YTECH SOLUÇÕES

Manual Operacional

Extreme Cloud IQ

Configurações Básicas

Finalidade do documento

- Orientar atividades básicas e recorrentes de configuração no Extreme Cloud IQ.
- Servir como guia rápido para continuidade operacional em ausência, férias ou transição técnica.
- Priorizar procedimentos executáveis, checklists e validações essenciais.

Versão: 1.4
Responsável técnico: Matheus Santana
Empresa: Ytech Soluções
Classificação: Uso interno

Sumário executivo

Este manual foi reduzido para concentrar apenas as atividades básicas que outro colaborador deve conseguir executar no Extreme Cloud IQ.

Capítulo	Atividade
1	Objetivo, escopo e referência
2	Acesso à plataforma e validações iniciais
3	Onboarding de APs
4	Organização de locais
5	Criação de Network Policy
6	Criação de SSID/WLAN
7	User Profiles e VLAN
8	Autenticação básica
9	Radio Profiles básicos
10	Aplicação da configuração e validação final

Regra operacional

- Antes de alterar qualquer configuração, confirme tenant, cliente, unidade, Network Policy e APs impactados.
- Sempre teste com cliente real após aplicar configuração.

1. Objetivo, escopo e referência

Este documento orienta a execução das configurações básicas e recorrentes no Extreme Cloud IQ, com foco em continuidade operacional e apoio a colaboradores da Ytech Soluções.

Este manual cobre

- Acesso ao tenant e validações iniciais.
- Onboarding de access points.
- Organização de locais: sites, buildings e floors.
- Criação de Network Policies, SSIDs, User Profiles e VLANs.
- Autenticação básica: PSK, PPSK básico e 802.1X/RADIUS básico.
- Radio Profiles básicos, aplicação da configuração e validação final.

Fora do escopo

- Troubleshooting avançado, análise profunda de RADIUS, Forescout/NAC e atributos dinâmicos.
- Otimização RF detalhada, roaming avançado, DFS, SDR, Cloud Config Groups e AirDefense.
- APIs, automações e customizações avançadas.

Referência técnica

- ExtremeWireless Cloud Install & Configuration Student Guide v26.2.3.
- Documentação oficial da Extreme Networks, quando houver divergência técnica ou alteração de interface.
- Experiência operacional da Ytech em ambientes Extreme Cloud IQ.

2. Acesso à plataforma e validações iniciais

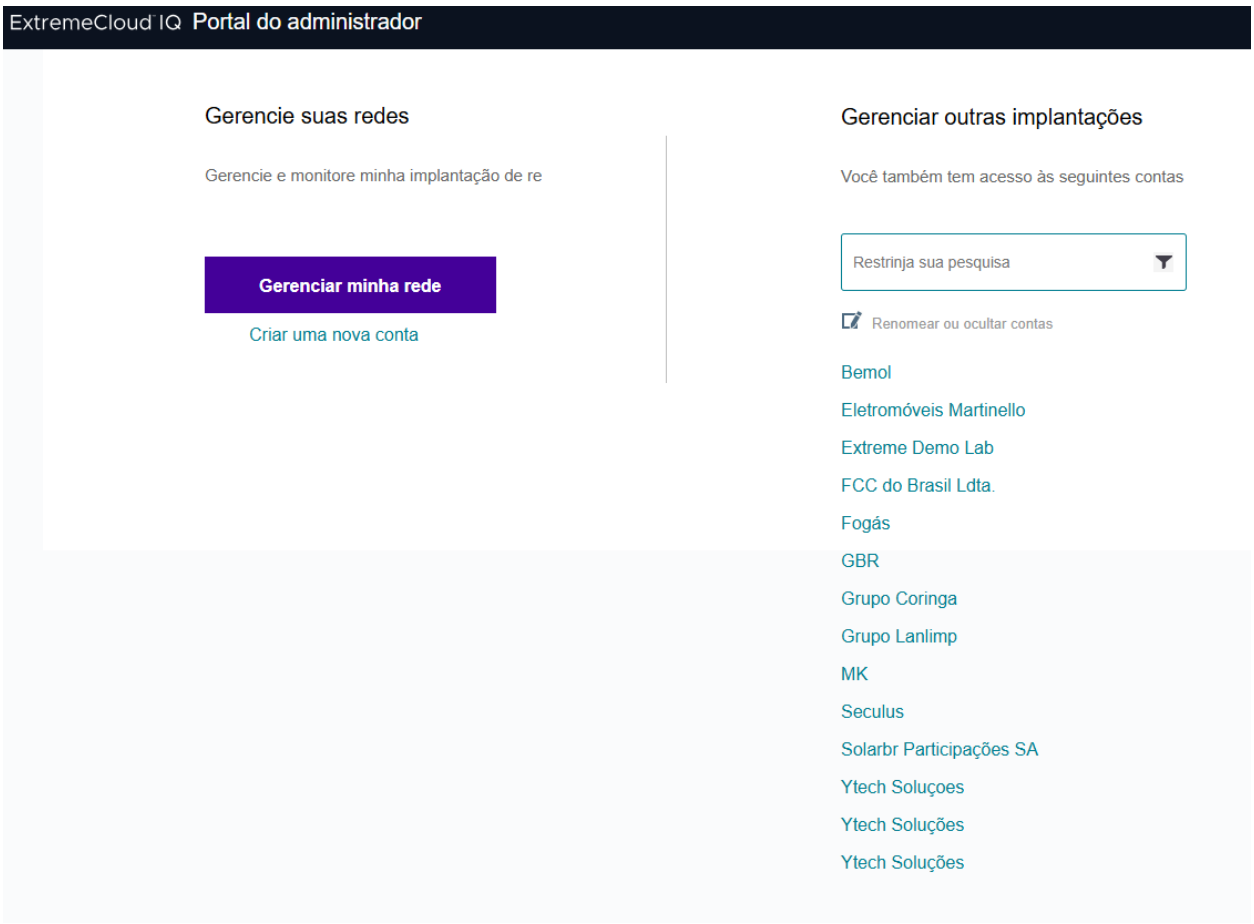

Figura 1 - Portal do administrador e seleção de tenant/implantação.

Use este procedimento antes de qualquer alteração. O objetivo é garantir que o colaborador está no ambiente correto e que a mudança não afetará APs, unidades ou clientes indevidos.

1. Acessar a plataforma Extreme Cloud IQ ou Extreme Platform ONE.
2. Informar usuário e senha e concluir o MFA, quando habilitado.
3. Selecionar o tenant correto no Account Switcher, se houver múltiplas contas.
4. Confirmar a interface em uso: XIQ Classic, XIQ New ou Extreme Platform ONE.
5. Confirmar cliente, unidade, site e Network Policy antes de alterar qualquer configuração.
6. Registrar evidência da tela inicial ou do escopo de alteração, quando a atividade for em produção.

Checklist obrigatório antes de alterar configurações
☐ Tenant correto validado
☐ Cliente e unidade corretos
☐ Interface correta confirmada
☐ Network Policy impactada identificada
☐ APs impactados identificados
☐ Janela de alteração aprovada, quando necessário

Erros comuns
- Alterar uma policy compartilhada sem verificar os APs associados.
- Cadastrar AP no tenant errado.
- Procurar um recurso no XIQ New quando ele está sendo mantido no XIQ Classic.
- Aplicar alteração em horário produtivo sem validação de impacto.

3. Onboarding de APs

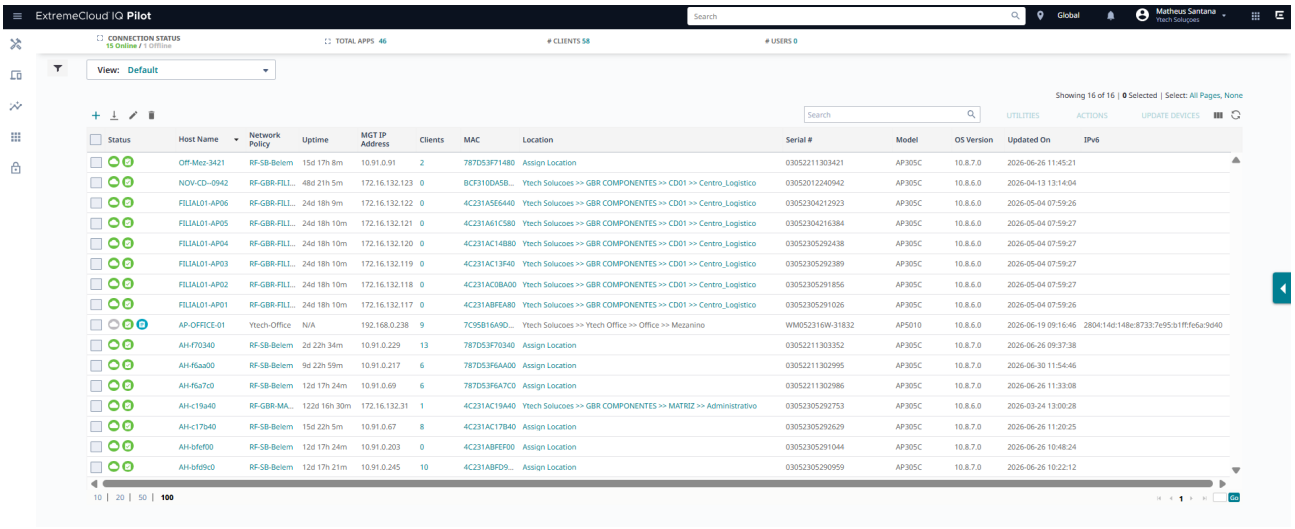

Figura 2 - Inventário de APs com status, policy, localização, serial e versão de software.

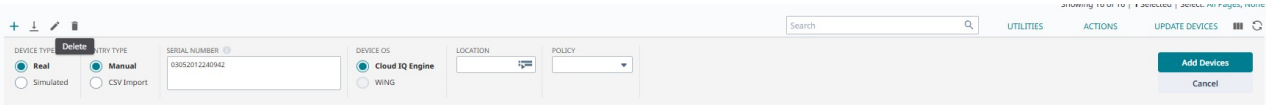

Figura 3 - Inclusão manual de AP por serial number, com seleção de tipo, sistema operacional, localização e policy.

Onboarding é o processo de adicionar um access point ao Extreme Cloud IQ para que ele seja licenciado, configurado e monitorado pela plataforma.

Pré-requisitos
☐ Serial number do AP
☐ Licença disponível
☐ Site/building/floor criado
☐ Network Policy definida
☐ VLAN de gerenciamento com DHCP
☐ DNS funcional
☐ Saída para internet liberada
☐ PoE compatível com o modelo do AP

1. Acessar o tenant correto.
2. Ir até a área de inventário ou dispositivos.
3. Selecionar Add Device ou opção equivalente.
4. Escolher o tipo Access Point.
5. Inserir o serial number do AP.
6. Associar a Network Policy correta, se aplicável.
7. Associar site, building e floor.
8. Salvar o cadastro.
9. Conectar o AP à rede física.
10. Aguardar o AP aparecer online e aplicar configuração pendente, se houver.

Validação
☐ AP aparece no inventário
☐ AP está online
☐ AP está gerenciado
☐ AP possui licença
☐ AP está no local correto
☐ AP recebeu a policy correta
☐ Não há alerta crítico

Quando o AP não aparece online
- Validar PoE, link físico, VLAN da porta, DHCP, gateway, DNS, firewall, serial number, tenant e licença antes de considerar defeito físico.

4. Organização de locais

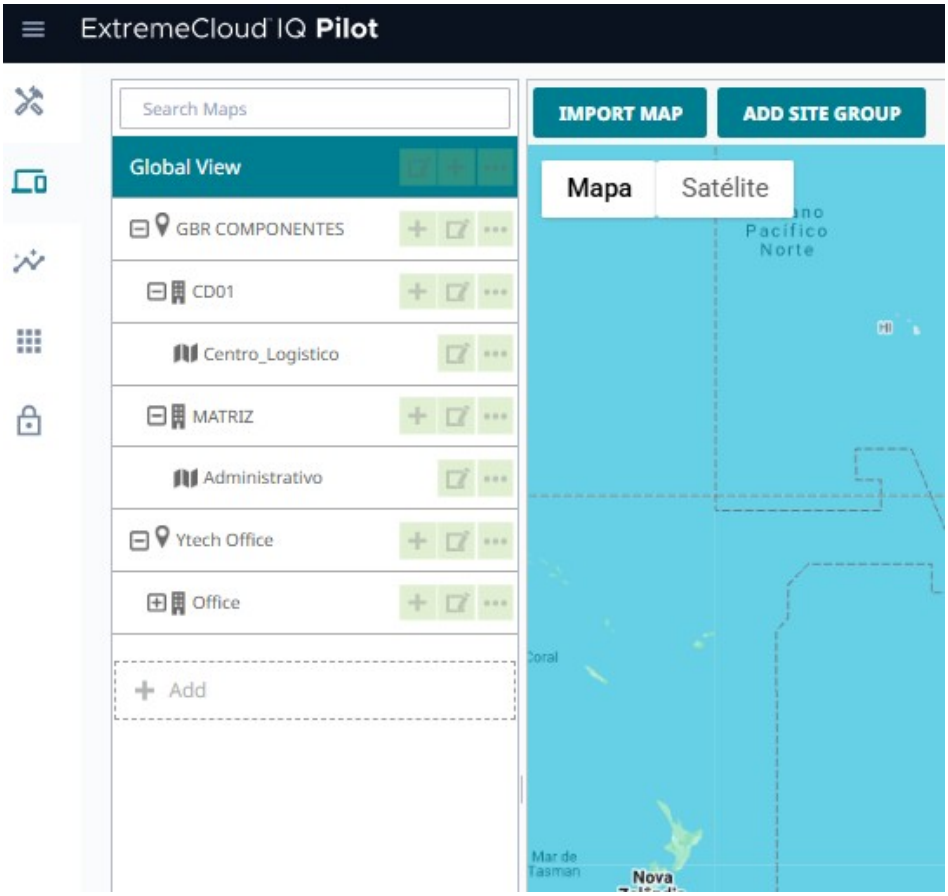

Figura 4 - Hierarquia de locais com site, building e floor para associação dos APs.

A hierarquia de locais facilita suporte, relatórios, aplicação de políticas e troubleshooting. Sempre que possível, associe o AP ao menor nível da hierarquia.

Nível	Uso recomendado
Site	Unidade principal, estado, filial ou localidade administrativa.
Building	Prédio, cidade, galpão, planta ou unidade física.
Floor	Andar, área operacional, setor, CD, loja, escritório ou planta baixa.

Padrão Ytech
- Cliente / Organização > Site > Building > Floor.
- Evitar nomes genéricos como Teste, Novo Local ou Unassigned.
- Manter padrão de nomenclatura por cliente e unidade.
- Não deixar APs sem localização definida.

1. Confirmar o cliente e a unidade.
2. Verificar se o site já existe.
3. Verificar se o building já existe.
4. Verificar se o floor já existe.
5. Criar níveis ausentes, se necessário.
6. Associar APs ao floor correto.
7. Validar a localização após o AP ficar online.

5. Criação de Network Policy

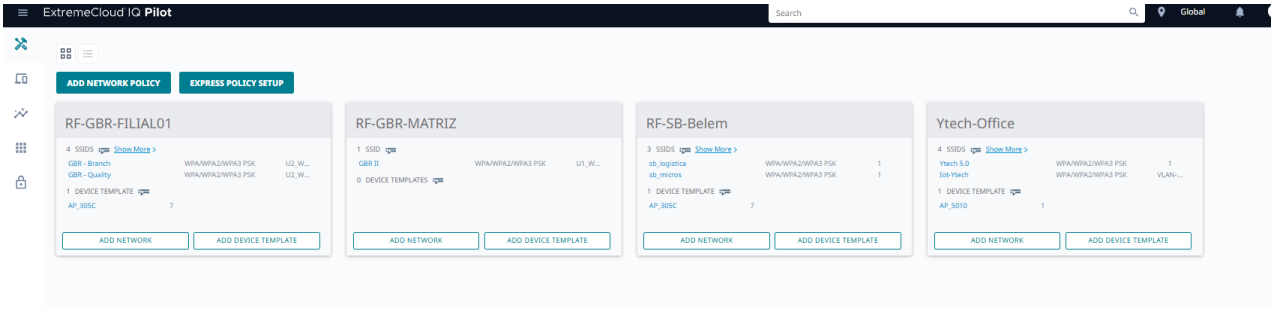

Figura 5 - Lista de Network Policies com SSIDs e Device Templates associados.

A Network Policy é o conjunto principal de configurações aplicado aos APs. Ela pode reunir SSIDs, User Profiles, Radio Profiles, Device Templates e objetos de autenticação.

Antes de criar ou alterar uma policy
☐ Nome e objetivo da policy definidos
☐ APs que usarão a policy identificados
☐ SSIDs necessários definidos
☐ User Profiles/VLANs definidos
☐ Radio Profiles definidos
☐ Impacto em produção avaliado

1. Acessar a área de Network Policies.
2. Criar nova policy ou abrir uma policy existente.
3. Definir nome padronizado.
4. Adicionar SSID/WLAN, se necessário.
5. Associar User Profiles.
6. Associar Radio Profiles e Device Templates, se aplicável.
7. Salvar a policy.
8. Associar a policy aos APs corretos.
9. Aplicar a configuração e validar.

Exemplo de nomenclatura	Quando usar
CLIENTE_UNIDADE_CORPORATIVO	SSID corporativo por unidade.
CLIENTE_UNIDADE_VISITANTES	Rede isolada para visitantes.
CLIENTE_UNIDADE_COLETORES	Rede operacional para coletores, scanners ou IoT.

Atenção
- Alterar uma Network Policy existente pode afetar todos os APs associados a ela.
- Quando houver dúvida de impacto, usar AP piloto ou criar uma nova policy.

6. Criação de SSID/WLAN

Imagem sugerida para próxima revisão: tela de criação ou edição de SSID/WLAN com método de autenticação e User Profile associado.

O SSID é a rede Wi-Fi anunciada aos clientes. No XIQ, ele deve ser associado a uma Network Policy e a um User Profile.

Informações necessárias
☐ Nome do SSID
☐ Tipo de autenticação
☐ User Profile
☐ VLAN de usuários
☐ Bandas utilizadas
☐ Escopo de APs
☐ RADIUS/NAC, se aplicável

1. Abrir a Network Policy correta.
2. Acessar Wireless Networks/WLANs.
3. Criar uma nova WLAN/SSID.
4. Definir o nome do SSID.
5. Escolher se o SSID será anunciado ou oculto.
6. Selecionar o método de autenticação.
7. Associar o User Profile correto.
8. Salvar a configuração.
9. Aplicar nos APs impactados.
10. Testar com cliente real.

Tipo	Uso básico
Open	Visitantes, testes ou captive portal.

PSK	Ambientes simples com senha compartilhada.
PPSK básico	Chaves individuais ou por grupo sem 802.1X.
802.1X/RADIUS	Rede corporativa com autenticação centralizada.

7. User Profiles e VLAN

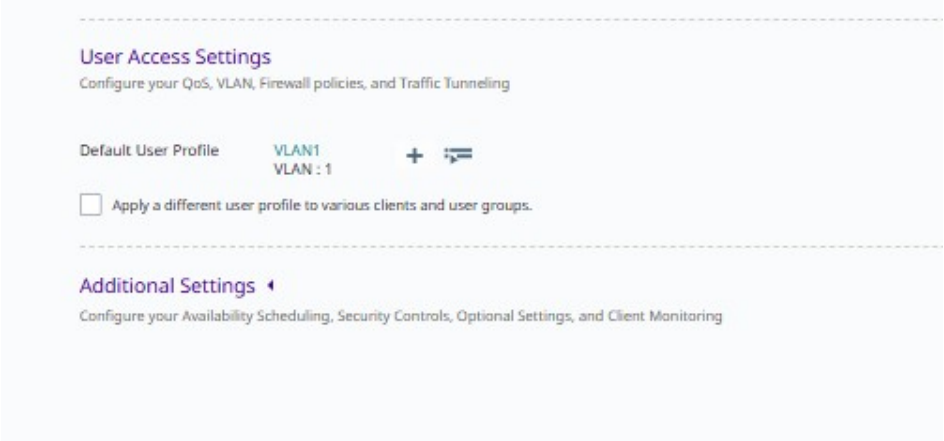

Figura 6 - Exemplo de associação de Default User Profile e configurações adicionais de acesso.

O User Profile define como o tráfego do cliente será tratado após a conexão ao SSID. Na prática, é um dos pontos mais importantes da configuração.

Conceito rápido

- SSID define como o cliente entra na rede.
- User Profile define como o cliente será tratado depois que entra.
- Em muitos incidentes, cliente conectado sem acesso está relacionado a User Profile, VLAN, DHCP ou firewall policy.

1. Acessar Common Objects ou a configuração guiada da policy.
2. Criar ou editar o User Profile.
3. Definir nome padronizado.
4. Associar VLAN correta.
5. Configurar firewall policy, se aplicável.
6. Configurar rate limit ou QoS, se necessário.
7. Salvar o perfil.
8. Associar o perfil ao SSID.
9. Aplicar nos APs e testar.

Validação do User Profile

☐ SSID associado ao perfil correto
☐ VLAN existe na rede cabeada
☐ Porta do AP permite a VLAN necessária
☐ DHCP ativo na VLAN
☐ Firewall policy permite tráfego esperado
☐ Cliente recebe IP da rede correta

Exemplo	Descrição
CORP_VLAN_10	Perfil corporativo na VLAN 10.
VISITANTES_VLAN_50	Visitantes isolados na VLAN 50.
COLETORES_VLAN_30	Coletores ou dispositivos operacionais na VLAN 30.

8. Configuração básica de autenticação

Este capítulo cobre apenas os métodos básicos necessários para atividades recorrentes. Configurações avançadas ficam no manual de Configuração Avançada.

8.1 PSK

1. Criar ou editar o SSID.
2. Selecionar WPA2/WPA3-Personal ou equivalente.
3. Definir senha forte.
4. Associar User Profile.
5. Salvar e aplicar.
6. Testar com cliente compatível.

8.2 PPSK básico

1. Criar grupo PPSK.
2. Criar usuário ou chave PPSK.

3. Associar o grupo ao User Profile correto.
4. Configurar SSID com PPSK.
5. Salvar e aplicar.
6. Testar chave válida e, se possível, chave inválida.

8.3 802.1X/RADIUS básico

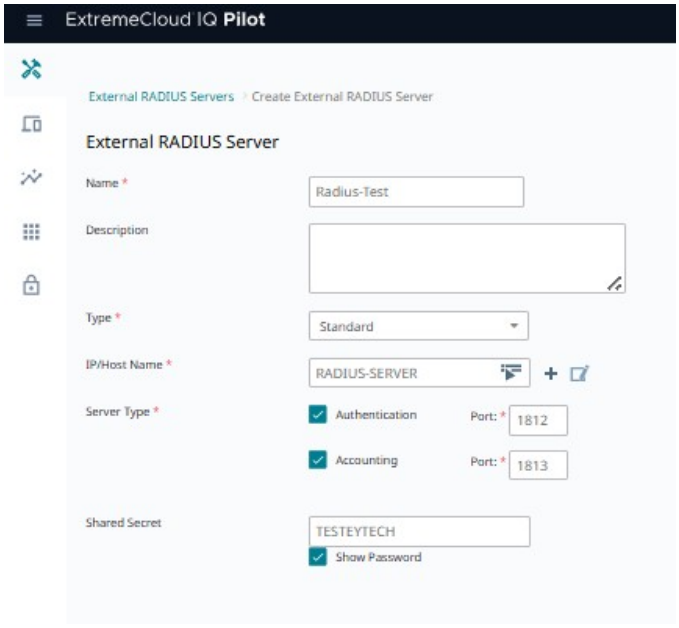

Figura 7 - Criação de servidor RADIUS externo com portas de autenticação e accounting.

Checklist RADIUS
☐ IP do servidor RADIUS
☐ Shared secret
☐ Porta 1812 liberada
☐ Porta 1813 liberada, se usar accounting
☐ AP cadastrado como NAS/client no RADIUS
☐ Usuário de teste ativo

1. Criar ou validar Authentication Server.
2. Configurar IP, portas e shared secret.
3. Criar ou editar SSID corporativo.
4. Selecionar WPA2/WPA3-Enterprise ou 802.1X.
5. Associar servidor RADIUS.
6. Definir User Profile padrão ou dinâmico.
7. Salvar e aplicar.
8. Testar autenticação com usuário válido.

Atenção em NAC/Forescout
- Validar se a tentativa chega ao RADIUS/NAC.
- Confirmar se o retorno aplica o User Profile esperado.
- Não concluir que a autenticação está correta apenas porque o cliente conectou com a senha do SSID.

9. Radio Profiles básicos

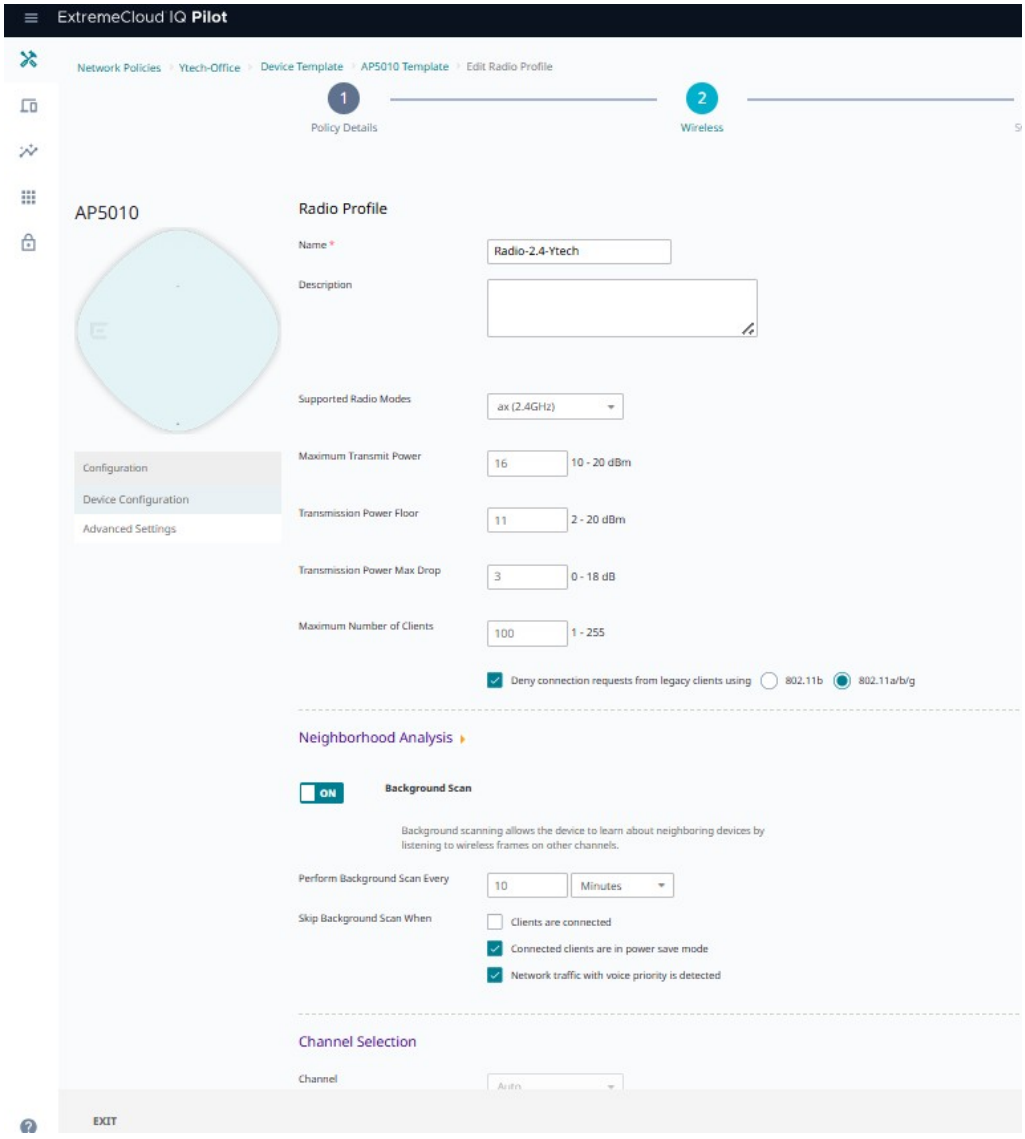

Figura 8 - Configuração básica de Radio Profile, incluindo modo, potência, limite de clientes e análise de vizinhança.

Radio Profiles definem parâmetros básicos dos rádios dos APs, como canal, potência, largura de canal e comportamento de bandas.

Parâmetro	Cuidados
2.4 GHz	Evitar potência excessiva; usar apenas quando necessário para legados/IoT.
5 GHz	Banda preferencial para a maioria dos clientes modernos.
6 GHz	Usar apenas quando APs e clientes forem compatíveis.
Largura de canal	Evitar larguras altas em ambientes densos sem análise prévia.
DFS	Pode causar troca de canal se houver detecção de radar.

1. Acessar Common Objects.
2. Ir até Radio Profiles.
3. Criar ou clonar um perfil existente.
4. Definir nome padronizado.
5. Ajustar potência, canais e largura de canal conforme necessidade.
6. Salvar o perfil.
7. Associar ao Device Template ou ao AP específico.
8. Aplicar a configuração.
9. Validar se SSID e clientes continuam operando.

Boas práticas

- Não realizar ajuste fino de rádio sem avaliar ambiente, densidade, clientes e interferência.
- Em ambientes críticos, basear mudanças em site survey ou evidências de monitoramento.
- Alterações de rádio podem afetar cobertura e roaming.

10. Aplicação da configuração e validação final

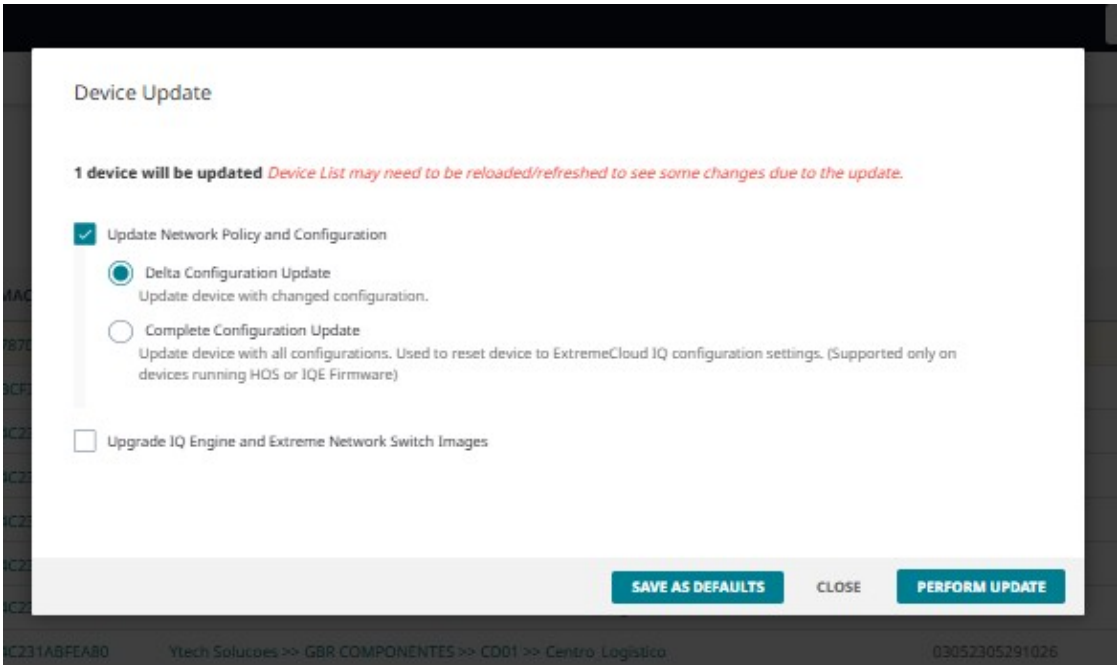

Figura 9 - Tela de atualização de dispositivo com aplicação da Network Policy e configuração.

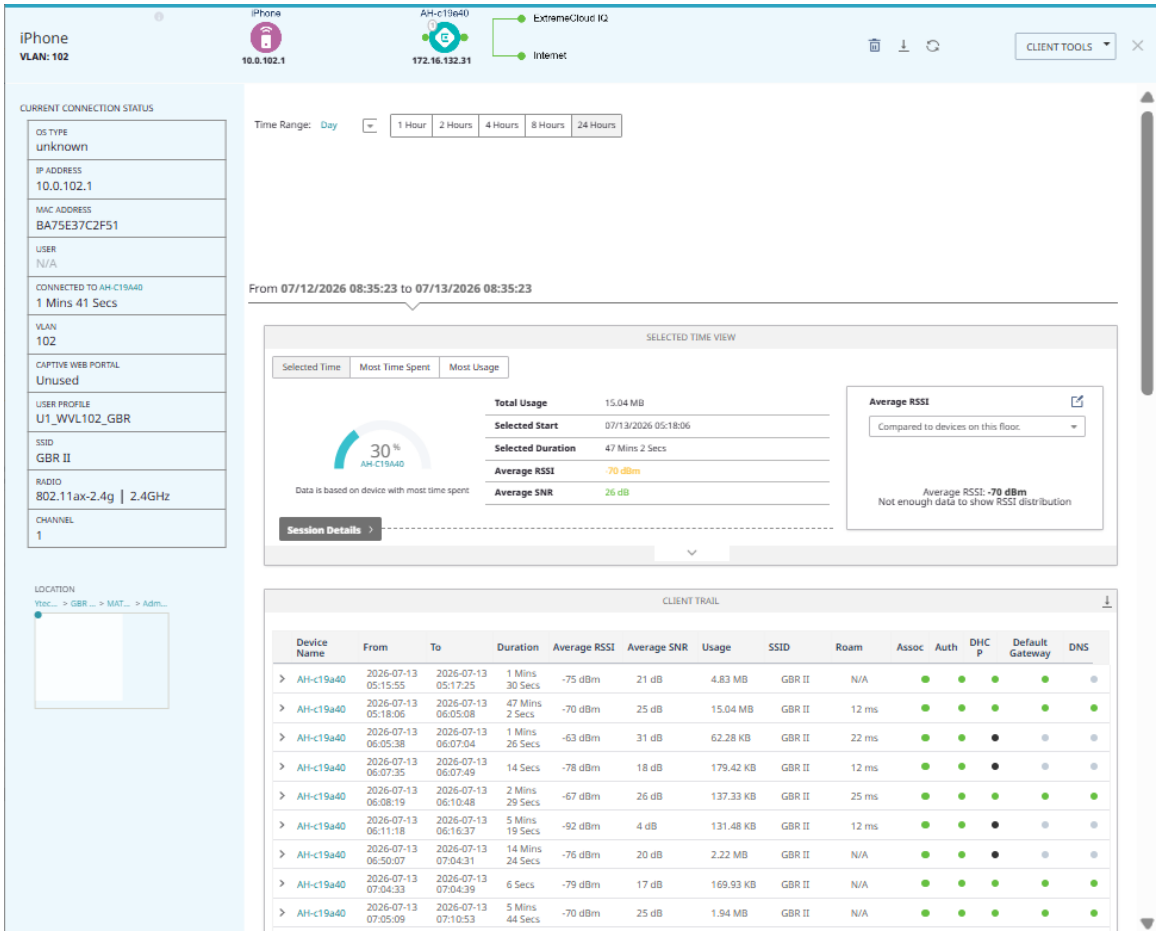

Figura 10 - Validação de cliente conectado com IP, VLAN, SSID, rádio, RSSI, SNR e trilha de conexão.

Após salvar alterações na plataforma, aplique a configuração aos APs impactados e valide o funcionamento com cliente real.

1. Finalizar a alteração desejada.
2. Salvar a configuração.
3. Verificar APs com update pendente.
4. Selecionar somente os APs impactados.

5. Aplicar a configuração.
6. Acompanhar o status do update.
7. Confirmar que os APs continuam online.
8. Testar SSID, autenticação, IP, VLAN e acesso.
9. Registrar evidências.

Validação final
☐ AP online
☐ Policy atualizada
☐ SSID anunciado
☐ Cliente conecta
☐ Cliente autentica
☐ Cliente recebe IP
☐ VLAN correta
☐ Gateway responde
☐ DNS responde
☐ Acesso esperado funciona
☐ Sem alerta crítico após alteração

Evidências recomendadas
☐ Print do AP online
☐ Print da policy
☐ Print do SSID
☐ Print do User Profile
☐ Print do cliente conectado
☐ IP e VLAN recebidos

Fechamento operacional
- A alteração só deve ser considerada concluída após teste com cliente real e validação do serviço esperado.
- Quando houver falha, registrar o ponto de falha: associação, autenticação, DHCP, VLAN, DNS, firewall ou aplicação.

Histórico de revisão

Versão	Data	Responsável	Alteração
1.3	13/07/2026	Matheus Santana / Ytech Soluções	Inclusão de prints operacionais e ajustes de revisão visual.
1.2	02/07/2026	Matheus Santana / Ytech Soluções	Versão enxuta com foco em atividades básicas: onboarding, Network Policy, SSID, User Profile, autenticação, Radio Profile e validação.
1.1	-	Ytech Soluções	Revisão ortográfica e melhoria visual.
1.0	-	Ytech Soluções	Criação inicial do Manual 01.
1.4	03/08/2026	Matheus Santana / Ytech Soluções	Padronização visual final da coleção e remoção da data da capa.