

Информация о продукте

RSA Authentication Agents for Microsoft® Windows®

Двухфакторная проверка подлинности для Microsoft Windows®

Краткий обзор

- Повышенная безопасность работы в среде Microsoft Windows®;
- Упрощенная процедура входа в систему;
- Сокращение числа обращений, связанных с паролями, в службу поддержки;
- Уменьшение необходимости использования процедур и политик, связанных с восстановлением пароля.

RSA Authentication Agents for Microsoft Windows® представляет собой решение, предназначенное для проверки подлинности пользователей перед предоставлением доступа к среде Microsoft Windows. Программное обеспечение RSA Authentication Agents for Microsoft Windows® позволяет использовать решение RSA SecurID® для проверки подлинности пользователей операционных систем, разработанных компанией Microsoft независимо от того, работают ли они в сетевом режиме и подключены к корпоративной сети или работают автономно и регистрируются для получения доступа к своему рабочему столу. Данное решение обеспечивает более высокий уровень безопасности, чем использование паролей, и более удобный механизм доступа к среде Windows, а также устраняет необходимость использования политик смены паролей и ведет журнал, в котором отражается вся информация, связанная с проверкой подлинности.

Двухфакторная система обеспечения безопасности

Решение RSA SecurID обеспечивает высокий уровень безопасности, т.к. в нем вместо паролей применяется двухфакторная проверка подлинности. Каждый пользователь получает уникальное устройство идентификации (токен), которое каждые шестьдесят секунд генерирует случайное число. В ответ на запрос пользователь вводит имя пользователя и passcode, который состоит из PIN-кода, за которым следует число, отображаемое в данный момент на токене. Комбинация PIN-кода пользователя (известного ему) и правильного кода, сгенерированного токеном, является подтверждением личности пользователя.

Удобный и унифицированный метод входа

Одной из проблем, с которой сталкиваются пользователи, является возможность утечки информации о пароле. С увеличением числа различных паролей пользователи начинают записывать их на листах бумаги или хранят их в отдельном файле, что приводит к снижению уровня безопасности. Проблема усугубляется наличием корпоративных политик, диктующих необходимость периодической смены паролей и требующих от пользователей выбирать такие последовательности символов, которые трудно запомнить.

Решение RSA Authentication Agents for Microsoft Windows позволяет использовать один и тот же метод проверки подлинности вне зависимости от того, идет ли речь о доступе в виртуальную частную сеть или защищенный web-ресурс, а также при регистрации в ОС Windows в домене или на локальном компьютере. Решение позволяет устранить необходимость в применении пароля и сократить число обращений в службу поддержки, поскольку устройство идентификации генерирует постоянно меняющиеся числа.

Проверка подлинности в режимах "online" и "offline"

Интерфейс пользователя является интуитивно понятным. При регистрации в домене Microsoft Windows с использованием RSA SecurID пользователь нажимает комбинацию клавиш CTRL, ALT, DEL и в ответ на запрос вводит свои имя пользователя и passcode, а не пароль. Эта информация отправляется в RSA® Authentication Manager, который вычисляет passcode и сравнивает результаты. В случае совпадения пользователю предоставляется доступ.

После успешной проверки подлинности в онлайн-режиме RSA Authentication Manager переходит к подготовке клиентской системы к проверке подлинности в автономном режиме. Выполняется генерация кодов для заранее определенного числа дней, и эти данные направляются клиентской системе. Когда пользователь пытается войти на свою рабочую станцию в автономном режиме, открывается диалоговое окно для ввода имени пользователя и passcode. RSA Authentication Agents for Microsoft Windows сравнивает полученные данные с имеющимися и в зависимости от результата предоставляет или отказывает в доступе.



The Security Division of EMC

Microsoft
GOLD CERTIFIED

Partner



Прозрачная интеграция с системой ввода пароля Microsoft

Решение RSA Authentication Agents for Microsoft Windows работает вместе с контроллером домена Microsoft Windows и службой каталога Microsoft Active Directory®. Информация о пользователях и группах в базе данных приложения RSA Authentication Manager синхронизирована со каталогом Microsoft Active Directory®. После успешной проверки подлинности пользователя RSA Authentication Manager передает его пароль в систему. Затем этот пароль передается контроллеру домена для завершения процедуры проверки и получения соответствующей квитанции от протокола Kerberos.

При работе в автономном режиме для проверки подлинности пользователя система сравнивает passcode пользователя с данными, хранящимися в специальном файле. Затем пароль передается ОС Windows для завершения процесса.

Система полностью совместима с политиками смены пароля. Система распознает, когда необходимо произвести смену пароля, и отображает диалоговое окно, содержащее уже заполненное поле с предыдущим паролем и поле для ввода нового пароля. Введенная информация передается в Active Directory и RSA Authentication Manager. Таким образом, пользователю не нужно запоминать свой пароль, при этом строго соблюдается политика смены паролей.

Интуитивно понятный интерфейс: пользователь нажимает комбинацию клавиш CTRL, ALT, DEL и в ответ на запрос вводит свой идентификатор и passcode, а не пароль. Эта информация отправляется в RSA® Authentication Manager, который вычисляет passcode и сравнивает результаты. В случае совпадения пользователю предоставляется доступ.

Расширенные возможности контроля

Законодательство о персональных данных и иные норматив но-правовые документы содержат требования об ограничении доступа к важной информации и необходимости проверки подлинности пользователей, имеющих доступ к этой информации. Решение Authentication Agents for Microsoft Windows позволяет отслеживать не только онлайн запросы, но и запросы пользователя, работавшего в автономном режиме, а затем вновь подключившегося к сети. Для этого производится считывание всех предыдущих операций, связанных с проверкой подлинности, и после очередной успешной проверки подлинности в сетевом режиме эта информация передается в RSA Authentication Manager.

Решение RSA Authentication Manager используется в виртуальных частных сетях, беспроводных сетях и Web-порталах, а также в среде ОС Microsoft Windows, оно выступает в качестве центрального хранилища данных аутентификации. Также RSA Authentication Manager располагает усовершенствованными функциями подготовки отчетов, ведет журналы учета аутентификации, отчеты о использовании систем и исключительных ситуациях.



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

The Security Division of EMC

©2004-2008 RSA Security Inc. Все права защищены.
RSA, RSA Security, enVision, SecurID и логотип RSA являются зарегистрированными товарными знаками или товарными знаками компании RSA Security Inc. на территории США и/или в других странах. Все прочие товарные знаки, упомянутые здесь, являются собственностью их законных владельцев.

SIDMS DS 0308