

Checklist Pixel + CAPI (installation propre en 2026)

La checklist que j'utilise chaque semaine quand j'audite un compte Meta Ads. Couvre l'installation du Pixel via GTM, la CAPI côté serveur, la vérification du domaine, les événements iOS 14+, l'EMQ, la déduplication, et le post-mortem après migration.

CHECKLIST · 35 elements · 6 pages

Quand j'audite un compte Meta Ads en sous-performance, je ne commence jamais par les créas ou les audiences. Je commence par le tracking. Parce que dans 8 cas sur 10, le vrai problème n'est ni la créa ni le ciblage : c'est le signal. Un EMQ à 5 détruit l'attribution, dégrade les lookalikes, et fait optimiser l'algo sur des fantômes. Le compte peut sembler stable, mais la machine en dessous tourne à moitié aveugle.

Cette checklist est le process exact que je déroule, dans l'ordre. 35 points organisés en 7 sections : fondation, déduplication, EMQ, événements, iOS et privacy, architecture, QA et post-mortem. Chaque point a sa raison d'être : ce n'est pas une compilation de bonnes pratiques internet, c'est ce qui casse réellement les comptes en 2026.

Compter 90 minutes la première fois, 30 minutes une fois rodé. Imprimer ou ouvrir sur un second écran, cocher au fur et à mesure. Si plus de 6 points sont rouges, ne pas patcher : reposer l'installation proprement avant toute optim créa ou budget.

- FONDATION : un seul Pixel par domaine, rattaché au bon Business Manager (pas un compte perso). Les Pixels orphelins liés à des comptes personnels deviennent inaccessibles dès qu'un membre part.
- FONDATION : domaine vérifié via DNS TXT dans BM > Sécurité de la marque > Domaines. Sans cette vérification, aucune attribution sur les utilisateurs iOS 14+ ayant refusé le tracking. Propagation DNS jusqu'à 72h.
- FONDATION : token d'accès CAPI généré via System User (BM > Paramètres système > Utilisateurs système), pas via OAuth personnel. Permissions ads_management + business_management. Les tokens perso expirent et cassent la CAPI sans alerte.
- FONDATION : token CAPI stocké dans une variable d'environnement chiffrée, jamais hardcodé dans le code client. Un token committé sur Git équivaut à donner l'accès complet au compte pub.
- FONDATION : action_source bien défini par type d'événement. Website events = 'website'. Leads CRM remontés a posteriori = 'system_generated'. Phone/in-store = 'physical_store'. Mauvais action_source = warnings dans Diagnostics et rejets silencieux.
- FONDATION : event_time est un timestamp Unix UTC, dans la fenêtre de 7 jours autour de l'occurrence réelle. Au-delà, Meta drop l'événement silencieusement. Pour les leads CRM remontés en différé, envoyer dans les 7 jours sinon perte définitive.
- DEDUPLICATION : chaque événement Pixel inclut un eventID unique (UUID v4 ou order_id). Sans eventID, chaque conversion est comptée deux fois (Pixel + CAPI) et le ROAS rapporté est gonflé artificiellement.
- DEDUPLICATION : la CAPI envoie EXACTEMENT le même event_id que le Pixel pour le même événement. Sensible à la casse, caractère par caractère. Généré une seule fois (page load ou création transaction), passé identique aux deux côtés.
- DEDUPLICATION : même event_name côté Pixel et côté CAPI (Pascal case standard Meta :

Purchase, AddToCart, Lead, InitiateCheckout, ViewContent). 'purchase' minuscule "" 'Purchase' = deux events séparés, dédup cassée.

- DEDUPLICATION : taux de déduplication vérifié dans Events Manager > détails event. Healthy = 40-70% sur les events principaux quand Pixel + CAPI tournent ensemble. 0% = event_id mal transmis quelque part.
- EMQ : objectif 7+/10 sur Purchase et Lead, 8+/10 idéalement. Sous 6 = matching dégradé, retargeting moins précis, attribution faussée. Passage 8,6 -> 9,3 documenté pour réduire CPA de 18% et lifter ROAS de 22%.
- EMQ : email (em) hashé SHA-256 sur chaque event utilisateur authentifié. Pré-hasher côté serveur (lowercase puis SHA-256). Le paramètre le plus haute valeur pour le matching, à pousser en priorité absolue.
- EMQ : téléphone (ph) hashé SHA-256 en complément de l'email. Normaliser d'abord : retirer espaces, tirets, parenthèses, ajouter indicatif pays avec + (ex : +212600000000), puis hasher. Email + téléphone = bien plus fort que l'un des deux seuls.
- EMQ : external_id (ton ID utilisateur CRM/interne) hashé SHA-256, passé sur chaque event du même user. Identifiant persistant qui survit à la suppression de cookies et au changement d'appareil. Le signal first-party le plus durable que tu possèdes.
- EMQ : fbp et fbc passés en CAPI SANS hashage. fbp lu depuis le cookie _fbp (format fb.1.{timestamp}.{random}). fbc construit depuis le fbclid de l'URL au moment du clic (format fb.1.{timestamp}.{fbclid}). Les hasher casse le matching à zéro.
- EMQ : ne jamais fabriquer un fbc s'il n'y a pas de fbclid réel dans l'URL. Inventer une valeur corrompt le score de qualité et déclenche des warnings data quality côté Meta.
- EVENTS : Purchase envoie systématiquement value (numérique sans symbole), currency (ISO 4217 : MAD, EUR, USD), content_ids (array de SKU), content_type ('product' ou 'product_group'), contents (array {id, quantity, item_price}). value absent = ROAS reporté à zéro.
- EVENTS : AddToCart et InitiateCheckout envoient value, currency, content_ids, num_items. Ces events mid-funnel alimentent les audiences retargeting et num_items est requis pour le bon fonctionnement des DPA.
- EVENTS : Lead envoie content_name (nom du formulaire ou de l'offre : 'Devis gratuit', 'Demo request') et content_category. Permet de breakdown la qualité des leads par offre dans Ads Manager. external_id si tu génères un ID CRM à la création du lead.
- EVENTS : ViewContent envoie content_ids, content_type, value (le prix du produit), currency. Sans content_ids, le retargeting DPA est cassé : impossible de remonter le produit exact que le user a vu.
- EVENTS : event_source_url passé sur tous les events CAPI website (URL complète de la page où l'événement a eu lieu). C'est l'une des erreurs CAPI les plus fréquemment flaggée dans l'onglet Diagnostics.
- IOS / PRIVACY : architecture hybride Pixel + CAPI obligatoire en 2025-2026. Pixel seul perd 30-50% des conversions iOS via ATT et ITP. La CAPI server-side n'est pas bloquée par le navigateur. C'est le minimum recommandé par Meta.
- IOS / PRIVACY : fbclid capturé au premier touchpoint et stocké en base/CRM avec le contact. Quand le lead convertit plus tard, le fbc est inclus dans la CAPI event pour recoller l'attribution sur un cycle de vente long.
- IOS / PRIVACY : la configuration AEM manuelle n'est plus requise depuis juin 2025. Meta a supprimé la limite des 8 events et l'interface de priorisation. Si tu travailles depuis une doc pré-2025, retire cette étape de ton process.
-

IOS / PRIVACY : CMP (consent management) gate à la fois le Pixel ET la CAPI pour les users EU/ EEA sans consentement. Envoyer en CAPI sans consentement est illégal indépendamment du gain EMQ. Champ data_processing_options = 'LDU' pour Limited Data Use CCPA si nécessaire.

- ARCHITECTURE : sGTM (server-side GTM) ou backend direct privilégiés aux plugins natifs (Shopify built-in, WooCommerce built-in) pour la fidélité. sGTM permet l'enrichissement server-side, le consent gating fin, et n'est pas bloqué par les adblockers.
- ARCHITECTURE : si tu es en sGTM, vérifier que le client GA4 enrichit le tag Meta CAPI avec fbp et fbc extraits de la requête navigateur. Mapping manquant = events CAPI sans cookies = EMQ artificiellement bas.
- ARCHITECTURE : tracking cross-domain (landing sur domaine A, checkout sur domaine B) : _fbp ne transfère pas automatiquement. Utiliser le param passing cross-domain Meta ou redirect via un sous-domaine first-party. Source majeure d'attribution cassée sur les funnels multi-domaines.
- QA : Test Events tab dans Events Manager utilisé avant tout go-live. Coller le test code, déclencher chaque event clé depuis un device de test. Confirmer apparition dans le tab avec params corrects sous 30 secondes.
- QA : Meta Pixel Helper (extension Chrome) ouvert sur le site. Vérifier : Pixel ID correct, event name correct, tous les params requis présents, pas de double fire du même event côté navigateur. Erreurs rouges = events cassés.
- QA : onglet Diagnostics dans Events Manager check hebdomadaire. Flagge les params manquants, les events hors fenêtre 7 jours, les domaines non vérifiés, les pertes de déduplication anormales. Configurer les alertes email pour ne pas dépendre du check manuel.
- QA : EMQ recalculé sur les 7 derniers jours. Après tout changement (nouveau flow checkout, intégration CRM, update consent), re-checker EMQ sous 48h. Une chute de plus d'un point = investiguer immédiatement.
- ATTRIBUTION : ad set en 7-day click + 1-day view pour la majorité des campagnes. Aligner la fenêtre de reporting sur celle de la campagne. Pour produits d'impulsion : 1-day click. B2B / high ticket : 7-day click seul. Fenêtres mismatchées = source #1 de ROAS gonflé en reporting.
- QA : pas de double fire du Pixel (base code hardcodé dans le header + GTM qui refire). Ouvrir Network tab > filter facebook.com/tr > exactement une requête par event attendu. Doubles fires gonflent reach et tordent les ratios funnel.
- POST-MORTEM : après chaque migration site, update CMS, refonte checkout, version bump Next.js. Les updates plateforme cassent régulièrement les dataLayer pushes, modifient les URL qui cassent event_source_url, ou retirent la capture fbclid. Re-audit complet = obligatoire à chaque déploiement significatif.

POUR FINIR

Si tu as déroulé la checklist et que tu as identifié 6 points rouges ou plus, la priorité absolue n'est pas de scaler ni de tester de nouvelles créas. C'est de remettre le tracking en état avant de remettre un euro de budget. Continuer à dépenser sur une architecture cassée, c'est financer le brouillard.

Reprendre cette checklist tous les 3 mois et à chaque migration significative (refonte site, changement de CMS, update de checkout, version bump Next.js). Les déploiements cassent régulièrement les dataLayer pushes ou les captures fbclid sans que ça se voie dans le reporting avant 2 ou 3 semaines.

