Document technique sur la sécurité de l'Assistant IA

Date de publication : avril 2026 | Diffusion : publique

Synthèse

L'Assistant IA est une interface conversationnelle intégrée à Jamf Pro, Jamf Account et Jamf Protect, basée sur Claude (Anthropic) via AWS Bedrock. Il fournit des outils de production permettant d'effectuer des requêtes d'inventaire, des analyses de configurations, des vérifications de conformité et des extractions de connaissances.

Le présent document décrit l'architecture de sécurité, les pratiques de traitement des données et les mesures de confidentialité qui régissent le fonctionnement de l'Assistant IA dans toutes les régions de Jamf Cloud (États-Unis, UE, APAC).

L'Assistant IA repose sur quatre principes de sécurité qui sont tous appliqués à l'architecture elle-même plutôt qu'au seul niveau des politiques et des prompts : désactivation par défaut, contrôle d'accès selon le principe du moindre privilège, mode lecture seule au niveau de l'API et réponses transparentes et attribuables. Les garde-fous d'AWS Bedrock assurent une surveillance supplémentaire du contenu et détectent rapidement les injections de prompt dans tous les environnements.

Présentation générale de l'architecture

Infrastructure

L'Assistant IA est déployé dans toutes les régions de Jamf Cloud. Les données des clients sont traitées dans la région où leur environnement Jamf est hébergé, et elles ne sont pas transférées au-delà des frontières régionales.

Région	Région AWS Bedrock	Statut
États-Unis	us-east-1	Production
Union européenne	eu-central-1	Production
Asie-Pacifique	ap-northeast-1	Production

Modèle

L'Assistant IA utilise Claude (Anthropic), auquel il accède via AWS Bedrock. Bedrock fournit la couche d'inférence entre l'infrastructure de Jamf et le modèle d'Anthropic. Pour connaître la version actuelle du modèle, consultez le Jamf Learning Hub.

Relation de sous-traitant d'Anthropic : Anthropic ne reçoit pas les données des clients et n'y a pas accès. L'inférence du modèle s'effectue au sein de l'infrastructure AWS Bedrock, qui fonctionne dans l'environnement AWS de Jamf. Les requêtes des clients, les résultats générés par les outils et le contexte des conversations sont traités au sein de Bedrock et ne sont pas

transmis à Anthropic. Pour plus d'informations sur la manière dont AWS Bedrock gère la confidentialité et la sécurité des données, consultez la documentation relative à la protection des données d'AWS Bedrock.

Caractéristiques de sécurité d'AWS Bedrock :

- Les données des clients ne sont pas utilisées pour entraîner ni affiner les modèles d'Anthropic.
- Les données sont traitées au sein de la région et ne quittent pas la région AWS où l'environnement du client est hébergé
- Conformité à la norme SOC 2 Type II
- Les mesures de sécurité d'entreprise d'AWS s'appliquent à toutes les demandes d'inférence

Mises à jour des modèles : Jamf gère les versions des modèles via AWS Bedrock. La version actuelle du modèle est indiquée sur le Jamf Learning Hub. Nous invitons les organisations soumises à des exigences en matière de gestion du changement à consulter régulièrement le Learning Hub pour se tenir informées des changements de version du modèle.

Architecture des outils

L'Assistant IA utilise une architecture d'appel d'outils : lorsqu'un utilisateur soumet une requête, le modèle détermine les outils à invoquer, les exécute via des API Jamf spécifiques en utilisant les autorisations de l'utilisateur, puis synthétise les résultats sous forme de réponse.

Tous les outils sont en lecture seule. Les outils de l'Assistant IA se répartissent en cinq catégories : la recherche d'informations (documentation Jamf et base de connaissances), l'accès aux configurations (politiques, profils de configuration, scripts, blueprints, etc.), les requêtes d'inventaire (données sur les appareils Mac et mobiles), la vérification de la conformité (évaluations par rapport aux critères CIS, NIST et DoD STIG, etc.), et le renseignement de sécurité (évaluations des risques liés aux applications mobiles). Les outils Jamf Protect (analyse des alertes, recherche de logiciels malveillants) sont disponibles en version bêta limitée. Pour consulter le catalogue actuel des outils et connaître les informations de disponibilité et les exigences relatives aux produits, rendez-vous sur le Jamf Learning Hub.

Flux de données tiers : trois outils interrogent des services externes qui ne font pas partie de l'infrastructure Jamf. Ces intégrations sont documentées dans un souci de transparence.

- **Apple OS Lookup** interroge l'API Global Device Management Framework (Cadre global de gestion des appareils, ou GDMF) d'Apple (gdmf.apple.com), un point de terminaison public d'Apple. Aucune donnée client n'est transmise : l'outil récupère uniquement des informations publiques concernant les versions du système d'exploitation Apple.

- **App Lookup** interroge l'API de recherche iTunes (itunes.apple.com) en tant que source de données secaondire pour obtenir des informations sur les versions et les correctifs des applications. Aucune donnée client n'est transmise : l'outil récupère uniquement des métadonnées d'applications accessibles au public.
- **Mobile App Risk** interroge la base de données Mobile Application Risk Intelligence (Renseignement de risque sur les applications mobiles, ou MARI) de NowSecure pour récupérer des évaluations de sécurité. Les seules données transmises sont l'identifiant de l'application dans la boutique (p. ex., l'identifiant de bundle iOS) et la plateforme (iOS ou Android). Aucune donnée relative aux appareils, à l'identité de l'utilisateur, ni à l'organisation n'est transmise.

Principes de conception en matière de sécurité

Désactivation par défaut. L'Assistant IA est désactivé dans toutes les organisations jusqu'à ce qu'un administrateur l'active explicitement dans Jamf Account. Chaque groupe d'outils doit être activé séparément : l'activation du module principal (Core) de l'Assistant IA n'entraîne pas automatiquement l'activation des outils Jamf Pro ni celle d'aucun autre produit susceptible d'être intégré à l'avenir. Aucune fonctionnalité d'IA n'est accessible aux utilisateurs tant que leur organisation n'a pas explicitement choisi de l'activer, et les administrateurs restent en mesure de désactiver n'importe quel groupe d'outils à tout moment.

Contrôle d'accès basé sur le principe du moindre privilège. Toutes les requêtes effectuées via l'outil s'exécutent dans les limites des autorisations de l'utilisateur authentifié, et les contrôles RBAC de Jamf Pro sont appliqués sans modification. L'Assistant IA ne bénéficie d'aucune élévation de privilèges et ne peut pas accéder à des données auxquelles l'utilisateur n'a pas déjà directement accès. Un utilisateur n'ayant pas l'autorisation de consulter une politique ne pourra pas y accéder via l'Assistant IA.

Application du mode lecture seule au niveau de la couche API. L'Assistant IA appelle les API de Jamf Pro en utilisant le jeton de session de l'utilisateur authentifié ; il n'existe pas de compte de service distinct doté de privilèges étendus. Tous les appels API émis par les outils de l'Assistant IA sont des requêtes GET. Aucun outil du système n'envoie de requête POST, PUT, PATCH ni DELETE à Jamf Pro. Cette contrainte architecturale est appliquée au niveau de la couche d'implémentation ; ce n'est pas une instruction ajoutée au niveau du prompt ni une politique susceptible d'être contournée par un prompt astucieux. Quelle que soit la façon dont une requête est structurée, l'Assistant IA ne peut pas modifier les configurations des appareils, déployer des politiques, supprimer des applications, ni modifier les états d'inscription.

Des réponses transparentes et attribuables. Chaque réponse est accompagnée de ses sources, pour permettre aux administrateurs de vérifier les réponses à l'aide de documents de référence. Les résultats fournis par l'outil au modèle se présentent sous forme de données structurées plutôt que de texte libre, ce qui permet de remonter à la source de chaque réponse.

Garde-fous Bedrock. Les garde-fous AWS Bedrock sont déployés dans tous les environnements de l'Assistant IA. La configuration des garde-fous comprend une surveillance des contenus visant à détecter plusieurs catégories de risques (violence, contenus à caractère sexuel, discours de haine, insultes, comportements inappropriés) ainsi qu'une détection à haute sensibilité des injections de prompt. Tous les événements liés aux garde-fous sont suivis et consignés, ce qui permet de disposer d'un historique complet des entrées et sorties signalées.

Traitement des données

Flux de données

Lorsqu'un utilisateur envoie une requête, la séquence suivante se déroule :

1. **Traitement de la requête :** la requête en langage naturel de l'utilisateur est reçue par le back-end de l'Assistant IA
2. **Exécution des outils :** les outils concernés interrogent les API Jamf en reprenant les autorisations de l'utilisateur authentifié
3. **Reconstitution du contexte :** la requête de l'utilisateur, les résultats pertinents de l'outil et le fil de conversation en cours sont préparés en vue de l'inférence
4. I**nférence du modèle :** la requête d'inférence est traitée par AWS Bedrock et une réponse est générée
5. **Présentation de la réponse :** la réponse générée est présentée à l'utilisateur dans l'interface Jamf

Nature des données traitées lors de l'inférence

Type de données	Traitement par la couche d'inférence	Remarques
Requête de l'utilisateur	Oui	Question en langage naturel telle qu'elle a été posée
Résultats de l'outil	Oui	Données d'inventaire, détails de configuration pertinents pour la requête
Historique de conversation	Oui	Historique complet des messages de la conversation en cours, chargé à partir du stockage persistant ; conservé pendant 30 jours
Identifiants ou jetons de l'utilisateur	Non	Ils ne sont jamais inclus dans le contexte du modèle
Contenu complet de la base de données	Non	Seuls les résultats utiles à la requête sont pris en compte

Résidence des données

L'Assistant IA respecte les limites régionales définies par Jamf en matière de données. Les requêtes d'inférence sont acheminées vers le déploiement AWS Bedrock situé dans la même région que l'environnement Jamf du client :

- **Clients américains :** les données sont traitées dans la région AWS us-east-1
- **Clients de l'UE :** les données sont traitées dans la zone AWS eu-central-1
- **Clients de la région APAC :** les données sont traitées dans la zone AWS ap-northeast-1

L'inventaire des appareils, les données de configuration et autres données propres au client ne sont pas non plus transférés d'une région à l'autre.

Remarque concernant la récupération de connaissances : la récupération de connaissances porte uniquement sur le corpus de documentation de Jamf ; elle n'accède pas à l'inventaire des appareils, aux détails de configuration, ni à d'autres données propres au client. Toutes les requêtes adressées à l'Assistant IA, y compris celles qui concernent la récupération de connaissances, sont traitées dans la région du client.

Isolement des sessions

Le périmètre de chaque conversation avec l'Assistant IA est circonscrit à l'utilisateur authentifié et à son organisation. Le contexte des conversations n'est pas partagé entre les utilisateurs ni entre les organisations. Une requête émanant d'une organisation ne peut pas faire apparaître les données d'inventaire ni les informations de configuration d'une autre.

Les conversations sont conservées pendant 30 jours, puis supprimées automatiquement et définitivement. Les règles de conservation sont appliquées au niveau de la couche de stockage via la méthode TTL de DynamoDB, et non au moyen d'une tâche de nettoyage planifiée qui pourrait être reportée ou ignorée. Chaque conversation n'est accessible qu'à l'utilisateur et à l'organisation qui l'ont créée. Les données relatives aux conversations sont stockées exclusivement dans l'infrastructure de Jamf : les requêtes et les réponses ne sont ni enregistrées ni conservées par AWS Bedrock ou Anthropic au-delà de la requête d'inférence elle-même.

Conservation et journalisation des audits

Le **contenu des conversations** est conservé pendant 30 jours. Au bout de 30 jours, les données relatives aux conversations sont supprimées et ne peuvent plus être récupérées.

Les **journaux d'audit** sont conservés dans Jamf Account, sous Historique d'activités → Assistant IA. Le journal d'audit consigne toutes les modifications administratives apportées à la configuration de l'Assistant IA, notamment :

- Activation et désactivation de l'Assistant IA
- Ajout, suppression ou mise à jour des groupes d'outils
- Identité (nom et adresse e-mail) de l'administrateur à l'origine de chaque modification

- Date et heure de chaque modification

Les entrées du journal d'audit sont accessibles aux utilisateurs disposant des rôles « Administrateur de l'organisation » et « Administrateur » dans Jamf Account. Le journal d'audit fournit un historique complet des modifications apportées à la configuration.

Type de données	Durée de conservation	Remarques
Contenu de la conversation	30 jours	Supprimé automatiquement ; ne peut pas être récupéré
Journal d'audit (modifications de configuration)	Durée de conservation standard de Jamf Account	Disponible dans l'historique d'activité de Jamf Account
Contexte d'inférence du modèle	Non conservé au-delà de la session	Supprimé en fin de la session
Entraînement des modèles	Sans objet	Anthropic n'utilise pas les données des clients d'AWS Bedrock pour l'entraînement de ses modèles

Contrôle d'accès

Authentification

L'Assistant IA hérite de la session Jamf de l'utilisateur authentifié. Il n'utilise aucune connexion, aucune clé API, ni aucun identifiant distincts. Les utilisateurs qui ne sont pas authentifiés dans leur environnement Jamf ne peuvent pas accéder à l'Assistant IA.

Pour activer l'Assistant IA, il faut disposer du rôle « Administrateur » ou « Administrateur de l'organisation » dans Jamf Account. Les utilisateurs standard et les rôles en lecture seule ne peuvent pas activer, désactiver, ni modifier les paramètres des groupes d'outils de l'Assistant IA. Toutes les modifications effectuées par les administrateurs sont consignées dans le journal d'audit « Historique des activités ».

Autorisation

Toutes les requêtes sur les outils sont exécutées dans les limites des droits de l'utilisateur authentifié. L'Assistant IA ne bénéficie d'aucune élévation de privilèges et ne contourne pas les contrôles d'accès basés sur le rôle de Jamf Pro :

- Les requêtes d'inventaire ne renvoient que les appareils que l'utilisateur est autorisé à consulter
- La configuration explique que les résultats tiennent compte des contrôles d'accès en place au niveau des objets
- L'accès aux données de conformité respecte le modèle RBAC standard de Jamf Pro
- Un utilisateur qui n'a pas accès à une politique ne peut pas en consulter des détails à l'aide de l'Assistant IA.

Activation et désactivation de l'Assistant IA

L'Assistant IA est désactivé par défaut pour toutes les organisations. Les administrateurs peuvent l'activer explicitement dans Jamf Account, sous Organisation → Assistant IA.

La **désactivation de l'Assistant IA** est immédiate et réversible. Il suffit à un administrateur de décocher la case « Activer l'Assistant IA » dans Jamf Account. Cette action désactive instantanément toutes les fonctionnalités de l'Assistant IA pour l'ensemble des utilisateurs de l'entreprise. Les différents groupes d'outils (outils en lecture seule de Jamf Pro) peuvent également être désactivés individuellement sans désactiver le module principal (« Core ») de l'Assistant IA.

La **délimitation du périmètre au niveau de l'environnement** apporte une couche de contrôle supplémentaire aux organisations qui souhaitent procéder à un déploiement plus prudent. Lorsqu'ils activent les outils en lecture seule de Jamf Pro, les administrateurs peuvent limiter leur accès à des environnements et des tenants spécifiques, au lieu de l'activer dans tous les environnements. Cela permet aux organisations d'explorer l'Assistant IA dans un environnement de test ou de préproduction avant de généraliser son déploiement, sans apporter aucune modification à l'environnement de production.

Disponibilité des outils par produit

Les informations relatives à la disponibilité actuelle des outils, aux exigences des produits et au stade de développement (versions « bêta ») sont mises à jour sur le Jamf Learning Hub.

Conformité

L'Assistant IA s'intègre au programme de conformité existant de Jamf. Pour consulter la liste à jour des certifications Jamf, rendez-vous sur le Jamf Trust Center ou contactez l'équipe chargée de votre compte.

Conformité AWS Bedrock (s'applique à la couche d'inférence) :

- SOC 2 Type II
- ISO 27001

FedRAMP et StateRAMP : l'Assistant IA n'est pas disponible dans les environnements agréés StateRAMP ni FedRAMP. Contactez l'équipe chargée de votre compte Jamf pour obtenir des informations détaillées sur les perspectives de disponibilité des outils dans les environnements FedRAMP et StateRAMP.

Tests d'intrusion : l'Assistant IA a été soumis à des tests d'intrusion dans le cadre du programme d'évaluation de la sécurité de Jamf. Les résultats sont mis à la disposition des clients qui ont signé un accord de confidentialité (NDA), sur simple demande adressée à l'équipe chargée de leur compte Jamf.

Résumé des mesures de sécurité

Contrôle	Mise en œuvre
Chiffrement en transit	TLS 1.2 ou plus pour toutes les communications
Chiffrement au repos	Chiffrement KMS AWS
Authentification	Hérite la session Jamf Pro ; aucun identifiant distinct n'est requis
Rôles d'administrateur requis	Administrateur ou administrateur d'organisation dans Jamf Account
Autorisation	Le modèle RBAC de Jamf Pro est appliqué à toutes les requêtes sur les outils ; aucune élévation de privilèges n'est possible
Résidence des données	Traitement local dans la région d'origine : États-Unis/UE/Asie-Pacifique, aucun transfert d'une région à une autre
Accès d'Anthropic aux données	Anthropic ne reçoit pas les données des clients ; l'inférence ne quitte pas AWS Bedrock
Entraînement des modèles	Les données des clients ne sont pas utilisées pour l'entraînement des modèles (AWS Bedrock)
Sous-traitants tiers	NowSecure (analyse des risques liés aux applications) : identifiants d'applications uniquement ; GDMF Apple (versions du système d'exploitation) : données publiques uniquement
Journalisation des audits	Modifications de configuration enregistrées dans l'historique d'activité du compte Jamf : utilisateur, action et horodatage
Conservation des conversations	30 jours
Opération en lecture seule	Règle appliquée au niveau de la couche d'implémentation : tous les appels à l'API Jamf Pro sont des requêtes GET ; le code de l'outil ne comporte aucune méthode d'écriture.
Isolement de session	Le périmètre des conversations est celui de l'utilisateur authentifié et de son organisation ; elles sont inaccessibles aux autres utilisateurs et organisations
Désactivation par défaut	Désactivé dans toutes les organisations jusqu'à ce qu'un administrateur l'active explicitement
Possibilité de désactivation	Immédiate : décocher la case « Activer l'Assistant IA » dans Jamf Account ; cette opération est réversible à tout moment
Définition du périmètre de l'environnement	Les outils Jamf Pro peuvent être restreints à des environnements ou des tenants spécifiques afin de contrôler leur déploiement.
Pare-feu d'application web (WAF)	Appliqué au niveau de la couche API Gateway dans les environnements de production et de test
Garde-fous Bedrock	Surveillance des contenus nuisibles et détection hautement sensible des injections de prompt ; tous les événements sont tracés et consignés
Tests de pénétration	Réalisés avant le lancement public du produit ; résultats disponibles dans le cadre d'un accord de confidentialité

Informations sur le document

Publication	Avril 2026
Diffusion	Publique
Emplacement	jamf.it/aiassistant

Pour plus d’informations

- **Jamf Trust Center :** certifications Jamf actuelles, documentation de conformité et position de sécurité : https://www.jamf.com/fr/trust-center/
- **Jamf Learning Hub :** catalogue à jour des outils de l’Assistant IA, configuration requise et version du modèle : https://learn.jamf.com/home
- **Ce document : l**a version la plus récente de ce document est disponible à l’adresse suivante : jamf.it/aiassistant
- **Vous avez des questions ?** Contactez l’équipe en charge de votre compte Jamf.