RSA AUTHENTICATION MANAGER 8

Core Messaging

KEY MESSAGES

Lowers Total Cost of Ownership

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

Delivers Flexibility and Convenience of a New, Risk-Based Authentication Method

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

Maximizes the Potential of Your Virtual Environment

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

Prepares for Advanced Threats Today

- An advanced risk engine can protect against advanced threats

INTRODUCTION

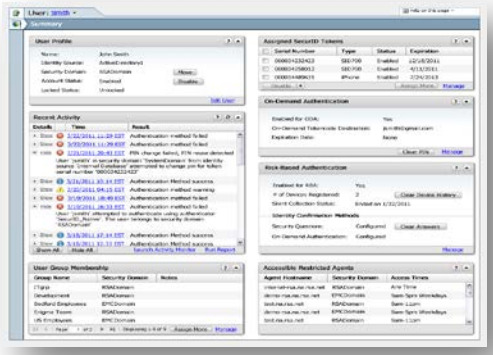
RSA® Authentication Manager 8 is the next major release of the RSA SecurID® platform, encompassing a range of new features - 40 in all - that lowers the total cost of ownership, delivers flexibility and convenience of a new risk-based authentication method, maximizes the potential of your virtual environment, and prepares for advanced threats that many organizations are facing today.

A RELEASE BUILT AROUND CUSTOMER REQUIREMENTS

From the outset, the goal of the release was to enhance the capability of the award-winning RSA Authentication Manager platform's to continue to deliver superior enterprise class performance to over 25,000 organizations worldwide. To do this, we listened to customers, and developed this release to address the key issues our customers are facing.

LOWERS TOTAL COST OF OWNERSHIP (TCO)

RSA Authentication Manager 8.0 includes a collection of built-in features that address the most time-consuming and costly tasks around managing an enterprise authentication suite.



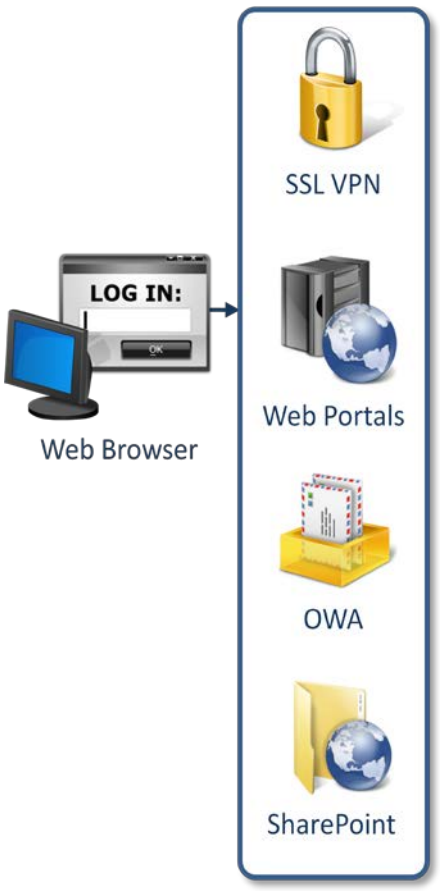
BENEFITS INCLUDE:

- Dramatically lowers time-to-resolution (TTR) for RSA SecurID-related help desk calls with a new User Dashboard that provides a convenient single-pane view for help desk administrators
- Saves time for you and your IT staff by allowing end users to manage the full lifecycle of their authenticator via a customizable, DMZ-deployable self-service console
- Enables rapid deployment of RSA SecurID software authenticators with configurable mobile platform profiles
- Reduces system management time with features such as consolidated system settings that provide a central location to set all the system features; critical system notifications that alert you when something is wrong; an import/export utility that allows you to move users/tokens between 8.0 deployments; and scheduled backup that ensures the continuity of business operations

PROOF POINTS FOR LOWERING TOTAL COST OF OWNERSHIP

- Reduces time-to-resolution (TTR) of help desk calls from an average of 8-10 minutes down to an industry-leading 1-2 minutes; up to 80% reduction in TTR
- Lowers time to deploy software authenticators from 1-2 minutes each, down to seconds for each user
- Decreases system time from 60-90 minutes down to 20 minutes
- Shrinks volume of help desk calls by 30-40% when using the Self Service console
- 50% improvement in serviceability with patch management that delivers only the delta changes

DELIVERS THE FLEXIBILITY AND CONVENIENCE OF RISK-BASED AUTHENTICATION



In addition to deploying RSA SecurID hardware and software authenticators, RSA Authentication Manager 8 now provides the option of deploying a new Risk-Based Authentication (RBA) method to protect web-based assets.

BENEFITS INCLUDE:

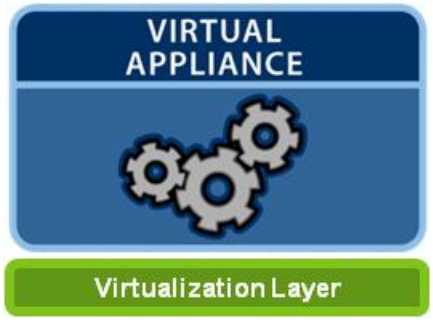
- Lowers the per user cost of authentication in your organization
- Expands use cases to cover applications and users (such as temporary employees, partners, contractors) that were previously viewed as too cost-prohibitive to cover with traditional strong authentication
- Increases security transparently without compromising user convenience. Delivers the ultimate convenience for end-users by preserving their logon experience of username/password
- Saves IT staff time by deploying and managing all authentication methods on a single console
- Offers a choice of using RBA or SMS in a single authentication method

PROOF POINTS FOR RISK-BASED AUTHENTICATION:

- Lowers authentication cost per user versus traditional hardware authenticators by up to 40%
- Covers the most popular web-based applications, including SSL-VPNs, Web Portals, Outlook Web Access (OWA), and Microsoft Sharepoint environments
- Utilizes the proven technology that delivers the power of risk based authentication currently in use for 350 million users
- Enables rapid deployment to hundreds or even thousands of users in a very short period of time (days not weeks).

MAXIMIZES THE POTENTIAL OF YOUR VIRTUAL ENVIRONMENT

Take full advantage of VMware ESX and ESXi virtualization in your organization to simplify deployment, administration, and on-going system management of RSA Authentication Manager 8.0. The platform is being released as a VMware Virtual Appliance.



BENEFITS INCLUDE:

- Saves time deploying and managing your authentication platform
- Maintain control of your deployment. Don't have a virtual environment? Stand up your own server and deploy VMware ESXi (freeware version) so you can maintain full control of your deployment. Or deploy in a clustered configuration to take advantage of the full range of virtualization tools.
- Saves time, infrastructure resources, and datacenter resources by using the full suite of VMware tools, including snapshots, VMotion, High Availability and more.
- Leverages infrastructure and virtualization skills you already have in your workplace

PROOF POINTS FOR THE VIRTUAL APPLIANCE:

- Certified VMWare® Ready Virtual Appliance
- Lightning fast deployment times…an industry leading 20 minutes from start to finish.
- Enjoy smaller, non-dedicated server resources
- Simplified patching enables quick updating.. All updates to the Virtual Appliance, underlying operating system, and RSA Authentication Manager are provided in single service pack or hot fix on a regular cadence, so you don't need to worry about managing various layers of the system individually.

PREPARES FOR ADVANCED THREATS TODAY

Deploy your authentication solution with a proven risk engine to protect against advanced threats. As threats evolve, the risk engine will similarly adapt (through RSA updates) to provide the highest level of multi-factor risk-based authentication available in the market.

BENEFITS OF PREPARING FOR ADVANCED THREATS TODAY:

- Protects your organization now and in the future
- Permits setting policies based on risk. Class different groups of users around policies that fit the goals and security policies of the organization. Internal users on company-owned devices coming in over the VPN are allowed more leeway than, for example, contractors coming in over a web portal using their own devices
- Provides true multi-factor authentication. Utilizes both Device and Behavioral characteristics, in addition to step-up authentication methods to give a high level of assurance that users are who they say they are.

PROOF POINTS

- Sophisticated self-learning Bayesian risk engine seeks out patterns of anomalous activity
- Over 90% of users will not be challenged, but a few select will receive a step-up authentication
- Proven 10 year market-tested technology
- Delivers the ultimate convenience: users only enter their username and password

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 http://www.emc.com/security/rsa-securid.htm

RSA AUTHENTICATION MANAGER 8 - COMING 1H 2013

http://www.emc.com/security/rsa-securid.htm