ADAPTIVE AUTHENTICATION ADAPTER FOR CA SITEMINDER®

Adaptive Authentication in CA SiteMinder Environments

Solution Brief

RSA®

EMC²®

RSA® Adaptive Authentication is a comprehensive authentication platform providing costeffective protection for large user bases. Adaptive Authentication is powered by Risk-Based Authentication, a risk assessment and authentication technology that operates transparently and classifies all users by measuring a series of risk indicators. This transparent authentication for the majority of users provides for a convenient online experience as users are only challenged when suspicious activities are identified and/or an organizational policy is violated. The strong authentication functionality of RSA Adaptive Authentication is offered to CA SiteMinder® environments through the RSA Adaptive Authentication Adapter, which enables integration of RSA's risk-based authentication technology with CA SiteMinder's user name and password verification system.

As the usage of online portals, SSL VPN applications, and web access management products continue to grow, so does the need for strong authentication to protect against unauthorized access to the information contained within them.

Providing single-factor authentication, or password only protection, creates a significant security threat to organizations. Single-factor authentication is easily defeated by hackers and can result in a security breach, financial loss, or loss of sensitive data such as personally identifiable information. Concurrently, many IT departments are grappling with business requirements to extend access to enterprise applications to an even broader audience – including vendors, suppliers, partners and customers.

Whether driven by compliance or the need to effectively manage information risk, organizations are faced with the challenge of providing strong multi-factor authentication to secure their assets and information while balancing cost and end user convenience.

The Right Choice for Authentication

A recent survey by RSA shows that on average, only 20-40% of the typical enterprise workforce is issued hardware or software tokens. The main reason for low deployment rates is often attributed to the acquisition cost and ongoing management of rolling out physical authenticators to every single user. As a result, organizations are considering new methods of authentication that will enable them to extend strong authentication to a broader user base and provide an additional layer of security without impacting the user experience. RSA® Adaptive Authentication is becoming a likely choice for authentication in multiple industries for protecting access to portals, VPNs and other enterprise applications.

A variety of authentication methods exist that can be used on top of the Adaptive Authentication platform including:

- **Invisible authentication.** Device identification and behavioral profiling
- **Out-of-band authentication.** Phone call, SMS and e-mail
- **Challenge questions.** Challenge questions or knowledge-based authentication

The ability to support most existing authentication technologies helps organizations that use Adaptive Authentication to be flexible in:

- How strongly they authenticate end users
- How they distinguish between new and existing end users
- What areas of the business to protect with strong authentication
- How to comply with changing regulations
- What risk levels they are willing to accept
- How to comply with the various requirements of the regions and countries where they operate

The Dynamics of Risk-based Authentication

RSA Risk-based Authentication is powered by a series of core technologies – device profiling, behavioral profiling, the RSA® Risk Engine, the RSA® eFraudNetwork™ service, the RSA® Policy Manager and the RSA® Multi-credential Framework.

Device Profiling

Profiling enables Adaptive Authentication to assure the identities of the vast majority of users transparently by comparing the profile of a given activity with their typical profile patterns. Device profiling analyzes the device profile (the physical laptop/PC from which the user accesses the website or application) and determines if the device is known as having been previously used by this user. The two main components of device profiling are unique device identification and statistical device identification.

Unique device identification distinguishes a device through the use of two main elements embedded on the user's laptop/PC – secure first party cookies and flash shared objects (sometimes referred to as "flash cookies"). Statistical device identification is a technology that analyzes the characteristics of a device to statistically identify a users' device.

Behavioral Profiling

Risk-Based Authentication also uses behavioral analysis to identify high-risk authentication attempts. Some parameters that are measured include velocity checking, IP address information, and time of day comparisons. Behavioral profiling analysis complements device profiling with user behavior to offer a form of multi-factor authentication that includes something you have (the device) and something you do (behavior).

RSA® Risk Engine

The RSA Risk Engine is a proven, self-learning technology that evaluates each online activity in realtime, tracking over one hundred indicators in order to detect suspicious activity. A unique risk score, between 0 and 1000, is generated for each activity. The higher the risk score, the greater the likelihood is that an activity is suspicious.

RSA® Policy Manager

The RSA Policy Manager enables organizations to instantly react to emerging, localized cybercrime patterns and effectively investigate activities flagged as high-risk. The Policy Manager translates organizational risk policy into decisions and actions through the use of a web-based Rules Management application, comprehensive rules framework, real-time configuration, and Performance Simulator for testing prior to being put into production.

RSA® eFraudNetwork™ Service

The RSA eFraudNetwork service is a crossorganization, cross-industry repository of cybercrime data gleaned from RSA's worldwide network of customers, end users, ISPs, Anti-Fraud Command Center (AFCC) and third party contributors. The eFraudNetwork community is dedicated to anonymously sharing and disseminating information on cybercrime activities. When suspicious activity is identified, the associated data, activity profile and device fingerprints are shared into the centralized data repository from which organizations that are active network members receive updates on a regular basis. This ongoing series of updates enables realtime proactive protection to hundreds of millions of online users worldwide and is one of the many sources that feeds the RSA Risk Engine in determining risk. The eFraudNetwork has been a valuable resource in identifying cybercrime activity and information associated with cybercriminal infrastructure used for both financial and non-financial attacks.

RSA has one of the world's largest security software-as-a-service (SaaS) practices, with more than 3,700 organizations relying on RSA Hosted Operations

RSA® Multi-credential Framework

The RSA Multi-credential Framework provides an abstraction layer that enables one software platform to support multiple authentication methods (based on end user segment and risk assessment) in a single deployment. With the Multi-credential Framework, different authentication methods are leveraged through policy settings to accommodate different end user populations, different online products and different risk levels.

Multiple Configuration Options

Adaptive Authentication can be configured in a number of ways to balance security and risk without compromising the user experience. Many organizations currently provide risk-based authentication for their entire user base and allow the RSA Risk Engine to determine those individuals that require additional protection. Other organizations choose an appropriate supplemental form factor based on a user's preference or the types of activities they conduct.

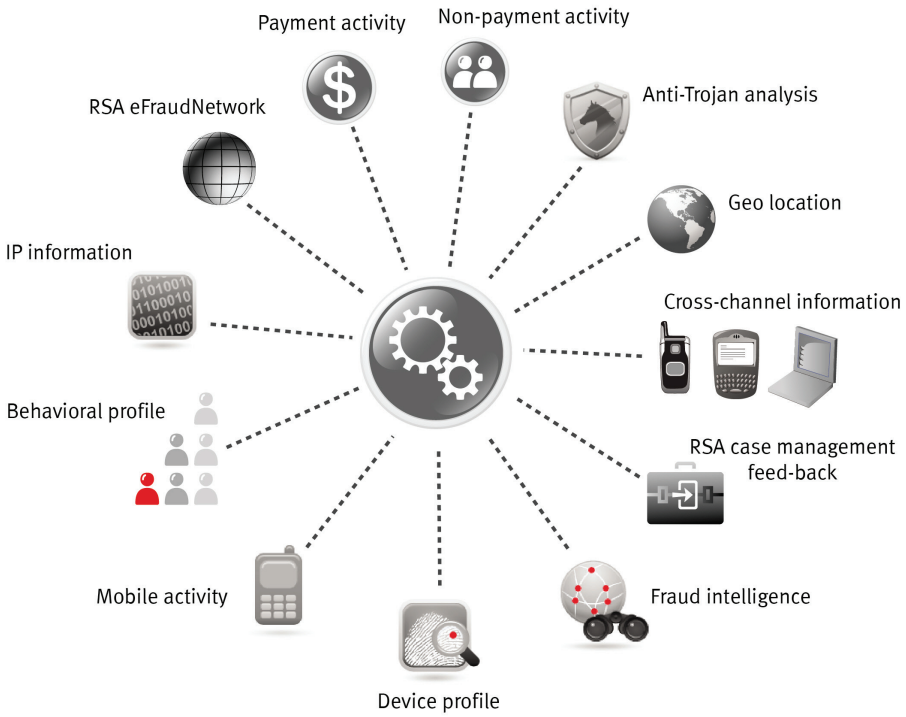
The RSA Risk Engine measures over one hundred indicators and assigns a unique risk score to each activity. RSA has one of the world's largest security software-as-a-service (SaaS) practices, with more than 3,700 organizations relying on RSA Hosted Operations.

On-premise or SaaS / Hosted Deployment Options

Organizations worldwide currently deploy Adaptive Authentication in two ways – as an on-premise installation that uses existing IT infrastructure or as a hosted authentication service that helps to manage the end user lifecycle. Recognizing that no two organizations share the exact same user authentication needs, RSA offers the widest possible range of authentication, deployment and customization options.

RSA has one of the world's largest security software-as-a-service (SaaS) practices, with more than 3,700 organizations relying on RSA Hosted Operations for a variety of products that offer this delivery model. RSA Hosted Operations has been providing SaaS products for more than seven years in the areas of card authentication, web authentication and identity verification.

The RSA Risk Engine measures over one hundred indicators and assigns a unique risk score to each activity.



RSA Adaptive Authentication Adapter for CA SiteMinder

Built into RSA Adaptive Authentication, the RSA Adaptive Authentication Adapter eliminates the need for custom integration, thereby significantly shortening and simplifying deployments; the configuration is performed via a configuration wizard.

The Adapter is compatible with both Adaptive Authentication on-premise and Adaptive Authentication SaaS/hosted. The Adaptive Authentication Adapter can be deployed as is or it can be branded and further customized using the configuration wizard or JSP pages. For example, a company logo or a different look-and-feel can be added to the authentication pages for unique branding.

An RSA Adaptive Authentication deployment in a SiteMinder environment includes the following components. Note that this integration requires a SiteMinder WAM system.

– **Custom Authentication Scheme** uses HTML formsbased authentication and utilizes the HTTP redirection capabilities of the SiteMinder web agent to direct users who pass first level authentication to a custom “challenge” page which will perform second level authentication.

– **Adaptive Authentication Adapter** gathers device forensics and fingerprint information from the client browser, sends the information to the Adaptive Authentication Server and returns the device token Network Architecture for Adaptive Authentication:

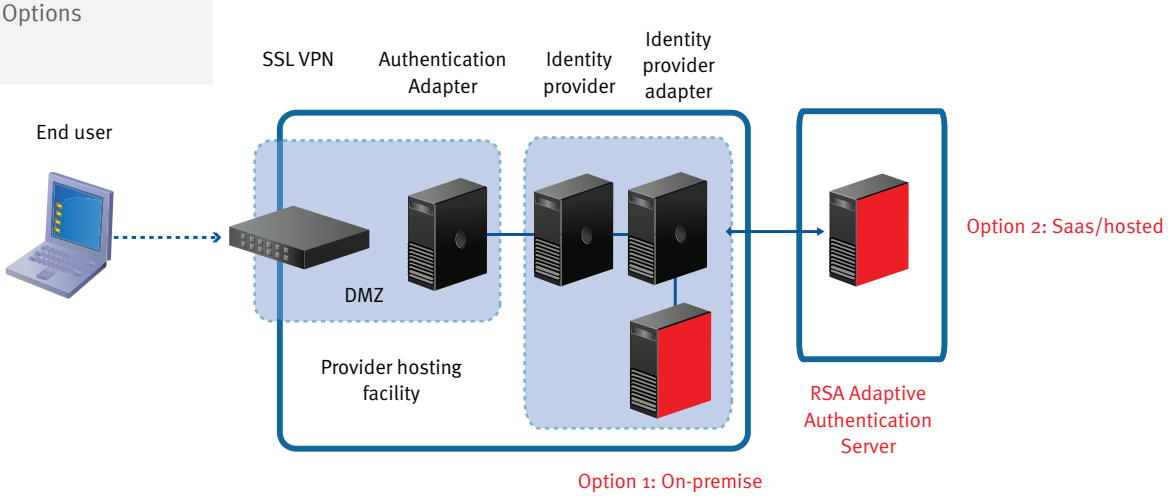
– **SiteMinder Adapter** provides the connection between the SiteMinder web agent and the Adaptive Authentication Adapter by creating the custom challenge page used by the custom authentication scheme.

– **Data Protection Server** is a web component that stores given data, returning a unique key, and retrieves previously stored data, using the provided key. The data is deleted immediately upon retrieval. The unused data objects will expire after a short period.

– **Adaptive Authentication Server** provides a web services (SOAP) interface performing invisible authentication of users attempting to access the protected application. After the invisible authentication is completed, the protected application gets a message, which allows the user to continue or prompts the user for additional authentication. In addition, the Adaptive Authentication server provides interfaces for initial enrollment of users into the system and administrative APIs allowing system administrators to manage user accounts and configure the system.

– **Adaptive Authentication Database** is a relational database used by the Adaptive Authentication server to store information, including user records, forensic snapshot information about end user machines, records of user actions and other metadata required for proper operation.

Network Architecture for Adaptive Authentication: Two Options



Use Case Scenarios

The following use cases illustrates the functionality of the Adaptive Authentication Adapter and its impact on an end user.

Use case 1 demonstrates how a legitimate user signs into the system. After a seamless process in which the user is successfully authenticated by RSA Adaptive Authentication, the user gets access to the system.

Use case 2 illustrates step-up authentication – the user signs in from an unrecognized device or receives a high risk score during the authentication process. The user is challenged by one of the challenge methods, as described below (challenge questions or out-of-band phone). Note that the order and availability of authentication options can be changed via user configuration according to organizational policies. For example, it is possible to use challenge questions and if the user fails the questions, then challenge via Out-of-band phone authentication.

Challenge Questions

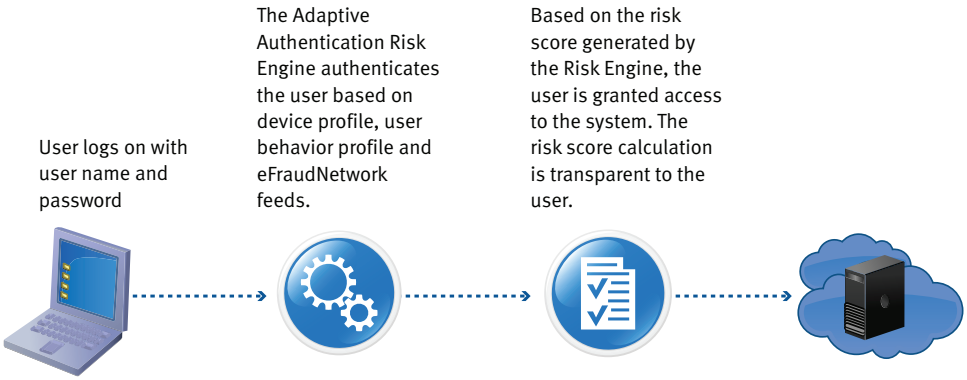
Sometimes referred to as "secret questions," challenge questions are an easy-to-use method to authenticate users, balancing security with convenience. They are a set of questions that are typically asked of a user during the enrollment process or a new account opening to obtain information on the individual. The questions are presented to a user at a later time and the information originally provided is used for verifying identity. The challenge questions method offers a large pool of questions that have been carefully selected through a combination of research, field tests and focus groups.

It provides a full framework for obtaining the answers from the user during the enrollment phase. To provide the utmost security, this method treats the questions themselves as "shared secrets," in addition to the commonly used practice of treating the answers as secrets, thereby providing an additional level of security. The challenge question authentication method randomly selects a configurable subset of questions from a very large pool of questions and presents them to a user. This prevents any single user or potential cybercriminal from seeing the entire set of possible questions and it prevents cybercriminals from determining which challenge questions were collected from each user and then attempting to "phish" this information.

Out-of-band phone Authentication

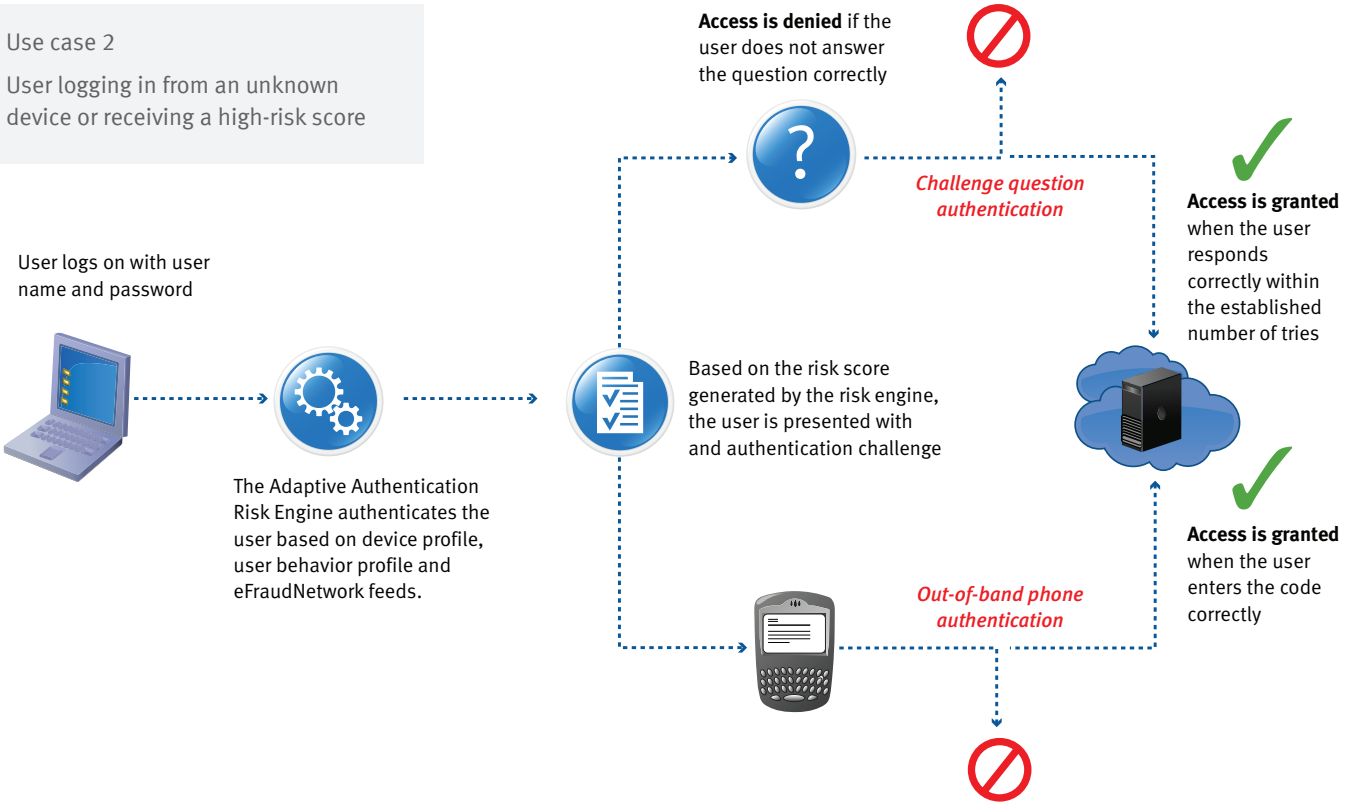
Use case 1

User logging in from a recognized device or receiving a low-risk score



Use case 2

User logging in from an unknown device or receiving a high-risk score



This provides powerful protection from Trojans, manin-the-middle attacks and other threats. Out-of-band (OOB) communication methods are a powerful authentication weapon because they circumvent the communication channel(s) that cybercriminals typically use. Out-of-band phone authentication provides many obvious benefits. It meets the demands by customers for a solution that is easy to use and understand. In addition, OOB phone authentication does not require users to buy new hardware or software and simply relies on any ordinary analog, VOIP or mobile telephone. The worldwide availability of the telephone also meets the organizational need for a global authentication solution.

Out-of-band phone authentication occurs when an activity is identified by the RSA Risk Engine to be highrisk or suspicious or when an institutional policy triggers it (e.g.,"Challenge all activities originating in Country X or Country Y."). In both scenarios, Adaptive Authentication challenges the user to reconfirm that they are who they claim to be. First, the system will ask the user to select one of the phone numbers (previously entered during enrollment) at which to receive a phone call. Next, the system generates an automated call informing the user of the activity details and prompting them to enter the confirmation number displayed on the web browser into the keypad on the mobile device or landline telephone. Once the number is entered correctly into the device/ phone, the online activity continues without disruption.

Prerequisites

CA SITEMINDER SYSTEM	
ADAPTIVE AUTHENTICATION SERVER – ON-PREMISE (V6 0.2.1 SP1) OR SAAS/HOSTED	
CA SITEMINDER PRODUCT SUPPORT	– SiteMinder V6 SP5
SERVER-SIDE REQUIREMENTS	Servlet container that supports: – Servlet specification 2.4 – JSP specification 2.0 – Java 5 JRE or JDK, depending on the servlet container

About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safe-guarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.
Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

AACA SB 0812