



STRIKEFORCE TECHNOLOGIES, INC.

ProtectID 2.2.3

Strong Authentication solution that protects identity of Users

BENEFITS

- Highest level of Authentication.
- Lower system cost.
- Easily integrates with existing or future systems.
- Multiple authentication choices.
- VPN users can be authenticated by highly secure mechanisms.
- Corporate networks (LAN, WiFi, WAN) can be made more secure.
- CITRIX networks can have greater security.
- SSO systems can be secured by two factor authentication.
- Authentication Redundancy.
- Authenticated Password Reset.

AUTHENTICATION SUPPORT

- Out-of-Band Authentication (Credentials entered into OOB channel)
 - Phone/PIN
 - Phone/OTP
- Out-of-Band Authentication (Credentials sent to OOB channel)
 - Phone/SMS
 - Phone/Voice OTP
 - Email/OTP
- Soft Token Authentication (OATH compliant)
 - BlackBerry OTP client
 - Windows OTP client for PCs
 - J2ME client for phones
- Hard Token Authentication (Key Fob)
- Capable of supporting biometrics (fingerprint, iris)

HOST OPERATING SYSTEMS

- Windows Server 2003
- Windows Server 2008

CLIENT OPERATING SYSTEMS

- Windows XP
- Windows Vista
- Macintosh
- Unix/Linux

INCLUDED COMPONENTS

- ProtectID Platform with Phone voice and PIN authentication
- Desktop Soft Token

PROTECTID INTEGRATED SUPPORT FOR:

- Radius
- Web Applications
- Citrix Agents – Secure Access Manager, Citrix Access Gateway
- Outlook Web Access - Form Authentication
- Oracle's Siebel CRM
- Oracle's PeopleSoft
- Oracle's OAAM
- Linux / Unix (PAM)
- Cisco Secure Access Control System
- Windows Desktop Login (GINA)
- CA Siteminder
- RSA Cleartrust
- Microsoft ISA Server

APPLICATIONS

- Online Banking Compliance for Retail Access (FFIEC, Red Flags)
- Online Financial Services Access
- Corporate Portal Access
- Enterprise Authentication
- Healthcare System access
- E-commerce
- Government agencies
- Homeland Security



STRIKEFORCE TECHNOLOGIES, INC.

ProtectID 2.2.3

Strong Authentication solution that protects identity of Users

Agent Interfaces

When a user attempts to access their system or application from their client device through a network, the ProtectID Agent captures the username and sends an authentication request to the ProtectID Server where the authentication functions are performed

- **Web Agent:** To secure web servers.
- **RADIUS Agent:** To secure systems that use RADIUS for authentication, such as, RAS servers, VPN servers, Oracle, Novell and 802.1x wi-fi LANs. Also, Solaris, Linux, HP-UX, MacOS and AIX can be secured via RADIUS.
- **Citrix Agent:** Add strong authentication for remote access to Citrix application servers.
- **GINA Agent:** Add strong authentication to Windows Desktop access.
- **ISA Agent:** Add strong authentication for SSL VPN access to SAP, Sharepoint, Outlook Web Access, etc.
- **ISAPI Agent:** Add strong authentication to IIS based web pages and applications.

Administration Function

This includes user provisioning and other administrative functions. There are three ways to register users:

- *Via the ProtectID Manager*
- *Self-Provisioning*
- *Active Directory Sync*

Audit Control & Logging

This function produces online information and monitoring of all accesses of the system as well as the authentications. Appropriate reporting that is necessary in managing registrations and the utilization of the ProtectID system is also produced through this function.

ProtectID APIs

ProtectID APIs are available for integrating into customer applications (HTTP & XML interfaces) as well as provisioning (HTTP interface).

DEPLOYMENT OPTIONS

- Small customer configuration – i.e. “ProtectID in-a-box”. This includes all the ProtectID functionality in a single Windows Server. This is ideal for small customers or evaluations.
- Large customer configuration – The ProtectID components can be distributed on multiple servers and can include redundant configurations for reliability. This is suitable for customers with multiple locations.
- Service Provider configuration – This configuration is suitable for companies that want to offer ProtectID as an authentication service. These could be telcos or managed service providers. The business model can be billing on a monthly basis or per transaction basis.
- ASP configuration – This configuration is suitable for companies that want to use ProtectID as an authentication service but do not want to host it themselves. The business model can be billing on a monthly basis or per transaction basis.