SECURE COMPUTING

STRONG AUTHENTICATION
Product Overview

www.securecomputing.com

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.

SafeWord RemoteAccess

Benefits

- Positively identifies remote VPN, Citrix, and Outlook Web Access users
- Token-generated passcodes change every time you log in
- Integrates seamlessly with Microsoft Active Directory
- Experience an easy, fast installation: runs on existing servers
- Streamlined management and deployment

Applications protected

- All major VPN and RADIUS devices
- Citrix MetaFrame web interface for MetaFrame Presentation Server (NFuse 1.7 or higher)
- Citrix MetaFrame Secure Access Manager
- Outlook Web Access

SafeWord server requirements

- Can run on existing hardware used for Active Directory
- Windows 2000 or 2003 domain controller
- Active Directory populated with remote users
- 256 MB RAM minimum; 512 MB or above for configuring the Web Agents
- 300 MB disk space minimum; 3 GB disk space recommended

SAFEWORD REMOTEACCESS™

RAPB-01-B

SafeWord RemoteAccess

Eliminate the password risk

Positively identify your remote users

SafeWord® RemoteAccess™ provides a complete strong authentication solution specifically designed to protect remote user access to private networks and applications. SafeWord RemoteAccess secures connections to VPNs, RADIUS-compliant devices, Citrix applications, and Outlook Web Access. With tight integration and simplified management through Active Directory, and with tokens that generate new passcodes with every user login, SafeWord RemoteAccess lets you easily and cost-effectively eliminate the password risk.

Passwords are the weakest link in your security

Increasingly, remote users are accessing networks and applications from anywhere in the world, and the most common way to identify these users is with only a password. But relying on passwords for security makes your network easy to break into. Passwords can easily be hacked using a wide variety of attacks, including sniffing, brute force attacks, dictionary attacks, personal information gathering, or simply tricking users into revealing their passwords. Industry experts estimate that 35 percent of corporate network passwords can be hacked within five minutes.

Conventional wisdom says passwords should be made more complicated (one government agency has a password policy that's 30 pages long!), but even the strictest password policy can be undermined by a simple Post-it. The practical reality is that complex passwords are harder to remember and more likely to be written down, taped to monitors, or hidden under keyboards. Or your users may just forget their complex password, causing your help desk costs to soar.

Strong authentication protects trusted connections

SafeWord RemoteAccess provides strong authentication—a simple and effective way to eliminate the risks of passwords for access to your VPNs, RADIUS devices, Citrix applications, and Outlook Web Access.

To understand strong authentication, think of your ATM card. When you withdraw money from your bank you use a combination of two security factors—something you have (your card) and something you know (your PIN). You probably wouldn't want your bank to allow withdrawals with just one of these factors, yet many application deployments that protect extremely valuable data, proprietary information, and mission-critical applications are protected by only one factor—a weak password.

SafeWord RemoteAccess delivers the extra security needed with tokens that generate new passcodes for every user login. Each user is assigned a token that can generate millions of unique codes based on an internal secret key. To log into your trusted applications, the user simply pushes a button on the token to generate the next one-time code, then enters this code along with a short memorized PIN.

The robust SafeWord authentication server verifies each token-generated passcode, allowing access only to users with valid codes and PINs. After being used once, a one-time passcode is then useless, eliminating the risk of outsiders stealing, copying, or reusing passwords. The combination of dynamic codes and two-factor authentication provides unbeatable security.

SafeWord tokens generate new passcodes for every user login

Simple management without redundant user accounts

SafeWord RemoteAccess installs rapidly and can be run on servers you already have in your network. Where other authentication systems may require extensive training, additional hardware, and complex configuration, SafeWord RemoteAccess can be set up in minutes.

SafeWord RemoteAccess provides unprecedented ease of management compared to other authentication products because the product utilizes existing user records in Active Directory. There is no need to create redundant user accounts in a separate database, saving administrative time and money.

Installing SafeWord RemoteAccess is quick and easy

In fact, SafeWord RemoteAccess is managed entirely through a plug-in to the Microsoft Management Console (MMC), allowing you to easily assign tokens to your remote users, manage user PINs, import token records, generate emergency backup passwords, and test tokens.

SafeWord RemoteAccess also simplifies strong authentication for your Citrix and Outlook Web Access users with a single login screen, adding a field for token-generated passcodes.

Dramatically reduce the time and cost of deployment

SafeWord RemoteAccess greatly simplifies the process of deploying tokens to your end-users. The embedded User Center allows your users to self-enroll their tokens, manage and update their PINs, and test their tokens. This optional self-enrollment capability can save your organization more than 80% of the costs typically associated with assigning and distributing tokens.

Users can enroll themselves in the User Center

Requirements

SafeWord RemoteAccess protects VPNs, RADIUS devices, Citrix MetaFrame applications (including web interface, Secure Access Manager, Presentation Server, and Password Manager), and Outlook Web Access. SafeWord RemoteAccess requires that users be managed through Active Directory, and its components can be installed on the Active Directory domain controller and the other servers already in your network.

Do you need additional features?

If you need to protect access to Web, wireless, or legacy systems, if you need a wider range of authentication options, or if you need more powerful features such as role-based authentication, consider Secure Computing SafeWord® PremierAccess™. An award-winning strong authentication and access control solution for enterprises, PremierAccess provides unparalleled flexibility, powerful access control features, and many authentication choices including hardware tokens, software tokens, smart cards, digital certificates, biometrics, and MobilePass®, which sends one-time passcodes to your cell phone or pager.

For more information on all Secure Computing products, please visit *www.securecomputing.com.*

SECURE® COMPUTING

www.securecomputing.com

Web site

For more information about SafeWord, please visit *www.safeword.com.* To order product evaluations, please visit *www.securecomputing.com/goto/safewordeval.*

Secure Computing Corporation

Corporate Headquarters
4810 Harwood Road
San Jose, CA 95124 USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100
Fax: +1.408.979.6501

European Headquarters
East Wing, Piper House
Hatch Lane
Windsor SL4 3QP UK
Tel: +44.1753.410900
Fax: +44.1753.410901

Asia/Pacific Headquarters
Hong Kong
1604-5 MLC Tower
248 Queen's Road East
Wan Chai Hong Kong
Tel: +852.2520.2422
Fax: +852.2587.1333

Japan Headquarters
Level 15 JT Bldg.
2-2-1 Toranomon Minato-ku
Tokyo 105-0001 Japan
Tel: +81.3.5114.8224
Fax: +81.3.5114.8226