



The Security Division of EMC

Resumen Técnico

# Novedades de RSA<sup>®</sup> Authentication Manager 7.1



RSA® Authentication Manager 7.1 es el próximo gran lanzamiento de la emblemática solución de autenticación de dos factores de RSA, disponible en todo el mundo para plataformas de software seleccionadas a partir del segundo trimestre de 2008. Este lanzamiento brinda nuevas funcionalidades y posiciona la plataforma para nuevos usos y aplicaciones.

---

## Tres Áreas de Mejoras Cruciales

---

### Opción de Continuidad del Negocio

La propuesta de valor de RSA ha dejado de ser tan solo una “empresa nominal” para convertirse en una solución estratégica de administración de riesgos de la información de nuestros clientes. La Opción de Continuidad del negocio (BCO, *Business Continuity Option*) agregada en la versión 7.1 responde a la pregunta: “¿Cómo evito disminuir el nivel de mi política de seguridad si tuviera que enviar todos mis empleados a trabajar desde sus hogares en el caso de una interrupción de las actividades comerciales?”.

### Métodos de Autenticación Extendida

Este nuevo lanzamiento amplía la variedad de tipos de autenticadores que se pueden implementar a los usuarios y administrar centralmente desde el servidor.

### Eficiencias Operacionales Mejoradas

Los clientes tendrán a su disposición un conjunto de herramientas que mejorarán las eficiencias operacionales, optimizarán las implementaciones y disminuirán el total de los costos de administración continuos.

---

## Puntos Destacados

---

### Eficiencias Operacionales Mejoradas

RSA Authentication Manager 7.1 incluye un conjunto de funciones solicitadas que facilitan la administración de la solución, disminuyen el costo total de propiedad y aprovechan los recursos de TI existentes.

**Soporte para LDAP Nativo** Este lanzamiento ofrece verdadero soporte nativo para LDAP con integración directa a Sun One™ y Active Directory®. Ya no es necesaria la sincronización. Varias fuentes de identidad pueden funcionar como almacén de datos. El LDAP nativo no requiere de ningún cambio en el esquema de la base de datos.

**Administración Basada en Web.** La nueva interfaz de administración está basada en navegador y no requiere espacio; no es necesario instalar un software cliente en la PC de administración. RSA Authentication Manager 7.1 se puede administrar remotamente desde cualquier PC con un navegador y una conexión a Internet.

**Administración Delegada de Múltiples Niveles.** Permite un control detallado del acceso administrativo, hasta el nivel de usuario/grupo y política. De este modo, se logra maximizar la inversión de los recursos de administración y ofrecer mayor seguridad, pues menos personas tienen “las llaves del reino”.

**Clustering de Servidores.** El uso de clustering permite agrupar los nodos de servidor para que parezcan uno solo. Es una manera fácil y económica de aumentar la escalabilidad y el performance. También aumenta la resiliencia al brindar failover adicional, lo que asegura una productividad máxima. *Disponible solamente con la licencia de servidor empresarial.*—

**Snap-in de Microsoft® Management Console (MMC).** Para los clientes que utilizan MMC como utilidad principal de administración, este complemento aporta consistencia y mayor facilidad de uso. Por medio de MMC, los administradores pueden realizar diversas tareas de usuario básicas y tareas de administración de tokens, como asignación o desactivación de tokens para un usuario.

**Servidor RADIUS.** El Servidor RADIUS 802.1x, que se eliminó de la versión 7.0, se implementó nuevamente en la versión 7.1. La inclusión del servidor RADIUS es más económica que la implementación de una solución de terceros y, al venir completamente incorporado en la consola de administración, facilita la configuración y la administración continua.

**RSA® Credential Manager.** RSA Credential Manager, el reemplazante de RSA® Deployment Manager (Web Express), funciona en estrecha integración con la interfaz de administración de Authentication Manager, no requiere instalación por separado y proporciona mayor funcionalidad que Deployment Manager. Estos incluyen:

- **Autoservicio.** Los usuarios finales disponen de una consola de autoservicio para solicitar diversos servicios, como el envío de tokens según demanda para accesos de emergencia. El módulo de autoservicio contribuye a reducir ostensiblemente el número de llamadas que recibe la mesa de ayuda de TI, ya que los usuarios ahora pueden administrar todos los aspectos de los ciclos de vida de sus tokens.
- **Provisioning del Flujo de Trabajo.** Los administradores pueden crear procesos por los cuales se puede aprobar a los solicitantes y enviar credenciales (disponible con la Licencia de Servidor Empresarial).

## Métodos de Autenticación Extendida

Junto con el soporte para credenciales tradicionales de los anteriores lanzamientos, RSA Authentication Manager 7.1 introduce nuevos autenticadores para usuarios finales. Así, se crean nuevas oportunidades para implementaciones flexibles y se disminuyen los costos de administración. Todos estos métodos siguen siendo administrados centralmente y soportados desde una consola de administración.

**Autenticador según Demanda.** El Autenticador según Demanda RSA SecurID® es un nuevo método de credenciales disponible con la versión 7.1. Ofrece códigos de token a los usuarios mediante mensajes de texto (SMS, *Short Message Service*) o correo electrónico y no requiere que se asignen tokens físicos o herramientas de software en una computadora portátil o en un teléfono inteligente. Los Autenticadores según Demanda no tienen fechas de vencimiento.

**Provisioning Dinámico de Valores Raíz (Seed) CT-KIP.** El protocolo de inicio por claves de token criptográficas es un protocolo de cliente-servidor que permite una configuración más rápida de tokens de software. Con CT-KIP, tanto el cliente como el servidor pueden generar un identificador en común (un archivo raíz) que se puede usar para autenticar el usuario ante el servidor. No es necesario enviar un archivo raíz al usuario remoto a través de la red. Así, la implementación de los tokens de software se hace más simple y breve.

**Soporte de Administración Incluido para el Proveedor de Mensajería Global Clickatell™.** Con el fin de enviar grandes cantidades de mensajes SMS a los usuarios, es necesario establecer una relación con un adionador de SMS de modo que sea posible dirigir los mensajes a un gateway portador. RSA ha incorporado en la consola de administración una interfaz que funciona con Clickatell, empresa global de mensajería móvil con acceso a más de 600 redes en casi 200 países.

## Opción de Continuidad del Negocio

Con la versión 7.1, la nueva Opción de Continuidad del Negocio hace aún más fácil aprovechar la autenticación de SecurID en un planeamiento organizacional ante una eventual interrupción de las actividades del negocio.

Las características de licencia de la Opción de Continuidad del Negocio permiten al cliente extender la licencia del servidor de manera temporaria para poder manejar el flujo de grandes cantidades de usuarios con acceso remoto (por ejemplo, en el caso de una interrupción de las actividades del negocio, cuando los empleados deben trabajar desde sus hogares). Es posible utilizar la nueva característica de la licencia hasta seis veces por cada período de licencia, durante 60 días en cada ocasión. Los términos de la licencia de la Opción de Continuidad del Negocio (BCO) duran 3 años.

La Opción de Continuidad del Negocio extiende la licencia del servidor y permite utilizar un número predefinido de Autenticadores RSA SecurID Según Demanda. Por ejemplo, un cliente compra una licencia BCO de 1.000 cuentas. Al utilizar la opción BCO, aparecen disponibles otras 1.000 cuentas de Autenticadores según Demanda listas para usarse. La implementación se puede hacer de inmediato mediante el módulo de Autoservicio de RSA Credential Manager (incluido), de modo que los usuarios se pueden incluir a sí mismos sin sobrecargar la mesa de ayuda de TI con sus solicitudes.

---

## Nuevas Posibilidades para las Aplicaciones

---

En conjunto, estas aplicaciones y características ofrecen una nueva manera de administrar e implementar RSA Authentication Manager. Por ejemplo, la inclusión de Autenticadores según Demanda, junto con las herramientas de autoservicio para usuarios finales, permite brindar servicio a un mayor número de usuarios de la base. A continuación presentamos algunos ejemplos.

**Soporte de una Base de Contratistas y Proveedores.** Muchas organizaciones enfrentan dilemas sobre cómo brindar soporte a empleados temporarios, contratistas y asociados de negocios invitados que solicitan acceso a los recursos de la red. El envío de Autenticadores según Demanda mediante el módulo de Autoservicio puede ser una excelente manera de implementar credenciales de modo temporario sin recurrir a la entrega de tokens para software o hardware. Es posible desarrollar específicamente un flujo de trabajo que se adapte a estas categorías de usuarios, con aprobadores de líneas de negocios en el back-end para mayor seguridad.

**Resultado:** Incorporación más rápida de contratistas o proveedores, costos de implementación más bajos y mínima pérdida por tokens irrecuperables.

**Soporte de una Base de Usuarios Ocasionales.** Muchos empleados no viajan o trabajan de modo remoto lo suficiente como para justificar el uso de un token tradicional. Sin embargo, en esos casos, es necesario tener listo un proceso veloz de iniciación automática capaz de brindar soporte a estos usuarios. Las nuevas características de Authentication Manager 7.1 resuelven esta situación con transparencia.

**Resultado:** Se implementa la política de autenticación de dos factores; queda establecido un proceso de soporte a cualquier usuario.

**Soporte de Autoservicio para “Usuarios Avanzados” Existentes.** Un viajero de negocios olvida el token en su hogar. Otro necesita restablecer su PIN. Un tercer viajero desea probar o volver a sincronizar su token de hardware. Normalmente, estas solicitudes desembocarían en una llamada a la mesa de ayuda de TI. Sin embargo, en la versión 7.1, RSA Credential Manager permite a los usuarios tomar el control de las herramientas disponibles y realizar por sí mismos estas tareas.

**Resultado:** Ahorros en la productividad para el usuario final y ahorros en la productividad y en los costos para la mesa de ayuda de TI.

**Planificación de la Continuidad del Negocio.** Muchas organizaciones se enfrentan al desafío de implementar un plan de recuperación ante desastres o pandemias que fuercen a todo el personal a acceder a la red remotamente sin debilitar la política de

seguridad para incluir a los usuarios sin tokens. La Opción de Continuidad del Negocio da una respuesta a este problema.

**Resultado:** La política de seguridad continúa vigente, incluso durante la interrupción de las actividades del negocio.

### Disponibilidad y Soporte de Plataformas

Se prevé lanzar RSA Authentication Manager 7.1 al público en general el segundo trimestre de 2008. Inicialmente, estará disponible en las siguientes plataformas de software: Windows®, Red Hat™ Linux y Sun Solaris™. En el próximo lanzamiento, se agregará soporte para otras plataformas, incluida RSA SecurID Appliance.

## RSA es su asociado de negocios de confianza

RSA, la División de Seguridad de EMC, es el principal proveedor de soluciones de seguridad para aceleración del negocio y ayuda a las más importantes organizaciones del mundo a alcanzar el éxito resolviendo los más complejos y delicados desafíos de seguridad. El enfoque hacia la seguridad centrado en la información que ofrece RSA protege la integridad y la confidencialidad de la información durante todo su ciclo de vida, sin importar dónde se la mueva, quién acceda a ella o cómo se la use.

RSA ofrece soluciones líderes en seguridad de identidad y control de acceso, prevención de pérdida de datos y encriptación, administración de información de seguridad y cumplimiento de normas, y protección contra fraudes. Estas soluciones brindan confianza a millones de identidades de usuarios, las transacciones que realizan y los datos que se generan. Para obtener más información, visite [www.RSA.com](http://www.RSA.com) y [argentina.emc.com](http://argentina.emc.com).



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

The Security Division of EMC

©2008 RSA Security Inc. Todos los derechos reservados. RSA, RSA Security, SecurID y el logotipo de RSA son marcas registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. Windows y Microsoft son marcas comerciales o marcas registradas de Microsoft Corporation en los Estados Unidos y otros países. EMC es una marca registrada de EMC Corporation. Todos los demás productos y servicios mencionados son marcas comerciales de sus respectivas empresas.

AS71 SB 0108