

# RSA AUTHENTICATION MANAGER

## Authentifizierung mit RSA SecurID gepaart mit der Benutzerfreundlichkeit und Flexibilität der risikobasierten Authentifizierung

### AUF EINEN BLICK

#### Flexibilität und Benutzerfreundlichkeit durch risikobasierte Authentifizierung

- Bereitstellung risikobasierter Authentifizierung neben Hardware- und Software-Authentifizierungskomponenten
- Geringere Kosten und breitere Anwendung der Authentifizierung im Unternehmen

#### Geringere Total-Cost-of-Ownership

- Zahlreiche integrierte Funktionen unterstützen bei den zeitaufwändigsten und kostspieligsten Aufgaben, die bei der Verwaltung einer unternehmensweiten Authentifizierungslösung anfallen
- IT-Mitarbeiter erreichen mit weniger Mitteln mehr

#### Leistungsfähigere virtuelle Umgebung

- Vollumfängliche Nutzung der Virtualisierung im Unternehmen sorgt für eine unkomplizierte Bereitstellung, Administration und laufende Systemverwaltung
- Nutzung von vorhandenem Know-how über Infrastruktur und Virtualisierung

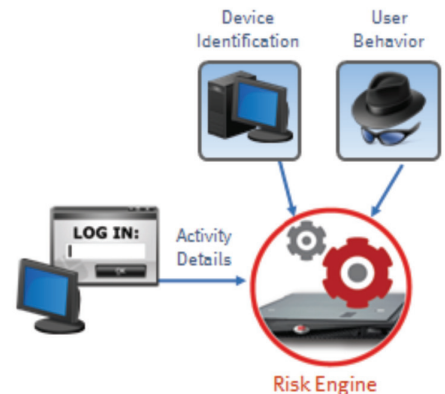
Die Sicherheit wird für Unternehmen, die mit immer knapperen IT-Budgets haushalten müssen, zunehmend zur Herausforderung, zumal sie auf eine wachsende Anwendergemeinschaft ausgedehnt werden muss. Der Hintergrund ist der, dass immer mehr Anwender mit nicht verwalteten Mobilgeräten über unkontrollierte Zugriffspunkte wie Webportale auf vertrauliche Daten zugreifen. Um diese Problematik anzugehen, müssen Unternehmen leistungsstarke Authentifizierungslösungen implementieren.

RSA® Authentication Manager 8.0 beinhaltet erstklassige RSA SecurID®-Authentifizierungstechnologie und bietet nun auch eine Risk Engine, um den Anforderungen moderner Unternehmen gerecht zu werden. RSA Authentication Manager dient zur Überprüfung von Authentifizierungsanfragen und zur zentralen Verwaltung von Authentifizierungsrichtlinien für den Zugriff auf Unternehmensnetzwerke.

Die Lösung nutzt die große Bandbreite an RSA SecurID-Authentifizierungskomponenten und ermöglicht die Zwei-Faktor-Anwenderauthentifizierung an mehr Virtual Private Networks (VPNs), drahtlosen Netzwerken, Webanwendungen, Geschäftsanwendungen und Umgebungen als alle anderen im Markt erhältlichen Systeme. Die virtuelle Appliance RSA Authentication Manager bietet die nötige Flexibilität zur Unterstützung zahlreicher Authentifizierungsmethoden, eine ausgereifte Risk Engine und eine einfache Handhabung. Darüber hinaus ist die Lösung zu branchenführenden Produkten und Anbietern kompatibel.

### LEISTUNGSSTARKE RISIKOBASIERTE AUTHENTIFIZIERUNG

Die risikobasierte Authentifizierung (RBA) von RSA Authentication Manager 8.0 ist optional lizenzierbar und erhöht die Sicherheit auf transparente Weise. Die risikobasierte Authentifizierung ist äußerst benutzerfreundlich, da die Anmeldung nach wie vor über das vertraute Verfahren mit Benutzername und Passwort erfolgt. Wird ein Anmeldeversuch als hohes Risiko eingestuft, wird der Anwender aufgefordert, einen zusätzlichen Identitätsnachweis zu erbringen. Bei diesem weiteren Authentifizierungsschritt müssen Anwender persönliche Fragen beantworten oder eine On-Demand-Authentifizierung per SMS durchführen.



### RISIKOBASIERTE AUTHENTIFIZIERUNG

Die risikobasierte Authentifizierung wurde zum Schutz des Zugriffs auf die gängigsten webbasierten Anwendungen entwickelt, darunter SSL-VPNs, Webportale, Outlook Web Access (OWA) und Microsoft SharePoint-Umgebungen. Da das Portfolio von RSA Authentication Manager nun auch die risikobasierte Authentifizierung beinhaltet, können Unternehmen jetzt auf kostengünstige Weise den Zugriff auf weitaus mehr Anwendungen als bisher sicherstellen.

Datenblatt

## VERWALTUNG

Zahlreiche integrierte Funktionen von RSA Authentication Manager unterstützen bei den zeitaufwändigsten und kostspieligsten Aufgaben, die bei der Verwaltung einer unternehmensweiten Authentifizierungslösung anfallen. Anwender arbeiten mit einer übersichtlichen Seitenansicht, die darauf ausgelegt ist, Helpdesk-Administratoren bei der Beantwortung der gängigsten Anwenderanfragen zu unterstützen, ohne dass mehrere Berichte oder Suchen ausgeführt werden müssen. IT-Mitarbeiter sparen dank der benutzerspezifisch anpassbaren Self-Service-Konsole Zeit, da Anwender die Möglichkeit haben, ihre Authentifizierungsmethoden selbst zu verwalten. Die Bereitstellung erfolgt in der DMZ des Netzwerks. Dort können Anwender ihre PIN ändern, ein Ersatz-Token anfordern, den Notfallzugriff beantragen und auf andere Dienste zur Fehlerbehebung zugreifen.

## BENUTZER-OBERFLÄCHE

- Bearbeiten der gängigsten Anwenderanfragen in einer übersichtlichen Seitenansicht
- Überwachung aktueller Authentifizierungsaktivitäten in Echtzeit
- Verwaltung von Token
  - o Aktivierung/Deaktivierung von Token
  - o Zuweisung von Token
  - o Sperren/Entsperren von Token
  - o Löschen von PINs
- Anzeigen von Benutzergruppenmitgliedschaften und zugänglichen Agents

The screenshot shows the RSA Authentication Manager dashboard for user John Smith. The dashboard is divided into several sections:

- User Profile:** Name: John Smith, Identity Source: Internal Database, Security Domain: SystemDomain, Account Status: Enabled, Locked Status: Locked. Notes: What is the John's mother's maiden name? Jones. Buttons: Disable, Unlock, Edit User, Authentication Settings.
- Assigned SecurID Tokens:** A table with columns: Serial Number, Type, Disabled, Replacement, PIN Set, New PIN, Next TC. One token is listed: 000104926674, SID 700, with PIN Set and Next TC checked.
- On-Demand Authentication (ODA):** Enabled for ODA: No, On-Demand Tokencode Destination: PIN Status: PIN Status, Expiration Date: Manage.
- Recent Authentication Activity:** A table with columns: Time, Activity Key, Result. It shows several failed authentication attempts for user 'jsmith'.
- User Group Membership:** A table with columns: User Group, Security Domain, Identity Source, Notes. One group is listed: Sales, SystemDomain, Internal Database.

## LEISTUNGSFÄHIGERE VIRTUELLE UMGEBUNG

Dank RSA Authentication Manager können Unternehmen die Virtualisierung mit VMware ESX oder ESXi vollumfänglich nutzen und so die Bereitstellung deutlich vereinfachen. Darüber hinaus verbessert die Virtualisierung die Verwaltbarkeit. Anhand vereinfachter Patch-Prozesse können Unternehmen ihre Systeme zudem schnell aktualisieren. Updates für die virtuelle Appliance, das zugrunde liegende Betriebssystem sowie die RSA Authentication Manager-Software sind in einem einzigen Service Pack enthalten. Somit müssen einzelne Systemebenen nicht mehr individuell verwaltet werden.

## INTEROPERABILITÄT

RSA Authentication Manager ist zu zahlreichen namhaften Produkten für Netzwerkinfrastrukturen und zu gängigen Betriebssystemen kompatibel. Das Programm „Secured by RSA“ ist eines der größten Alliance-Programme seiner Art und führt mehrere Hundert ergänzende Lösungen zusammen. Dazu zählen über 400 Produkte von mehr als 200 Anbietern. „Secured by RSA“ unterstützt Unternehmen dabei, deren maximale Flexibilität und den Investitionsschutz sicherzustellen. Führende Anbieter von Lösungen für den Remote-Zugriff, VPNs, Firewalls, drahtlosen Netzwerkgeräten, Webservern und Geschäftsanwendungen bieten eine integrierte Unterstützung für RSA Authentication Manager.

## KONTAKT

Weitere Informationen darüber, wie Sie mithilfe von Produkten, Services und Lösungen von EMC Ihre Unternehmens- und IT-Herausforderungen angehen können, erhalten Sie bei Ihrem zuständigen Kundenbetreuer oder autorisierten Vertragshändler. Alternativ besuchen Sie uns im Internet unter [www.emc.com/rsa](http://www.emc.com/rsa).

[www.emc.com/rsa](http://www.emc.com/rsa)

EMC2, EMC, das EMC-Logo, RSA und das RSA-Logo sind Warenzeichen oder eingetragene Warenzeichen der EMC Corporation in den Vereinigten Staaten oder anderen Ländern. VMware ist ein eingetragenes Warenzeichen von VMware, Inc. in den Vereinigten Staaten und anderen Ländern. © Copyright 2013 EMC Corporation. Alle Rechte vorbehalten. Veröffentlicht in den USA. 0113 Datenblatt H11403

EMC geht davon aus, dass die Informationen in diesem Dokument zum Zeitpunkt der Veröffentlichung korrekt sind. Die Informationen können ohne Ankündigung geändert werden.

