# RSA AUTHENTICATION MANAGER

## The strength of SecurID Authentication combined with the convenience and flexibility of Risk-Based Authentication

## AT A GLANCE

**Delivers Flexibility and Convenience by offering Risk-Based Authentication**

- Deploy Risk-Based Authentication alongside hardware and software-based authenticators
- Lower costs and widen the use cases for authentication in your organization

**Lowers Total Cost of Ownership**

- Utilize a suite of built-in features that addresses the most time-consuming and costly tasks associated with managing an enterprise authentication suite
- Allow your IT staff to do more with less

**Maximizes the Potential of Your Virtual Environment**

- Take full advantage of virtualization in your organization to ease deployment, administration, and on-going system management
- Leverage infrastructure and virtualization skills you already have on hand

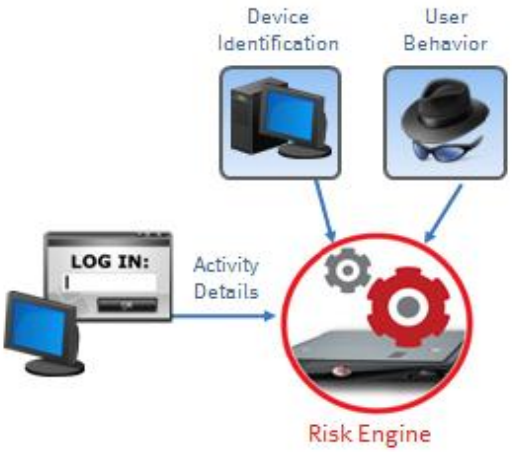
Security is a constantly evolving challenge for organizations that are managing shrinking IT budgets while, at the same time, needing to expand security to a larger population of users. This is compounded by users accessing sensitive data using unmanaged mobile devices via uncontrolled access points such as web portals. Organizations face the challenge of implementing strong authentication to combat these expanding challenges.

RSA® Authentication Manager 8 delivers the world class strength of RSA SecurID® Authentication technology and now also offers a risk engine to meet the challenges and needs of today's organizations. RSA Authentication Manager is designed to verify authentication requests and centrally administer user authentication policies for access to enterprise networks.

Utilizing the widest range of RSA SecurID authenticators, RSA Authentication Manager provides two-factor user authentication to more virtual private networks (VPNs), wireless networks, web applications, business applications and operating environments than any other system available today. The RSA Authentication Manager virtual appliance provides the flexibility to support a wide range of authentication methods, an advanced risk engine, ease of manageability, and interoperability with industry leading products and vendors.

## THE POWER OF RISK-BASED ANALYTICS

RSA Authentication Manager 8 offers Risk-Based Authentication (RBA), which is optionally licensable and designed to transparently increase security. RBA offers end user convenience by preserving the familiar username/password logon experience. Only when a logon attempt is deemed high risk must a user provide additional proof of identity. During a "step-up" authentication challenge, users are able to provide additional proof of identity by either answering life questions or completing an on-demand (SMS) authentication.



## RISK-BASED AUTHENTICATION

RBA is designed to protect access to the most common web-based applications including SSL VPNs, Web Portals, Outlook Web Access (OWA), and Microsoft SharePoint environments. With the addition of RBA into the RSA Authentication Manager portfolio, organizations can now cost-effectively secure access to a wider range of applications than ever before.

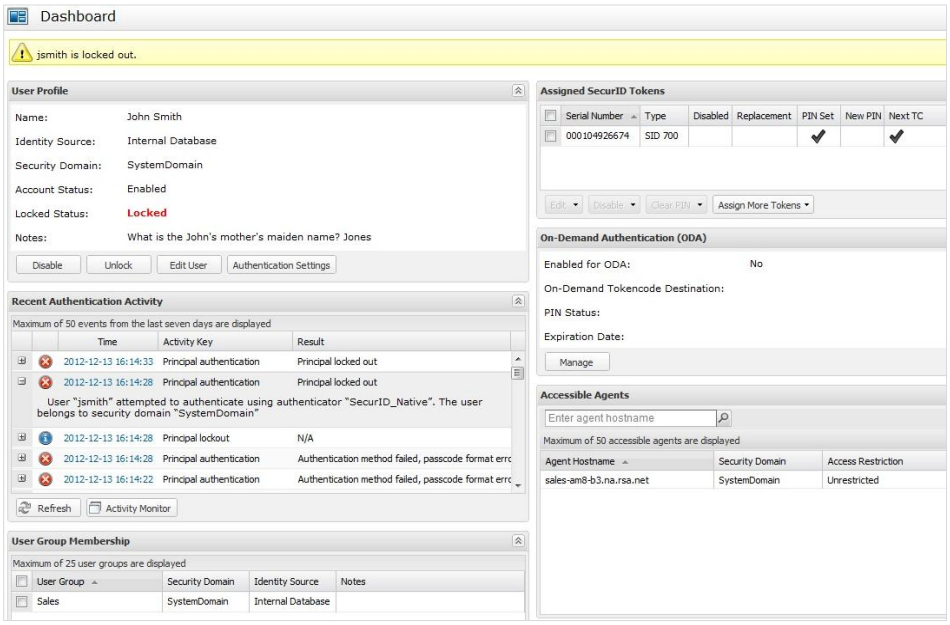
The RSA Risk Engine is a proven technology that powers the most convenient method of strong authentication. Not a static, rules-based system, the risk engine employs a combination of real-time device and behavioral analytics and dynamically adapts its risk model as new information is collected. Low-risk users are authenticated transparently while high-risk users are prompted to provide an additional proof of identity. RBA offers strong authentication that is cost-effective and convenient for both end users and IT administrators.

## MANAGEABILITY

RSA Authentication Manager includes a collection of built-in features that addresses the most time-consuming and costly tasks associated with managing an enterprise authentication suite. The user dashboard is a convenient single-pane view designed to enable Help Desk administrators to quickly address the most common user inquiries without needing to run multiple reports or searches. The customizable Self Service Console is another feature that saves IT staff time by empowering users to manage their authentication methods. Deployed in the DMZ area of the network, the self-service portal allows users to change their own PIN, request a replacement token, request emergency access, and access other troubleshooting services.

## USER DASHBOARD

- Address the most common user inquiries in a single-pane view
- Monitor real-time recent authentication activity
- Manage tokens
  - Enable/disable
  - Assign more tokens
  - Unlock/lock
  - Clear PIN
- View user group membership and accessible agents




## FLEXIBILITY

RSA Authentication Manager is designed to deliver choice and flexibility including a range of authenticators: hardware tokens, software tokens, on-demand authentication and Risk-Based Authentication. An organization can mix and match their preferred type of authenticators and easily provision and manage users on a single console.

Choice and flexibility extends to deployment options. RSA Authentication Manager is offered on a hardware appliance and a virtual appliance. The virtual appliance allows organizations to take full advantage of VMware ESX or ESXi virtualization, which dramatically simplifies deployment. There are a number of reasons why an organization may prefer a hardware or virtual appliance deployment. RSA Authentication Manager is designed to support a wide range of options even including a combination of virtual and physical appliances.

## INTEROPERABILITY

RSA Authentication Manager is interoperable with many of the major network infrastructure and operating system products on the market. The Secured by RSA program, one of the largest alliance programs of its type, brings together hundreds of complementary solutions. Including more than 400 products from over 200 vendors, Secured by RSA helps assure that organizations have maximum flexibility and investment protection. Leading vendors of remote access products, VPNs, firewalls, wireless network devices, web servers, and business applications have built in support for RSA Authentication Manager.

## CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.emc.com/rsa.