RSA SECURID[®] Management Console

AT A GLANCE

- Centralized Management of the entire RSA SecurID environment
- Supports a variety of authentication methods through a single management console
- Integrates with 400+ industry leading partner solutions out of the box
- Offered as a virtual or hardware appliance – or you can mix and match within the same deployment

USER DASHBOARD

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

RSA AUTHENTICATION MANAGER

Whether you choose to deploy hardware tokens, software tokens, risk-based authentication, on-demand (SMS) – or a combination of all of these authentication methods – the RSA Authentication Manager is the central management console behind the RSA SecurID solution.

Centralized Management

The RSA Authentication Manager software allows RSA SecurID administrators to centrally manage user profiles, authentication methods, as well as applications and agents across multiple physical sites. The RSA Authentication Manager software verifies the user's identity for authentication requests and centrally administers authentication policies for the organizations' end users. Whether you choose one authentication method, or choose to mix and match authentication methods to meet varying end user needs, the RSA SecurID environment can be managed from one management console. The console is designed to address the most time-consuming and costly tasks associated with managing an enterprise authentication solution – even end users benefit from the self-service console. Users can change their own PIN codes, request a replacement token, request emergency access, and troubleshoot without ever contacting the helpdesk directly.

1	jsmith is locked	l out.														
User Profile							Ass	Assigned SecurID Tokens								
Na	ne: John Smith						0	Ser	ial Number 🔺	Туре	Disabled	Replacement	PIN Set	New PIN	Next TC	
Ide	lentity Source: Internal Database					1	000	101926671	SID 700			1		1		
Se	curity Domain:	Syste	mDomain													
Act	count Status:	Enabl	ed													
	ocked Status: Locked							at .	Dispble -		· · As	sign More Token:	s •			
	Notes: What is the John's mother's maiden name? Jones						00	On-Demand Authentication (ODA)								
i i i										deadon (c	JUN)					
	Disable Unlock		Edit User	Authentication Settings			En	abled	for ODA:			No				
Der	Recent Authentication Activity							On-Demand Tokencode Destination: PIN Status:								
Maximum of 50 events from the last seven days are displayed																
	Tim		Activity Key		esult		Ex	Expiration Date:								
	2012-12-13	012-12-13 16:14:33 Principal authentication Principal locked out		locked out		Manage										
3	2012-12-13 16:14:28 Principal authentication			entication P	Principal locked out											
	User "jamith" attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "SystemDomain"					or "SecurID_Native". The user		Accessible Agents								
								Enter agent hostname								
	-	2012-12-13 16:14:28 Principal lockout N/A 2012-12-13 16:14:28 Principal authentication Authentication method failed, passcode format errc							n of 50 access	ble agents						
	-		- 1						ostname 🔺			curity Domain		cess Restric	ction	
Ŧ	2012-12-13	16:14:22	Principal authe	entication A	uthenti	cation method failed, passcode format erro	sa	es-am	18-b3.na.rsa.i	net	S)	stemDomain	Un	restricted		
2	Refresh 🗍 A	ctivity Mor	nitor													
lise	Jser Group Membership															
	imum of 25 user ara		nlaved													
	User Group *	opo di e ui	Security Dom	ain Identity Sou	urce	Notes										
m	Sales		SystemDoma	in Internal Dat	tabase											

Risk Engine

The RSA Risk Engine in built-in to the RSA Authentication Manager to enable Risk-Based Authentication. The Risk Engine is a proven technology that powers the most convenient method of authentication that maintains the traditional username and password login experience, while calculating risk level for the transaction.

RSΛ

Interoperability

Leverage the 400+ fully supported technology integrations offered with the RSA Ready Partner Program, free of charge. RSA Ready technology integrations are available for wide range of applications, free of charge. The RSA SecurID technology integrations are jointly tested by both organizations and documented to ensure a positive customer experience. RSA offers interoperability with 400+ products from over 200 certified partners.

World Class Replication and Uptime

The RSA Authentication Manager software works in a primary/replica configuration. A single primary enables the central management, logging, reporting of the system, while up to 15 replicas (Enterprise edition license) guarantee geographic coverage, load balancing, and disaster recovery options. Taken together, the primary/replica configurations mean that this critical security service doesn't have to be taken down or suspended for any reason, giving your organization the confidence to protect your applications with near 100% uptime.

Flexibility

The RSA Authentication Manager is available as a hardware appliance or a virtual appliance.

Hardware Appliance Versions:

- Appliance 130 Designed to satisfy the requirements for simple, costeffective deployments.
- **Appliance 250** Designed with dual power and redundant hard drives for organizations that require high availability (HA).

Virtual Appliance Versions:

- VMware
- Microsoft Hyper-V

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, <u>contact</u> your local representative or authorized reseller or visit us at <u>www.emc.com/rsa</u>. $\mathsf{EMC}^2, \mathsf{EMC},$ the EMC logo, RSA SecurID, and RSA are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is a registered trademark or trademark of VMware, Inc., in the United States and other jurisdictions. © Copyright 2014 EMC Corporation. All rights reserved. Published in the USA. 12/14; Data Sheet; H13822

EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

