YTECH SOLUÇÕES

Manual Operacional

Extreme Cloud IQ

Troubleshooting Básico e Mitigação

Finalidade do documento
Padronizar o diagnóstico inicial de falhas de conectividade e experiência Wi-Fi, indicando verificações objetivas, mitigações de baixo risco e os dados mínimos para escalonamento.

Versão: 1.2
Responsável técnico: Matheus Santana
Empresa: Ytech Soluções
Classificação: Uso interno

1. Objetivo, escopo e limites

Este manual orienta o primeiro atendimento de incidentes no Extreme Cloud IQ. O objetivo é localizar a camada da falha, restaurar o serviço com o menor impacto possível e produzir evidências úteis quando o caso precisar de análise especializada.

Incluído	Fora do escopo desta versão
AP offline, configuração pendente e SSID ausente	Projeto de cobertura, site survey e redesenho de RF
Associação, autenticação, DHCP, DNS e acesso	Upgrade em massa, rollback de firmware e RMA
Sinal, interferência, utilização e roaming	Alterações amplas sem janela ou plano de retorno
Coleta básica de eventos, logs e testes	Diagnóstico avançado de controladoras XIQ-C

Princípio operacional
Não alterar várias camadas ao mesmo tempo. Registre o estado inicial, teste uma hipótese, aplique uma mudança reversível e valide o resultado.

2. Método Ytech de troubleshooting

Comece pelo impacto e avance da camada física ao serviço. Se o sintoma já aponta para uma dependência comum — por exemplo, vários clientes acessam por IP, mas não por nome — investigue diretamente essa dependência.

Etapa	Pergunta-chave	Resultado esperado
1. Delimitar	Um cliente, vários clientes, um AP, um local ou toda a rede?	Escopo e horário definidos
2. Reproduzir	O erro é contínuo ou intermitente?	Sintoma reproduzível ou janela conhecida
3. Localizar	Falha em AP, rádio, associação, autenticação, IP ou serviço?	Camada provável identificada
4. Mitigar	Existe ação segura e reversível?	Serviço restaurado sem ampliar impacto
5. Confirmar	O cliente refez todo o fluxo com sucesso?	Associação, IP, DNS e aplicação validados
6. Registrar	Quais evidências sustentam a conclusão?	Linha do tempo e dados anexados

2.1 Dados mínimos antes de atuar

- Local, SSID, AP e rádio envolvidos; MAC do cliente e, quando disponível, endereço IP.
- Data, hora e timezone da ocorrência; início, duração e frequência.
- Quantidade e tipo de dispositivos afetados; sistema operacional e versão/driver.
- Mensagem exibida ao usuário e última condição conhecida como funcional.
- Alterações recentes em política, VLAN, DHCP, RADIUS, firewall, firmware ou infraestrutura.

3. Triagem rápida por sintoma

Sintoma	Primeira validação	Camada provável
AP aparece offline	Energia/PoE, link, IP, gateway, DNS e horário	Infraestrutura ou acesso à nuvem
Configuração pendente	Conectividade do AP, status de atualização e auditoria	Cloud/configuração
SSID não aparece	AP/radio online, política aplicada, agenda e banda	Configuração ou RF
Cliente não conecta	Eventos do cliente, compatibilidade, senha e segurança	Associação/autenticação
Conecta, mas não recebe IP	VLAN, porta do switch, escopo e relay DHCP	Rede cabeada/DHCP
Recebe IP, mas não navega	Gateway, DNS, ACL, firewall e captive portal	Serviços/rede
Lento ou instável	RSSI/SNR, retries, utilização, canal e cliente	RF/capacidade/terminal

4. AP offline ou sem comunicação com a nuvem

4.1 Verificação

- Confirme se o problema afeta um AP ou o local inteiro.
- Valide energia PoE, LED, link físico e erros na porta do switch.
- Confirme endereço IP, máscara, gateway, DNS e horário/NTP.
- Teste saída por IP e resolução por nome; verifique bloqueio, proxy ou inspeção TLS.
- Correlacione a última comunicação no Extreme Cloud IQ com eventos do switch/firewall.

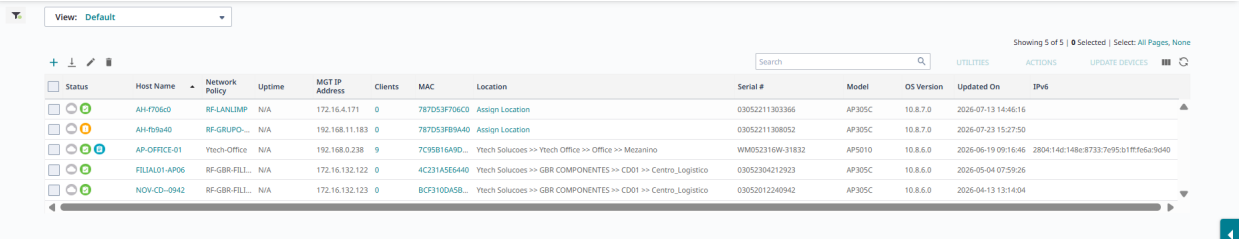


Figura 1 — Inventário de dispositivos com indicadores de estado e APs offline.

4.2 Mitigações básicas

Causa provável	Mitigação segura	Validação
Sem energia ou PoE insuficiente	Corrigir alimentação/porta; reiniciar a porta somente com autorização	AP inicia e mantém link
VLAN nativa ou DHCP incorretos	Restaurar configuração conhecida da porta/escopo	AP recebe IP válido
Gateway/DNS/NTP indisponível	Restabelecer dependência; evitar IP estático improvisado	Nome resolve e horário está correto
Firewall ou inspeção TLS	Liberar o fluxo cloud conforme política aprovada e excluir inspeção indevida	AP volta a comunicar
Falha isolada persistente	Coletar logs e realizar reinício controlado após registrar estado	Estabilidade após reinício

Evite
Excluir o AP, resetar para padrão ou trocar firmware antes de confirmar energia, rede, DNS e horário. Essas ações podem apagar contexto e aumentar o tempo de recuperação.

5. Configuração pendente ou auditoria divergente

- Confirme que o AP está online e com comunicação estável.
- Verifique se a política e o local corretos estão associados ao dispositivo.
- Revise alterações recentes e o status da última atualização.
- Compare a configuração desejada com o estado reportado; não force repetidamente enquanto o AP oscila.

Situação	Mitigação
AP online e atualização pendente	Executar atualização controlada em um equipamento e acompanhar o resultado.
AP offline ou instável	Restaurar conectividade antes de reenviar configuração.
Divergência após mudança recente	Revisar a mudança, dependências e compatibilidade; usar plano de retorno se necessário.
Falha repetida em vários APs	Suspender expansão da alteração e escalar com eventos e horário.

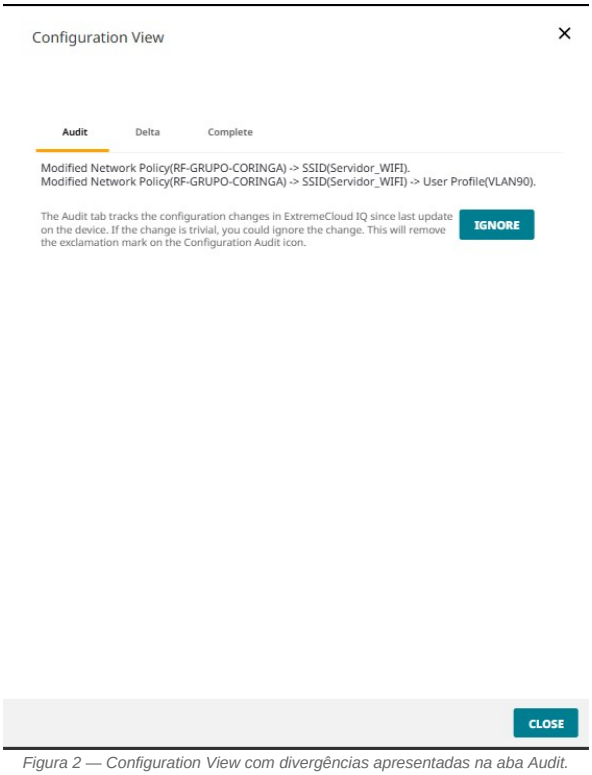
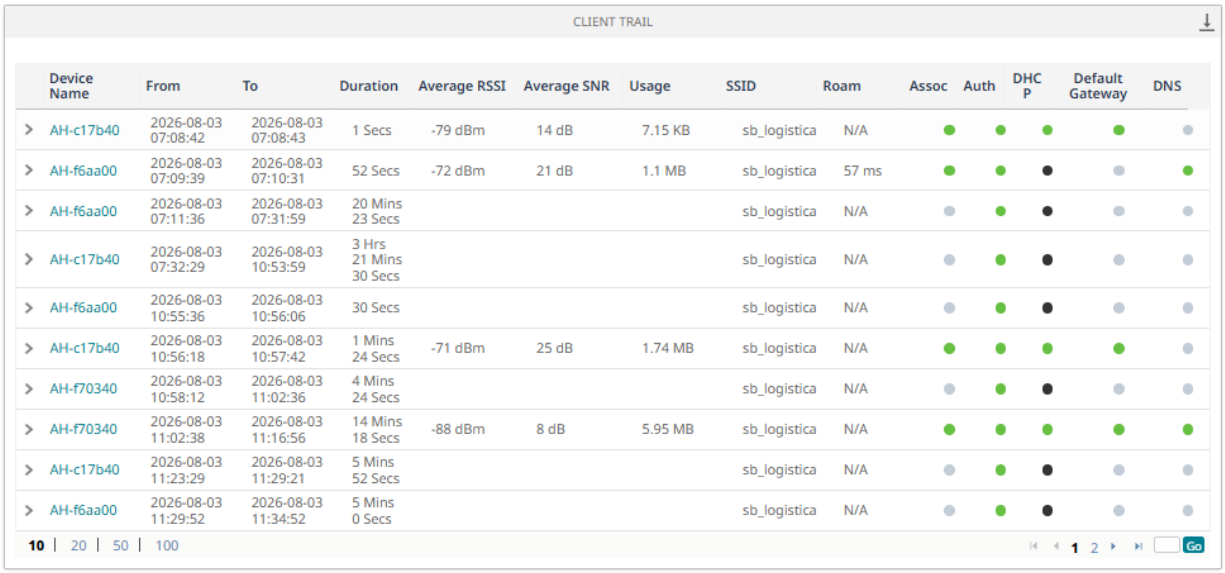


Figura 2 — Configuration View com divergências apresentadas na aba Audit.

6. SSID ausente ou cliente não associa

6.1 SSID não é anunciado

- Confirme se outros clientes veem o SSID e se o problema ocorre em todos os APs.
- Valide AP e rádio online, política aplicada, disponibilidade do SSID, agenda e bandas habilitadas.
- Verifique compatibilidade do cliente com banda, canal e taxas básicas; alguns terminais não suportam todos os canais.
- Compare com um cliente conhecido e próximo ao AP.



Device Name	From	To	Duration	Average RSSI	Average SNR	Usage	SSID	Roam	Assoc	Auth	DHCP	Default Gateway	DNS
AH-c17b40	2026-08-03 07:08:42	2026-08-03 07:08:43	1 Secs	-79 dBm	14 dB	7.15 KB	sb_logistica	N/A					
AH-f6aa00	2026-08-03 07:09:39	2026-08-03 07:10:31	52 Secs	-72 dBm	21 dB	1.1 MB	sb_logistica	57 ms					
AH-f6aa00	2026-08-03 07:11:36	2026-08-03 07:31:59	20 Mins 23 Secs				sb_logistica	N/A					
AH-c17b40	2026-08-03 07:32:29	2026-08-03 10:53:59	3 Hrs 21 Mins 30 Secs				sb_logistica	N/A					
AH-f6aa00	2026-08-03 10:55:36	2026-08-03 10:56:06	30 Secs				sb_logistica	N/A					
AH-c17b40	2026-08-03 10:56:18	2026-08-03 10:57:42	1 Mins 24 Secs	-71 dBm	25 dB	1.74 MB	sb_logistica	N/A					
AH-f70340	2026-08-03 10:58:12	2026-08-03 11:02:36	4 Mins 24 Secs				sb_logistica	N/A					
AH-f70340	2026-08-03 11:02:38	2026-08-03 11:16:56	14 Mins 18 Secs	-88 dBm	8 dB	5.95 MB	sb_logistica	N/A					
AH-c17b40	2026-08-03 11:23:29	2026-08-03 11:29:21	5 Mins 52 Secs				sb_logistica	N/A					
AH-f6aa00	2026-08-03 11:29:52	2026-08-03 11:34:52	5 Mins 0 Secs				sb_logistica	N/A					

10 | 20 | 50 | 100 — 1 2 — Go

Figura 3 — Client Trail com as etapas de associação, autenticação, DHCP, gateway e DNS.

6.2 Cliente vê o SSID, mas não associa

Verificação	Indício	Mitigação
Eventos/Client Trail	Rejeição, timeout ou incompatibilidade	Corrigir a causa indicada e repetir uma tentativa limpa
Perfil salvo no terminal	Parâmetros antigos ou senha em cache	Esquecer a rede e recriar o perfil
Segurança e recursos 802.11	Apenas um modelo/driver falha	Atualizar driver/OS ou testar política compatível
Sinal e distância	RSSI baixo ou alta repetição	Aproximar para teste e tratar RF separadamente

7. Falhas de autenticação

Primeiro diferencie associação Wi-Fi de autenticação. Um cliente pode enxergar o SSID e ainda falhar por credencial, política, certificado, RADIUS ou diretório.

Método	Verifique	Mitigação básica
PSK/PPSK	Senha, validade, vínculo e perfil salvo	Corrigir credencial; remover perfil antigo e testar novamente
MAC Authentication	Formato da MAC, cadastro, política e resposta do servidor	Ajustar cadastro/política após confirmar a MAC real
802.1X/RADIUS	Hora, certificado, identidade, método EAP, reachability e shared secret	Corrigir dependência; testar com usuário e terminal conhecidos
Portal cativo	Redirecionamento, DNS, certificado e liberação pré-autenticação	Restaurar dependências e abrir nova sessão

Leitura dos eventos RADIUS
Access-Reject indica que o servidor recebeu e rejeitou a solicitação; timeout indica ausência de resposta ou perda no caminho. Trate os dois sintomas de forma diferente.

8. Cliente conecta, mas não recebe endereço IP

- Confirme associação/autenticação concluídas antes de investigar DHCP.
- Identifique a VLAN efetivamente atribuída ao cliente, inclusive atributos RADIUS.
- Valide tagging/trunk entre AP e switch, VLAN permitida, SVI/gateway e DHCP relay.
- Confirme escopo ativo, endereços disponíveis e resposta Offer/ACK.
- Compare com outro cliente no mesmo SSID/AP e com o mesmo perfil de autorização.

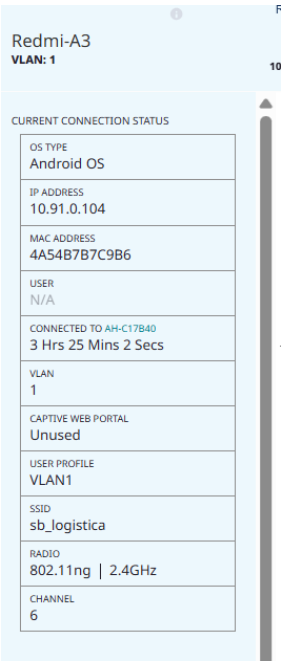


Figura 4 — Painel lateral com IP, MAC, VLAN, SSID, rádio e canal do cliente.

Indício	Causa provável	Mitigação
Endereço 169.254.x.x	Sem resposta DHCP	Restaurar caminho VLAN/relay/servidor
Alguns usuários falham	VLAN dinâmica ou pool específico	Revisar atributo RADIUS e escopo associado
Todos falham em um AP	Porta/trunk ou mapeamento local	Comparar a porta com AP funcional
Todos falham no local	Gateway, relay ou DHCP comum	Restaurar o serviço compartilhado

9. Cliente recebe IP, mas não acessa a rede

Teste	Se falhar	Próxima ação
Ping ao gateway	VLAN, gateway, isolamento ou ACL local	Validar rota local e políticas
Ping a IP permitido	Roteamento, firewall ou upstream	Seguir o caminho e checar bloqueios
Resolução DNS	DNS, DHCP option ou ACL	Testar servidor configurado e corrigir opção/fluxo
Acesso por nome e HTTPS	Proxy, certificado, portal ou aplicação	Correlacionar com logs do serviço
Outro cliente no mesmo AP	Problema específico do terminal	Recriar perfil, atualizar e comparar

Teste de confirmação
Após a mitigação, desconecte e reconecte um cliente de teste. Confirme nova associação, autenticação, endereço IP, gateway, DNS e aplicação — não considere resolvido apenas porque o painel ficou verde.

10. Lentidão, instabilidade e roaming

- Delimite se o problema é de um cliente, modelo, AP, rádio, local ou horário.
- Compare RSSI, SNR, retries, taxa, utilização de canal e volume de clientes.
- Procure interferência co-canal/adjacente e fontes não Wi-Fi; correlacione com o horário.
- Lembre que a decisão de roaming é principalmente do cliente. Compare driver, potência, banda e AP escolhido.
- Teste próximo ao AP e com outro terminal antes de alterar canais, potência ou taxas básicas.

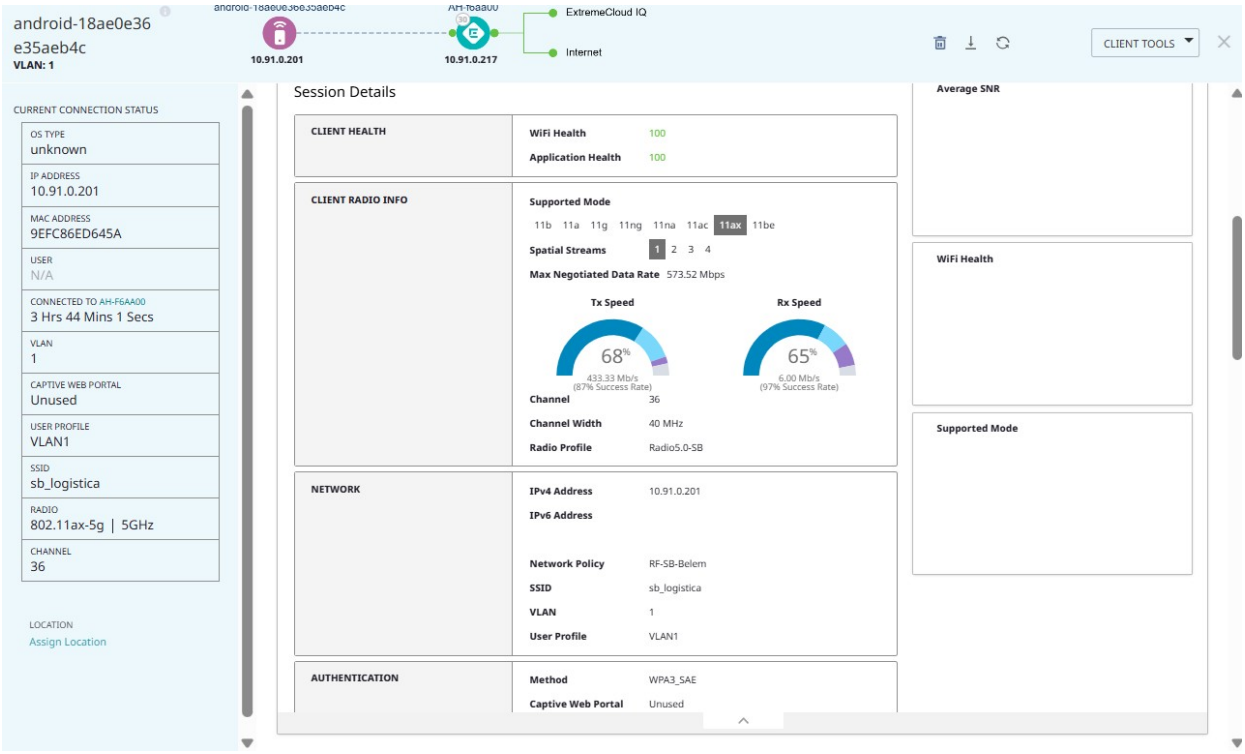


Figura 5 — Session Details com saúde, rádio, velocidades e parâmetros de rede do cliente.

Cenário	Mitigação inicial
Cliente isolado	Atualizar driver/OS, recriar perfil e comparar com terminal conhecido.
Sinal fraco em área específica	Reposicionar o usuário para contingência e registrar necessidade de análise de cobertura.
Alta utilização	Identificar consumo, distribuir carga quando possível e programar análise de capacidade.
Interferência/retries elevados	Confirmar persistência; evitar troca manual ampla de canais sem análise.
Roaming tardio	Validar cobertura sobreposta e cliente; testar ajustes somente em escopo controlado.

11. Evidências e ferramentas básicas

Fonte	Registrar
Extreme Cloud IQ — AP/cliente	Status, política, local, rádio, RSSI/SNR, VLAN, IP e linha do tempo.
Eventos e Client Trail	Tentativas de associação, autenticação, DHCP, roaming e mensagens de erro.
Switch/DHCP/RADIUS/firewall	Porta, VLAN, leases, códigos de resposta, bloqueios e timestamps.
Testes	Origem/destino, ping por IP/nome, horário e resultado.
Captura de pacotes	Somente quando o evento não explica a falha; limitar interface, cliente e janela.

11.1 Comandos básicos no AP, quando autorizados

Objetivo	Comando de referência
Endereçamento	show ip interface
Rota padrão	show ip route / show default
DNS	show dns
Relógio	show clock
Eventos locais	show log

Atenção
A sintaxe pode variar conforme plataforma e versão. Acesso CLI é complementar: registre a saída e não execute mudanças sem procedimento aprovado.

12. Escalonamento

Escale quando a mitigação segura não restaurar o serviço, quando houver impacto amplo/recorrente, suspeita de defeito ou necessidade de alterar firmware, RF ou política em larga escala.

Campo obrigatório	Conteúdo
Impacto	Usuários, locais, SSIDs, APs e serviços afetados.
Linha do tempo	Início, duração, recorrência, timezone e última condição funcional.
Identificadores	MAC/serial do AP, MAC do cliente, IP, VLAN, usuário anonimizado.
Evidências	Capturas de tela, eventos, logs, testes e mensagens completas.
Ações realizadas	O que foi alterado, resultado e eventual retorno.
Objetivo	Qual comportamento deve ser restaurado e como validar.

13. Checklist final de atendimento

✓	Controle
☐	Escopo, horário e impacto registrados.
☐	AP, SSID, rádio e cliente identificados.
☐	Camada provável definida antes de alterar configuração.
☐	Dependências comuns verificadas: VLAN, DHCP, DNS, gateway, RADIUS e firewall.
☐	Mitigação reversível aplicada e documentada.
☐	Fluxo completo validado com cliente de teste.
☐	Evidências e critério de escalonamento preenchidos.

14. Referências e controle de versão

Referência técnica principal: Extreme Cloud IQ – Controller – Troubleshooting Student Guide v23.4.0, Extreme Networks. O conteúdo deste manual foi resumido e adaptado ao atendimento básico do Extreme Cloud IQ; funções exclusivas do Controller não foram convertidas em procedimentos operacionais.

Versão	Data	Responsável	Alteração
1.0	03/08/2026	Matheus Santana / Ytech Soluções	Emissão inicial: troubleshooting básico, mitigação e escalonamento.
1.1	03/08/2026	Matheus Santana / Ytech Soluções	Inclusão das capturas operacionais do Extreme Cloud IQ.
1.2	03/08/2026	Matheus Santana / Ytech Soluções	Padronização visual final da coleção e remoção da data da capa.