YTECH SOLUÇÕES

Manual Operacional

Extreme Cloud IQ

Configurações Avançadas

Finalidade do documento
Orientar configurações avançadas do Extreme Cloud IQ com foco em segurança, serviços, desempenho e aplicação controlada de mudanças, sem substituir projeto, homologação ou procedimento específico do fabricante.

Versão: 1.1
Responsável técnico: Matheus Santana
Empresa: Ytech Soluções
Classificação: Uso interno

1. Objetivo, escopo e pré-requisitos

Este manual complementa os módulos de configuração básica, gerenciamento e troubleshooting. As funções descritas podem modificar autenticação, tráfego, acesso administrativo, rádio ou sistema operacional dos APs; portanto, devem ser aplicadas com escopo controlado.

- Registrar o estado atual, os dispositivos afetados e o resultado esperado.
- Validar compatibilidade de modelo, firmware, licença e recursos habilitados.
- Testar primeiro em um AP, local ou política de laboratório.
- Definir janela, critério de sucesso e plano de retorno antes da atualização.

Regra de segurança
Não utilizar Supplemental CLI, troca de sistema operacional, túneis ou ajustes avançados de rádio como tentativa exploratória em produção.

2. Captive Web Portal e ExtremeGuest Essentials

2.1 Escolha do método

Opção	Uso indicado	Dependências
Portal hospedado no AP	Aceite de política, autenticação, autorregistro ou emissão de PPSK	SSID compatível, HTTPS e regras de acesso
Portal hospedado na nuvem	Login social ou validação por PIN	Acesso aos serviços cloud e walled garden
Portal com RADIUS	Validação de credenciais corporativas	Servidor RADIUS, rota, segredo e políticas
ExtremeGuest Essentials	Portal e análise de visitantes gerenciados em nuvem	Serviço habilitado e SSID associado

2.2 Procedimento controlado

1. Crie ou selecione o SSID e confirme o método de autenticação compatível.

2. Habilite o Captive Web Portal e escolha o tipo de registro ou autenticação.

3. Configure página, certificado, redirecionamento, tempo de sessão e walled garden.

4. Associe o perfil de acesso entregue após a autenticação.

5. Teste com um novo cliente, inclusive expiração, reconexão e falha de credencial.

Ponto crítico
Libere no walled garden somente DNS, portal e destinos necessários à autenticação. Uma lista excessiva pode permitir acesso antes do login.

3. Universal Platform AP e alteração de sistema operacional

APs Universal Platform podem operar com sistemas compatíveis distintos. A alteração de OS modifica a forma de gerenciamento e pode remover a configuração vigente.

1. Confirme que o modelo é Universal Hardware e que o sistema de destino é suportado.

2. Registre serial, versão, localização, política e estado atual.

3. Garanta conectividade, alimentação estável e janela de manutenção.

4. Use a ação de alteração de OS/Bootloader disponibilizada para o dispositivo.

5. Acompanhe reinicialização, onboarding, licença e associação à política correta.

6. Valide rádios, SSIDs, clientes e gerenciamento após a conversão.

Plano de retorno
Antes da conversão, documente como restaurar o sistema anterior e como o equipamento será recuperado se não retornar à nuvem.

4. Supplemental CLI e SSH Proxy

Supplemental CLI aplica comandos não expostos pela interface. Pode ser definido globalmente, na Network Policy ou em configuração específica do dispositivo. O nível mais específico pode criar diferenças difíceis de rastrear.

Nível	Aplicação	Cuidado
Global	Disponibiliza o recurso e controles gerais de acesso	Restringir operadores e origem
Network Policy	Replica comandos para dispositivos da política	Homologar sintaxe por modelo/firmware
Dispositivo	Exceção pontual	Registrar a divergência e a justificativa
SSH Proxy	Acesso administrativo intermediado pela nuvem	Usar credencial individual e sessão autorizada

- Utilize somente comandos documentados e compatíveis.
- Não duplique na CLI uma configuração já gerenciada pela interface.
- Inclua comando de reversão e saída esperada na mudança.
- Após aplicar, revise o audit e confirme que a configuração permanece sincronizada.

5. Atualização de configuração, validação e rollback

1. Revise o delta da configuração antes do envio.
2. Escolha um lote pequeno e preserve conectividade de gerenciamento.
3. Aplique a atualização e aguarde o resultado completo.
4. Verifique endereço, VLAN, DNS, rota, SSIDs e comunicação com a nuvem.
5. Em caso de falha, interrompa a expansão e execute o retorno planejado.
6. Registre horário, resultado, eventos e dispositivos afetados.

Resultado	Ação
Sucesso e audit consistente	Prosseguir gradualmente para o próximo lote.
Falha com AP online	Revisar delta, dependências e mensagem; não reenviar repetidamente.
AP sem comunicação	Restaurar conectividade antes de nova configuração.
Impacto inesperado	Executar rollback e validar o serviço anterior.

6. Configurações avançadas da Network Policy

6.1 Policy Settings

- Device Credentials: defina credenciais administrativas únicas, protegidas e compatíveis com a política de acesso.
- IP Tracking: associe grupos e métodos apenas quando houver necessidade de correlacionar usuários, IPs e políticas.
- LLDP/CDP: habilite conforme a infraestrutura e evite divulgação desnecessária em interfaces não confiáveis.
- HIVE/Profile: mantenha consistência entre políticas e evite objetos legados sem uso.

6.2 Management Settings

- Management Options: habilite somente protocolos administrativos necessários.
- Traffic Filter: restrinja tráfego destinado ao plano de gerenciamento.
- Management IP Filter: limite as redes de origem autorizadas a acessar o AP.
- Syslog: defina servidor, severidade, conectividade e retenção antes de depender dos registros.

Validação de acesso
Sempre confirme uma origem administrativa permitida antes de aplicar filtros. Um filtro incorreto pode bloquear o gerenciamento local e dificultar a recuperação.

7. Segurança e serviços complementares

Recurso	Finalidade	Controle recomendado
Device Data Collection	Enviar dados de clientes, dispositivos e aplicações ao XIQ	Coletar somente o necessário à operação
Presence Analytics	Analisar presença e permanência de dispositivos	Revisar privacidade, escopo e retenção
WIPS/AirDefense	Detectar ou responder a ameaças e APs não autorizados	Começar em detecção e validar falsos positivos
Location Server	Encaminhar dados de localização a serviço compatível	Validar destino, conectividade e governança

Mitigação segura
Em WIPS, evite contenção automática até que regras, legislação aplicável e risco de interferência em redes legítimas tenham sido avaliados.

8. Serviços de rede

Serviço	Uso	Validação mínima
Access Console	Acesso controlado a dispositivos ou serviços	Credenciais, origem, timeout e auditoria
ALG	Tratamento de protocolos que negociam sessões adicionais	Protocolos necessários e impacto de timeout
Layer 2 IPsec VPN	Extensão segura de tráfego de camada 2	Peers, criptografia, MTU, rota e redundância
Bonjour Gateway	Descoberta de serviços entre segmentos	VLANs, tipos de serviço e limite de propagação
Private Client Groups	Isolamento lógico de usuários e dispositivos	Método de associação, membros e comunicação permitida

8.1 Princípios de implantação

- Crie o objeto reutilizável antes de vinculá-lo à política.
- Aplique o menor escopo possível e evite propagação ampla de broadcast/multicast.
- Teste ida, retorno, resolução e tamanho de pacote quando houver túnel.
- Documente dependências externas, chaves e responsáveis sem registrar segredos no manual.

9. QoS, Classifier Maps e Marker Maps

QoS deve refletir requisitos reais das aplicações. Classifier Maps identificam o tráfego; Marker Maps definem ou preservam marcações utilizadas para priorização ao longo do caminho.

1. Identifique aplicações, origem/destino, protocolo e requisito de latência.

2. Classifique o tráfego com critérios objetivos e mutuamente compreensíveis.

3. Defina marcação coerente com switches, firewalls e WAN.

4. Aplique limites ou prioridade sem comprometer tráfego essencial.

5. Valide filas, perdas, latência e marcação ponta a ponta.

Evite
Marcar todo o tráfego como prioritário elimina o valor do QoS. Preserve uma classe padrão e documente exceções.

10. Configurações avançadas de rádio e SDR

Parâmetro	Efeito	Risco de ajuste inadequado
Canal e largura	Capacidade e sobreposição espectral	Interferência e incompatibilidade
Potência	Área de cobertura e equilíbrio AP/cliente	Células grandes, assimetria ou lacunas
Taxas básicas	Tempo de ar e alcance útil	Clientes legados deixam de associar
WMM QoS	Priorização de voz, vídeo e dados	Classificação inconsistente
Sensor Mode	Varredura e monitoramento RF	Redução da capacidade de atendimento
SDR/ACSP	Otimização dinâmica de rádio	Mudanças inesperadas sem baseline

- Colete baseline de RSSI, SNR, utilização, retries, clientes e canais.
- Altere um conjunto relacionado de parâmetros por vez.
- Respeite domínio regulatório, canais DFS e compatibilidade dos terminais.
- Monitore após a mudança e retorne ao baseline se os critérios piorarem.

11. Common Objects

Objeto	Aplicação
Auto Provisioning	Classificar e associar automaticamente novos dispositivos conforme regras controladas.
Port Types	Padronizar função, VLAN, PoE e comportamento de portas Ethernet.
Application Sets	Agrupar aplicações para política, visibilidade ou QoS.
Client Mode Profiles	Definir funcionamento do AP como cliente em cenários suportados.
Access Consoles/IP Tracking Groups	Reutilizar controles de acesso e rastreamento.
Tunnel Policies/VPN Service	Padronizar terminação e parâmetros de túneis.
sFlow Receivers	Definir coletores de telemetria e amostragem.
Network Services/Subnetwork Space	Reutilizar serviços e espaços de endereçamento.

Governança de objetos
Antes de editar um Common Object, identifique todas as políticas que o utilizam. Uma alteração no objeto pode afetar vários locais simultaneamente.

12. Validação e checklist final

✓	Controle
☐	Escopo, modelos, firmware e licenças confirmados.
☐	Configuração atual e dependências registradas.
☐	Mudança homologada em AP, política ou local de teste.
☐	Janela, comunicação e plano de retorno definidos.
☐	Delta revisado antes da atualização.
☐	Gerenciamento, SSIDs, autenticação, IP, DNS e aplicações validados.
☐	Audit consistente e eventos sem falhas recorrentes.
☐	Documentação e evidências atualizadas.

12.1 Controle de versão

Versão	Data	Responsável	Alteração
1.0	03/08/2026	Matheus Santana / Ytech Soluções	Emissão inicial sem imagens, baseada no guia Advanced Configuration v26.2.3.
1.1	03/08/2026	Matheus Santana / Ytech Soluções	Padronização visual final da coleção e remoção da data da capa.

Referência técnica: ExtremeWireless Cloud - Advanced Configuration Student Guide v26.2.3, Extreme Networks. Foram excluídos os módulos de BLE/iBeacon e APIs, conforme escopo definido para este manual.