



Mapa de TAG de política

Configuração de CLI:

```
wireless tag policy default-policy-tag
description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

Etapa 5: Navegue até Configuração > Sem fio > Ponto de acesso. Selecione o ponto de acesso responsável pela difusão deste SSID. No menu Editar AP, atribua a Tag de política criada.

The screenshot shows the 'Edit AP' configuration page in the Meraki dashboard. The left sidebar displays a list of access points, with 'AP2-AIR-AP3802I-D-K9-2' selected. The main content area is divided into several tabs: General, Interfaces, High Availability, Inventory, Geolocation, ICap, Advanced, and Support Bundle. The 'General' tab is active, showing various configuration fields. A red box highlights the 'Tags' section, where the 'Policy' dropdown menu is set to 'default-policy-tag'. Other fields in the 'Tags' section include 'Site' (default-site-tag), 'RF' (default-rf-tag), and 'Write Tag Config to AP' (ENABLED). The 'Version' section shows the Primary Software Version as 17.12.2.35.

Mapeando TAG de política para AP

Defina as configurações de AAA:

Etapa 1: Crie um servidor Radius:

Navegue até Configuration > Security > AAA. Clique na opção "Adicionar" na seção Servidor/Grupo. Na página "Criar servidor AAA Radius", digite o nome do servidor, o endereço IP e o segredo compartilhado.

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

[+ Add](#) [Delete](#)

RADIUS **Servers** Server Groups

Create AAA Radius Server

Name*	<input type="text"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	<input type="text"/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="text"/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		

[Cancel](#) [Apply to Device](#)

Configuração do servidor

Configuração de CLI

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

Etapa 2: Crie um grupo de servidores Radius:

Selecione a opção "Adicionar" na seção Grupos de servidores para definir um grupo de servidores. Alterne os servidores a serem incluídos na mesma configuração de grupo.

Não é necessário definir a interface de origem. Por padrão, o 9800 usa sua tabela de roteamento para descobrir a interface a ser usada para acessar o servidor RADIUS e geralmente usa o gateway padrão.

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

[Servers / Groups](#) [AAA Method List](#) [AAA Advanced](#)

[+ Add](#) [× Delete](#)

RADIUS

[Servers](#) **[Server Groups](#)**

Create AAA Radius Server Group

Name* ⓘ Name is required

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance DISABLED

Source Interface VLAN ID

Available Servers

Assigned Servers

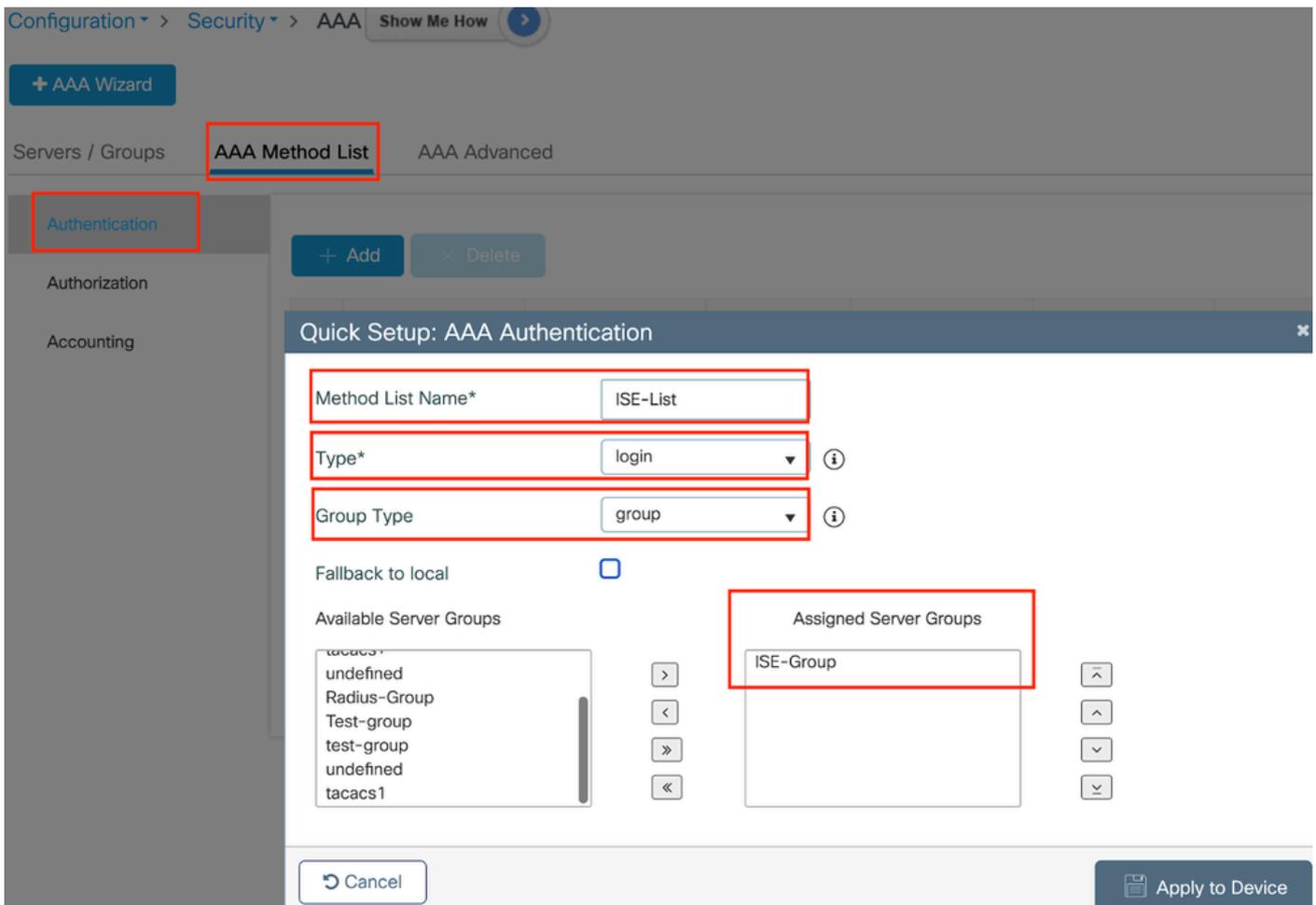
Grupo de servidores

Configuração de CLI

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5
```

Etapa 3: Configure a lista de métodos AAA:

Navegue até a guia AAA Method List (Lista de métodos AAA). Em Autenticação, clique em Adicionar. Defina um nome de lista de métodos com Type como "login" e Group type como "Group". Mapeie o grupo de servidores de autenticação configurado na seção Grupo de servidores atribuído.



lista Método de autenticação

Configuração de CLI

```
aaa authentication login ISE-List group ISE-Group
```

Navegue até a seção Lista de métodos de autorização e clique em "Adicionar". Defina um nome de lista de métodos e defina o tipo como "network" com o Tipo de grupo como "Group". Alterne o servidor RADIUS configurado para a seção Grupos de servidores atribuídos.

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add × Delete

Quick Setup: AAA Authorization

Method List Name* network

Type* network i

Group Type group i

Fallback to local

Authenticated

Available Server Groups

Assigned Server Groups

tacacs1
undefined
Radius-Group
Test-group
test-group
undefined
tacacs1

ISE-Group

Lista de métodos de autorização

Configuração de CLI

```
aaa authorization network network group ISE-Group
```

Configuração do ISE:

Adicionar WLC como um dispositivo de rede no ISE

Etapa 1: Navegue até Administração > Dispositivos de rede e clique em Adicionar. Insira o endereço IP, o nome de host e o segredo compartilhado do controlador nas Configurações de autenticação Radius

Network Devices

Name

Description

 IP Address * IP : / 32 

Adicionar dispositivo de rede

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Show

shared secret

Etapa 2: Criar entrada de usuário

Em Gerenciamento de identidades > Identidades, selecione a opção Adicionar.

Configure o nome de usuário e a senha que o cliente deve usar para a autenticação da Web

✓ Network Access User

* Username

Status Enabled

Email

✓ Passwords

Password Type:

* Login Password

Adicionar credenciais de usuário

Etapa 3: Navegue até Administração > Gerenciamento de identidades > Grupos > Dispositivos registrados e clique em Adicionar.

Insira o endereço MAC do dispositivo para criar uma entrada no servidor.

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

- Endpoint Identity Groups
 - Blocked List
 - GuestEndpoints
 - Profiled
 - RegisteredDevices**
 - Unknown
- User Identity Groups

Endpoint Identity Group List > RegisteredDevices

Endpoint Identity Group

* Name: **RegisteredDevices**

Description: Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints

+ Add Remove

Save

MAC Address Static Group Assignment Endpoint Profile

Adicionar endereço MAC do dispositivo

Etapa 4: Criar Política de Serviço

Navegue para Política > Conjuntos de políticas e selecione o sinal "+" para criar um novo conjunto de políticas

Este conjunto de políticas é para autenticação da Web do usuário, em que um nome de usuário e uma senha para o cliente são criados no Gerenciamento de identidades

Policy Sets → User-Webauth

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users		

Options

Política do Serviço de Autenticação da Web

Da mesma forma, crie uma política de serviço MAB e mapeie pontos finais internos sob a política

de autenticação.

Policy Sets -> Test-MAB

Reset

Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	Test-MAB		Normalised Radius-RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
	Default		Internal Endpoints	0	Options

Política de serviço de Autenticação MAB

Verificar

Configuração do controlador

<#root>

```
show wireless tag policy detailed
```

```
default-policy-tag
```

```
Policy Tag Name : default-policy-tag
```

```
Description      : default policy-tag
```

```
Number of WLAN-POLICY maps: 1
```

```
WLAN Profile Name      Policy Name
```

```
-----  
Mac_Filtering_Wlan
```

```
Web-Filter-Policy
```

<#root>

```
show wireless profile policy detailed
```

```
Web-Filter-Policy
```

```
Policy Profile Name      :
```

```
Web-Filter-Policy
```

Description :
Status :
ENABLED
VLAN :
2074
Multicast VLAN : 0

<#root>

show wlan name

Mac_Filtering_Wlan

WLAN Profile Name :

Mac_Filtering_Wlan

=====
Identifier : 9
Description :
Network Name (SSID) :

Mac_Filtering_Wlan

Status :

Enabled

Broadcast SSID :

Enabled

Mac Filter Authorization list name :

network

Webauth On-mac-filter Failure :

Enabled

Webauth Authentication List Name :

ISE-List

Webauth Authorization List Name : Disabled

Webauth Parameter Map :

Web-Filter

<#root>

show parameter-map type webauth name Web-Filter

Parameter Map Name :

Web-Filter

Type :

webauth

Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window :

Enabled

Webauth success-window :

Enabled

Consent Email : Disabled
Activation Mode : Replace
Sleeping-Client : Disabled
Webauth login-auth-bypass:

<#root>

show ip http server status

HTTP server status:

Enabled

HTTP server port:

80

HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:

Enabled

HTTP secure server port:

443

show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping

WLAN Profile Name	Policy Name	VLAN	Flex
Mac_Filtering_Wlan	Web-Filter-Policy	2074	ENAB

Estado da política do cliente no controlador

Navegue até a seção Dashboard > Clients para confirmar o status dos clientes conectados. O cliente está atualmente em estado pendente de autenticação da Web

[Clients](#)
[Sleeping Clients](#)
[Excluded Clients](#)

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

1 - 1 of 1 clients

Detalhes do cliente

```
show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type	ID	State	Protocol	Method
6c7e.67e3.6db9	AP2-AIR-AP3802I-D-K9-2	WLAN	9	Webauth Pending	11ac	Web

```
<#root>
```

```
show wireless client mac-address 6c7e.67e3.6db9 detail
```

```
Client MAC Address :
```

```
6c7e.67e3.6db9
```

```
Client MAC Type : Universally Administered Address
```

```
Client DUID: NA
```

```
Client IPv4 Address :
```

```
10.76.6.150
```

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
```

```
Client Username :
```

```
6c7e67e36db9
```

```
AP MAC Address : 1880.902b.05e0
```

```
AP Name: AP2-AIR-AP3802I-D-K9-2
```

```
AP slot : 1
```

```
Client State : Associated
```

```
Policy Profile :
```

```
Web-Filter-Policy
```

Flex Profile : N/A
Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List

Method : Web Auth
Webauth State :

Get Redirect

Webauth Method :

Webauth

Após a autenticação da Web bem-sucedida, o estado do gerenciador de políticas do cliente passa para EXECUTAR

<#root>

show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A

Troubleshooting

A funcionalidade do recurso Web Auth on MAC Failure depende da capacidade do controlador para disparar a autenticação da Web em caso de falha de MAB. Nosso objetivo principal é coletar rastreamentos de RA com eficiência do controlador para solução de problemas e análise.

Coleta de traços radioativos

Ative o Radio Active Tracing para gerar rastreamentos de depuração de cliente para o endereço MAC especificado na CLI.

Etapas para ativar o rastreamento radioativo:

Verifique se todas as depurações condicionais estão desabilitadas

```
clear platform condition all
```

Habilitar depuração para o endereço MAC especificado

```
debug wireless mac <H.H.H> monitor-time <Time in seconds>
```

Após reproduzir o problema, desative a depuração para interromper a coleta de rastreamento do RA.

```
no debug wireless mac <H.H.H>
```

Quando o rastreamento do RA é interrompido, o arquivo de depuração é gerado no bootflash do controlador.

```
show bootflash: | include ra_trace  
2728          179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

Copie o arquivo para um servidor externo.

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

Exibir o log de depuração:

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Ativar rastreamento de RA na GUI,

Etapa 1: Navegue até Troubleshooting > Radioactive Trace. Selecione a opção para adicionar uma nova entrada e insira o endereço MAC do cliente na guia Adicionar endereço MAC/IP designada.

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Started**

Wireless Deb

Last Run

+ Add x Delete v Start ■ Stop

Add MAC/IP Address

MAC/IP Address*

Enter a MAC/IP Address every newline

Cancel Apply to Device

Rastreamento radioativo

Capturas de pacotes incorporados:

Navegue até Troubleshooting > Captura de Pacotes. Insira o nome da captura e especifique o endereço MAC do cliente como o MAC do filtro interno. Defina o tamanho do buffer como 100 e escolha a interface de uplink para monitorar os pacotes de entrada e saída.

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane

Inner Filter Protocol DHCP

Inner Filter MAC

Buffer Size (MB)* 100

Limit by* Duration 3600 secs ≈ 1.00 hour

Available (12) Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0

Captura de pacotes incorporada

Observação: selecione a opção "Monitorar tráfego de controle" para visualizar o tráfego redirecionado para a CPU do sistema e injetado novamente no plano de dados.

Selecione Start para capturar pacotes

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	<input type="button" value="Start"/>

Iniciar captura

Configuração de CLI

```
monitor capture TestPCap inner mac <H.H.H>  
monitor capture TestPCap buffer size 100  
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both  
monitor capture TestPCap start
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

Exportar captura de pacotes para servidor TFTP externo

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```

The screenshot shows the Cisco Packet Tracer interface. At the top, there are '+ Add' and 'Delete' buttons. Below is a table of capture configurations:

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	Start Export

The 'Export' button in the 'Action' column is highlighted with a red box. Below the table, there are navigation arrows and a '10' dropdown menu. A dialog box titled 'Export Capture - TestPCap' is open, showing 'Export to*' set to 'desktop' and an 'Export' button highlighted with a red box.

Exportar captura de pacotes

Exemplo de cenário durante a autenticação MAC bem-sucedida, um dispositivo cliente se conecta à rede, seu endereço MAC é validado pelo servidor RADIUS através de políticas configuradas e, após verificação, o acesso é concedido pelo dispositivo de acesso à rede, permitindo a conectividade da rede.

Quando o cliente se associa, o controlador enviará uma solicitação de acesso ao servidor ISE,

O nome de usuário é o endereço MAC do cliente, pois é a autenticação MAB

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
```

O ISE envia Access-Accept porque temos uma entrada de usuário válida

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

Transição do estado da política do cliente para Mac Auth concluída

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29 Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

O cliente está no estado IP learn após a autenticação MAB bem-sucedida

```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d29
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

Estado do gerenciador de políticas do cliente atualizado para EXECUTAR, a Autenticação da Web é ignorada para o cliente que conclui a autenticação MAB

2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD

Verificação usando Captura de Pacotes Incorporada

No.	Time	Source	Destination	Length	Protocol	Info
53	02:42:52.710961	10.76.6.156	10.197.224.122		RADIUS	Access-Request id=0
54	02:42:52.778951	10.197.224.122	10.76.6.156		RADIUS	Access-Accept id=0

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x0 (0)
Length: 422
Authenticator: 19c6635633a7e6b6f30070b02a7f753c
[The response to this request is in frame 54]
Attribute Value Pairs
> AVP: t=User-Name(1) l=14 val=6c7e67b72d29
> AVP: t=User-Password(2) l=18 val=Encrypted
> AVP: t=Service-Type(6) l=6 val=Call-Check(10)
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
> AVP: t=Framed-MTU(12) l=6 val=1485

Pacote Radius

Exemplo onde a falha de autenticação MAC para um dispositivo cliente

Autenticação Mac iniciada para um cliente após associação bem-sucedida

2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Success
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cl
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]

O ISE enviaria Access-Reject, pois essa entrada de dispositivo não está presente no ISE

2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000

Autenticação da Web iniciada para o dispositivo do cliente como MAB falhou

```
2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cli
```

Quando o cliente inicia uma solicitação HTTP GET, o URL de redirecionamento é enviado para o dispositivo cliente, pois a sessão TCP correspondente é falsificada pelo controlador.

```
2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6
```

O cliente inicia um HTTP Get para o URL de redirecionamento e, depois que a página carrega, as credenciais de login são enviadas.

O controlador envia uma solicitação de acesso ao ISE

Esta é uma autenticação da Web, pois um nome de usuário válido é observado no pacote Access-Accept

```
2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
```

Access-Accept recebido do ISE

```
2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

A Autenticação da Web foi bem-sucedida e a transição do estado do cliente para o estado RUN

```
2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db
```

Verificação por meio de capturas EPC

O cliente conclui o handshake TCP com o endereço IP virtual do controlador e carrega a página do portal de redirecionamento. Depois que o usuário envia o nome de usuário e a senha, podemos observar uma solicitação de acesso radius do endereço IP de gerenciamento do controlador.

Após a autenticação bem-sucedida, a sessão TCP do cliente é fechada e no controlador o cliente passa para o estado RUN.

15649	08:52:51.122979	10.76.6.150	192.0.2.1	TCP	58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650	08:52:51.123986	192.0.2.1	10.76.6.150	TCP	443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=4022788871
15651	08:52:51.125985	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652	08:52:51.126992	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
15653	08:52:51.126992	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654	08:52:51.126992	192.0.2.1	10.76.6.150	85,1,64	TLSv1.2 Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655	08:52:51.129982	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656	08:52:51.129982	10.76.6.150	192.0.2.1	1,64	TLSv1.2 Change Cipher Spec, Encrypted Handshake Message
15657	08:52:51.130989	10.76.6.150	192.0.2.1	640	TLSv1.2 Application Data
15658	08:52:51.130989	10.76.6.150	192.0.2.1	160	TLSv1.2 Application Data
15659	08:52:51.130989	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3
15665	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment i
15667	08:52:51.191976	192.0.2.1	10.76.6.150	2496	TLSv1.2 Application Data
15668	08:52:51.192983	192.0.2.1	10.76.6.150	48	TLSv1.2 Encrypted Alert
15673	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15676	08:52:51.197987	10.76.6.150	192.0.2.1	48	TLSv1.2 Encrypted Alert
15677	08:52:51.197987	10.76.6.150	192.0.2.1	TCP	58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0

Fluxo TCP com pacote radius

15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
 Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
 Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
 User Datagram Protocol, Src Port: 65433, Dst Port: 1812
 RADIUS Protocol

```
Code: Access-Request (1)
Packet identifier: 0x3 (3)
Length: 457
Authenticator: fd400f7e3567dc5a63cfefaeaf379eaa
[The response to this request is in frame 15663]
Attribute Value Pairs
  AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
  AVP: t=User-Name(1) l=10 val=testuser
  AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
  AVP: t=Message-Authenticator(00) l=16 val=501b124c30216efdf5973086d99f3a185
  AVP: t=Service-Type(6) l=6 val=Dialog-Framed-User(5)
  AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
  AVP: t=User-Password(2) l=18 val=Encrypted
```

Pacote RADIUS enviado ao ISE com credenciais de usuário

A captura do Wireshark do lado do cliente para validar o tráfego do cliente está sendo redirecionado para a página do portal e validar o handshake TCP para o endereço IP virtual/servidor Web do controlador

Time	Source	Destination	Length	Protocol	Info
105	08:51:34.203945	10.76.6.150	10.76.6.145	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
108	08:51:34.206602	10.76.6.145	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)
234	08:51:39.028084	10.76.6.150	7.7.7.7	HTTP	GET / HTTP/1.1
236	08:51:39.031420	7.7.7.7	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)

Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
 Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
 Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
 Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637

Hypertext Transfer Protocol

Line-based text data: text/html (9 lines)

```
<HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
<HEAD>\n
<TITLE> Web Authentication Redirect</TITLE>\n
<META http-equiv="Cache-control" content="no-cache">\n
<META http-equiv="Pragma" content="no-cache">\n
<META http-equiv="Expires" content="-1">\n
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
</HEAD>\n
</HTML>
```

Captura do lado do cliente para validar a URL de redirecionamento

O cliente estabelece o handshake TCP para o endereço IP virtual do controlador

Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1	TCP	58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PERM
117	08:51:34.211190	192.0.2.1	10.76.6.150	TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr=0
118	08:51:34.211275	10.76.6.150	192.0.2.1	TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150	TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLSv1.2 Server Hello, Certificate
125	08:51:34.220835	192.0.2.1	10.76.6.150	783	TLSv1.2 Server Key Exchange, Server Hello Done

Handshake de TCP entre o cliente e o servidor web

A sessão é encerrada após a autenticação bem-sucedida da Web,

144	08:51:34.235915	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491089
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLSv1.2 Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1	TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLSv1.2 Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150	TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

Sessão TCP fechada após o cliente concluir a autenticação da Web

Artigo relacionado

[Entender depurações sem fio e coleta de logs em controladores LAN sem fio Catalyst 9800](#)

[Autenticação baseada na Web no 9800](#)

[Configure a autenticação da Web local no 9800](#)

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.