

# RSA® Authentication Manager Express

Strong, Affordable Authentication from the Leader in Authentication Solutions

## At a Glance

- Delivers proven multi-factor authentication technology
- Optimized for the limited resources of small and mid-sized organizations up to 2,500 users
- Provides a seamless transition from passwords to strong authentication
- Enables authentication to be tailored dynamically to the user profile and to the level of risk associated with the authentication attempt
- Compatible out-of-the-box with leading SSL VPNs and Web applications for ease of deployment and use in any environment

Today's organizations are faced with the challenges of an increasingly mobile workforce, stricter regulations and advanced threats that target sensitive information and intellectual property. Weak, password-only protection is not a match for savvy cybercriminals, and is no longer considered an effective method for preventing unauthorized users from accessing company resources. As small to mid-sized organizations move more and more of their information online and provide remote access to their data resources using SSL VPNs and Web Applications, strong authentication becomes a business requirement.

When evaluating the options, organizations must consider a strong authentication solution as one that provides the right balance of security without unnecessarily inconveniencing end users or becoming a drain on IT budget and resources.

## Strong, Affordable Authentication


RSA Authentication Manager Express delivers strong, multi-factor authentication that is optimized for the unique security, convenience and budget requirements of your organization. A stronger and more secure alternative to password-only protection, RSA Authentication Manager Express enables organizations to extend anytime, anywhere information access confidently to remote employees, partners, contractors, and clients. The proven technology delivers strong authentication that can be tailored to an organization's resource constraints, risk tolerance, and the profile of its users.

### Seamless Migration from Passwords to Multi-factor Authentication

RSA Authentication Manager Express delivers a seamless, strong authentication solution for users through Risk-Based Authentication – providing invisible, behind-the-scenes protection of web-based resources (SSL VPNs and Web Applications) against unauthorized access. Users continue to use their standard username and password, while the RSA Risk Engine evaluates dozens of factors associated with the authentication in each of these three categories:

- Something the user knows, such as an existing username and password
- Something the user has, such as a laptop or desktop PC
- Something the user does, such as recent account activity

The RSA Risk Engine determines a level of assurance for the user based on the similarity of these factors to previously recorded authentication events. When the calculated assurance level is equal to or above the level established by an organization's policy, the user is authenticated. Therefore, in cases of typical user behavior, multi-factor authentication is transparent, achieved without the user having to provide anything other than a password.



In cases where characteristics of an authentication attempt are dissimilar to previously recorded authentication events—for example, authenticating from an unrecognized device—the user is prompted for additional proof of identity. Options for additional proof of identity include answering challenge questions or submitting an authorization code delivered to a phone via SMS (text) message or e-mail.

### **Straightforward Installation, Deployment, and User Provisioning**

RSA Authentication Manager Express offers organizations the fastest path to multi-factor authentication without compromising on security. The solution comes pre-installed and ready to use on a secure and convenient Appliance platform. From its intuitive browser-based management console to its certified integration with leading SSL VPNs and Web servers, RSA Authentication Manager Express makes installation and integration with your existing environment trouble free.

Deploying Risk-Based Authentication with RSA Authentication Manager Express is as effortless as pointing the server to an existing user population in Microsoft Active Directory and selecting the minimum assurance level required for authentication. The RSA Risk Engine begins silently collecting information from user authentications to establish individual user profiles for evaluation and for comparison with future authentication attempts. Once the system has sufficient information to create a user profile, it automatically begins enforcing the authentication policy and providing multi-factor authentication. From the end user perspective, the continued use of passwords offers a seamless transition to multi-factor authentication. With RSA Authentication Manager Express, passwords become more secure without the need for users to learn a new system, perform additional steps, or manage multiple credentials.

### **Self-learning, Proven Risk Engine**

The same RSA Risk Engine in RSA Authentication Manager Express is used to safeguard the accounts of more than 250 million online banking customers worldwide. Proven and secure, the RSA Risk Engine provides identity assurance and reduces the burden on end users to complete additional authentication steps. Not a static rules-based system, the RSA Risk Engine employs a combination of real-time device and behavioral analytics and adapts its risk model dynamically as new information about devices, individuals, and entire user population is collected. Low-risk users are authenticated silently while high-risk users are challenged.

With RSA Authentication Manager Express, you control how and when users get challenged based on your organization's risk policy.

### **Device Analysis**

Device analysis in RSA Authentication Manager Express silently examines the end user's PC or laptop—dynamically and upon each authentication attempt— by collecting and evaluating dozens of unique device characteristics. Based on this analysis, the RSA Risk Engine can determine if the device is a trusted machine used previously by the account holder. If the machine is trusted, the user is authenticated with a valid password only. If the machine is unrecognized, however, the user is required to provide additional proof of identity. With device analysis, the end user's machine becomes a trusted second factor of authentication without the need to provision static credentials or to deploy any additional software.

### **Behavioral Analysis**

Behavioral analysis evaluates user patterns, authentication and account activity, and other factors to assess the overall risk associated with each authentication attempt. Behavioral risk is calculated by comparing the current authentication request with the user's own authentication history, the known behavior of other users in the population, and behavioral signatures typical of an unauthorized access attempt. If the risk is low, then the user's behavior provides yet another authentication factor that silently confirms the account holder's identity.

The capabilities and components offered in RSA Authentication Manager Express work together to deliver a true multi-factor authentication solution that is optimized for the unique security, convenience, and cost requirements of small and mid-sized organizations. Part of the Authentication family of products from RSA, the leader in authentication solutions, RSA Authentication Manager Express offers organizations the fastest path to multi-factor authentication without compromising on security.



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

©2010 EMC Corporation. All Rights Reserved.  
EMC, EMC, RSA and the RSA logo are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products and services mentioned are trademarks of their respective companies.

AMX\_DS\_1210