



RSA[®]

The Security Division of EMC

Информация о продукте

**RSA[®] Authentication Manager 7.1 -
НОВЫЕ ВОЗМОЖНОСТИ**

RSA® Authentication Manager 7.1 является самой современной версией ведущей системы двухфакторной аутентификации от компании RSA из числа представленных на рынке. Использование данной системы на некоторых операционных системах началось со второго квартала 2008 года. Данная версия содержит новый набор функциональных возможностей, а также расширяет функциональность решения и сферу применения для новых приложений.

Три основные области усовершенствования

Опция обеспечения непрерывности бизнеса

Произведенные компанией RSA усовершенствования поднимают возможности системы с уровня «надежная система аутентификации» до уровня той стратегической информационной системы управления рисками, которая востребована нашими клиентами. Опция Business Continuity Option (Обеспечения непрерывности бизнеса (BCO)), интегрированная в версию 7.1, дает ответ на вопрос: «Как мне не ослабить безопасность ИТ-инфраструктуры, если я перевел всех сотрудников в режим работы на дому на время спада деловой активности?»

Расширенный метод аутентификации

В новой версии снова увеличено число типов аутентификаторов, которые могут применять пользователи и которыми можно управлять с сервера централизованно.

Повышенная производительность труда

Клиенты могут рассчитывать на получение набора инструментов, который повысит производительность труда, позволит рационализировать процесс развертывания системы и снизит общие текущие административные расходы.

Основные показатели

Повышенная производительность труда

Система RSA Authentication Manager 7.1 включает в себя набор необходимых функций, которые облегчают управление системой, снижают совокупные затраты владельца и расширяют возможности существующих ИТ-ресурсов.

Встроенная поддержка протокола LDAP. Новая версия предоставляет встроенные средства поддержки протокола LDAP для интеграции с Sun One™ и Active Directory®. Многочисленные источники идентификационной информации одновременно могут служить и местами ее хранения. Наличие встроенной поддержки LDAP более не вызывает необходимости менять схему хранения данных.

Web-интерфейс управления. Новый административный Web-интерфейс не требует дополнительных ресурсов, а именно: нет необходимости устанавливать клиентское приложение на ПК администратора. Дистанционное управление системой RSA Authentication Manager 7.1 может осуществляться с любого ПК, на котором имеется Web-браузер и доступ в Интернет.

Многоуровневое администрирование с передачей прав. Данная функция обеспечивает многоуровневое администрирование вплоть до уровня пользователя/группы пользователей и политик. Данная функция максимально повышает эффективность инвестиций в административные ресурсы и обеспечивает повышенную степень безопасности благодаря тому, что «ключами от замка» владеет меньшее число лиц.

Кластеризация серверов. Кластеризация позволяет группировать серверные узлы в единое целое. Данная функция является простым и дешевым способом повышения масштабируемости и производительности. Кроме того, дополнительные средства переключения при отказе увеличивают способность системы к восстановлению работоспособности, что гарантирует минимальное время простоя. *(Эта опция доступна только для владельцев лицензий уровня Enterprise (корпоративная))*

Встраиваемый модуль консоли управления Microsoft® Management Console (MMC). Для пользователей, которые уже используют MMC в качестве основного управленческого средства, этот дополнительный модуль обеспечивает совместимость ресурсов и облегчает работу. С помощью MMC администраторы могут выполнять множество задач абонентского обслуживания и управления токенами, например, присвоение токена пользователю или блокировка токена.

Сервер RADIUS. Сервер 802.1x RADIUS, который отсутствовал в версии 7.0, снова включен в состав версии 7.1. Наличие сервера RADIUS в пакете позволяет снизить затраты в ситуации, когда необходимо внедрить решения третьих производителей. Этот сервер полностью интегрирован в консоль управления, что существенно упрощает его установку и текущее управление им.

RSA® Credential Manager. Являясь заменой системе RSA® Deployment Manager (Web Express), система RSA Credential Manager тесно связана с интерфейсом управления системой Authentication Manager, не требует отдельной установки и обеспечивает функциональные возможности, превосходящие возможности Deployment Manager. Среди них:

– **Self Service (Самообслуживание)** Настраиваемая консоль самообслуживания предоставляет конечным пользователям возможность выполнения ряда операций, включая получение токенов On-demand (по запросу) для аварийного доступа. Модуль Self Service способен значительно уменьшить количество обращений в службу ИТ-поддержки, так как пользователи получают права на управление всеми параметрами своих токенов.

– **Планирование последовательности операций.** Администраторы могут разработать процессы идентификации абонентов и предоставления токенов *(Эта функция доступна только для владельцев лицензий уровня Enterprise (корпоративная))*.

Расширенный метод аутентификации

Помимо традиционных токенов, применявшихся в предыдущих версиях системы, в RSA Authentication Manager 7.1 представлены новые типы аутентификаторов, которые позволяют применять различные схемы внедрения системы и тем самым снижать административные расходы. Как и прежде, управление системой осуществляется через консоль администрирования.

On-demand Authenticator. RSA SecurID® On-demand Authenticator представляет собой новый метод доставки идентификационной информации, доступный в версии 7.1. Токен-код пользователя пересылается ему через систему передачи коротких сообщений (SMS) или по электронной почте, при этом ни наличия аппаратного токена, ни установки программного обеспечения на компьютере или мобильном телефоне не требуется. Технология On-demand Authenticator не предусматривает ограничений по срокам действия.

Dynamic Seed Provisioning (CT-KIP). Cryptographic token key initiation protocol (Криптографический протокол инициации токена) представляет собой клиент-серверный протокол, который ускоряет процесс установки программных токенов. При использовании CT-KIP клиент и сервер могут генерировать уникальный ключ – так называемый вектор начальной генерации (seed), – который затем может быть использован при аутентификации пользователя на сервере. Пересылка данного файла удаленному пользователю по сети не требуется. Это позволяет облегчить процесс размещения программных токенов и сократить время на развертывание системы.

Встроенная административная поддержка для международной службы передачи сообщений Clickatell™. Пересылка пользователям большого количества SMS-сообщений возможна при участии агрегатора рассылок SMS. В этом случае сообщения направляются через его шлюз. Компанией RSA в консоль управления встроен интерфейс для взаимодействия со службой Clickatell - международной компанией, занимающейся рассылкой сообщений на мобильные устройства и обеспечивающей доступ более чем к 600 сетям почти в 200 странах.

Опция обеспечения непрерывности бизнеса

Имеющаяся в версии 7.1. новая опция Business Continuity Option (BCO) дает еще большее преимущество способу аутентификации SecurID при планировании работы в случае неожиданных нарушений нормального режима работы предприятия.

Функция лицензирования **Business Continuity Option** предоставляет пользователю возможность расширить рамки серверной лицензии на период интенсивной работы большого числа удаленных пользователей, например, во время проблем с деятельностью предприятия, когда сотрудники вынуждены работать на дому. Эта функция может быть активирована до шести раз в течение срока действия лицензии, каждый раз на период в 60 дней. Срок действия лицензии BCO составляет 3 года. Опция Business Continuity Option расширяет рамки серверной лицензии и дает возможность использовать предварительно заданное число аутентификаторов RSA SecurID On-demand Authenticator. Например, пользователь приобрел лицензию BCO на 1 000 рабочих мест, тогда при вызове опции BCO он немедленно получает дополнительные 1000 мест On-demand Authenticator. Развертывание системы происходит непосредственно во время работы с помощью модуля Self Service пакета RSA Credential Manager (включено в поставку), поэтому пользователи получают возможность действовать самостоятельно, не перегружая службу поддержки запросами на оказание помощи.

Появление новых возможностей у приложений

Используемые совместно, названные приложения и функции открывают новые возможности по развертыванию и управлению системой RSA Authentication Manager. Например, технология On-demand Authenticator совместно с инструментами самообслуживания конечных пользователей дает возможность работать с гораздо большим их количеством. Далее представлены несколько примеров.

Поддержка базы подрядчиков и поставщиков. Перед многими организациями стоит задача: что делать с временными работниками, подрядчиками и деловыми партнерами – посетителями, которые нуждаются во временном доступе к сетевым ресурсам. Выдача аутентификаторов On-demand Authenticators с помощью модуля Self Service может быть прекрасным способом предоставления прав доступа без необходимости выдачи аппаратных и программных токенов. Для того, чтобы гарантировать сохранение безопасности, можно разработать регламенты, описывающие последовательность операций по предоставлению разрешений таким категориям пользователей.

Результат: Ускоренное включение в работу подрядчиков/поставщиков, уменьшение расходов на развертывание системы, уменьшение потерь за счет невозвращенных аппаратных токенов.

Поддержка базы нерегулярных пользователей. Многие сотрудники не совершают поездок или работают удаленно недостаточное количество времени для того, чтобы предоставление им традиционных токенов было бы оправданным. Тем не менее, если возникнет такая необходимость, то система должна предоставлять возможность быстрой и гибкой настройки поддержки таких пользователей. Новые функции системы Authentication Manager 7.1 позволяют эффективно решить данную проблему.

Результат: Усиление политики двухфакторной аутентификации. Внедренная технология позволяет обеспечить поддержку любого пользователя.

Поддержка функции самообслуживания существующего «ключевого пользователя». Один командированный сотрудник забыл токен дома. Другому требуется восстановление PIN. Еще кому-то необходимо проверить или восстановить синхронизацию аппаратного токена. Обычно такие проблемы решаются с помощью звонков в службу ИТ-поддержки, но система 7.1 the RSA Credential Manager дает возможность пользователям применить имеющиеся в наличии инструменты управления и выполнить эти задачи самостоятельно.

Результат: Повышение производительности конечного пользователя, а также повышение производительности и снижение затрат службы ИТ-поддержки.

Планирование непрерывности бизнеса. Многие организации испытывают затруднения, пытаясь восстановить свою деятельность после каких-либо нарушений, если глобальный план такого восстановления предусматривает удаленный доступ к сети всего штата сотрудников, причем должен быть обеспечен достаточный уровень безопасности при подключении пользователей, не имеющих токенов. Новая опция Business Continuity Option предоставляет возможность решения данной задачи.

Результат: Безопасность поддерживается на неизменном уровне даже в случае нарушения нормального режима деятельности организации.

Готовность к работе и поддержка платформы

Система RSA Authentication Manager 7.1 представлена на рынке со второго квартала 2008 года. В первое время данная система будет доступна для работы на следующих программных платформах: Windows®, Red Hat™ Linux и Sun Solaris™. Поддержка других платформ, в том числе и ПАК RSA SecurID Appliance, будет реализована в следующей версии.

RSA – это Ваш проверенный партнер

Компания RSA, входящая в состав корпорации EMC, – ведущий разработчик систем безопасности для повышения эффективности бизнеса. RSA помогает лидерам глобального рынка решать самые сложные задачи в сфере безопасности. Решения RSA построены вокруг информации. Они обеспечивают ее целостность и конфиденциальность на протяжении всего жизненного цикла, независимо от того, где она находится, кто с ней работает и каким образом она используется.

RSA предлагает уникальные решения в сфере идентификации пользователей, управления доступом к данным, предотвращения утечки данных, шифрования, управления защищенными инфраструктурами, соответствия законодательным требованиям и предотвращения несанкционированных действий. Эти решения применяются для защиты личных данных миллионов пользователей, сведений о выполняемых ими операциях и данных, создаваемых в результате выполнения этих операций. Дополнительные сведения приведены на сайтах www.RSA.com и www.EMC.com.



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

The Security Division of EMC

©2008 RSA Security Inc. Все права защищены. Логотипы RSA, RSA Security и SecurID являются зарегистрированными товарными знаками или товарными знаками, принадлежащими компании RSA Security Inc. в Соединенных Штатах и/или других странах. Windows и Microsoft являются зарегистрированными товарными знаками или товарными знаками, принадлежащими корпорации «Microsoft» на территории Соединенных Штатов Америки и/или других стран. EMC является товарным знаком, принадлежащим корпорации EMC. Все остальные продукты и услуги, упомянутые в тексте, являются торговыми марками, принадлежащими соответствующим компаниям.

AS71 SB 0108