jamf

Guide pratique de la gestion moderne des appareils Apple avec la DDM

Des mises à jour plus rapides, une meilleure visibilité sur les appareils et une charge de travail manuel réduite pour les parcs Apple en pleine croissance.

Lorsque les environnements Apple se développent, les workflows traditionnels provoquent souvent des problèmes opérationnels. Les petites équipes informatiques, déjà confrontées à de lourdes charges de travail, le voient bien : les mises à jour sont plus lentes, les informations sur l'état des appareils n'arrivent pas assez vite et les tâches de nettoyage manuel se multiplient. La DDM peut vous aider.

Comment la DDM fait-elle gagner du temps et améliore-t-elle les résultats ?

Des workflows plus simples

Les outils et les processus basés sur la DDM simplifient la gestion des appareils en limitant le recours aux scripts, les échanges d'informations entre serveur et appareils, et les workflows manuels.

Meilleure visibilité des appareils à l'échelle du parc

Comme ce protocole permet aux appareils de signaler spontanément leur état, les équipes informatiques obtiennent des informations en temps réel sur chaque appareil et chaque application.

Des mises à jour plus rapides

Le fait que les appareils émettent des alertes en cas de changement de configuration améliore l'efficacité, la rapidité et la fiabilité de l'application des correctifs et des mises à jour du système d'exploitation.

Une meilleure expérience pour l'utilisateur final

Comme les appareils réagissent à leurs changements d'état, ils peuvent exécuter davantage de mises à jour de sécurité et de changements de configuration en arrière-plan, sans perturber le travail quotidien.

Qu'est-ce que la DDM et quel est son intérêt ?

La DDM est un protocole pour macOS, iOS, iPadOS watchOS, visionOS et tvOS qui permet aux appareils Apple de signaler les changements de configuration, d'appliquer des configurations et de réagir aux changements d'état, tout cela de façon autonome. Dans Jamf, les capacités de gestion déclarative des appareils prennent notamment la forme des Blueprints.

L'abandon des commandes de serveurs de la MDM traditionnelle au profit du protocole DDM a plusieurs avantages :

- Il évite les recours répétés à des commandes serveur qui ralentissent le système
- Il permet le signalement proactif des changements d'état des appareils
- L'application des règles conformité se fait sur l'appareil lui-même, ce qui rend la remédiation quasi instantanée
- Le suivi manuel est réduit

La simplification de la gestion, un atout pour la sécurité

La DDM simplifie les flux de gestion et renforce votre posture de sécurité :

- **Elle réduit le risque de dérive de la configuration**
- **Elle accélère l'application des mises à jour**
- **Elle normalise et renforce les profils de référence**
- **Elle soutient une réponse automatisée, sur l'appareil**

Tous ces avantages réduisent la part manuelle des workflows courants et contribuent à la cohérence de la conformité à grande échelle. La DDM favorise également une approche proactive de la cybersécurité, indispensable pour faire face à un paysage d'attaques toujours plus sophistiqué au fil de l'évolution de votre organisation. Un appareil capable d'agir immédiatement et d'isoler les tentatives d'attaque ou les activités suspectes préserve la sécurité du réseau.

La DDM peut être un avantage pour votre organisation dès maintenant

L'intérêt de la DDM ne réside pas seulement dans son évolutivité et dans le temps qu'elle permet de gagner aux équipes informatiques. Elle peut également vous permettre de mettre en place des workflows inédits dans l'ensemble de votre organisation.

L'homogénéité des configurations sur l'ensemble des appareils renforce la fiabilité et la cohérence de votre organisation.

Et c'est un aspect essentiel. L'harmonisation des règles et des configurations à l'échelle de l'organisation offre plusieurs avantages :

- Moins de tickets d'assistance et de corrections manuelles
- Une posture de sécurité plus solide et davantage de protection contre les défauts de configuration susceptibles d'ouvrir la porte à un accès non autorisé
- Un comportement prévisible d'un appareil à l'autre qui facilite le dépannage

La DDM détecte les erreurs

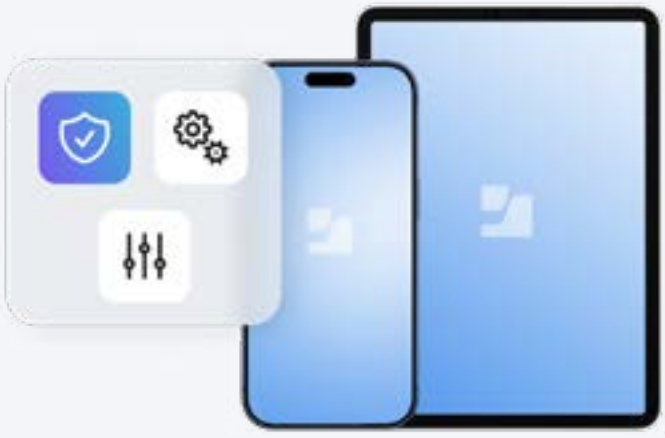
Lorsque les outils de gestion et de sécurité fonctionnent en harmonie, ils détectent les incohérences plus tôt et peuvent mettre en œuvre la remédiation plus rapidement, bien souvent sans que le personnel ait à intervenir. De même, l'automatisation de la configuration et de la mise en conformité réduit l'erreur humaine.

La DDM préserve les configurations de référence

Avec la DDM, les mises à jour et les profils de référence restent intacts : au moindre écart, votre système est configuré pour corriger automatiquement tous les problèmes, à l'exception de ceux qui sont exceptionnellement complexes.

Le résultat : les employés subissent moins de problèmes techniques et de ralentissements, et ne remarquent même pas que des protocoles de sécurité s'exécutent en arrière-plan.

Le service informatique a plus de temps à consacrer aux problématiques techniques qui peuvent faciliter le travail quotidien dans toute l'entreprise.



Les rapports spontanés des appareils changent tout ou presque

Signalement proactif de l'état des appareils

Avec la DDM, les appareils alertent automatiquement le serveur de gestion en cas de modification de valeurs clés (la version du système d'exploitation, par exemple). Cette actualisation spontanée de l'inventaire garantit l'application proactive des mises à jour.

Une meilleure visibilité sur le parc

Lorsque les appareils communiquent spontanément avec le serveur de gestion, le service informatique bénéficie d'une vue continue sur l'ensemble de son parc.

Il est ainsi possible de connaître en un coup d'oeil :

- La localisation de l'appareil
- L'état de la configuration
- La version du système d'exploitation et les applications installées

Le service informatique peut également voir quels appareils ont réagi à des attaques ou à des comportements suspects, et de quelle manière.

Même s'il n'a pas besoin d'intervenir directement grâce aux automatismes de la DDM, il obtient de précieuses informations sur les domaines où la sécurité doit être renforcée, ou sur les membres de l'entreprise qui ont besoin d'un petit rappel sur les risques de l'hameçonnage.

Lorsque les équipes informatiques ont de la visibilité sur les changements qui affectent les appareils de l'ensemble de leur parc en temps réel, les surprises sont rares. Si un appareil n'est soudainement plus conforme, parce que l'utilisateur a supprimé son code secret ou une application essentielle, le service informatique le sait instantanément.

La rapidité du signalement et de la correction peut faire toute la différence. Sans cela, une attaque de logiciel malveillant sophistiquée pourrait passer inaperçue pendant des heures, jusqu'à la prochaine communication planifiée entre l'appareil et le serveur.

Des cycles de mise à jour plus prévisibles

L'application des mises à jour est un problème de longue date.

Avant la DDM

Sans la DDM, chaque fois qu'il faut mettre à jour le système d'exploitation, les applications, les règles ou les configurations, le service informatique est confronté à un éventail de problèmes :

- Les employés repoussent sans cesse des mises à jour vitales pour éviter de s'interrompre dans leur travail
- Les commandes MDM qui forcent l'application des mises à jour critiques peuvent réduire à néant des heures d'effort
- Sans une connaissance claire et détaillée de l'état des appareils, les mises à jour se font à l'aveuglette, avec les problèmes imprévus que cela entraîne.

Utilisation de la DDM

Les choses se présentent différemment dans les écosystèmes qui utilisent le protocole DDM.

Guidé par les règles définies par le service informatique, chaque appareil signale continuellement son état et offre une image claire de ce qui se passe en temps réel. L'état des mises à jour – en attente, en cours de téléchargement, en cours d'installation ou en erreur – est toujours visible sans qu'il faille courir après les appareils ni attendre les retours des utilisateurs.

- La DDM tient les utilisateurs informés. Les appareils émettent des notifications avant les mises à jour afin de permettre aux utilisateurs de choisir le meilleur moment pour l'installation.
- S'ils n'agissent pas, l'appareil applique la mise à jour de lui-même.
- L'heure et la date d'application sont indiquées dans le fuseau horaire local afin de programmer la mise à jour en dehors des heures de travail. Les appareils utilisant le protocole DDM peuvent même mettre à jour un appareil hors tension : la mise à jour s'effectuera dès que l'utilisateur le remettra en marche.
- Le service informatique n'envoie pas les mises à jour à l'aveuglette ; une grande part des installations peut se faire sans aucune intervention, avec une visibilité totale sur l'état des appareils et des réponses préprogrammées aux problèmes de conformité les plus courants.

Les appareils restent sécurisés et à jour sans intervention constante de l'équipe, et sans interrompre ni détruire le travail des utilisateurs finaux.

Une planification proactive plutôt qu'une approche réactive, axée sur le dépannage et la remédiation

La DDM limite les interventions de dépannage réactives en transférant le contrôle du serveur de gestion à l'appareil.

En cas de problème, c'est l'appareil qui signale son changement d'état au serveur, sur la base des règles et des instructions définies par le service informatique.

Il peut aussi bien s'agir d'une mise à jour interrompue à cause d'une batterie faible, d'un manque d'espace de stockage, ou d'une modification de la sécurité comme l'état du chiffrement FileVault.

Avec un tel degré de visibilité, même si une assistance directe s'avère nécessaire, le service informatique peut souvent intervenir avant que l'utilisateur ne soit affecté.

Quels sont les effets de la planification proactive sur l'entreprise ?

L'expérience de mise à jour est plus prévisible et mieux contrôlée. Le service informatique passe moins de temps à suivre l'avancement des processus et à dépanner des appareils individuels, et peut se concentrer sur les objectifs.

N'oublions pas non plus le facteur « ça marche, tout simplement ».

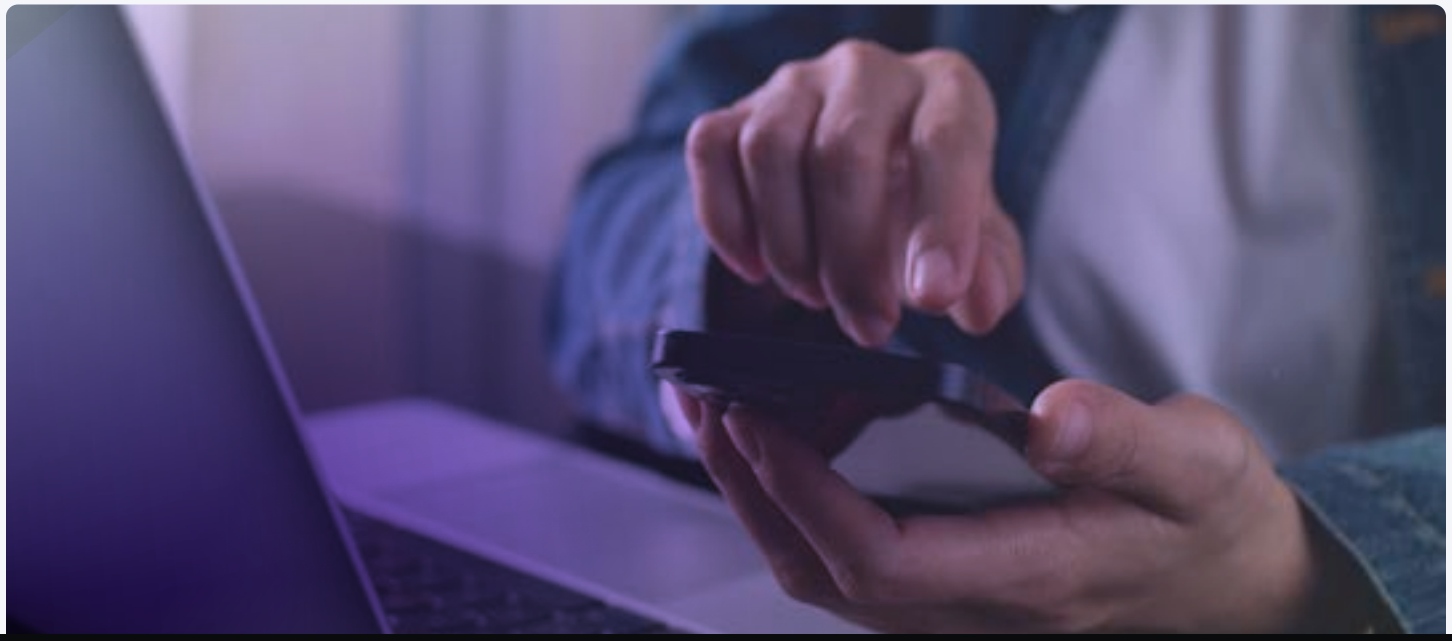
Lorsque les appareils sont configurés de manière cohérente, mis à jour en continu et guidés par une intelligence intégrée, il y a tout simplement moins de problèmes à résoudre. Les réponses automatisées maintiennent les appareils en conformité avec les règles, réduisent les frictions pour les utilisateurs et minimisent les recours à l'assistance.

Étendre, automatiser et rationaliser les workflows avec la DDM

La DDM est un protocole de gestion moderne qui aide les équipes informatiques en pleine croissance à gérer les appareils plus efficacement, à réduire les frictions opérationnelles et à évoluer plus efficacement.

C'est aussi une alliée pour l'expérience utilisateur : les mises à jour se font en arrière-plan et la conformité est automatisée. Le résultat : une productivité accrue et des employés plus heureux.

Gagnez du temps, évoluez sans effort et renforcez la cybersécurité grâce à la DDM.



jamf

www.jamf.com/fr/

Découvrez comment la DDM simplifie la gestion et renforce la sécurité.
Demandez une version d'essai gratuite.