



RSA® Authentication Manager

Le moteur de sécurité niveau entreprise de l'authentification RSA SecurID®

En bref...

- Un moteur de sécurité à deux facteurs de qualité entreprise pour l'authentification de plus de 25 millions d'utilisateurs de RSA SecurID® dans le monde
- Une extensibilité répondant aux besoins des entreprises de toutes dimensions
- Une interopérabilité avec plus de 350 produits et 200 fournisseurs – sans coût additionnel
- Une gamme flexible de méthodes d'habilitation avec administration centrale

La protection et granatité d'identité

La protection d'identité regroupe des fonctionnalités et méthodologies permettant de réduire les risques liés à l'anonymat ou à l'utilisation inappropriée des comptes utilisateurs. Elle apporte aux entreprises l'assurance nécessaire lorsqu'elles autorisent des identités de confiance à interagir avec les systèmes et accéder à l'information librement et en toute sécurité, ou lorsqu'elles ouvrent de nouvelles voies de croissance du chiffre d'affaires, de satisfaction clients et de contrôle des coûts.

RSA Authentication Manager est un standard de fait dans le domaine de la protection d'identité. Sa couverture fonctionnelle répond aux exigences des quatre domaines clés de la protection d'identité : gestion et politique d'habilitation ; authentification ; autorisation et intelligence. Le portefeuille de solutions RSA de protection d'identité fait évoluer l'authentification des utilisateurs du cadre de mesure unique de sécurité vers un cadre de modèle de confiance persistant basé du contrôle d'utilisation de chaque identité et de ses prérogatives. Les identités de confiance gérées par RSA permettent de sécuriser les transactions quotidiennes

et de bénéficier de nouveaux modes de développement en fournissant des accès sécurisés aux collaborateurs, clients et partenaires dans un contexte faisant un arbitrage optimal entre les risques encourus, les coûts et l'ergonomie d'utilisation.

Le logiciel RSA® Authentication Manager est le module d'administration de RSA SecurID®. Il valide les requêtes d'authentification et centralise les politiques d'accès aux réseaux d'entreprise. Grâce à son intégration transparente aux authentificateurs RSA SecurID et à RSA® Authentication Agent, cette solution permet de déployer un système performant d'authentification à deux facteurs pour contrôler les accès à une quantité incomparable de réseaux (VPN ou sans fil), d'applications Web et métier et d'environnements d'exploitation (notamment Microsoft® Windows®).

Performances et extensibilité incomparables

RSA Authentication Manager répond aux besoins des entreprises de toutes dimensions. Bâti sur une architecture multiprocesseur de qualité entreprise, il peut indifféremment prendre en charge 25 ou des millions d'utilisateurs par serveur – et des centaines d'authentifications simultanées par seconde. Largement déployé dans des entreprises leaders de tous secteurs d'activité (banques, administrations, industrie, distribution, hautes technologies, santé, etc.) et dans le monde entier, il est également utilisé par de très nombreuses PME. Le produit est proposé en deux versions : une édition de base et l'édition Entreprise.

Réplication de bases de données

La fonction de réplication permet de concevoir une configuration réseau flexible, d'équilibrer la charge, de maximiser les performances et de réduire les coûts d'administration.

L'édition de base intègre un serveur primaire et un serveur répliqué ; l'administration des utilisateurs est gérée sur le premier et dupliquée sur le second (les deux pouvant gérer



The Security Division of EMC

les requêtes d'authentification). Les agents RSA Authentication gèrent l'équilibrage de la charge entre serveurs en contrôlant les temps de réponse pour diriger chaque requête sur le serveur le plus performant.

L'édition Entreprise, dédiée aux déploiements moyens à grands, intègre un serveur primaire et jusqu'à 15 répliques par domaine – avec la capacité de réunir jusqu'à six domaines distincts. Chaque serveur de déploiement peut être constitué d'un cluster comportant jusqu'à quatre machines pour optimiser l'équilibrage des tâches d'administration et d'authentification. Cette architecture permet aux administrateurs de contrôler l'ensemble des connexions en temps réel, de mettre à jour les politiques de sécurité simultanément pour tous les réseaux mondiaux et de développer une topologie réseau maximisant les performances.

Administration et contrôle supérieurs

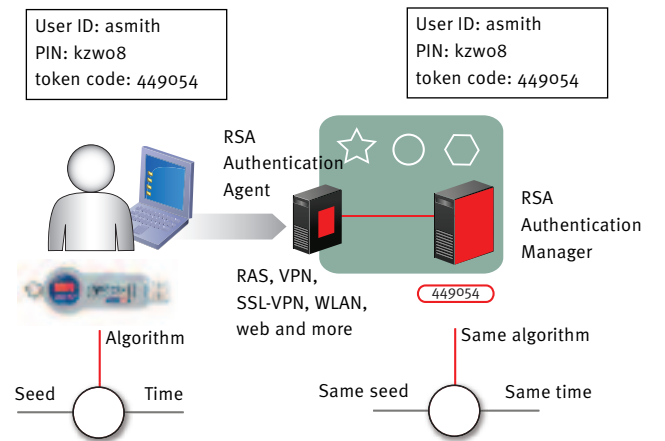
RSA Authentication Manager présente des caractéristiques exclusives de flexibilité et de contrôle. Ne nécessitant pas l'installation d'un logiciel d'administration sur le PC, son serveur Web intégré permet d'accéder à la console d'administration avec n'importe quel navigateur Web. En outre, le serveur Juniper® Steel Belted RADIUS, inclus bénéficie d'une administration intuitive et ergonomique au sein de la même console.

Grâce à l'intégration native LDAP, RSA Authentication Manager peut pointer en temps réel vers une ou plusieurs bases d'habilitations pour obtenir des informations sur les utilisateurs et les groupes. Plusieurs sources LDAP peuvent être prévues sans changement de schéma (par exemple, Microsoft Active Directory® et Sun One™). Par ailleurs, un composant pour la console d'administration Microsoft (MMC) permet de manipuler les enregistrements utilisateur directement dans son interface.

L'édition de base et l'édition Entreprise intègrent RSA® Credential Manager, un module logiciel dédié aux solutions en libre-service (édition de base et Entreprise) et au workflow de provisioning (Entreprise uniquement) pour accélérer l'ajout d'utilisateurs et l'affectation de prérogatives.

Audit et reporting

RSA Authentication Manager journalise toutes les transactions et activités des utilisateurs. Ces données peuvent être exploitées à des fins d'audit, de comptabilité ou de reporting de conformité. Les rapports prédéfinis peuvent totalement personnalisés pour des besoins de suivi des activités



Authentification à deux facteurs RSA SecurID, basée sur la synchronisation temporelle.

et des incidents, des synthèses d'utilisation, etc. En plus de ses fonctions de reporting, le produit permet aussi de surveiller en direct l'ensemble des activités ou celles de certaines branches dans les déploiements globaux.

Une large gamme de méthodes d'habilitation

RSA Authentication Manager supporte de multiples authentificateurs : clés matérielles, jetons logiciels (sur PC ou téléphones intelligents), authentification à la demande (avec mots de passe à usage unique fournis par e-mail ou SMS), etc. L'ensemble de ces habilitations est géré centralement dans une interface commune.

Une interopérabilité immédiate

RSA Authentication Manager est interopérable avec la plupart des infrastructures réseau et systèmes d'exploitation – plus de 350 produits de 200 éditeurs – et offre des gages supérieurs de flexibilité et de protection des investissements. Des fournisseurs leaders de produits d'accès à distance, de VPN, de pare-feux, de réseaux sans fil, de serveurs Web et d'applications métier intègrent en standard le support de RSA Authentication Manager.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2008 RSA Security Inc. Tous droits réservés.

RSA, RSA Security, SecurID, SecurID Ready et le logo de RSA sont des marques ou marques déposées de RSA Security Inc. aux Etats-Unis et/ou dans d'autres pays. Microsoft et Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays. EMC est une marque déposée d'EMC Corporation. Toutes les autres produits et services mentionnés sont la propriété de leurs détenteurs respectifs.

FR SIDAM DS 0508