Politiques - Apple

Les politiques Apple

Les politiques Apple définissent les paramètres de gestion que Cerberus Enterprise applique aux appareils Apple via MDM. Ces paramètres sont configurés depuis le tableau de bord dans l'éditeur de politiques Apple.

Avant de commencer

La gestion des appareils Apple nécessite la configuration d'Apple Management (APNs). Si nécessaire, consultez la page Configuration d'Apple Management (APNs).

Ouvrez l'éditeur de stratégies Apple

Dans le tableau de bord, ouvrez **Stratégies** et cliquez sur **Créer une nouvelle stratégie Apple**. Pour modifier une stratégie Apple existante, cliquez sur la ligne correspondante dans le tableau des stratégies.

Mise en page de l'éditeur

L'éditeur de stratégies Apple est organisé en sections extensibles. En haut de la page, vous pouvez toujours modifier :

- **Nom** (obligatoire)
- **Identifiant** (lecture seule)
- **Description** (facultative)

Sections de politique

Les sections ci-dessous correspondent aux panneaux actuellement disponibles dans l'éditeur de politiques Apple :

- **Gestion des applications** : configurez les restrictions liées aux applications et gérez les applications installées.
- **Paramètres du code PIN** : configurez les exigences du code PIN et les règles associées.
- **Sécurité** : contrôlez les fonctionnalités telles que le déverrouillage automatique et le déverrouillage biométrique.

- **iCloud** : autorisez ou désactivez des services iCloud spécifiques (sauvegarde, synchronisation du trousseau, relais privé, etc.).
- **Multimédia** : autorisez ou désactivez l'appareil photo et les fonctionnalités associées.
- **Cellulaire** : contrôlez les paramètres liés à la connectivité cellulaire (paramètres des données cellulaires de l'application, eSIM, modifications de forfait).
- **Réseau** : contrôlez les paramètres de partage de proximité, d'impression sans fil et d'autres options de connectivité.
- **Comptes** : limitez les modifications de comptes et (facultativement) configurez les comptes Google et Mail.

> De nombreuses options dans l'éditeur de stratégies Apple incluent une info-bulle qui documente les exigences et les versions de système d'exploitation prises en charge.

Enregistrer, supprimer et appareils associés

Utilisez **la politique de sauvegarde** pour appliquer vos modifications. Le bouton est désactivé lorsqu'il n'y a pas de modifications en attente, ou lorsque la licence est expirée.

Lorsque vous modifiez une stratégie existante, la page affiche également une action "**Supprimer la stratégie**". L'éditeur peut afficher une liste des "**appareils associés**" en bas, afin que vous puissiez voir le nombre d'appareils qui utilisent actuellement cette stratégie.

Pages suivantes

- Code PIN : configurez les exigences du code PIN et les options de sécurité associées.
- Restrictions : définissez les fonctionnalités autorisées et les limitations au niveau du système d'exploitation.
- Applications et profils : configurez les applications installées et les profils de configuration.

Stratégie Apple : Code d'accès

La section **Paramètres du code d'accès** permet de configurer les exigences relatives au code d'accès de l'appareil et les règles de sécurité associées (par exemple, la longueur et la complexité minimales).

Options

Dans l'éditeur de stratégies Apple, les options de code d'accès sont configurées à l'aide d'une combinaison de boutons et de champs numériques. De nombreux champs incluent des info-bulles qui indiquent les versions de système d'exploitation prises en charge et les exigences de supervision.

Boutons d'activation/désactivation du code d'accès

- **Modifier au prochain authentification** : force un changement de mot de passe lors de la prochaine authentification de l'utilisateur.
- **Exiger un code alphanumérique** : exige qu'au moins une lettre et un chiffre soient présents.
- **Exiger un code complexe** : nécessite un code complexe (sans motifs répétitifs ou séquentiels et avec au moins un caractère non alphanumérique).
- **Exiger un code** : nécessite un code sans exigences supplémentaires de longueur ou de qualité. Remarque : la configuration d'autres paramètres de code implique l'utilisation d'un code.

Champs numériques

- **TentativesInfructueuses:RéinitialisationEnMinutes**: nombre de minutes avant la réinitialisation du compteur de tentatives échouées (nécessite MaximumFailedAttempts).
- **Nombre maximal de tentatives infructueuses** : nombre de tentatives autorisées avant que l'appareil ne soit effacé/bloqué (plage : 2–11).
- **Période de grâce maximale en minutes** : durée pendant laquelle l'appareil peut être déverrouillé sans nécessiter le code d'accès (0 = aucune).
- **Délai maximal d'inactivité en minutes** : durée pendant laquelle l'appareil peut rester inactif avant le verrouillage (plage : 0–15).
- **Durée maximale de validité du code PIN en jours** : durée pendant laquelle le code PIN est valide avant qu'un changement ne soit imposé (plage : 0–730).

- **Nombre minimum de caractères complexes** : nombre minimal de "caractères complexes" (plage : 0–4).
- **LongueurMinimale** : longueur minimale du code (plage : 0–16).
- **Limite du nombre de codes utilisés** : nombre maximum de codes utilisés pour éviter la réutilisation de vieux codes (plage : 1–50).

Politique Apple : Restrictions

La section Restrictions contrôle les fonctionnalités du système d'exploitation autorisées sur les appareils Apple gérés. Dans l'éditeur de politique Apple, ces options sont présentées sous forme de panneaux regroupés avec plusieurs interrupteurs.

> De nombreuses restrictions ne sont prises en charge que sur des versions spécifiques du système d'exploitation et peuvent nécessiter des appareils supervisés. Consultez les info-bulles du tableau de bord pour connaître les exigences.

Sécurité

- **Autoriser le déverrouillage automatique**
- **Autoriser l'utilisation de l'empreinte digitale pour le déverrouillage**
- **Autoriser la modification de l'empreinte digitale**

iCloud

- **Autoriser l'accès au carnet d'adresses iCloud**
- **Autoriser la sauvegarde iCloud**
- **Autoriser les favoris iCloud**
- **Autoriser le calendrier iCloud**
- **Autoriser le bureau et les documents iCloud**
- **Autoriser la synchronisation des documents iCloud**
- **Autoriser la synchronisation iCloud Freeform**
- **Autoriser la synchronisation du trousseau iCloud**
- **Autoriser l'accès aux e-mails iCloud**
- **Autoriser l'accès aux notes iCloud**
- **Autoriser l'accès à la bibliothèque de photos iCloud**
- **Autoriser iCloud Private Relay**
- **Autoriser les rappels iCloud**

Multimédia

- **Autoriser l'appareil photo**
- **Autoriser la modification du partage de fichiers**

- **Autoriser l'accès aux fichiers via la clé USB**

Cellulaire

- **Autoriser la modification des données cellulaires de l'application**
- **Autoriser la modification des données cellulaires**
- **Autoriser la modification du profil eSIM**
- **Autoriser les transferts sortants eSIM**

Réseau

- **Autoriser AirDrop**
- **Autoriser les requêtes AirPlay entrantes**
- **Autoriser AirPrint**
- **Autoriser le stockage des informations d'identification AirPrint**
- **Autoriser la découverte AirPrint iBeacon**
- **Autoriser la modification des paramètres Bluetooth**
- **Autoriser la modification des paramètres de partage Bluetooth**
- **Autoriser l'accès au lecteur réseau pour les fichiers**
- **Autoriser la modification du partage de connexion Internet**

Comptes (restriction)

Le panneau Comptes contient à la fois des restrictions et (facultativement) des paramètres de configuration des comptes. Le commutateur de restriction contrôle si l'utilisateur peut modifier les comptes système.

- **Autoriser la modification des comptes**

Politique Apple : Applications et profils

Cette section explique comment configurer les applications gérées et les profils de configuration pour les appareils Apple.

Gestion des applications

Le panneau **Gestion des applications** contient à la fois les restrictions générales relatives aux applications et une liste des applications gérées.

Restrictions générales concernant les applications

- **Autoriser les applications clips**
- **Autoriser l'installation d'applications**
- **Autoriser la désinstallation des applications**
- **Autoriser les téléchargements automatiques d'applications**
- **Autoriser la dissimulation des applications**
- **Autoriser le verrouillage des applications**
- **Autoriser les achats intégrés**

Applications gérées

Utilisez **Ajouter une application** pour ajouter une application à la stratégie. Chaque application gérée est affichée sous forme de carte. Vous pouvez développer la carte pour modifier ses paramètres et supprimer l'application à l'aide de l'action de suppression.

- **Identifiant de l'App Store** : l'identifiant de l'application sur l'App Store pour les applications gérées.
- **Identifiant de l'application (Bundle ID)** : l'identifiant de l'application, utilisé pour l'installation.
- **Comportement de l'installation** : contrôle si l'application doit rester installée ou si elle peut être installée/désinstallée par l'utilisateur.
- **Attribution** : type d'attribution de licence.
- **Licence VPP** : type de licence VPP utilisée pour l'installation via l'App Store.

Comptes

Le panneau **Comptes** vous permet de configurer les comptes qui sont appliqués aux appareils gérés. Il comprend également un interrupteur pour restreindre la modification des comptes.

Restriction

- **Autoriser la modification du compte** : lorsque cette option est désactivée, les utilisateurs ne peuvent pas modifier les comptes, tels que les comptes Apple et les comptes Internet.

Ajouter des comptes

Utilisez **Ajouter un compte Google** ou **Ajouter un compte de messagerie** pour ajouter des informations de compte à la stratégie. Chaque compte s'affiche sous forme de carte avec ses champs de configuration.

Informations d'identification des comptes des utilisateurs

Les cartes Google et Mail fournissent une option pour activer/désactiver les **informations d'identification des comptes des utilisateurs**. Lorsqu'elle est activée, le système applique les informations d'identification au niveau de chaque utilisateur. Lorsqu'elle est désactivée, vous devez saisir l'identité du compte dans la stratégie.

champs d'identification des comptes Google

- **Nom visible**: le nom affiché à l'utilisateur pour le compte.
- **Adresse e-mail Google** : l'adresse e-mail de l'utilisateur.
- **Nom complet** : le nom complet de l'utilisateur.

Champs du compte de messagerie

Les comptes de messagerie incluent les champs d'identification ainsi que la configuration des serveurs entrants et sortants. Les noms d'hôte sont obligatoires.

- **Nom visible**: le nom affiché à l'utilisateur pour le compte de messagerie.
- **Adresse e-mail**: l'adresse e-mail de l'utilisateur.
- **Nom complet** : le nom complet de l'utilisateur.

Serveur entrant

- **Type de serveur** : protocole de messagerie (par exemple IMAP ou POP).
- **Méthode d'authentification** : méthode d'authentification pour le serveur.
- **Préfixe du chemin IMAP** : affiché uniquement lorsque le type de serveur est IMAP.
- **Nom d'hôte** : obligatoire.
- **Port** : numéro de port du serveur (1 à 65 535).

Serveur sortant

- **Méthode d'authentification**
- **Nom d'hôte** : obligatoire.
- **Port** : numéro de port du serveur (1 à 65 535).

Options S/MIME

Pour les comptes de messagerie, vous pouvez également configurer le comportement du chiffrement et de la signature S/MIME.

Chiffrement

- **Chiffrement S/MIME**
- **Identité, paramètre pouvant être modifié par l'utilisateur**
- **Activation de l'interrupteur par message**
- **Modifiable par l'utilisateur**

Signature

- **Signature S/MIME**
- **Identité, paramètre pouvant être modifié par l'utilisateur**
- **Modifiable par l'utilisateur**

> Les options de compte et de restriction incluent des infobulles dans le tableau de bord qui expliquent les prérequis et les versions de système d'exploitation prises en charge.