



# Guia de Operações e Implantação do OmniTWAG

Criado por [OmniTouch](#)

Este guia é destinado a operadores de rede, administradores de sistema e clientes que estão implantando o OmniTWAG.

## Índice

- [1. Introdução](#)
- [2. O que é WiFi Offload?](#)
- [3. Arquitetura de Implantação](#)
- [4. Fluxo de Cobrança](#)
- [5. Fluxo de Autenticação](#)
- [6. Guia de Configuração](#)
- [7. Configuração do Ponto de Acesso](#)
- [8. Integração Hotspot 2.0](#)
- [9. Monitoramento e Gestão](#)
- [10. Solução de Problemas](#)
- [11. Conformidade com Padrões](#)

## Introdução

OmniTWAG (Trusted WiFi Access Gateway) é uma implementação compatível com padrões de um 3GPP TWAG que permite que operadores de redes móveis descarreguem com segurança o tráfego de assinantes de redes celulares para pontos de acesso WiFi, mantendo uma autenticação segura baseada em SIM.

O TWAG autentica assinantes WiFi usando suas credenciais SIM via EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement), o mesmo mecanismo de autenticação usado em redes celulares. Isso proporciona um acesso WiFi seguro e contínuo para assinantes móveis sem a necessidade de senhas WiFi separadas.

### Principais Benefícios

#### Para Usuários Finais:

- **Zero Configuração:** Funciona imediatamente com SIM compatível
- **Experiência Sem Custura:** Conexão automática como celular
- **Seguro:** Sempre usa WiFi criptografado (WPA2)
- **Sem Senhas:** Autenticação baseada em SIM

#### Para Operadores Móveis:

- **Alívio da Capacidade da Rede:** Reduz a carga nas estações base celulares
- **Descarregamento Controlado:** Apenas assinantes autorizados podem se conectar
- **Melhoria na Experiência do Usuário:** WiFi geralmente oferece maior largura de banda
- **Eficiência de Custos:** A infraestrutura WiFi é menos cara que a celular
- **Identidade Consistente:** Mesmo IMSI usado para WiFi e celular
- **Integração de Cobrança:** Pode cobrar pelo uso de WiFi, se desejado

#### Para Locais/Empresas:

- **Segurança de Grau Operador:** Sem risco de compartilhamento de senhas
- **Escalabilidade:** Suporta milhares de usuários sem provisionamento manual
- **Gestão Simplificada:** Sem necessidade de distribuir senhas WiFi

## O que é WiFi Offload?

WiFi offload permite que operadores de redes móveis redirecionem o tráfego de dados dos assinantes de redes celulares congestionadas para redes WiFi.

### Como o TWAG Habilita o Descarregamento

O TWAG atua como o gateway de autenticação entre:

- **Pontos de Acesso WiFi** (via protocolo RADIUS)
- **Rede Central Móvel** HSS/HLR (via interface Diameter SWx)

Quando o dispositivo de um assinante se conecta a um AP WiFi configurado para descarregamento:

1. O dispositivo se identifica usando seu IMSI (do cartão SIM)
2. O AP WiFi encaminha solicitações de autenticação para o TWAG via RADIUS
3. O TWAG se comunica com o HSS do operador para recuperar vetores de autenticação
4. A autenticação de desafio-resposta EAP-AKA ocorre entre o dispositivo e o TWAG
5. Após a autenticação bem-sucedida, o dispositivo recebe acesso WiFi
6. Opcionalmente, o tráfego pode ser tunelado de volta para a rede central móvel ou sair localmente

## Arquitetura de Implantação

### Topologia da Rede

#### Legenda de Interface:

- **STa\*:** interface RADIUS/Diameter entre AP WiFi e TWAG (não 3GPP para AAA)
- **SWx:** interface Diameter entre TWAG (Servidor AAA 3GPP) e HSS
- **S2a/S2b:** interface de túnel GTP para backhaul para a rede local (opcional)
- **SGi:** Interface para redes de dados de pacotes externas (Internet)
- **802.11:** interface de rádio WiFi
- **EAPOL:** EAP sobre LAN (autenticação 802.1X)

Omnitouch OmnitWAG v0.1.0

Licensed to: Omnitouch  
© 2025 Omnitouch

Resources

Configuration

Diameter

Diameter Test

RADIUS Clients

Access Points

Client Usage

RADIUS Clients

1 Accepted0 Authenticating0 Rejected

IDENTITY	AUTH STATUS	LAST UPDATED	SESSION DURATION
0313380900001867@wlan.mnc380.mcc313.3gppnetwork.org	Accepted	2025-10-12 10:31:50	5m 24s

Usage Summary

Session ID	00000010
Session Time	5m 14s
Data Downloaded	193.32 MB
Data Uploaded	427.73 MB
Total Data	621.05 MB
Packets In / Out	237674 / 326001
Status	>
Last Update	2025-10-12 10:37:03

Authentication State

Accounting Session ID	-
Called Station ID (AP MAC:SSID)	64-D9-89-1D-A4-20:ONS
Calling Station ID (Client MAC)	86-81-69-A7-B4-B2

Cenários de Implantação

Cenário 1: Saída Local (Recomendado para Desempenho)

Benefícios:

- Menor latência (sem retorno ao núcleo)
- Carga reduzida na rede central
- Melhor experiência do usuário para aplicações de alta largura de banda
- Economia de custos na capacidade de backhaul

Cenário 2: Roteamento de Rede Local (Túnel GTP)

Benefícios:

- Aplicação consistente de políticas
- Cobrança/ faturamento centralizados
- Políticas de VPN/segurança corporativa aplicáveis
- Mobilidade contínua entre WiFi e celular

Opções de Conexão SWx

Opção 1: Conexão Direta ao HSS

Caso de Uso: Implantações simples, ambientes de laboratório, um único HSS

Benefícios:

- Menor latência (sem salto através do DRA)
- Configuração simplificada
- Solução de problemas mais fácil

Opção 2: Via DRA (Agente de Roteamento Diameter)

Caso de Uso: Implantações multi-HSS, cenários de roaming, redes de grande escala

Benefícios:

- Lógica de roteamento centralizada
- Balanceamento de carga entre múltiplos HSS
- Suporte a roaming (roteia para o HSS local)
- Redundância e failover
- Persistência de sessão

Fluxo de Cobrança

O TWAG pode ser totalmente integrado para enviar solicitações de cobrança online baseadas em Diameter Gy para um Sistema de Cobrança Online (OCS).

Isso permite a contabilidade de todos os dados consumidos no WiFi, em relação ao saldo do cliente, e é entregue via AP no RADIUS e convertido para Gy pelo TWAG e encaminhado para o DRA/OCS.

Em todos os modos, o uso é rastreado pelas métricas do TWAG.

Resources

Configuration

Diameter

Diameter Test

RADIUS Clients

Access Points

Client Usage

Client Usage & Accounting

3 Sessions

0 Active

↓ 204.4 MB / ↑ 623.07 MB

Session ID	User	Client MAC	AP / SSID	Status	Duration	Data Usage
00000010	0313380900001867@wla...	86-81-69-A7-B4-B2	10.7.15.72	▷	4m 10s	↓ 193.3 MB / ↑ 427.72 MB
0000000F	0313380900001867@wla...	86-81-69-A7-B4-B2	10.7.15.72	◁	8h 27m	↓ 4.12 MB / ↑ 146.5 MB
0000000E	0313380900001867@wla...	86-81-69-A7-B4-B2	10.7.15.72	◁	16m 9s	↓ 6.98 MB / ↑ 48.85 MB

Licensed to: Omnitouch

© 2025 Omnitouch

Modos de Cobrança

O TWAG suporta três modos de cobrança online:

1. Cobrança Desativada

Nenhuma solicitação de controle de crédito é enviada. Nenhuma autorização de saldo é realizada.

Casos de Uso:

- Redes WiFi abertas/gratuitas
- Ambientes de laboratório/teste
- Redes com cobrança offline apenas (contabilidade RADIUS para faturamento)

Fluxo:

2. Apenas Autorização

Um CCR-Initial (Credit-Control-Request) é enviado para o OCS no início da sessão WiFi para validar se o assinante tem saldo, mas o saldo não é descontado durante a sessão.

Casos de Uso:

- Validar se o assinante tem conta/saldo ativo
- Impedir acesso WiFi para contas suspensas
- Verificar elegibilidade de serviço sem rastreamento de cota
- Permitir WiFi como serviço bônus/ilimitado para clientes pagantes

Fluxo:

Configuração:

- OCS é consultado no início da sessão (CCR-I) e no final (CCR-T)
- Nenhuma mensagem CCR-Update enviada durante a sessão
- Assinante autorizado com base no status da conta, não na cota
- Uso reportado no final da sessão apenas para fins informativos

3. Cobrança Online Gy Completa (Implementação Completa)

O fluxo de cobrança online padrão 3GPP é seguido. Todo o uso no WiFi é passado para o OCS para cobrança, com o assinante sendo desconectado uma vez que exceda sua cota.

Casos de Uso:

- Serviços de dados pré-pagos
- WiFi pago por uso
- Planos baseados em cota (por exemplo, 10GB de limite mensal)
- Cobrança e desconexão em tempo real

Fluxo:

Configuração:

- OCS consultado no início da sessão (CCR-I), durante a sessão (CCR-U) e no final (CCR-T)
- Cota solicitada em partes configuráveis (por exemplo, 10MB, 50MB, 100MB)
- CCR-Update acionado em um limite configurável (por exemplo, 80% da cota concedida)
- Temporizador de validade aciona re-autorização se a cota não for esgotada
- Desconexão forçada quando a cota for esgotada
- Dedução de saldo em tempo real

Fluxo de Autenticação

Sequência Completa de Autenticação EAP-AKA

Pontos Chave no Fluxo de Autenticação

- MAR/MAA é o fim da comunicação com HSS: Após receber o MAA (Multimedia-Auth-Answer) com XRES, o TWAG lida com todas as verificações subsequentes localmente.
- TWAG realiza a verificação de RES: O HSS fornece a resposta esperada (XRES), mas o TWAG a compara com o RES real do UE. O HSS NÃO está envolvido nesta comparação.
- A autenticação acontece no TWAG: Isso é diferente de alguns diagramas que mostram o HSS fazendo a verificação—na arquitetura 3GPP real, o servidor AAA (TWAG) realiza a comparação.

Formato de Identidade

O dispositivo responde com sua identidade permanente (IMSI) no formato NAI:

5055700000000000001@lan.mnc057.mcc505.3gppnetwork.org

Formato: 061t;IMSI=&@lan.mnc&1t;MNC>.mcc&1t;MCC>.3gppnetwork.org

Nota - O primeiro dígito, antes do IMSI, é a identidade, geralmente 0, mas pode ser outro número de um único dígito para SIMs / dispositivos multi-IMSI.

Chave de Sessão Mestre (MSK)

A Chave de Sessão Mestre (MSK) é uma chave criptográfica de 512 bits (64 bytes) derivada durante a autenticação EAP-AKA. Ela serve como o material de chave raiz para proteger a conexão WiFi.

Derivação da MSK:

- Tanto UE quanto TWAG derivam independentemente a mesma MSK
- UE deriva de CK/IK computados pelo SIM
- TWAG deriva de CK/IK recebidos do HSS
- MSK = PRF(CK || IK, "Full Authentication", IMSI, ...)

Uso da MSK:

- Derivação da PMK: PMK = primeiros 256 bits (32 bytes) da MSK
- Handshake WPA2 4-Way: Tanto UE quanto AP usam PMK para derivar PTK
- Criptografia de Dados: Todos os quadros de dados WiFi criptografados com Chave Temporal (TK) da PTK

Por que a MSK é Crítica:

- Confidencialidade: Sem MSK, o tráfego WiFi seria não criptografado

- **Integridade:** Previne a adulteração de quadros WiFi
- **Vínculo de Autenticação:** Liga a autenticação EAP à criptografia WiFi
- **Proteção contra Repetição:** MSK nova previne ataques de repetição
- **Perfeita Segurança de Avanço:** Comprometimento de uma MSK não afeta outras

### Recuperação de Resincronização

Se o dispositivo detectar uma discrepância no número de sequência (SQN fora de sincronia), ele inicia a resincronização:

1. O dispositivo computa AUTS (Token de Autenticação - Sincronização)
2. Envia EAP-AKA Synchronization-Failure com AT-AUTS
3. TWAG encaminha AUTS para HSS
4. HSS resincroniza o número de sequência e gera novos vetores
5. A autenticação é tentada novamente com vetores frescos

Isso é transparente para o usuário final e não requer intervenção do operador.

## Guia de Configuração

O TWAG é configurado via arquivos de configuração Elixir no diretório config/. A configuração principal em tempo de execução está em config/runtime.exs.

Para implantações em produção, a configuração é gerenciada centralmente. O abaixo é apenas uma referência, quaisquer valores alterados em um nó de produção serão perdidos na próxima vez que a orquestração automatizada for executada.

### Configuração Diameter

Localizado em config :diameter\_ex:

```
config :diameter_ex,
  diameter: %{
    # Nome do serviço para a pilha Diameter
    service_name: :omnitouch_twag,

    # Endereço IP local para vincular o serviço Diameter
    listen_ip: "10.5.198.200",

    # Porta local para conexões Diameter (padrão é 3868)
    listen_port: 3868,

    # Host de Origem Diameter
    host: "omnitwag",

    # Realm de Origem Diameter (corresponde ao seu realm de rede)
    realm: "epc.mnc057.mcc505.3gppnetwork.org",

    # Pares Diameter (HSS, DRA, servidores AAA)
    peers: [
      %{
        # Host de Origem Diameter do par
        host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",

        # Realm de Origem Diameter do par
        realm: "epc.mnc057.mcc505.3gppnetwork.org",

        # Endereço IP do par (pode ser HSS diretamente ou DRA)
        ip: "10.179.2.140",

        # Porta do par (padrão é 3868)
        port: 3868,

        # Usar TLS para segurança de transporte
        tls: false,

        # Protocolo de transporte (:diameter_tcp ou :diameter_sctp)
        transport: :diameter_tcp,

        # Iniciar conexão com o par (true) ou esperar o par se conectar (false)
        initiate_connection: true
      }
    ]
  }
}
```

**Formato de Realm** segue 3GPP TS 23.003:

epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Onde:

- MNC = Código da Rede Móvel (por exemplo, 057)
- MCC = Código do País Móvel (por exemplo, 505 para a Austrália)

Omnitouch OmnitWAG v0.1.0

Licensed to: Omnitouch  
© 2025 Omnitouch

Resources

Configuration

Diameter

Diameter Test

RADIUS Clients

Access Points

Client Usage

Diameter Peers

1 Connected0 Disconnected

PEER	REALM	IP ADDRESS	STATUS
omni-nick2-hss01.epc.mnc380.mcc313.3gppnetwork.org	epc.mnc380.mcc313.3gppnetwork.org	tcp://10.179.2.140:3868	Connected
Basic Information			
Connection Initiation	OmnitWAG -> Peer		
Transport	tcp		
Product Name	pyHSS		
Advertised Applications	3GPP_cx, 3GPP_gx, 3GPP_rx, 3GPP_s13, 3GPP_s6a, 3GPP_sh, 3GPP_slh		

**Nota sobre o Uso do DRA:** Para usar o OmniDRA, configure o IP do par para apontar para o DRA em vez de diretamente para o HSS. O DRA então roteará mensagens para o HSS apropriado com base nas regras de roteamento (Destination-Realm, intervalo de IMSI, etc.).

### Configuração RADIUS

Localizado em config :omnitwag:

```
config :omnitwag,
  radius_config: %{
    # Lista de sub-redes IP de origem permitidas para clientes RADIUS
    # Lista vazia = permitir todos (não recomendado para produção)
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],

    # Segredo compartilhado para clientes RADIUS
    # Todos os APs devem usar este segredo
    secret: "YOUR_STRONG_SECRET_HERE"
  }
}
```

OmniTouch OmniTWAG v0.1.0

Licensed to: OmniTouch  
© 2025 OmniTouch

Resources

Configuration

Diameter

Diameter Test

RADIUS Clients

Access Points

Client Usage

Access Points


1 AP

1 Total Clients

NAS IP ADDRESS LAST SEEN	AP MAC / SSID UPTIME	SSID	CLIENTS
10.7.15.72 2025-10-12 10:31:50	64-D9-89-1D-A4-20:ONS 5m 33s	-	1

Access Point Details

Called Station ID (AP MAC:SSID)	64-D9-89-1D-A4-20:ONS
Client Count	1
First Seen	2025-10-12 10:31:49
Framed MTU	1400
Last Seen	2025-10-12 10:31:50
NAS IP Address	10.7.15.72
NAS Port Type	Wireless-802.11



Melhores Práticas de Segurança:

- Use segredos compartilhados RADIUS fortes (20+ caracteres)
- Configure allowed\_source\_subnets para restringir o acesso dos APs
- Use regras de firewall para restringir ainda mais o acesso às portas 1812/1813

Exemplo de configuração de sub-rede:

allowed\_source\_subnets: ["10.7.15.0/24", "192.168.1.0/24"]

Se vazio, todas as fontes são permitidas (apenas adequado para laboratório/teste).

Configuração de Monitoramento Prometheus

Localizado em config :omnitwag:

```
config :omnitwag,
  prometheus: %{
    # Porta para o endpoint de métricas do Prometheus
    port: 9568
  }
```

Acesse as métricas em: http://<twag-ip>:9568/metrics

Resumo de Portas

Porta	Protocolo	Propósito
1812	UDP	Autenticação RADIUS
1813	UDP	Contabilidade RADIUS
3868	TCP	Diameter (SWx para HSS/DRA)
443	TCP	Portal Web HTTPS
8444	TCP	API REST HTTPS
9568	TCP	Métricas Prometheus

Configuração do Ponto de Acesso

Pontos de Acesso Suportados

OmniTWAG funciona com qualquer AP WiFi que suporte:

- **WPA2-Enterprise** (autenticação 802.1X)
- Funcionalidade de **cliente RADIUS**
- Método de autenticação **EAP-AKA**

Plataformas testadas: Cisco Aironet, Aruba, Ubiquiti UniFi, Ruckus, APs baseados em hostapd

Requisitos Gerais de Configuração do AP

1. Modo de segurança **WPA2-Enterprise (802.1X)**
2. **Servidor RADIUS** apontando para o endereço IP do TWAG
3. **Porta de autenticação RADIUS:** 1812
4. **Porta de contabilidade RADIUS:** 1813 (opcional, mas recomendado)
5. **Segredo compartilhado RADIUS:** Deve corresponder à configuração do TWAG
6. **Método EAP:** EAP-AKA (ou "Todos")

Exemplo de Configuração do AP Cisco

Configuração CLI:

```
! Configurar servidor RADIUS
radius-server host 10.5.198.200 auth-port 1812 acct-port 1813 key YOUR_SHARED_SECRET

! Configurar SSID com 802.1X
dot11 ssid OPERATOR-WIFI
  vlan 10
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2

! Associar SSID com a interface de rádio
interface Dot11Radio0
  encryption mode ciphers aes-ccm
  ssid OPERATOR-WIFI
```

Interface Web:

1. Navegue até **Segurança -- AAA -- Servidor RADIUS**
2. Adicione o servidor RADIUS: 10.5.198.200:1812 com segredo compartilhado
3. Navegue até a configuração **WLAN**
4. Defina a Segurança como **WPA2-Enterprise**
5. Defina o método EAP como **EAP-AKA** ou **Todos**
6. Atribua o grupo de servidores RADIUS

Exemplo de Configuração do hostapd

Para APs baseados em Linux (OpenWrt, sistemas embarcados):

```
# /etc/hostapd/hostapd.conf
```

```
interface=wlan0
driver=nl80211
ssid=OPERATOR-WIFI

# WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
ieee8021x=1

# Configuração RADIUS
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# Configuração EAP
eap_server=0

# Hotspot 2.0 (Opcional - para descarregamento automático)
interworking=1
internet=1
anqp_3gpp_cell_net=505,057
domain_name=wlan.mnc057.mcc505.3gppnetwork.org
nai_real=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
roaming_consortium=505057
hs20=1
```

Melhores Práticas de Arquitetura de Rede

**Importante:** Coloque os APs e o TWAG em segmentos de rede confiáveis. Use regras de firewall para:

- Permitir apenas que os APs acessem as portas 1812/1813 do TWAG
- Permitir que o TWAG acesse a porta 3868 do HSS
- Restringir o acesso de gestão ao painel do TWAG (porta 443)

Integração Hotspot 2.0

Visão Geral do Hotspot 2.0 (Passpoint)

Hotspot 2.0 (também chamado de Passpoint ou 802.11u) é um padrão da WiFi Alliance que permite a descoberta e conexão automática e segura de redes WiFi sem interação do usuário. É a tecnologia chave para descarregamento WiFi sem costura.

Principais Recursos:

- **Descoberta Automática de Redes:** O dispositivo encontra redes compatíveis com base em critérios
- **Autenticação Automática:** Usa credenciais SIM (EAP-AKA) sem entrada do usuário
- **Associação Inicial Criptografada:** OSEN (OSU Server-only Authentication) para provisionamento seguro
- **Acordos de Roaming:** Suporta redes visitadas (como roaming celular)
- **Priorização:** O dispositivo prefere redes de propriedade do operador

Configuração do AP Hotspot 2.0

Requisitos para o AP:

1. **Suporte a 802.11u:** Capacidade de consulta/resposta ANQP
2. **WPA2-Enterprise:** Autenticação 802.1X
3. **Suporte a EAP-AKA:** Deve suportar o método EAP-AKA
4. **Configuração ANQP:** Anunciar informações corretas do operador

Exemplo de Configuração (AP baseado em hostapd):

```
# Configuração Hotspot 2.0 / Passpoint
interworking=1
internet=1
asra=0
esr=0
uesa=0

# Configuração ANQP
anqp_3gpp_cell_net=505,057
domain_name=omnitouchns.com,wlan.mnc057.mcc505.3gppnetwork.org

# Configuração do Realm NAI
nai_real=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# Formato: <codificação>,<realm>,<método-eap>[auth-id:auth-val]
# 21 = EAP-AKA
# 2:1 = Tipo de Credencial: SIM
# 5:7 = Método EAP Tunelado: Nenhum (EAP-AKA direto)

# Consórcio de Roaming
roaming_consortium=505057
# MCC=505 (EUA), MNC=057 (específico do operador)

# Informações do Local (opcional)
venue_group=1
venue_type=8
venue_name=eng:Rede WiFi Pública do Operador

# Configuração WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
rsn_pairwise=CCMP
ieee8021x=1

# Configuração RADIUS (aponta para OmniTWAG)
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# Configuração do SSID
ssid=OperatorWiFi
utf8_ssid=1

# Indicação Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:Rede WiFi do Operador
```

Comportamento de Descarregamento Automático

Como Funciona o Descarregamento Automático:

1. Dispositivo com perfil Passpoint realiza varredura WiFi periódica
2. Envia consulta ANQP para APs detectados
3. Se a resposta ANQP corresponder ao perfil (MCC/MNC, consórcio de roaming):
  - Prioridade é ALTA (rede local) ou MÉDIA (parceiro de roaming)
4. Se a prioridade ≥ limite e sinal > mínimo:
  - Autenticação automática EAP-AKA
5. Se a autenticação for bem-sucedida e a prioridade > conexão atual:
  - Mudar para WiFi, desconectar dados celulares
6. Monitorar qualidade do sinal e manter conectividade

Fatores de Prioridade:

1. **Local vs. Roaming:** Rede local (correspondência MCC/MNC) preferida em relação ao roaming
2. **Força do Sinal:** Sinal mais forte preferido
3. **Segurança:** WPA2-Enterprise preferido em relação a aberto/WPA2-PSK
4. **Política:** O operador pode configurar redes preferidas
5. **Sobrescrição do Usuário:** O usuário pode desativar manualmente o WiFi ou preferir celular

---

## Monitoramento e Gestão

### Painel Web

Acesse o painel de monitoramento em tempo real em: <https://<twag-ip>/>

#### Recursos:

- **Visualização de Clientes RADIUS:** Assinantes ativos, status de autenticação, detalhes da sessão
- **Visualização de Pontos de Acesso:** APs conectados, contagens de clientes, informações do SSID
- **Visualização de Uso do Cliente:** Dados de contabilidade, tempo de sessão, uso de dados
- **Visualização de Pares Diameter:** Status de conexão HSS/DRA

### Integração Prometheus

Configure o Prometheus para coletar métricas do TWAG:

```
# prometheus.yml
scrape_configs:
- job_name: 'omnitwag'
  static_configs:
  - targets: ['10.5.198.200:9568']
  metrics_path: '/metrics'
  scrape_interval: 15s
```

#### Métricas Disponíveis:

##### Métricas do Servidor RADIUS:

- radius\_access\_request\_count - Total de pacotes RADIUS Access-Request recebidos
- radius\_access\_accept\_count - Total de pacotes Access-Accept enviados
- radius\_access\_reject\_count - Total de pacotes Access-Reject enviados
- radius\_access\_challenge\_count - Total de pacotes Access-Challenge enviados
- radius\_accounting\_request\_count{status\_type} - Total de pacotes Accounting-Request (marcados por status: start, stop, interim\_update, accounting\_on, accounting\_off)
- radius\_active\_clients\_count - Clientes atualmente autenticados (consultados a cada 5 segundos)
- radius\_access\_points\_count - Pontos de acesso registrados (consultados a cada 5 segundos)

##### Métricas de Autenticação EAP-AKA:

- eap\_aka\_identity\_count - Trocas de Identidade EAP-AKA
- eap\_aka\_challenge\_count - Trocas de Desafio EAP-AKA
- eap\_aka\_sync\_failure\_count - Falhas de sincronização (eventos de resync SQN)
- eap\_aka\_auth\_success\_count - Autenticações bem-sucedidas
- eap\_aka\_auth\_reject\_count - Autenticações rejeitadas

##### Métricas do Protocolo Diameter:

- diameter\_message\_count(application, command, direction) - Total de mensagens Diameter (marcadas por aplicação, tipo de comando e direção)

##### Métricas de Memória do VM Erlang:

- vm\_memory\_total - Total de memória alocada (bytes)
- vm\_memory\_processes - Memória usada por processos Erlang (bytes)
- vm\_memory\_processes\_used - Memória usada por processos Erlang excluindo memória alocada não utilizada (bytes)
- vm\_memory\_system - Memória usada pelo sistema de execução Erlang (bytes)
- vm\_memory\_atom - Memória usada por átomos (bytes)
- vm\_memory\_atom\_used - Memória usada por átomos excluindo memória alocada não utilizada (bytes)
- vm\_memory\_binary - Memória usada por binários (bytes)
- vm\_memory\_code - Memória usada por código carregado (bytes)
- vm\_memory\_ets - Memória usada por tabelas ETS (bytes)

##### Métricas do Sistema VM Erlang:

- vm\_system\_info\_process\_count - Número atual de processos Erlang
- vm\_system\_info\_port\_count - Número atual de portas
- vm\_system\_info\_atom\_count - Número atual de átomos
- vm\_system\_info\_schedulers - Número de threads de agendamento
- vm\_system\_info\_schedulers\_online - Número de agendadores atualmente online

##### Métricas do Agendador VM Erlang:

- vm\_statistics\_run\_queue - Comprimento total de todas as filas de execução
- vm\_total\_run\_queue\_lengths\_total - Comprimento total de todas as filas de execução (agendadores totais)
- vm\_total\_run\_queue\_lengths\_cpu - Comprimento total das filas de execução do agendador de CPU
- vm\_total\_run\_queue\_lengths\_io - Comprimento total das filas de execução do agendador de IO

#### Coleta de Métricas:

- Métricas RADIUS e EAP-AKA são emitidas em tempo real à medida que os eventos ocorrem
- Contagens de clientes ativos e pontos de acesso são consultadas a cada 5 segundos
- Métricas VM são consultadas a cada 5 segundos do runtime Erlang
- Todas as métricas são expostas no formato Prometheus em <http://<twag-ip>:9568/metrics>

### Registro

O TWAG usa o Logger do Elixir para registro estruturado.

#### Ver Logs (systemd):

```
# Registro em tempo real
journalctl -u twag -f

# Últimas 100 linhas
journalctl -u twag -n 100

# Logs desde a última inicialização
journalctl -u twag -b

# Logs para intervalo de tempo específico
journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-12 11:00:00"
```

#### Mensagens de Log Chave:

- Servidor RADIUS ouvindo na porta 1812 - Servidor iniciado
- De {IP}: Solicitação de Acesso recebida - Solicitação RADIUS do AP
- Fase 1: Resposta de Identidade - Identidade EAP inicial
- Fase 2: Desafio AKA - Desafio enviado ao dispositivo
- Autenticação ACEITA - Autenticação bem-sucedida
- Autenticação REJEITADA - Autenticação falhou
- AP Registrado: {IP} - Novo AP detectado

---

## Solução de Problemas

### Falhas de Autenticação

**Sintoma:** Cliente não consegue se conectar ao WiFi

#### Passos de Diagnóstico:

1. Verifique os logs do TWAG: `journalctl -u twag -f`
2. Verifique se o segredo compartilhado RADIUS corresponde entre o AP e o TWAG.
3. Confirme se os pacotes RADIUS estão chegando ao TWAG: `tcpdump -i eth0 port 1812`
4. Verifique o provisionamento do assinante no HSS/configuração

#### Causas Comuns:

- Segredo compartilhado RADIUS incorreto
- Firewall bloqueando UDP 1812/1813
- Desvio RES/XRES (Ki do SIM errado ou configuração do HSS)
- Número de sequência (SQN) fora de sincronia (deve se recuperar automaticamente via resync)
- Problemas de conectividade de rede entre o AP e o TWAG

### Problemas de Conexão Diameter

**Sintoma:** Par Diameter não se conectando ao HSS/DRA

Passos de Diagnóstico:

- 1. Verifique a conectividade de rede: telnet <hss-ip> 3868
- 2. Verifique a configuração Diameter (Host de Origem, Realm de Origem, IP do par)
- 3. Revise os logs do HSS/DRA para tentativas de conexão
- 4. Verifique se o firewall permite TCP 3868

Causas Comuns:

- IP/porta do par incorretos na configuração
- Firewall bloqueando TCP 3868
- Desvio de Host/Realm
- HSS/DRA não aceitando conexão do TWAG

Problemas de Desempenho

Sintoma: Autenticação lenta (>5 segundos)

Passos de Diagnóstico:

- 1. Verifique o tempo de resposta do HSS
- 2. Meça a latência da rede: ping <hss-ip>, mtr <hss-ip>
- 3. Monitore o uso de recursos do TWAG: top, htop
- 4. Revise as configurações de tempo limite de solicitação Diameter

Causas Comuns:

- Tempo limite de consulta HSS ou resposta lenta
- Alta latência de rede
- Exaustão de recursos do TWAG (CPU/memória)
- Muitas autenticações simultâneas

Ferramentas de Depuração

Captura de Pacotes

```
# Capturar tráfego RADIUS
tcpdump -i eth0 -n port 1812 or port 1813 -w radius.pcap

# Capturar tráfego Diameter
tcpdump -i eth0 -n port 3868 -w diameter.pcap

# Capturar de AP específico
tcpdump -i eth0 -n host 10.7.15.72 and port 1812 -w radius-ap1.pcap
```

Analise com Wireshark (suporta dissetores RADIUS e Diameter).

Console Interativo

Anexe-se ao TWAG em execução para depuração ao vivo:

```
# Shell remoto para o TWAG em execução
iex -sname debug --remsh twag@hostname --cookie <cookie>
```

Do console IEx:

```
# Listar todos os clientes autenticados
CryptoState.keys()

# Obter estado de cliente específico
CryptoState.get("0505338057900001867@ulan.mnc057.mcc505.3gppnetwork.org")

# Listar todos os APs
APState.list()

# Listar sessões de contabilidade
ClientUsage.list()
```

Mensagens de Erro Comuns

Mensagem de Erro	Significado	Solução
Falha na validação do Message-Authenticator	Desvio de segredo compartilhado	Verifique se o segredo RADIUS corresponde no AP e no TWAG
Falha na verificação do RES: esperado <RES>, recebido <RES>	Resposta de autenticação incorreta	Verifique Ki do SIM, verifique o provisionamento do HSS
Tempo limite de conexão do par Diameter	Não consegue alcançar o HSS	Verifique a rede, firewall, configuração do HSS
Falha ao decodificar mensagem EAP	Pacote EAP malformatado	Verifique o firmware do AP, pode precisar de atualização do AP
Subtipo EAP-AKA desconhecido	Mensagem EAP-AKA não suportada	Dispositivo usando variante EAP-AKA não padrão
Requerida sincronização do número de sequência	SQL fora de sincronia	Normal, dispositivo irá resincronizar automaticamente

Conformidade com Padrões

OmniTWAG implementa as seguintes especificações 3GPP e IETF:

- **3GPP TS 23.402:** Melhorias de arquitetura para acessos não 3GPP
- **3GPP TS 24.302:** Acesso ao EPC via redes de acesso não 3GPP
- **3GPP TS 29.273:** Interfaces SWx/SWm baseadas em Diameter
- **3GPP TS 33.402:** Aspectos de segurança de acessos não 3GPP
- **3GPP TS 35.206:** Especificação do algoritmo Milenage
- **RFC 2863:** Autenticação RADIUS
- **RFC 2866:** Contabilidade RADIUS
- **RFC 3579:** Suporte RADIUS para EAP
- **RFC 4187:** Protocolo de autenticação EAP-AKA
- **RFC 5448:** EAP-AKA' (versão aprimorada)

Resumo

OmniTWAG, criado por [OmniTouch](#), fornece uma solução completa e compatível com padrões para descarregamento WiFi 3GPP:

- 1. **Implantação Flexível:** Suporta saída local ou tráfego roteado para casa
- 2. **Baseado em Padrões:** Implementa protocolos 3GPP SWx, EAP-AKA, RADIUS
- 3. **Autenticação Segura:** Autenticação mútua baseada em SIM com resync automático
- 4. **Criptografia Forte:** Chaves derivadas da MSK fornecem criptografia WPA2
- 5. **Pronto para Hotspot 2.0:** Habilita descarregamento totalmente automático e sem toque
- 6. **Controle do Operador:** Mantém identidade, política e opcionalmente cobrança
- 7. **Conectividade Flexível:** Conexão direta ao HSS ou via OmniDRA para roteamento/balanceamento de carga