



The Security Division of EMC

Technical Brief

RSA® Authentication Manager 7.1



RSA® Authentication Manager 7.1 is the latest release of RSA's flagship two-factor authentication solution, available worldwide on select software platforms. This release delivers a new set of functionality as well as positions the platform for new uses and applications.

Three Core Enhancement Areas

Business Continuity Option

The RSA value proposition has moved beyond just that of being the "token company" to becoming a strategic information risk management solution to our customers. The Business Continuity Option, added in 7.1, answers the question, "How could I prevent lowering my security policy if I had to send all my employees to work from home during a business disruption?"

Extended Authentication Methods

The new release further expands the types of authenticators that can be deployed to users and centrally managed at the server.

Enhanced Operational Efficiencies

Customers can expect a suite of tools that will increase operational efficiencies, streamline deployments and lower overall on-going management costs.

Highlights

Enhanced Operational Efficiencies

RSA Authentication Manager 7.1 includes a suite of requested features that make the solution easier to manage, lowers total cost of ownership and leverages existing IT resources.

Native LDAP Support. The release delivers true native LDAP support for direct integration with Sun One™ and Active Directory®. No more synchronization. Multiple identity sources can serve as the data stores. Native LDAP requires no change to the database schema.

Web-based Management. The new administration interface is browser-based and is zero-footprint, meaning that no client software is required to be installed on the admin PC. RSA Authentication Manager 7.1 can be remotely administered from any PC with a browser and Internet connection.

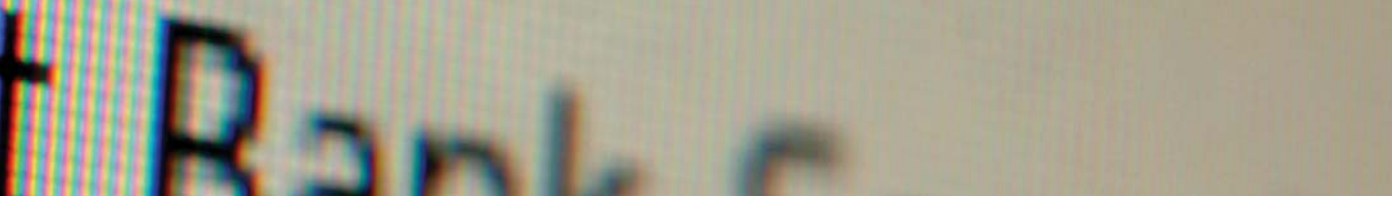
Delegated Multi-level Administration. This enables granular administrative access control down to a user/group and policy level. It maximizes administration resource investment and delivers increased security by ensuring that fewer individuals hold the "keys to the kingdom."

Microsoft® Management Console (MMC) Snap-in. For customers already using MMC as their primary management utility, this plug-in provides consistency and added ease of use. Through MMC, admins can perform a variety of basic user and token management tasks, such as assigning or disabling a token to a user.

RADIUS Server. The 802.1x RADIUS Server that disappeared in 7.0 has been brought back in 7.1. Having the RADIUS server included lowers costs compared to implementing a third-party solution, and it is fully embedded into the management console so that setup and on-going management is made easy.

RSA® Credential Manager. The replacement for RSA® Deployment Manager (Web Express), RSA Credential Manager is tightly coupled with the management interface of Authentication Manager, requires no separate install and delivers a range of functionality beyond what Deployment Manager produced. These are:

- **Self Service.** A configurable self-service console is available for end users to request a variety of services, including issuing On-demand token codes for emergency access. The Self Service module can dramatically reduce the call volume into the IT help desk because users are empowered to manage all aspects of their token lifecycles.
- **Workflow Provisioning.** Admins can create processes by which requestors are approved and credentials are issued (available with Enterprise Server License).



Extended Authentication Methods

Along with support for the traditional credentials from previous releases, RSA Authentication Manager 7.1 introduces new end-user authenticators that create opportunities for flexible deployments and lower management costs. All of these methods continue to be centrally managed and supported from the administration console.

On-demand Authenticator. The RSA SecurID® On-demand Authenticator is a new credential method available with the release of 7.1. It delivers token codes to users via short message service (SMS) or e-mail, and requires no physical token to be assigned or software to be installed on a laptop or smart phone. On-demand Authenticators do not have expiration dates.

Dynamic Seed Provisioning (CT-KIP). Cryptographic token key initiation protocol is a client-server protocol that enables more rapid setup of software tokens. Using CT-KIP, both the client and the server can generate a unique identifier – a seed file – that can then be used to authenticate the user to the server. No seed file needs to be sent over the network to the remote user. This can make the deployment of software tokens smoother and shorten deployment times.

Built-in Management Support for Global Messaging Vendor Clickatell™. To send out large numbers of SMS messages to users, a relationship with an SMS aggregator must be established so messages can be routed to a carrier gateway. RSA has built into the management console an interface to use with Clickatell, a worldwide mobile messaging company with access to over 600 networks in almost 200 countries.

Business Continuity Option

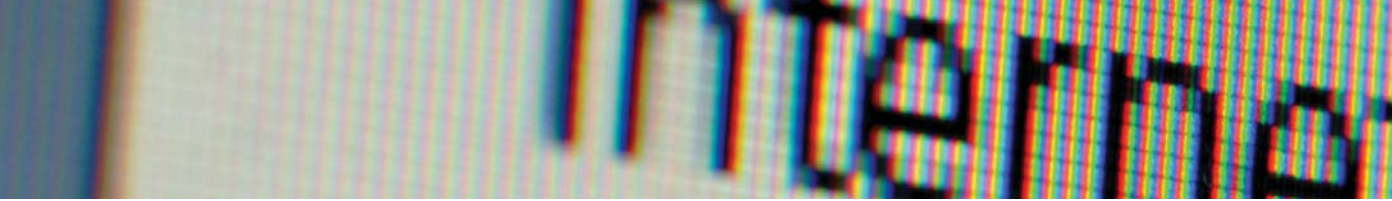
With the release of 7.1., the new Business Continuity Option makes it even easier to leverage SecurID authentication into organizational planning for an unanticipated business disruption.

The Business Continuity Option licensing feature allows a customer to temporarily expand a server license for a period of time to meet the in-flux of large numbers of remote access users, e.g., during a business disruption when employees must work from home. The new licensing feature can be invoked up to six times every license term for a time frame of 60 days each time. BCO license terms are for 3 years.

The Business Continuity Option expands the server license and enables a pre-defined number of RSA SecurID On-demand Authenticators to be used. Example, a customer purchases a 1,000 seat BCO license; when the BCO option is invoked, an additional 1,000 seats of On-demand Authenticators instantly become available to utilize. Deployment is done on the fly with the Self Service module found in RSA Credential Manager (included) so that users can on-board themselves without overwhelming the IT help desk with requests.

Opening New Doors for Applications

Taken together, these applications and features present a new way for RSA Authentication Manager to be managed and deployed. For example, the inclusion of On-demand Authenticators, coupled with end-user self service tools, opens up the possibility that a greater population of the user base can be served. A few examples follow.



Supporting a Base of Contractors and Vendors. Many organizations struggle with how to support temporary employees, contractors and visiting business partners who require access to network resources. Issuing On-demand Authenticators via the Self Service module can be a great way temporarily deploy credentials without having to provision hardware or software tokens. A workflow can even be written specifically to accommodate each of these user categories with business line approvers on the back end for added security.

Result: Faster on-boarding of contractors/vendors, lower deployment costs, minimized loss from unrecoverable tokens.

Supporting a Base of Occasional Users. Many employees do not travel or work enough remotely to justify having a traditional token. However, when it does happen, there needs to be rapid, self-initiating process in place to support these users. The new features of Authentication Manager 7.1 seamlessly handle this situation.

Result: Two-factor authentication policy is enforced, an established process is in place to support any user.

Self-Service Support for Existing "Power Users". A business traveler forgets his token at home. Another needs a PIN reset. Still another wants to test or resynchronize her hardware token. Normally these requests would result in a call into the IT help desk, but in 7.1 the RSA Credential Manager empowers users to take control of the available tools and perform these tasks on their own.

Result: Productivity savings for the end-user and productivity and cost savings at the IT help desk.

Business Continuity Planning. Many organizations are challenged with how to implement a pandemic or disaster recovery plan that calls for the entire work force to access the network remotely, while not lowering the security policy to accommodate those users who have not been issued tokens. The new Business Continuity Option provides an answer to this issue.

Result: Security policy remains in force even during a business disruption.

Availability and Platform Support

RSA Authentication Manager 7.1 is scheduled for general availability in Q2 2008. It will initially be made available on the following software platforms: Windows®, Red Hat™ Linux and Sun Solaris™. Other platform support, including that for the RSA SecurID Appliance, will follow in the next release.

RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2008 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Windows and Microsoft are registered trademarks or trademarks of the Microsoft Corporation in the U.S. and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

AS71 SB 0108