

## **Logiciel SafeNet Authentication Manager**

### **Logiciel**

Posté par : JulieM

Publié le : 19/7/2011 11:00:00

**SafeNet, Inc.**, leader mondial en sécurité des informations, annonce la disponibilité immédiate de sa nouvelle solution de vérification des informations d'identification pour terminaux mobiles. Cette solution permet une utilisation sécurisée des terminaux mobiles grand public les plus populaires (iPhone et iPad) sur les réseaux d'entreprise.

**SafeNet Authentication Manager (SAM)**, qui fait partie de SafeNet Fully Trusted Authentication Environnement, permet désormais aux entreprises de mettre en œuvre une stratégie d'authentification complète pour de nombreux types de terminaux, et notamment les terminaux mobiles personnels. En intégrant la gestion des informations d'identification dans un programme d'authentification unifié, les entreprises peuvent avoir l'assurance que seuls les terminaux mobiles personnels autorisés ont accès aux réseaux et aux ressources de l'entreprise.



**La « consommation » des technologies de l'information** est-à-dire l'utilisation de terminaux informatiques personnels pour accéder aux réseaux de l'entreprise est devenue en 2011 l'une des préoccupations majeures des départements informatiques. En effet, un certain nombre de problèmes de sécurité et d'administration se posent lorsque des utilisateurs accèdent aux réseaux d'entreprise via leurs smartphones, tablettes PC et ordinateurs personnels. Un défaut de vérification et de contrôle des informations d'identification des terminaux mobiles personnels peut exposer les réseaux à des failles de données et à des accès non autorisés. Avec le nombre accru de terminaux grand public capables d'accéder à des données sensibles appartenant à l'entreprise et aux clients, les départements informatiques doivent s'efforcer de trouver l'équilibre entre les exigences en matière de productivité et la mise en œuvre d'actions adaptées dans le domaine de la sécurité.

« Le nombre croissant de smartphones, tablettes PC et autres terminaux grand public accédant aux réseaux de l'entreprise constitue un enjeu majeur de sécurité », souligne **Lawrence Pingree**, Directeur de recherche chez Gartner. « L'accès à des données critiques de l'entreprise au moyen de terminaux non fiables et souvent inconnus fait courir un risque extrêmement important. Compte tenu de la forte diffusion dans le grand public des terminaux mobiles, il n'est guère réaliste d'envisager une restriction de l'utilisation de ces smartphones et tablettes PC. Il est en revanche tout à fait possible de gérer ce risque en recourant à des capacités d'authentification permettant de valider ces terminaux en vue de sécuriser leur accès. »

**SafeNet permet désormais aux entreprises de sécuriser** et de gérer l'accès des

terminaux mobiles grand public sur le réseau de l'entreprise, exactement comme elles gèrent leurs propres ressources. En permettant la mise en œuvre unifiée des programmes d'authentification, des politiques de sécurité et d'un contrôle des informations d'identification pour les terminaux appartenant aux salariés, [SafeNet Authentication Manager](#) (SAM) permet aux entreprises d'améliorer la productivité de leurs salariés tout en réduisant le coût de la gestion de l'information ainsi que les ressources d'administration. De surcroît, grâce à SAM, les entreprises peuvent administrer de manière centralisée et globale l'ensemble des contraintes d'authentification liées aux réseaux locaux, aux VPN, aux applications SaaS et aux environnements virtualisés.

« Le périmètre de sécurité et les terminaux qui y accèdent ont normalement changé, ce qui contraint les entreprises à repenser l'accès à leurs réseaux, notamment en ce qui concerne les terminaux mobiles », précise **Andrew Young**, Vice-président Authentification chez SafeNet. « SafeNet Authentication Manager permet à nos clients d'évoluer au fil du temps. Il leur permet d'élargir leur infrastructure de sécurité afin de rester en phase avec l'émergence de nouveaux terminaux et d'assurer la pérennité de la protection de leurs données. »