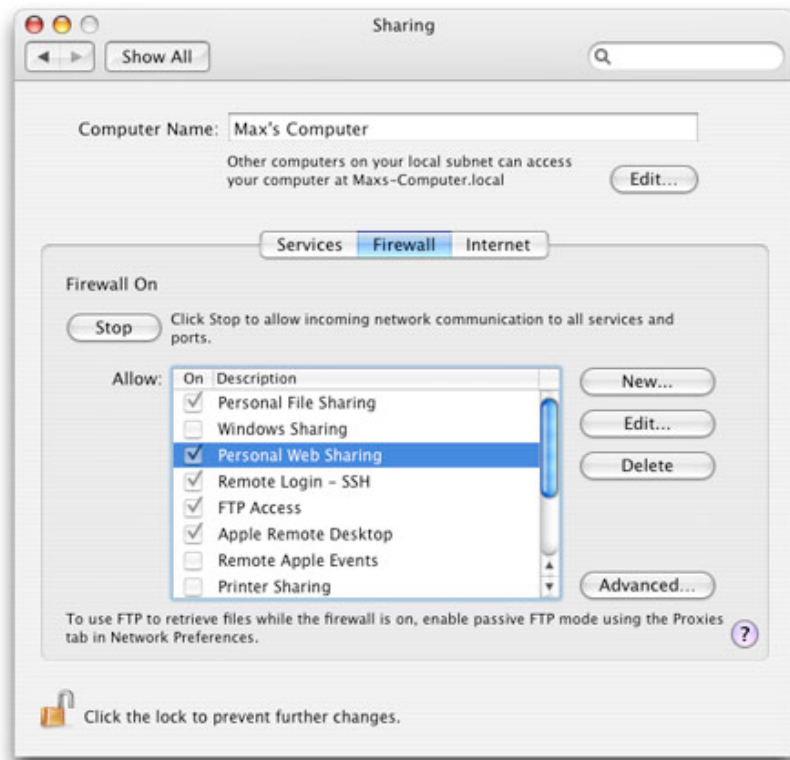




Sécurité

Mac OS X surveille la boutique.

Liberté n'est pas synonyme de négligence. Une sécurité efficace vous permet de gérer votre activité sans aucune barrière. Mac OS X fournit un niveau de sécurité optimal en utilisant des standards de l'industrie, des logiciels open source et une architecture système bien pensée dès le départ. Cette conception intelligente contre ainsi les multiples virus et spywares qui attaquent les ordinateurs de nos jours.



Configuration sécurisée par défaut

L'approche sécuritaire d'Apple protège votre Mac contre les attaques sur les réseaux privés ou publics, comme Internet, dès la sortie de l'emballage. Tous les ports de communication sont fermés et tous les services natifs – partage de fichiers personnels, partage de fichiers Windows, partage Web, connexion à distance, accès FTP, Apple Events à distance et partage d'imprimantes – sont désactivés par défaut. Le compte administrateur Mac OS X, contrairement au compte administrateur Windows, désactive l'accès aux fonctions essentielles du système d'exploitation. De nombreux utilisateurs utilisent systématiquement un compte administrateur sur leur PC Windows, ce qui les expose aux attaques de virus. La configuration par défaut de Mac OS X, au contraire, vous protège des utilisateurs malintentionnés qui peuvent facilement prendre le contrôle de votre système.

Pare-feu personnel

Tout le courrier indésirable qui circule actuellement sur Internet est envoyé par des boîtes provenant le plus souvent d'ordinateurs Windows. Les cyber-pirates recherchent les ordinateurs les plus fragiles. Le pare-feu personnel intégré à Tiger protège votre Mac des accès non-autorisés en surveillant l'intégralité du trafic entrant. Lorsque vous activez le pare-feu personnel de Mac OS X, seules sont autorisées les connexions entrantes que vous avez choisies. Et désormais avec le mode discret, votre Mac ne signalera même pas son existence à ceux qui recherchent des ordinateurs à attaquer.

Mise à jour automatique

Nouveautés Tiger

Prise en charge de Kerberos pour les réseaux VPN

Tirez parti d'une authentification basée sur Kerberos pour les connexions par signature unique à un réseau VPN.

Assistant pour les certificats

Demandez, générez et gérez facilement des certificats pour de petits groupes de travail avec cet utilitaire complet proposé par un acteur majeur pour un coût modique.

Journaux du pare-feu

Tenez un journal de toutes les activités du pare-feu telles que les sources, les destinations et les tentatives bloquées.

Mode discret du pare-feu

Bénéficiez d'une sécurité optimale en vous assurant que tout trafic non-autorisé ne reçoit aucune réponse — pas même un indice qui signifierait l'existence de votre ordinateur.

Norme GSCIS (Government Smart Card Interface Standard)

Utilisez des Smart Cards sécurisées qui répondent aux normes du ministère de la Défense américain.

Téléchargements sécurisés

Recevez un message d'alerte lorsque le système ou une application tente de télécharger des fichiers dont le type ou la source n'est pas fiable.

Mémoire virtuelle sécurisée

Renforcez la sécurité de vos informations importantes en vérifiant que les données transitoires stockées dans la mémoire virtuelle restent confidentielles.

Authentification par Smart Card

Utilisez une Smart Card pour accéder à votre système ou à votre Trousseau.

Synchronisation du Trousseau .Mac

Synchronisez votre Trousseau sur vos différents Mac en utilisant votre compte .Mac.

Prise en charge des certificats dans le Carnet d'adresses

Visualisez les informations de certificats dans votre Carnet d'adresses pour tous les contacts qui fournissent leur code public.

Importation/exportation depuis/vers le Trousseau

Importez et exportez facilement des certificats vers et depuis votre Trousseau.

Assistant mot de passe

Utilisez l'Assistant mot de passe pour choisir un mot de passe sécurisé.

Vous avez oublié votre mot de passe ?

Réinitialisez simplement le mot de

Mac OS X peut télécharger automatiquement des mises à jour de logiciels. Ainsi, vous êtes certain de disposer des tout derniers correctifs de sécurité et versions de logiciels, directement fournis par Apple. Apple appose une signature numérique sur les mises à jour – vous pouvez nous faire confiance.



Le mot de passe de tout utilisateur est directement défini depuis la fenêtre de connexion si vous avez défini un mot de passe maître pour votre système.

Accès au Trousseau

Organisez facilement les éléments du Trousseau avec la nouvelle interface utilisateur de style iTunes, qui comprend aussi un champ de recherche permettant de localiser facilement un mot de passe spécifique ou tout autre élément.

FileVault

Protégez les informations de votre Mac des regards indiscrets avec [FileVault](#), qui utilise la toute dernière norme de sécurité employée par les autorités officielles, le cryptage AES-128, pour protéger votre travail. Il effectue un cryptage et un décryptage automatiques, si bien que vous ne vous en rendez même pas compte. FileVault protège des regards indiscrets toutes les informations contenues dans votre répertoire personnel (dossier Départ), si bien que vos secrets professionnels, vos listes de souvenirs à rapporter de vacances et vos comptes personnels resteront parfaitement confidentiels.

Un trousseau sécurisé

Pour gérer plus facilement la quantité grandissante de mots de passe et d'autorisations caractérisant l'informatique en réseau, Mac OS X inclut un Trousseau. Celui-ci stocke l'ensemble des informations indispensables à l'utilisation d'images disques cryptées et à la connexion à des serveurs de fichiers, ftp ou Web. Mac OS X ajoute automatiquement les données de votre compte [Mac](#) à votre Trousseau. Dès que vous ouvrez une session sous Mac OS X, le système ouvre votre Trousseau. Il est inutile de saisir vos nom d'utilisateur et mot de passe pour accéder aux données qu'il contient. Libre à vous, néanmoins, de verrouiller ce Trousseau lorsque le système est en mode Suspension d'activité ou inactif. Dans ce cas, Mac OS X vous invitera à spécifier votre mot de passe la prochaine fois que vous tenterez d'accéder à ces données sécurisées. Les autres utilisateurs ne peuvent accéder ni à votre Trousseau ni à son contenu.



Suppression définitive

A présent, vous avez la possibilité d'effacer définitivement les fichiers sensibles devenus inutiles. Avec l'effacement sécurisé du contenu de la Corbeille, il n'existe plus aucune trace d'un fichier ou dossier supprimé. Le mode de suppression classique se contente de supprimer le nom du fichier du répertoire du disque, mais les données demeurent intactes. L'effacement sécurisé du contenu de la Corbeille remplace aussitôt le contenu de ce fichier par des données aléatoires, de manière à supprimer ce fichier et à rendre sa reconstruction impossible.



Cryptage d'images disque

Pour plus de sécurité, vous pouvez crypter une partie de votre disque dur au moyen d'une image disque et la transmettre par e-mail à des utilisateurs disposant du mot de passe adéquat. Il vous suffit d'ouvrir l'utilitaire Outils disque dur, de créer une nouvelle image et d'activer le cryptage. L'image s'affichera comme un volume sur votre bureau. Si votre Trousseau est verrouillé, ou si vous transmettez cette image disque à une autre personne, l'image est sécurisée. Si votre Trousseau est déverrouillé, vous pouvez copier, déplacer et supprimer des fichiers comme vous le feriez sur tout autre volume.



La sécurité avant tout

Apple met son code source à la disposition des développeurs et exploite des logiciels [open source](#) éprouvés ; la communauté des développeurs examine les mesures de sécurité du système, souligne les points faibles, débat des solutions et applique les améliorations permettant de combler d'éventuelles failles. Grâce à cette coopération inhérente au développement de logiciels Open Source, Apple et la communauté Open Source peuvent fournir un système plus sécurisé et répondre rapidement aux problèmes de sécurité. Apple travaille en étroite collaboration avec les organismes de contrôle de la sécurité [CERT](#) et [FIRST](#).

Sécurité des réseaux

Fruit de ces efforts, [Darwin](#), fondation Open Source de Mac OS X, constitue la base sécuritaire dont vous avez besoin dans l'environnement actuel. Darwin offre Kerberos, Secure Shell (OpenSSH), une structure permettant des transactions Web sécurisées (OpenSSL), le cryptage de données WPA (Wi-Fi Protected



Access) pour les réseaux sans fil et un réseau VPN (Virtual Private Network) L2TP pour un accès à distance sécurisé aux réseaux d'entreprise.

Mac OS X protège vos données et veille sur votre Mac.

[Accueil](#) > [Mac OS X](#) > [Caractéristiques](#) > Sécurité

Copyright © 2005 Apple Computer, Inc. All rights reserved.