

Questions techniques

Q. *DeviceLock est une solution logicielle ou matérielle?*

R. DeviceLock est une solution 100% logicielle.

Q. *Que fait exactement DeviceLock?*

R. DeviceLock contrôle l'accès des utilisateurs à tous les types de périphériques : clés USB et FireWire, adaptateurs Bluetooth et Wi-Fi, lecteurs CD-ROM, disquettes, etc. Typiquement, DeviceLock permet aux administrateurs système de bloquer l'accès à certains périphériques pour utilisateurs ou groupe d'utilisateurs définis. Et d'autoriser dans le même temps d'autres utilisateurs ou groupe d'utilisateurs à utiliser ces mêmes périphériques.

Q. *DeviceLock est-il un logiciel de chiffrage, qui crypte les données?*

R. Non. DeviceLock ne crypte aucune donnée. Il ne fait que contrôler l'accès à des périphériques.

Q. *Comment DeviceLock protège-t-il les données?*

R. DeviceLock intercepte toutes les demandes d'accès à des périphériques, émises par les utilisateurs du réseau administré. Pour chaque demande, il vérifie si l'utilisateur a reçu ou non l'autorisation d'utiliser le matériel sollicité. Si oui, l'utilisateur peut s'en servir. Sinon, il reçoit un message "accès refusé", et ne peut utiliser le matériel en question.

Q. *Quels périphériques DeviceLock peut-il contrôler?*

R. Les ports USB, FireWire (IEEE 1394), les ports séries (COM) (dont les modems internes), les ports parallèles (LPT), les ports InfraRouge (IrDA), les adaptateurs Bluetooth, Wi-Fi (sans fil), les adaptateurs réseau, les lecteurs CD et DVD (dont les graveurs), les lecteurs de disquettes, les lecteurs de bande / périphérique de sauvegarde, tous les périphériques de stockage amovibles (dont les clés USB, les lecteurs flash, les disques durs externes, les lecteurs ZIP, etc.).

Q. *DeviceLock fonctionne-t-il sous UNIX (Linux, FreeBSD, etc.), et sous Mac?*

Q. *DeviceLock fonctionne-t-il sous Windows 95, Windows 98 ou Windows Me?*

R. DeviceLock ne fonctionne ni sous UNIX ni sous Mac. Il fonctionne uniquement sous Windows NT 4.0, Windows 2000, Windows XP ou Windows Server 2003. Cependant, il existe un autre produit appelé DeviceLock Me, qui peut fonctionner sous Windows 95/98/Me. En comparaison de DeviceLock, DeviceLock Me offre des fonctionnalités plus limitées – il ne peut contrôler que des périphériques USB, FireWire, Bluetooth, Wi-Fi et InfraRouge.

Q. *DeviceLock doit-il être installé sur tous les ordinateurs du réseau ou uniquement sur le serveur?*

R. DeviceLock doit être installé sur chaque ordinateur que l'on souhaite sécuriser. DeviceLock est doté d'un petit agent (DeviceLock Service) invisible pour l'utilisateur, qui fonctionne sur chaque ordinateur.

Q. DeviceLock permet-il l'administration réseau à distance?

R. Oui. DeviceLock est doté d'une console d'administration centralisée. Les administrateurs peuvent ainsi gérer à distance et de manière centralisée les agents DeviceLock de chacun des ordinateurs du réseau.

Q. DeviceLock peut-il être déployé à distance vers les ordinateurs du réseau?

R. Oui. Les administrateurs peuvent déployer les agents DeviceLock sur chaque ordinateur du réseau à partir de la console centrale. De plus, les agents DeviceLock peuvent être déployés en utilisant le package MSI et les Politiques de Groupe (GPO) de Active Directory.

Q. Dois-je me connecter manuellement à chaque ordinateur du réseau pour changer leurs autorisations?

R. Vous pouvez effectivement le faire manuellement. Toutefois, si vous avez un réseau important, vous préférerez peut-être configurer les autorisations sur plusieurs ordinateurs cibles en une seule passe grâce à la fonction Autorisations par lots. Dans un domaine Active Directory les autorisations DeviceLock peuvent également être gérées par les Politiques de Groupe (GPO).

Q. Les utilisateurs peuvent-ils désactiver DeviceLock à partir de leurs postes de travail, afin de passer outre le système?

R. Non. Seuls les utilisateurs qui ont des privilèges d'administration peuvent gérer DeviceLock. Si votre réseau est configuré correctement et que les utilisateurs n'ont pas de privilège d'administration, il leur est impossible de désactiver DeviceLock.

Q. DeviceLock délivre-t-il les autorisations au moment où l'utilisateur se connecte au système?

R. Non. Les autorisations s'appliquent immédiatement après que l'administrateur les ait déployées à partir de la console centrale d'administration.

Q. Qu'arriverait-il si deux utilisateurs ou plus étaient connectés au même moment sur le même ordinateur (pour Terminal Server ou XP Fast User Switching)?

R. DeviceLock contrôle en temps réel les demandes d'accès par les utilisateurs à des périphériques. Chaque utilisateur a son propre contexte de sécurité et DeviceLock sait à tout moment quels utilisateurs tentent d'accéder à un périphérique. En cas de demande simultanée par deux utilisateurs pour un même périphérique, le système est donc parfaitement capable de permettre l'accès à un utilisateur et de le refuser à l'autre.

Q. Est-il possible, pour certains types de périphérique, de configurer des autorisations pour des groupes d'utilisateurs?

R. Oui. Vous pouvez configurer des autorisations par groupes d'utilisateurs comme par utilisateurs distincts.

Q. Où DeviceLock va-t-il identifier les comptes utilisateurs ou groupes d'utilisateurs?

R. DeviceLock les puise dans le sous-système de sécurité Windows. Il s'agit de comptes standards, qui s'utilisent de manière standard dans Windows (p. ex. pour connexion au système, autorisations fichiers/dossiers, etc.).

Q. DeviceLock fonctionne-t-il avec Active Directory?

R. Oui. La configuration et les autorisations DeviceLock peuvent être modifiées à partir des Politiques de Groupe et déployées par l'intermédiaire de Active Directory. Par ailleurs, DeviceLock s'appuie sur les comptes Active Directory, ainsi que des contrôleurs du domaine.

Q. Est-il possible de protéger l'accès aux périphériques avec un mot de passe?

R. Non. DeviceLock est un logiciel de contrôle professionnel qui agit en amont et ne supporte pas ce type de solutions traditionnelles, qui offrent de faibles niveaux de protection.

Q. Peut-on protéger l'accès à un périphérique uniquement pendant certaines périodes?

R. Oui. Vous pouvez définir la/les périodes de la journée, ainsi que le/les jours de la semaine pendant lesquels l'utilisateur aura le droit d'utiliser le matériel ciblé.

Q. Est-il possible de bloquer un port USB tout en permettant l'accès au clavier et à la souris USB?

R. Oui. Vous pouvez bloquer complètement les ports USB, tout en permettant l'utilisation de certains périphériques de type : souris, clavier, imprimante, scanner, modem ou adaptateur Bluetooth.

Q. Est-ce que je peux permettre l'utilisation d'un périphérique pour la lecture mais pas pour l'écriture/la gravure de fichiers?

R. Oui. Vous pouvez permettre la lecture et interdire l'écriture/la gravure pour tous les périphériques de type disquettes, CD-ROM, lecteur flash, clé USB, ZIP, etc..