

# RSA® Authentication Manager Express

Une solution d'authentification forte et économique, signée du leader du marché

## En bref :

- Technologie d'authentification multi-facteurs éprouvée
- Solution adaptée aux contraintes budgétaires des PME/PMI comptant jusqu'à 2 500 utilisateurs
- Transition aisée d'un système de protection par mot de passe à une authentification forte
- Authentification qui s'adapte dynamiquement en fonction du profil utilisateur et du niveau de risque associé à chaque tentative d'authentification
- Solution compatible et prête à l'emploi immédiatement avec les VPN SSL et applications Web leaders du marché, afin de faciliter le déploiement et l'utilisation sur tout type d'environnement

Aujourd'hui, les entreprises doivent composer avec la mobilité accrue de leurs équipes, l'intensification de la pression réglementaire et la sophistication des menaces qui pèsent sur leurs informations sensibles et autres éléments de propriété intellectuelle. Impuissants face à la sagacité des cybercriminels, les systèmes de protection par mot de passe s'avèrent incapables de bloquer les accès non autorisés aux ressources de l'entreprise. De fait, à l'heure où les PME mettent en ligne une part croissante de leurs données et multiplient les accès distants via VPN SSL et applications Web, les systèmes d'authentification forte s'imposent comme une évidence.

Au moment des choix, les entreprises devront privilégier une solution d'authentification forte en tant que solution plus sécurisée, sans toutefois imposer des contraintes inutiles aux utilisateurs, ni grever les budgets et ressources informatiques.

## Une authentification forte à un prix abordable

RSA Authentication Manager Express propose une solution d'authentification forte multi-facteurs optimisée pour les contraintes de sécurité, de commodité et de budget de votre entreprise. Alternative plus puissante et plus sécurisée qu'une protection par simple mot de passe, RSA Authentication Manager Express permet d'offrir aux utilisateurs distants (salariés, partenaires, sous-traitants et clients) un accès aux données en toute confiance, en tout lieu et à tout moment. Basée sur une technologie éprouvée, la solution offre un service d'authentification forte paramétrable en fonction des contraintes de ressources de l'entreprise, de son niveau de tolérance au risque et du profil de ses utilisateurs.

### Migration transparente d'une protection par mot de passe vers une authentification multi-facteurs

Grâce à sa technologie d'authentification basée sur les risques, RSA Authentication Manager Express offre aux utilisateurs une authentification forte totalement transparente. En effet, la solution intervient en arrière-plan pour protéger les ressources Web (VPN SSL et applications Web) contre tout accès non autorisé. Ainsi les utilisateurs continuent d'utiliser leurs identifiants classiques (nom d'utilisateur et mot de passe), tandis que le moteur RSA Risk Engine procède à l'évaluation de dizaines de facteurs associés à l'authentification dans chacune des trois catégories suivantes :

- Ce que connaît l'utilisateur (nom d'utilisateur et mot de passe existants, par exemple)
- Ce que possède l'utilisateur (ordinateur portable ou PC de bureau, par exemple)
- Ce que fait l'utilisateur (activité récente enregistrée sur son compte, par exemple)

RSA Risk Engine attribue alors un niveau de confiance à l'utilisateur en fonction de la similitude de ces facteurs avec les événements d'authentification précédemment enregistrés. Dès lors que ce niveau est égal ou supérieur au niveau défini dans les protocoles de sécurité de l'entreprise, l'utilisateur est authentifié. Ainsi, face à un schéma d'utilisation standard, l'authentification multi-facteurs s'opère en toute transparence pour l'utilisateur qui n'a aucune autre information à saisir que son mot de passe.

En revanche, lorsque les caractéristiques d'une tentative d'authentification diffèrent des événements d'authentification précédemment enregistrés – comme dans le cas d'une demande d'authentification à partir d'un équipement non identifié – le système invite l'utilisateur à fournir des preuves additionnelles d'identité. Parmi les options de preuve, il pourra lui être demandé de répondre à certaines questions spécifiques ou de soumettre un code d'autorisation envoyé sur son mobile (SMS) ou par e-mail.

### Simplicité d'installation, de déploiement et de provisioning des utilisateurs

RSA Authentication Manager Express s'impose comme le moyen idéal pour profiter rapidement des avantages de l'authentification multi-facteurs – sans transiger sur la sécurité. Cette solution est livrée préinstallée et prête à l'emploi sur une appliance alliant sécurité et commodité. De sa console de gestion Web intuitive à son intégration certifiée avec les principaux VPN SSL et serveurs Web... tout est prévu pour faciliter l'installation et l'intégration de RSA Authentication Manager Express à votre environnement existant.

Avec RSA Authentication Manager Express, le déploiement d'un système d'authentification basé sur les risques est un jeu d'enfant : il suffit de pointer le serveur vers une base d'utilisateurs existante dans Microsoft Active Directory et de sélectionner le niveau de sécurité minimum requis pour l'authentification. Le moteur RSA Risk Engine commence alors à collecter en silence des informations à partir des sessions d'authentification afin d'établir les profils individuels des utilisateurs. L'objectif : évaluer et comparer ces profils lors des futures tentatives d'authentification. Dès que le système dispose de suffisamment d'informations pour créer un profil utilisateur, il démarre la mise en application des règles d'authentification définies et automatise l'exécution de l'authentification multi-facteurs. Côté utilisateur, le maintien des mots de passe permet de migrer en toute transparence vers un système d'authentification multi-facteurs. Ainsi, RSA Authentication Manager Express renforce le niveau de sécurité de la protection par mot de passe, sans que les utilisateurs aient besoin de se former, sur un nouveau système, d'exécuter des étapes d'authentification supplémentaires ni de gérer de multiples habilitations.

### RSA Risk Engine : un moteur d'analyse des risques auto-apprenant et éprouvé

C'est le même moteur RSA Risk Engine, protégeant déjà les comptes bancaires en ligne de plus de 250 millions de clients à travers le monde qui est intégré à RSA Authentication Manager Express. Réputé pour sa fiabilité et sa sécurité, RSA Risk Engine garantit la validité des identités tout en affranchissant les utilisateurs des contraintes relatives à la réalisation d'étapes d'authentification complémentaire. À la différence des systèmes statiques basés sur des règles, RSA Risk Engine emploie une combinaison d'analyses comportementales et matériels en temps réel. Il adapte ainsi son modèle de risque en dynamique, au gré des nouvelles informations collectées sur les équipements, les personnes et l'ensemble des utilisateurs.

Les utilisateurs à faible risque sont authentifiés en silence, tandis que les utilisateurs à haut risque sont challengés et invités à fournir des informations complémentaires. Avec RSA Authentication Manager Express vous contrôlez « comment » et « quand » les utilisateurs seront challengés en se basant sur la politique de risque de l'entreprise.

### Analyse matériels

La fonction d'analyse matériels de RSA Authentication Manager Express permet d'observer de manière discrète, dynamique et systématique le PC fixe ou portable de l'utilisateur à chaque tentative d'authentification. Pour ce faire, la solution recueille et évalue des dizaines de caractéristiques propres à chaque équipement. À partir de cette analyse, RSA Risk Engine détermine si l'équipement correspond à une machine précédemment utilisée par le titulaire du compte et peut donc être jugée digne de confiance. Si tel est le cas, l'utilisateur est authentifié à l'aide de son seul mot de passe. En revanche, si la machine n'est pas reconnue, l'utilisateur est prié de fournir des preuves d'identité supplémentaires. Grâce à l'analyse matériels, l'équipement de l'utilisateur devient un second facteur d'authentification, sans besoin de provisionner des habilitations statiques ni de déployer de logiciel supplémentaire.

### Analyse comportementale

L'analyse comportementale évalue les schémas d'utilisation, les événements d'authentification, l'activité des comptes et d'autres facteurs afin d'évaluer le risque global associé à chaque tentative d'authentification. Le risque comportemental est calculé en comparant la demande d'authentification en cours avec l'historique d'authentification de l'utilisateur, les comportements connus des autres utilisateurs d'une même population, et les signatures comportementales caractéristiques d'une tentative d'accès non autorisée. Si le risque est jugé faible, le comportement de l'utilisateur suffit à constituer un facteur d'authentification complémentaire qui permet de confirmer de manière silencieuse l'identité du titulaire du compte.

Les synergies entre ses divers composants et fonctionnalités font de RSA Authentication Manager Express une véritable solution d'authentification multi-facteurs adaptée aux besoins des PME/PMI en termes de sécurité, de commodité et de coûts. Partie intégrante de la gamme Authentification de RSA – le leader des solutions d'authentification – RSA Authentication Manager Express constitue le moyen le plus rapide de profiter pleinement des avantages de l'authentification multi-facteurs, sans transiger sur la sécurité.



[www.rsa.com](http://www.rsa.com)

©2010 EMC Corporation. Tous droits réservés.  
EMC, EMC, RSA et le logo RSA sont des marques ou des marques déposées d'EMC Corporation aux États-Unis et/ou dans d'autres pays. Les autres produits et services cités sont des marques de leurs propriétaires respectifs.  
AMX\_DS\_1210