



# RSA® Authentication Manager

## Security Engine der Enterprise-Klasse für die RSA SecurID®-Authentifizierung

### Übersicht

- Security Engine der Enterprise-Klasse für die leistungsstarke Zwei-Faktor-Authentifizierung von über 25 Millionen RSA SecurID®-Benutzern weltweit
- Hohe Skalierbarkeit zur Anpassung an die Anforderungen kleiner bis großer Unternehmen
- Kompatibel zu mehr als 350 Produkten von über 200 Herstellern ohne Aufpreis
- Ermöglicht die zentrale Verwaltung verschiedener Authentifizierungsmethoden

### Identity Assurance

Die Identitätsprüfung umfasst alle Funktionen und Methoden zur Minimierung der Geschäftsrisiken, die mit Identitätsbetrug und Benutzerkontenmissbrauch verbunden sind. Durch die Identitätsprüfung schaffen Unternehmen mehr Vertrauen, da Benutzer mit zuverlässigen Identitäten auf flexible und sichere Weise mit Systemen interagieren und auf Informationen zugreifen können. Dadurch ergeben sich neue Möglichkeiten, den Umsatz zu steigern, die Kunden zufriedenzustellen und die Kosten im Griff zu behalten.

Der RSA Authentication Manager hat sich als De-facto-Standard für die Identitätsprüfung etabliert. Das System bietet umfassende Funktionen in den vier Bereichen, die die Identitätsprüfung erfordert: Verwaltung und Richtlinien für Zugangsdaten, Authentifizierung, Autorisierung und vertrauliche Informationen. Durch das RSA-Portfolio für die Identitätsprüfung wird die Benutzerauthentifizierung von einer einzelnen Sicherheitsmaßnahme auf ein beständiges Vertrauensmodell erweitert, das als Basis dafür dient, wie eine Identität verwendet wird und welche Möglichkeiten sie bietet.



The Security Division of EMC

Mit RSA-Lösungen verwaltete, zuverlässige Identitäten sorgen für mehr Vertrauen bei den täglichen Transaktionen und unterstützen neue Geschäftsmodelle, indem sie einen sicheren Zugriff für Mitarbeiter, Kunden und Partner schaffen und zudem ein Gleichgewicht zwischen Risiko, Kosten und Bedienkomfort herstellen.

Der RSA® Authentication Manager ist die Verwaltungskomponente der RSA SecurID®-Lösung. Sie dient zur Überprüfung von Authentifizierungsanfragen und zur zentralen Verwaltung von Authentifizierungsrichtlinien für den Zugriff auf Unternehmensnetzwerke. In Kombination mit RSA SecurID-Authentifizierungskomponenten und dem RSA® Authentication Agent bietet die Lösung eine starke Zwei-Faktor-Authentifizierung. Sie schützt den Zugriff auf mehr VPNs, Wireless-Netzwerke, Webanwendungen, Geschäftsanwendungen und Betriebsumgebungen (darunter auch das Betriebssystem Microsoft® Windows®) als jedes andere System am Markt.

### Hohe Leistungsfähigkeit und Skalierbarkeit

Der RSA Authentication Manager eignet sich für die Anforderungen von Unternehmen verschiedenster Größe. Das System basiert auf einer Multiprozessor-Architektur der Enterprise-Klasse und kann mit nur 25 ebenso wie mit mehreren Millionen Benutzern pro Server arbeiten und dabei Hunderte gleichzeitiger Authentifizierungsvorgänge bewältigen. Die Lösung wird im Bankwesen, in Behörden, im Einzelhandel, in der Fertigungs- und Hightech-Branche sowie im Gesundheitswesen in aller Welt eingesetzt und ist in zwei Versionen erhältlich: Base Edition und Enterprise Edition.

### Datenbankreplikation

Die Funktion zur Datenbankreplikation des RSA Authentication Manager ermöglicht eine flexible Netzwerkkonfiguration und Load Balancing, um die Leistung zu steigern und dadurch die Verwaltungskosten zu senken.

Die Base Edition beinhaltet einen Primary Server und eine Replica. Die Benutzerverwaltung erfolgt auf dem Primary, und alle Daten werden auf dem Replica Server gespiegelt. Beide Server eignen sich für die Verarbeitung von Authentifizierungsanfragen. Die RSA Authentication Agents gleichen die Auslastung beider Server aus, indem sie Antwortzeiten



erkennen und die Anfrage entsprechend weiterleiten, um eine optimale Leistung zu garantieren.

Die Enterprise Edition wurde für mittlere und große Unternehmen entwickelt. Sie beinhaltet einen Primary Server und bis zu fünfzehn Replica Server in einem Realm und bietet die Möglichkeit, maximal sechs separate Realms zusammenzuführen. Administratoren können die Authentifizierung der Benutzer an ihrem Netzwerk überall auf der Welt in Echtzeit verfolgen, Sicherheitsrichtlinien im internationalen Netzwerk zeitgleich aktualisieren und eine globale Netzwerktopologie entwickeln, um die Leistung des Netzwerks zu steigern.

### Verwaltung und Steuerung

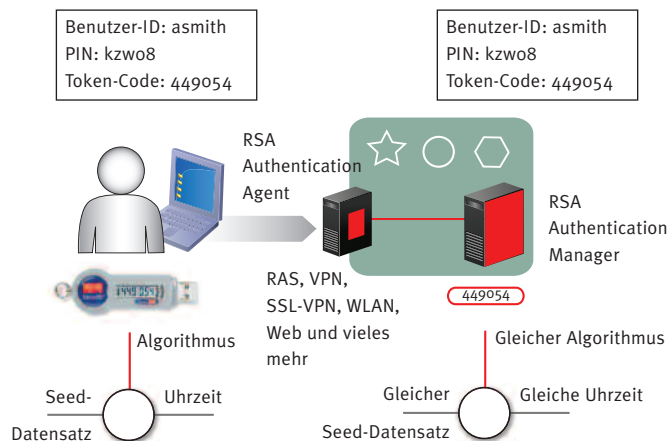
Der RSA Authentication Manager bietet eine äußerst flexible Verwaltung und Steuerung. Auf dem Desktop des Administrators muss keine zusätzliche Software installiert werden, da ein integrierter Webserver den Zugriff auf die Managementkonsole über jeden beliebigen Browser ermöglicht. Der im Lieferumfang enthaltene Juniper® Steel Belted RADIUS-Server wird ebenfalls vollständig innerhalb der intuitiven, übersichtlichen Administrationskonsole verwaltet.

Durch die native LDAP-Integration kann der RSA Authentication Manager auf einen oder mehrere zuverlässige Datenspeicher verweisen, um Benutzer- und Gruppendaten in Echtzeit abzurufen. Es können mehrere LDAP-Quellen definiert werden, darunter Microsoft Active Directory® und Sun One™; Schemaänderungen sind nicht erforderlich. Mithilfe eines Snap-Ins für die Microsoft Management Console können Benutzerdatensätze direkt über eine MMC-Oberfläche geändert werden.

Sowohl die Base Edition als auch die Enterprise Edition beinhalten den RSA® Credential Manager, ein vollständig integriertes Softwaremodul, das einen Self-Service für Benutzer (Base und Enterprise) und Workflow-Bereitstellung (nur Enterprise) bietet, um die Zuweisung von Zugangsdaten an Benutzer deutlich zu beschleunigen.

### Auditing und Berichte

Da der RSA Authentication Manager alle Transaktionen und Benutzeraktivitäten protokolliert, können Administratoren diese Lösung auch für Auditing, Accounting und Compliance einsetzen. Im Lieferumfang enthalten sind zahlreiche Berichtsvorlagen, die sich mit geringem Aufwand an die jeweiligen Bedürfnisse anpassen lassen, u.a. Übersichten zur Systemaktivität oder Protokolle zu Auffälligkeiten, Vorkommnissen oder zur Nutzung bestimmter Ressourcen. Neben den Berichtsfunktionen bietet das Produkt auch eine Überwachung von Aktivitäten in Echtzeit, bei der ein Administrator alle oder ausgewählte Aktivitäten anzeigen kann.



### Zeitsynchrone Zwei-Faktor-Authentifizierung mit RSA SecurID

### Vielfältige Methoden für Zugangsdaten

Der RSA Authentication Manager unterstützt die Authentifizierungskomponenten verschiedenster Gerätetypen, von herkömmlichen Hardware-Token über Software-basierte Token zur Installation auf PCs und Smartphones bis hin zur On-Demand-Authentifizierung, durch die einmalig verwendbare Token-Codes per SMS oder E-Mail bereitgestellt werden. Alle diese Zugangsdaten werden zentral über eine gemeinsame Oberfläche verwaltet.

### Sofortige Zusammenarbeit mit anderen Systemen

Der RSA Authentication Manager ist zu zahlreichen namhaften Produkten für Netzwerkinfrastrukturen und zu gängigen Betriebssystemen kompatibel: Mehr als 350 Produkte von über 200 Anbietern sorgen für maximale Flexibilität und Investitionsschutz im Unternehmen. Führende Anbieter von Lösungen für den Remote-Zugriff, VPNs, Firewalls, drahtlosen Netzwerkgeräten, Webservern und Geschäftsanwendungen bieten eine integrierte Unterstützung für den RSA Authentication Manager.



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

©2008 RSA Security Inc. Alle Rechte vorbehalten.  
RSA, RSA Security, SecurID, SecurID Ready und das RSA Logo sind Warenzeichen oder eingetragene Warenzeichen von RSA Security Inc. in den Vereinigten Staaten und anderen Ländern. Microsoft und Windows sind Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und anderen Ländern. EMC ist ein eingetragenes Warenzeichen der EMC Corporation. Alle weiteren hier aufgeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber.

SIDAM DS 0208