YTECH SOLUÇÕES

Manual Operacional

Extreme Cloud IQ

Gerenciamento e Monitoramento Básico

Finalidade do documento

- Orientar atividades recorrentes de consulta, gerenciamento e monitoramento no Extreme Cloud IQ.
- Servir como guia rápido para continuidade operacional em ausência, férias ou transição técnica.
- Priorizar verificações simples, evidências e critérios de escalonamento.

Versão: 1.3
Responsável técnico: Matheus Santana
Empresa: Ytech Soluções
Classificação: Uso interno

Sumário executivo

Regra operacional

- Antes de concluir qualquer análise, confirme tenant, cliente, unidade, AP, SSID e período analisado.
- Quando houver anormalidade, registre evidências antes de alterar configurações, reiniciar dispositivos ou escalar o caso.

1. Objetivo, escopo e referência

Este documento orienta colaboradores da Ytech Soluções na execução de atividades básicas e recorrentes de gerenciamento, consulta e monitoramento de ambientes Wi-Fi administrados pelo Extreme Cloud IQ.

O foco é permitir que outro colaborador consiga consultar informações essenciais do ambiente, identificar anormalidades simples e registrar evidências para continuidade operacional, suporte ou escalonamento.

Este manual cobre

- Acesso ao menu Manage.
- Consulta de dispositivos.
- Verificação de status de APs.
- Uso básico de ações e utilitários.
- Monitoramento básico de APs e clientes.
- Consulta de eventos e logs.
- Consulta de licenciamento.
- Verificação básica de servidores em Policy Settings.
- Consulta básica de ML Insights.
- Rotina operacional de monitoramento.

Este manual não cobre

- Troubleshooting avançado.
- Ajustes avançados de RF.
- Criação ou alteração profunda de Network Policies.
- Configuração avançada de SNMP.
- Backup, restore ou reset de VIQ.
- Análise avançada de ML Insights.
- Configuração avançada de usuários administrativos.
- Correção detalhada de falhas RADIUS, roaming ou performance.

Referência técnica

- ExtremeWireless Cloud Management Student Guide v26.2.3.
- Documentação oficial da Extreme Networks.
- Experiência operacional da Ytech em ambientes Extreme Cloud IQ.
- Manual Operacional Ytech - Instalação e Configuração Inicial.

2. Visão geral do menu Manage

A maior parte das atividades de gerenciamento ocorre no menu Manage. Este menu concentra consultas de dispositivos, clientes, eventos, alarmes e relatórios.

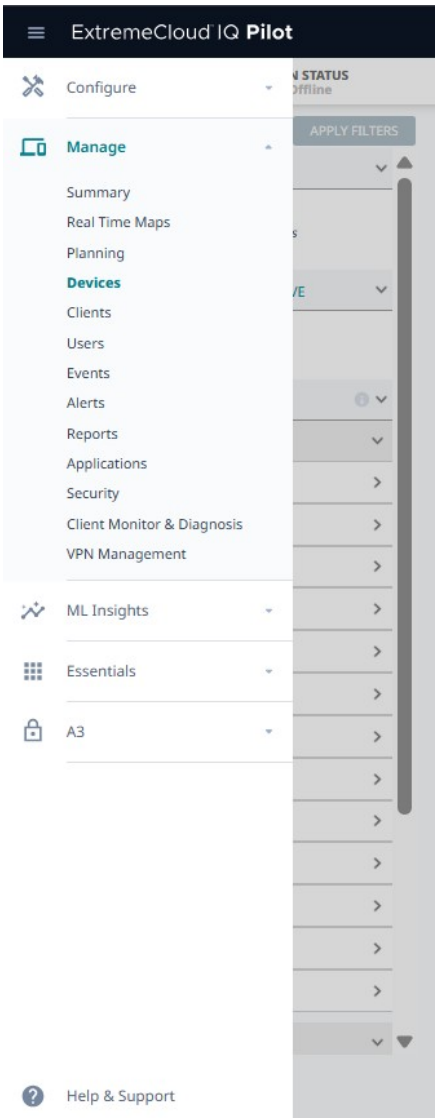

Figura 1 — Menu Manage expandido no Extreme Cloud IQ.

Uso principal do menu Manage

- Consultar dispositivos.
- Validar APs online e offline.
- Consultar clientes conectados.
- Acessar eventos e alarmes.
- Acessar relatórios e diagnósticos básicos.

Procedimento

1. Acessar o Extreme Cloud IQ.
2. Confirmar o tenant correto.
3. Confirmar cliente e unidade.
4. Acessar o menu lateral.
5. Selecionar Manage.
6. Escolher a área desejada: Devices, Clients, Events, Alarms ou Reports.
7. Aplicar filtros de site, período ou dispositivo, quando necessário.

Checklist inicial

- ☐ Tenant correto validado
- ☐ Cliente correto identificado
- ☐ Unidade ou site confirmado
- ☐ Menu Manage acessado
- ☐ Filtros aplicados corretamente
- ☐ Período de análise definido

Erros comuns
- Consultar dados no tenant errado.
- Esquecer filtro de site ou unidade.
- Analisar período incorreto.
- Validar apenas o dashboard e não abrir os detalhes do dispositivo ou cliente.
- Confundir XIQ Classic, XIQ New e Extreme Platform ONE.

2.1 Summary e visão consolidada

A tela Summary reúne indicadores de uso, clientes, aplicações e desempenho do ambiente. Use filtros de localização e período para evitar conclusões baseadas em um escopo incorreto.

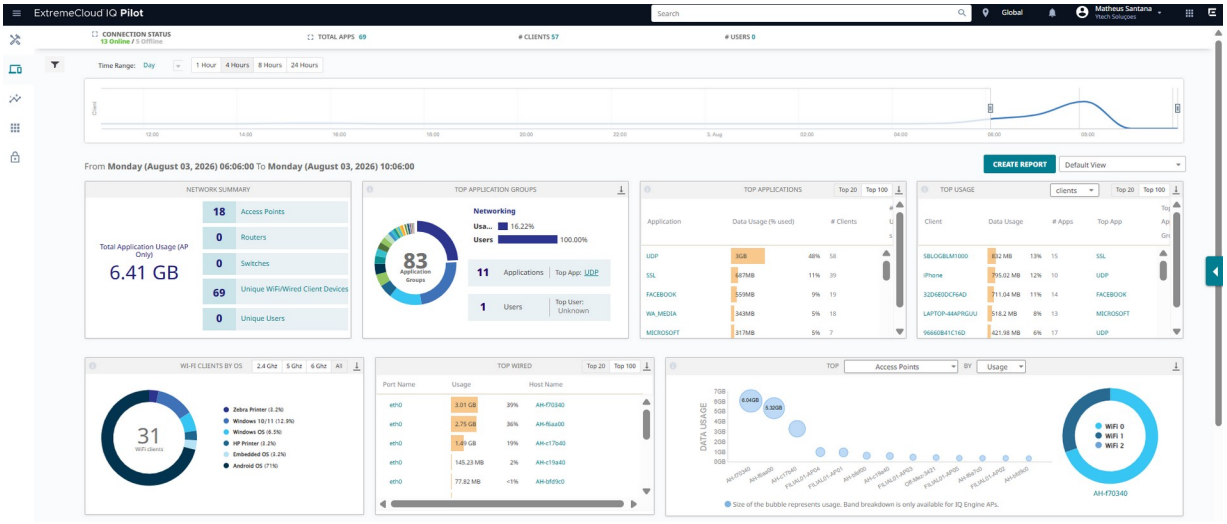

Figura 2 — Summary com indicadores consolidados do ambiente.

O que verificar
☐ Localização e período corretos
☐ Quantidade de clientes e dispositivos
☐ Uso e aplicações com maior consumo
☐ Indicadores fora do comportamento esperado

3. Gerenciamento de dispositivos

A área Devices permite visualizar, consultar, adicionar, atualizar e administrar APs e outros equipamentos registrados no Extreme Cloud IQ.

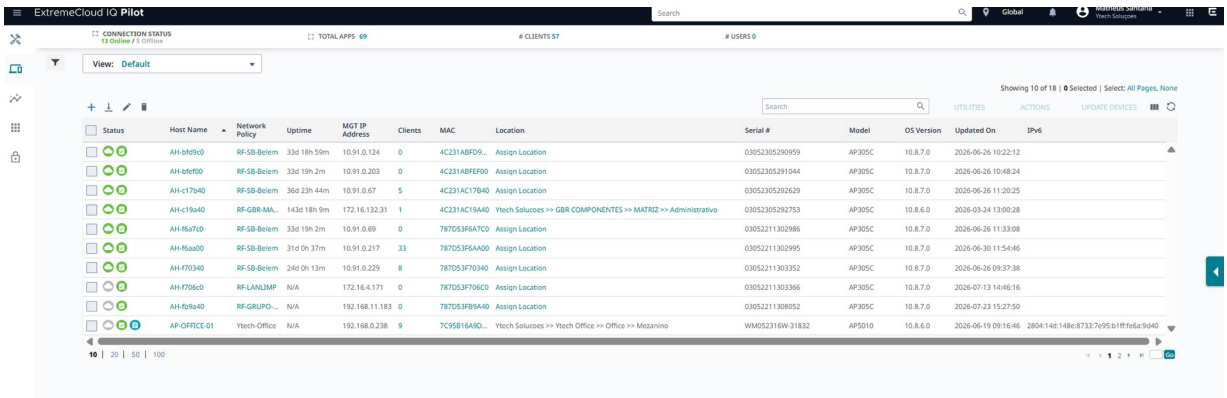

Figura 3 — Inventário de dispositivos em Manage > Devices.

Informações importantes na lista de dispositivos
- Status de conexão.
- Hostname.
- Network Policy.
- Uptime.
- IP de gerenciamento.
- Quantidade de clientes.
- MAC address.
- Localização.
- Serial number.
- Modelo.
- Versão do sistema.
- Data da última atualização.
- Indicador de configuração pendente.

Indicação	Interpretação
Ícone verde/cloud verde	Dispositivo conectado ao Extreme Cloud IQ.
Ícone cinza	Dispositivo desconectado ou sem comunicação com a nuvem.
Ícone de auditoria/update	Indica se a configuração do AP precisa ser atualizada.

Procedimento

1. Acessar Manage.
2. Selecionar Devices.
3. Pesquisar o AP por hostname, serial number, MAC address ou IP.
4. Validar o status do AP.
5. Confirmar Network Policy associada.
6. Confirmar localização.
7. Confirmar modelo e versão de software.
8. Verificar se há configuração pendente.
9. Clicar no hostname para abrir detalhes de monitoramento, se necessário.

Validação

- ☐ AP encontrado no inventário
- ☐ Status identificado
- ☐ Hostname validado
- ☐ Serial number validado
- ☐ Network Policy confirmada
- ☐ Localização confirmada
- ☐ Versão de software identificada
- ☐ Indicador de atualização verificado

Atenção

- AP online no inventário não significa necessariamente que o serviço Wi-Fi está íntegro.
- Para confirmar funcionamento, valide também SSID, clientes conectados, eventos, alarmes e, quando necessário, teste com cliente real.

4. Ações e utilitários em APs

Utilities e Actions permitem executar ações operacionais em dispositivos selecionados, como diagnóstico, ping, atualização, reboot, associação de policy e alteração de localização.

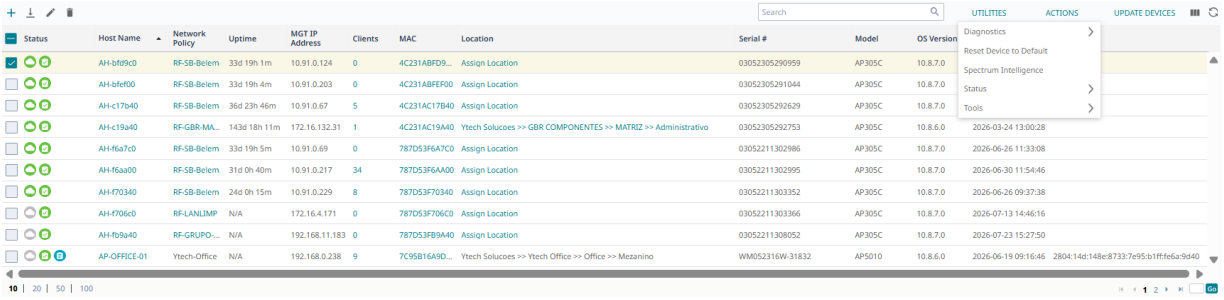

Figura 4 — Menu Utilities exibido após a seleção de um AP.

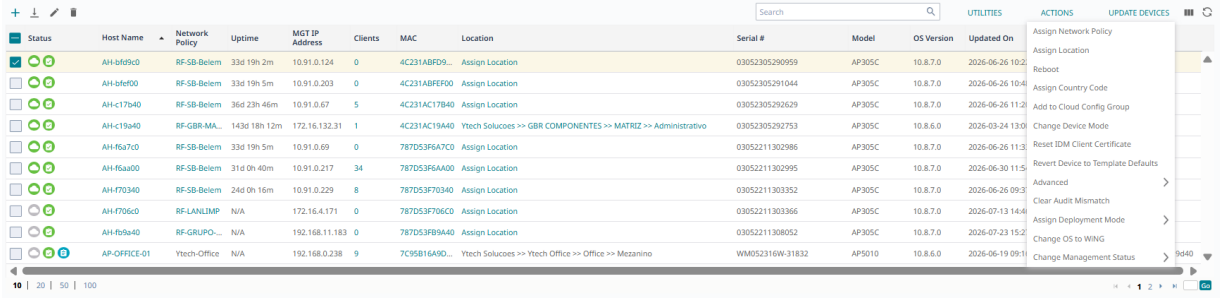

Figura 5 — Menu Actions disponível para o dispositivo selecionado.

Ações comuns

- Executar ping.
- Acessar diagnósticos.
- Atualizar configuração.
- Reiniciar dispositivo.
- Associar localização.
- Associar Network Policy.

Procedimento - Executar ping pelo XIQ

1. Acessar Manage > Devices.
2. Localizar o AP desejado.
3. Selecionar o AP.
4. Abrir o menu Utilities.
5. Selecionar Diagnostics.
6. Selecionar Ping.
7. Informar o destino do teste.
8. Executar o teste.
9. Registrar o resultado, se estiver tratando incidente.

Procedimento - Acessar Actions do AP

1. Acessar Manage > Devices.
2. Selecionar o checkbox do AP.
3. Acessar o menu Actions.
4. Verificar as ações disponíveis.
5. Selecionar a ação desejada somente após validar impacto.
6. Confirmar execução.
7. Registrar evidência, quando aplicável.

Cuidados antes de executar ações

- ☐ AP correto selecionado
- ☐ Tenant correto validado
- ☐ Unidade/localização confirmada
- ☐ Impacto avaliado
- ☐ Janela de alteração confirmada, se houver risco
- ☐ Evidência registrada antes da ação

Atenção

- Reboot, update ou mudança de policy podem causar impacto no serviço.
- Evite executar ações em múltiplos APs simultaneamente sem validar escopo e janela de alteração.

5. Monitoramento de APs

O monitoramento de APs permite verificar se o equipamento está online, saudável, com a policy correta e sem alarmes relevantes.

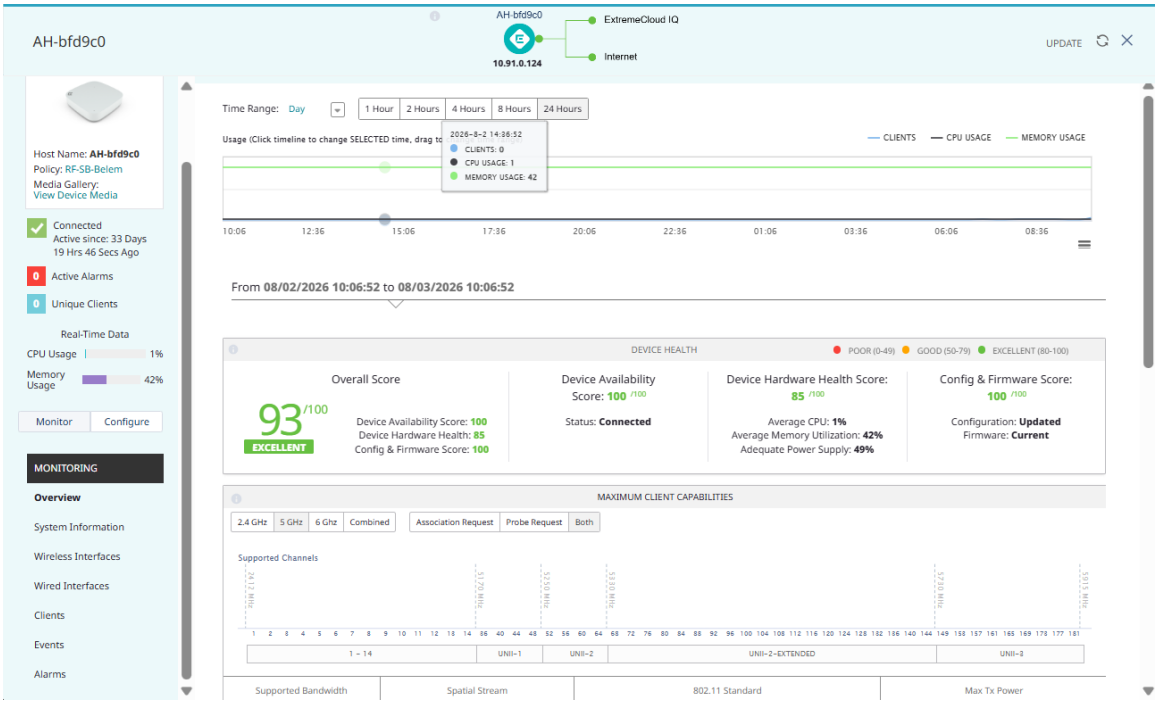

Figura 6 — Visão de monitoramento e saúde de um access point.

Quando usar

- Cliente informa instabilidade em uma unidade.
- AP aparece offline ou com alerta.
- SSID não aparece em determinada área.
- Há suspeita de problema de rádio, cabo, porta ou atualização.
- É necessário validar saúde geral de um AP.

Procedimento

1. Acessar Manage > Devices.
2. Localizar o AP por hostname, serial, MAC ou IP.
3. Clicar no hostname do AP.
4. Verificar o status geral do dispositivo.
5. Validar Network Policy associada.
6. Verificar uptime e versão de software.
7. Consultar interfaces wireless.
8. Consultar interfaces cabeadas, quando necessário.
9. Verificar clientes conectados.
10. Consultar eventos e alarmes do AP.

O que verificar

- ☐ AP está online
- ☐ AP está com a policy correta
- ☐ AP está na localização correta
- ☐ AP possui clientes conectados, quando esperado
- ☐ Interfaces wireless estão ativas
- ☐ Não há alarme crítico ativo
- ☐ Não há update pendente indevido
- ☐ Versão de software está compatível com o ambiente

Situação	Possível significado
AP online sem clientes	Pode ser normal, mas validar SSID, rádio e localização.
AP offline	Validar energia, PoE, switch, VLAN, DHCP, DNS e internet.
AP com update pendente	Configuração foi alterada e ainda não aplicada.
AP com muitos clientes	Verificar carga, rádio e possível necessidade de redistribuição.
AP com alarme ativo	Consultar eventos antes de qualquer ação.

Cuidados

- Não reiniciar AP sem validar impacto.
- Não aplicar update em múltiplos APs sem janela ou autorização.
- Não concluir falha física antes de validar rede cabeada e comunicação cloud.

6. Monitoramento de clientes

O monitoramento de clientes permite verificar como um dispositivo está conectado à rede Wi-Fi: SSID, AP associado, IP, VLAN, RSSI, SNR, autenticação e histórico de conexão.

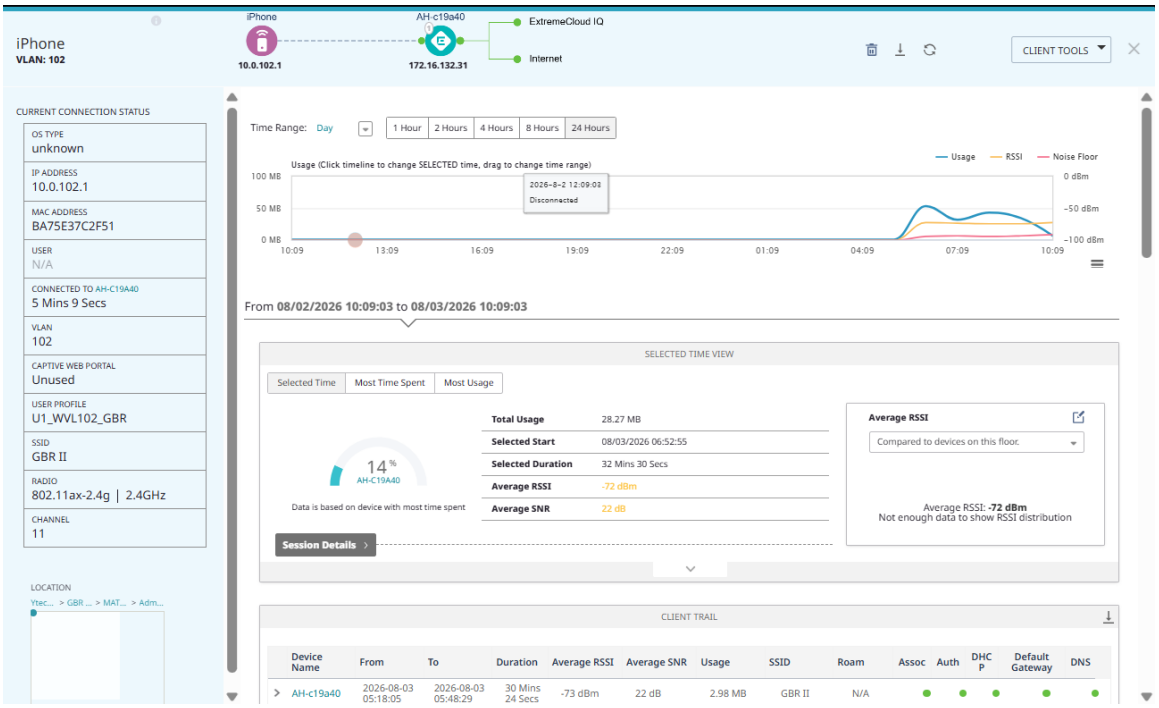

Figura 7 — Informações operacionais de um cliente conectado.

Quando usar
- Cliente não consegue acessar a rede.
- Cliente conecta, mas não navega.
- Cliente recebe IP incorreto.
- Cliente apresenta lentidão.
- Cliente está conectado a AP distante.
- É necessário validar RSSI, SNR, VLAN ou SSID.

Procedimento

1. Acessar Manage > Clients ou Client Monitor.
2. Pesquisar pelo MAC, hostname, usuário ou IP.
3. Abrir os detalhes do cliente.
4. Confirmar SSID conectado.
5. Confirmar AP associado.
6. Confirmar IP recebido.
7. Confirmar VLAN.
8. Verificar RSSI e SNR.
9. Verificar eventos de associação, autenticação, DHCP, gateway e DNS.
10. Registrar evidência, se houver anormalidade.

O que verificar
- ☐ Cliente aparece conectado
- ☐ SSID está correto
- ☐ AP associado está coerente com a localização
- ☐ IP foi recebido
- ☐ VLAN está correta
- ☐ RSSI está aceitável
- ☐ SNR está aceitável
- ☐ Autenticação teve sucesso
- ☐ DHCP teve sucesso
- ☐ Gateway e DNS aparecem como válidos, quando disponível

Situação	Possível causa
Cliente não aparece	Pode estar desconectado, em outro SSID, outro tenant ou fora do período consultado.
Cliente conecta sem IP	Validar VLAN, DHCP, User Profile e porta do switch.
Cliente com RSSI baixo	Sinal fraco, AP distante, barreira física ou roaming inadequado.
Cliente com SNR baixo	Interferência ou ruído elevado.
Cliente autentica, mas não navega	Validar VLAN, gateway, DNS e firewall policy.
Cliente em AP distante	Possível problema de roaming ou potência excessiva.

Parâmetros úteis
- RSSI indica intensidade do sinal recebido pelo cliente.
- SNR indica relação sinal/ruído. Quanto maior, melhor.
- VLAN indica a rede lógica onde o cliente foi alocado.
- SSID indica a rede Wi-Fi usada pelo cliente.
- AP associado indica em qual access point o cliente está conectado.

Cuidados
- Não avaliar apenas o sinal. Cliente pode ter bom RSSI e ainda falhar em DHCP, DNS ou autenticação.
- Sempre confirmar se o cliente está no SSID e VLAN esperados.
- Para coletores, impressoras e IoT, validar também compatibilidade de banda e segurança.

7. Logs e eventos

Logs e eventos ajudam a identificar quem alterou algo, quando ocorreu uma falha e quais eventos foram registrados pela plataforma.

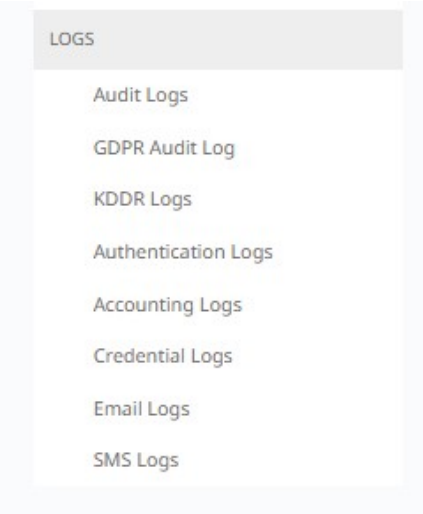

Figura 8 — Categorias de logs disponíveis em Global Settings.

Quando usar
- Investigar alteração realizada por administrador.
- Validar tentativa de autenticação.
- Verificar sessões de usuários.
- Coletar evidências para suporte.
- Entender quando determinado evento começou.

Log	Quando consultar
Audit Logs	Para verificar alterações administrativas.
Authentication Logs	Para validar autenticações PPSK, RADIUS ou portal.
Accounting Logs	Para consultar sessões de usuários.
Credential Logs	Para credenciais expiradas.
Event Logs	Para eventos de APs, clientes ou sistema.

Procedimento - Consultar Audit Logs

1. Acessar Global Settings.
2. Ir até Logs.
3. Selecionar Audit Logs.
4. Definir o período de análise.
5. Filtrar por usuário, categoria ou descrição, se necessário.
6. Verificar quem executou a ação.
7. Registrar evidência, se aplicável.

Procedimento - Consultar Authentication Logs

1. Acessar Global Settings.
2. Ir até Logs.
3. Selecionar Authentication Logs.
4. Definir período de análise.
5. Pesquisar por cliente, usuário ou SSID, quando disponível.
6. Verificar se houve sucesso ou falha de autenticação.
7. Registrar evidência.

O que registrar como evidência
- ☐ Tipo de log consultado
- ☐ Período analisado
- ☐ Usuário ou cliente analisado
- ☐ Horário do evento
- ☐ Descrição do evento
- ☐ Resultado encontrado

Cuidados
- Sempre ajustar o período de análise.
- Conferir timezone/horário do evento.
- Não usar logs isoladamente: correlacionar com cliente, AP, SSID e horário informado.
- Em caso de incidente crítico, exportar ou capturar print antes que o histórico fique difícil de localizar.

7.1 Eventos do menu Manage

Manage > Events apresenta eventos reportados pelos dispositivos. Antes da análise, ajuste o período e aplique filtros por equipamento, local ou categoria. Registre horário, dispositivo e descrição do evento relevante.

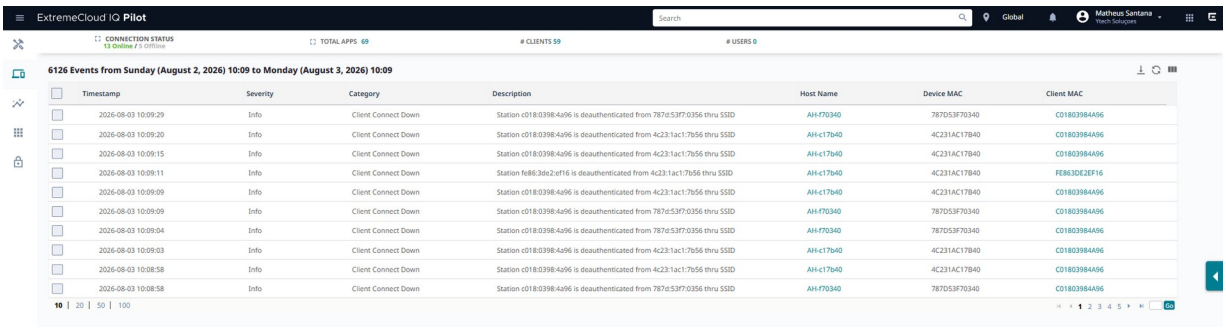

Figura 9 — Eventos reportados pelos dispositivos em Manage > Events.

O que verificar
☐ Período e timezone confirmados
☐ Dispositivo ou local correto
☐ Evento correlacionado ao horário da ocorrência
☐ Evidência exportada ou registrada

7.2 Relatórios operacionais

Manage > Reports permite gerar relatórios pontuais ou recorrentes. Defina o tipo de relatório, o escopo, o período e os destinatários antes de salvar o agendamento. Revise o primeiro resultado antes de adotar uma recorrência.

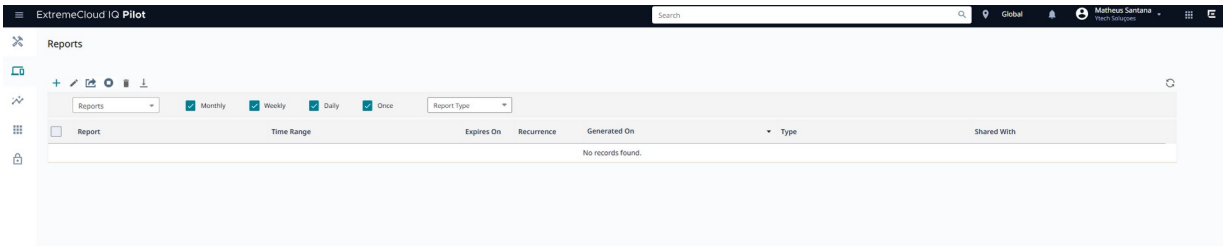

Figura 10 — Área de relatórios do Extreme Cloud IQ.

O que verificar
☐ Tipo de relatório adequado
☐ Localização e período definidos
☐ Recorrência e destinatários revisados
☐ Primeira execução validada

8. Administração e licenciamento

A área de administração reúne configurações globais da conta, licenciamento e opções de gerenciamento da instância.

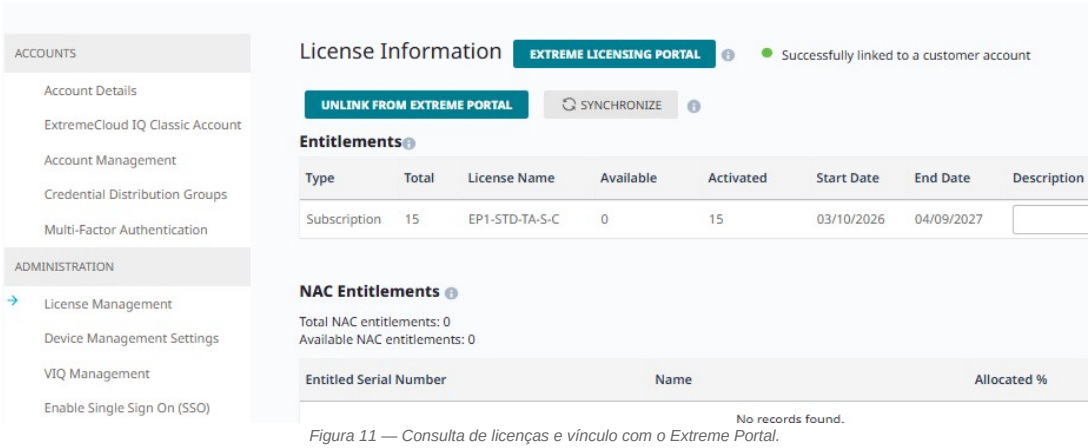

Figura 11 — Consulta de licenças e vínculo com o Extreme Portal.

Quando usar
- Validar se há licenças disponíveis.
- Verificar licenças ativadas ou alocadas.
- Confirmar vínculo com Extreme Portal.
- Consultar configurações globais com cuidado.

Procedimento - Consultar licenças

1. Acessar Global Settings.

2. Entrar em Administration.
3. Acessar License Management.
4. Verificar licenças disponíveis.
5. Verificar licenças ativadas.
6. Verificar licenças alocadas.
7. Validar datas de início e expiração, quando disponível.
8. Registrar evidência, se necessário.

O que verificar

- ☐ Tipo de licença
- ☐ Total disponível
- ☐ Total ativado
- ☐ Total alocado
- ☐ Data de início
- ☐ Data de expiração
- ☐ Conta vinculada ao Extreme Portal

Cuidados

- Não desvincular conta do Extreme Portal sem autorização.
- Não alterar configurações globais sem entender impacto.
- Em caso de falta de licença, não tentar corrigir removendo APs sem validação.
- Registrar evidência antes de acionar comercial, fabricante ou suporte.

Fora do escopo operacional deste manual

- Backup/restore de VIQ.
- Reset de base VIQ.
- Supplemental CLI.
- Alterações globais avançadas.

9. Servidores em Policy Settings

Policy Settings pode conter servidores e serviços importantes para o funcionamento e gerenciamento da rede, como DNS, NTP, Syslog, SNMP e RADIUS. Neste manual, o foco é consulta e validação básica.

Quando usar

- Validar servidor configurado em uma policy.
- Conferir NTP, DNS, Syslog ou SNMP.
- Apoiar análise de logs, autenticação ou monitoramento externo.
- Verificar se a policy possui servidor esperado pelo cliente.

Servidor	Função
DNS	Resolução de nomes.
NTP	Sincronização de horário.
Syslog	Envio de logs para servidor externo.
SNMP	Gerenciamento por ferramenta externa.
RADIUS	Autenticação, accounting ou NAC.

Procedimento - Consultar servidores da policy

1. Acessar Configure.
2. Entrar em Network Policies.
3. Abrir a policy desejada.
4. Acessar Policy Details ou Policy Settings.
5. Consultar servidores configurados.
6. Validar IP, hostname e finalidade.
7. Confirmar se a configuração condiz com o ambiente do cliente.
8. Registrar evidência, se houver divergência.

Cuidados

- Não alterar servidores de policy sem validar impacto.
- Alterações em NTP, DNS, RADIUS ou SNMP podem afetar múltiplos APs.
- Em ambientes com NAC, validar RADIUS com o responsável do cliente.
- SNMP pode exigir configuração em mais de um ponto da policy. A configuração completa deve ficar no Manual 04.

10. ML Insights: Network 360, Scorecard e Client 360

ML Insights reúne o Network 360 Monitor, o Network Scorecard e o Client 360. Essas visões apoiam a identificação de tendências de saúde, disponibilidade, Wi-Fi, serviços e experiência dos clientes; qualquer suspeita deve ser confirmada nos detalhes do AP, cliente, evento ou log.

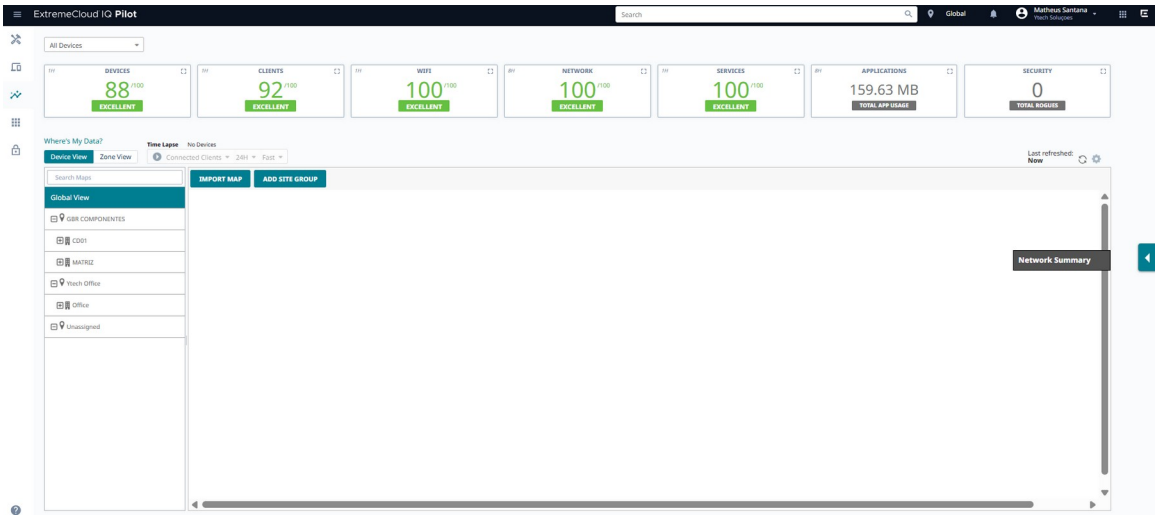

Figura 12 — Network 360 Monitor.

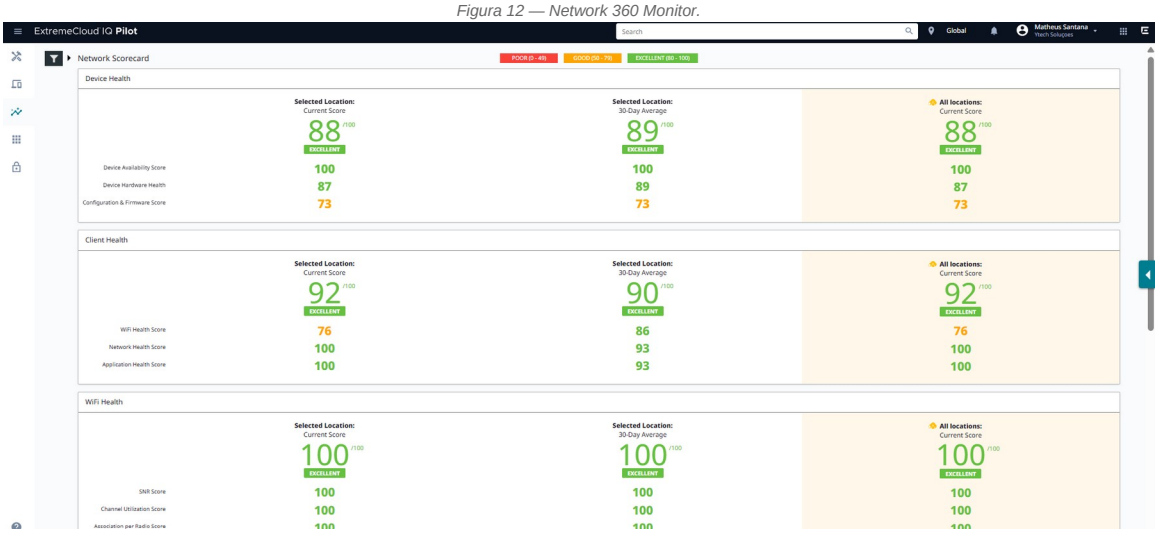

Figura 13 — Network Scorecard e indicadores consolidados.

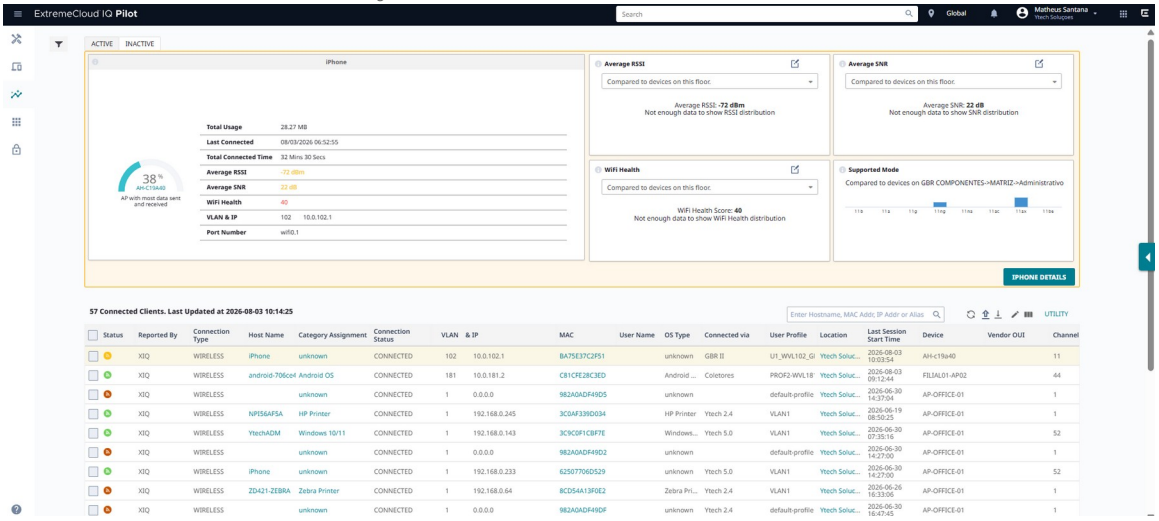

Figura 14 — Client 360 e lista de clientes monitorados.

Quando usar

- Verificar saúde geral da rede.
- Identificar clientes com problemas recorrentes.
- Observar tendências de qualidade.
- Complementar análise de APs, clientes e eventos.

O que verificar

- ☐ Saúde geral da rede
- ☐ Clientes com baixa experiência
- ☐ APs ou locais com maior incidência de problema
- ☐ Alertas ou insights relevantes
- ☐ Tendências de degradação

Procedimento

1. Acessar ML Insights ou área equivalente.
2. Verificar a visão geral de saúde.
3. Consultar indicadores de rede.
4. Consultar indicadores de clientes.
5. Identificar itens críticos ou recorrentes.
6. Validar os achados em Devices, Clients ou Logs.
7. Registrar evidência se houver anormalidade.

Cuidados

- Não usar ML Insights como única evidência.
- Confirmar qualquer suspeita nos detalhes do AP, cliente ou log.
- Avaliar período analisado antes de concluir degradação.

11. Rotina operacional de monitoramento

Este checklist deve ser usado em rotina diária, semanal ou antes de reuniões operacionais com clientes.

Checklist rápido

- ☐ Confirmar tenant correto
- ☐ Verificar APs offline
- ☐ Verificar APs com update pendente
- ☐ Verificar alarmes críticos
- ☐ Validar APs sem localização
- ☐ Consultar clientes com baixa qualidade
- ☐ Consultar logs relevantes
- ☐ Verificar licenças disponíveis
- ☐ Registrar evidências e escalar casos críticos

Frequência	Atividade
Diária	Verificar APs offline, alarmes críticos e clientes afetados.
Semanal	Revisar APs sem localização, updates pendentes e licenças.
Sob demanda	Consultar logs, clientes específicos, RADIUS e eventos.
Antes de mudança	Registrar estado atual do ambiente.
Após mudança	Validar APs, clientes, SSIDs e alertas.

Fechamento operacional

- Uma análise só deve ser considerada concluída quando houver evidência mínima do estado do ambiente.
- Em caso de falha, registrar o ponto observado e escalar quando necessário.

Histórico de revisão

Versão	Data	Responsável	Alteração
1.0	13/07/2026	Matheus Santana / Ytech Soluções	Criação inicial.
1.1	03/08/2026	Matheus Santana / Ytech Soluções	Inclusão de prints operacionais, Summary, Events, Reports e ampliação de ML Insights.
1.2	03/08/2026	Matheus Santana / Ytech Soluções	Refino visual para alinhar capa, tipografia, espaçamento, tabelas e cabeçalho ao Manual 01.
1.3	03/08/2026	Matheus Santana / Ytech Soluções	Padronização visual final da coleção e remoção da data da capa.