

RSA Authentication Agents for Microsoft® Windows®

Two-factor user authentication for the Microsoft Windows® environment

At a Glance

- Improves security for Microsoft Windows® environments
- Provides a simple, consistent sign-on method for users
- Lowers password-related help desk calls
- Reduces the need for password reset procedures and policies

RSA Authentication Agents for Microsoft Windows® software is an authentication solution that proves the identity of users before allowing access to the Microsoft Windows environment. RSA Authentication Agents for Microsoft Windows software enable customers to use the RSA SecurID® solution to authenticate Microsoft operating system users, whether they are online and connected to the corporate network or offline and logging on to their desktop. The solution provides stronger security than passwords, provides a simple method for users to sign on to the Windows environment, eliminates the need for password change policies and provides an audit log of all authentication events.

Strong, Two-factor Security

The RSA SecurID solution offers strong security by replacing passwords with two-factor user authentication. Each user is assigned a unique authentication device (token) that generates an unpredictable, time-sensitive number every sixty seconds. When prompted, the user enters their userID and passcode, which comprises a personal identification number (PIN), followed by the number displayed on their SecurID token at that moment. The combination of the user's PIN (something they know) followed by the correct code (something they have) is accepted as proof of the user's identity.

Ease of use, Consistent Log on Method

One problem facing users is the proliferation of passwords. To cope with the increasing number of passwords, users write them down or store them in a file – both of which lead to poor security practices. The problem is magnified by corporate policies that force periodic password changes and require users to select hard-to-remember character strings.

RSA Authentication Agents for Microsoft Windows provide the ability for the user to use the same authentication method – whether accessing a VPN, wireless network or protected web resource or when signing on to Microsoft Windows, online or offline. Because the authenticator produces a constantly changing value, it eliminates the need for password change policies and reduces the number of password-related help desk calls.

Online or Offline User Authentication

The user interface is intuitive. When an RSA SecurID user is signing on to a Microsoft Windows domain, after pressing CTRL, ALT, DEL they are prompted to enter their userID and passcode rather than a password. This information is sent to the RSA® Authentication Manager which calculates the passcode and compares the results before granting access.

After a successful online authentication, the RSA Authentication Manager prepares the client system for offline authentication. The Authentication Manager pre-calculates valid codes for a pre-determined number of days and sends those to the client system. When the user attempts to logon to their desktop offline, they are prompted for their userID and passcode. The RSA Authentication Agents for Microsoft Windows then compare this information to the store of valid codes and grants or denies access.





Seamless Integration with Microsoft Passwords

The RSA Authentication Agents for Microsoft Windows work in conjunction with Microsoft Windows domain controller and Microsoft Active Directory® directory service. The RSA Authentication Manager database synchronizes with Active Directory directory service for user and group information. When a user successfully authenticates, the RSA Authentication Manager delivers the user's password to the system. The password is then presented to the domain controller to complete the authentication process and the delivery of the Kerberos ticket.

In offline mode, the system compares the end user's passcode to the information stored in the local RSA SecurID pre-calculated passcode file to authenticate the user. The locally stored password is then presented to Microsoft Windows operating system to complete the process.

Password change policies are easily accommodated. The system recognizes when a password is to be changed and presents the user with a screen that pre-populates the old password field and asks for the new password. The information is then passed to both Active Directory directory service and the RSA Authentication Manager. In this manner, the user is never required to remember their Microsoft password while corporate password change policies are still accommodated.

The intuitive user interface: after pressing CTRL, ALT, DEL users are prompted to enter their userID and passcode rather than a password. This information is sent to the RSA Authentication Manager, which calculates the passcode and compares the results before granting access.

Robust Auditing Capability

Due to privacy laws and compliance regulations, companies are frequently required to limit access to sensitive information and prove who accessed the information. With the RSA Authentication Agents for Microsoft Windows, not only are the online requests captured, but when an offline user reconnects to the network all offline authentication events are captured and optionally uploaded to the RSA Authentication Manager upon the next successful online authentication.

Because the RSA Authentication Manager can be used in conjunction with VPN, wireless network and web access as well as the Microsoft Windows environment, it acts as a central repository for all authentication activity. The RSA Authentication Manager also offers a robust reporting tool to help generate audit logs, usage reports and exceptions activity.



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

The Security Division of EMC

©2004-2008 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Microsoft, Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

SIDMS DS 0308