RSA SECURID®

Risk-Based Authentication

AT A GLANCE

- Delivers proven multi-factor authentication technology to a wide range of web-based applications.
- Enables authentication based on transparent analysis of end user device and behavior.
- Offers convenient username and password login experience
- Mix and match hardware tokens, software tokens, and Risk-Based Authentication to support varying end user needs

Today's organizations are faced with the challenges of an evolving IT environment – users are diverse and remote, IT budgets are limited, and threats are advancing. As organizations move more information online and provide remote access to end users, strong authentication is a crucial component in the security strategy. While ensuring your key assets are protected, it is also important to consider the end user convenience of IT policies to increase the return on investment.

INTELLIGENCE-DRIVEN AUTHENTICATION

In addition to software and hardware-based tokens, RSA offers risk-based authentication for users would prefer a tokenless authentication experience. RSA SecurID® risk-based authentication offers the traditional user name and password login experience, but with the increased security benefits of a multi-factor authentication solution. Behind the user name and password login is the RSA Risk Engine. The Risk Engine evaluates each attempted login and activity in real-time by tracking hundreds of risk indicators and determines the risk associated with each request by looking at three key factors:

- Something the user knows, such as an existing user name and password
- Something the user has, such as a laptop or mobile device
- Something the user does, such as recent account activity

The risk engine scores each authentication request using knowledge about the client device and by analyzing end user behavior.

RISK ENGINE

The RSA Risk Engine used in the RSA SecurID Risk-Based Authentication solution is an adapted version of the Risk Engine used in the RSA Adaptive Authentication solution, but optimized for the enterprise rather than the consumer. The RSA Risk Engine protects millions of users by dynamically adapting the risk model based on newly collected device characteristics and behavioral information – in real time.

Device Profiling

By collecting and evaluating dozens of unique device characteristics, the RSA Risk Engine silently examines the end user's PC, laptop, or mobile device – dynamically and upon each authentication attempt. Based on this analysis, the RSA Risk Engine can determine if the user is authenticating from a trusted device. If the device is trusted, the user can typically be authenticated with a user name and password only; if the machine is unrecognized, the user will be required to provide additional proof of identity through "step-up" authentication.

Behavior Profiling

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 end user's 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 activity.

PRODUCT SPECIFICATIONS

- Supports a minimum of 5 and maximum of 50,000 users.
- Available as a perpetual license with annual maintenance required (separate from RSA SecurCare Maintenance)
- Available with the Base and Enterprise editions of RSA Authentication Manager.
- Risk-Based and On-Demand Authentication are supported on a single license.

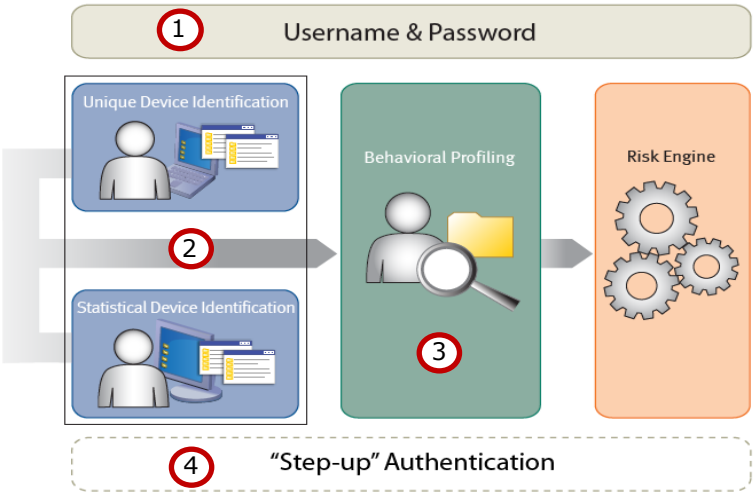
PLATFORM REQUIREMENTS:

- RSA Authentication Manager 8.x and higher.

Identity Confirmation

Low-risk users are authenticated transparently while high-risk users may be prompted to provide additional proof of identity through step-up authentication. Step-up authentication options include On-Demand Authentication and Challenge Questions.

- On-Demand Authentication: The user must correctly enter a one-time passcode that is sent out-of-band to a pre-defined mobile number via SMS (text) or email.
- Challenge Questions: The user must correctly answer one or more pre-enrolled security questions.



1st Factor: Something you **KNOW**

2nd Factor: Something you **HAVE**

3rd Factor: Something you **DO**

Step-Up: Something you **KNOW OR HAVE**

MIX AND MATCH AUTHENTICATION METHODS

RSA Risk-Based Authentication can be used as a standalone multi-factor authentication solution, or it can be used with RSA SecurID hardware and software tokens. Different types of users have different needs – mix and match your RSA SecurID authentication methods to support each type of end user, while managing your entire RSA SecurID environment from one management console.

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.

RSA