v-GO® am™

Any authenticator to any application with no integration
Support for multi-authentication • Support for graded authentication • Easy to deploy and administer

Security does not thrive on passwords alone. While still functional, passwords fall short of providing truly secure data protection as required by an increasing number of organizations. More and more businesses and government agencies are turning to strong authentication methods, such as smart cards, biometrics and tokens, to fulfill their data-protection needs.

But these devices pose an integration and administration challenge for organizations, especially for those that don't want to be locked into a particular vendor or technology. The cost, effort and complexity of deploying even one strong authentication solution can dissuade many organizations from even attempting it. Furthermore, many organizations actually want to mix and match several different user authentication technologies as their needs dictate.

The ideal solution for these organizations is v-GO Authentication Manager, a robust authentication management solution that enables organizations to advance their authentication initiatives. By acting as a mediating layer between authenticators and v-GO Single Sign-On, v-GO AM enables any authenticator to work with any application. On the user authentication side, v-GO AM interfaces to all of the leading authentication devices, either natively or through market-leading middleware technologies. On the application side, v-GO AM works with v-GO SSO, which signs on to all applications. v-GO SSO accepts user authentication from any supported device via v-GO AM, and signs on to any application using the appropriate user ID and complex password.

Support for Multi-Authentication

Many organizations would like to use different authenticators for different user groups or locations. For example, they may wish to deploy tokens to their remote users, smart cards to their corporate office users and passwords to their contractors - all to access some of the same applications. With v-GO AM, there is no incremental cost or effort to accomplish this. Because v-GO SSO provides a common interface to applications and v-GO AM interfaces to all of these authenticators, setting a few configuration switches in the v-GO AM Console is all that is required to deploy all of these authenticators to various user groups.

Support for Graded Authentication

Consider this common scenario: A user who typically accesses a corporate network through a smart card or biometric device forgets her card one day or injures her hand so that it won't be recognized by a fingerprint scanner. With v-GO AM, the user may still access some applications with a password, though she will be locked out of applications requiring strong authentication. Which applications she may use was decided by a system administrator empowered by v -GO AM to control which applications users may access with which authenticator.

Easy to Deploy and Administer

v-GO AM is easy to deploy and configure, requiring no user involvement to get it up and running. Standard software deployment tools can be used to push out the client components that add on to v-GO SSO. v-GO AM's intuitive and easy to navigate administration console is used to configure the minimal required settings.

The console's highly functional interface gives administrators control over which applications users can access with which authenticators, as well as which functions of v-GO AM they may execute based on the type of authenticator. This high level of control ensures that users have as much access as makes sense to applications they need despite their location and authentication method, while giving organizations an unsurpassed level of data protection best suited to their requirements.

Administrators have the options of setting default user authenticators, allowing and disallowing the use of multiple authenticators. They also may allow or disallow the use of multiple authenticators interchangeably during a single session and between sessions. Through the management console, administrators have the ability to audit who accesses what application with which kind of authenticator, and keep records of failed strong authentication requests. In addition, v-GO AM extends v-GO SSO's event log to report the authenticator name, authenticator status and grade level for each logon event.

v-GO Authentication Manager

Authentication Options

v-GO AM integrates with most authentication methods and provides support for both primary login and re-authentication requests (i.e. forced re-authentication, session time-out or application specific authentication request) for both connected and disconnected use.

Strong Authentication

- Full support for any MS CAPI CSP compliant smart card, such as Gemplus and Schlumberger cards
- Full support for Entrust Entelligence, which uses PKI cryptographic services for key encryption
- Support for biometric devices via the SAFLINK interface
- Full support for RSA SoftID, automatically generates and submits the one-time passcode and PIN
- Full Support for biometric devices integrated into the SAFLink platform
- Full Support for Ensure Technologies XyLoc proximity cards
- Full Support for Digital Persona fingerprint authentication system

Central Administration

Console GUI based Administrative Console provides configuration and control over AM settings and authenticators, including:

- Allow or disallow the use of multiple authenticators for users.
- Specify which authenticator is the default primary authenticator.
- Specify which authenticators are required for enrollment and which are optional.
- Restrict access to specific applications based upon the assigned grade-level of the authenticator used.
- Allow or disallow the use of multiple authenticators interchangeably for initial logon and subsequent authentication events.
- Enable graded authentication support to be turned on or off.
- Configure graded authentication on a per-application basis.

Deployment

- Deploys using most deployment tools - Windows Installer (MSI), SMS, Tivoli, Zenworks, Novadigm, etc.
- Configurable First-Time-Use to set-up authenticators; authenticators can also be set up post FTU
- Settings centrally configurable and adjustable
- Fully integrates with v-GO Session Manager

Event Logging & Reporting

- Administrator controlled logging of user v-GO AM events and activities including successful and failed logons, and the grade level in which the attempt was made
- Log events to the Windows Event viewer, an XML file, or support virtually any other method via Event API
- Generate usage reports based on user object detail

Minimum System Requirements

AM Client Agent

- Microsoft® Windows® 2000 (SP1+), XP (SP1 or SP2), Server 2003
- 120 MHz Pentium processor and 64 MB RAM
- Disk space: a complete Installation requires ~1 MB
- Internet Explorer 6.0 or higher with 128-bit encryption
- Citrix MetaFrame support requires MetaFrame 1.8 or higher
- Installation via MSI package requires Windows Installer 2.0 or higher
- Strong authenticators likely have their own system requirements, which may differ from v-GO AM's requirements. Please refer to the strong authenticator's documentation to review the system requirements.

AM Administrative Console

- Microsoft® Windows® 2000 (SP1+), XP (SP1 or SP2), Server 2003
- 100 MHz Pentium-compatible processor and 64 MB RAM
- .NET Framework 1.1
- Windows Installer 2.0 or higher
- Disk Space: ~4 MB for MSI installer; ~31 MB for EXE installer, overall ~15 MB for the installed program and data
- Directory requirements: Active Directory, SSun Java System Directory 5.1 or higher, Novell eDirectory 8.5 or higher, or other LDAP v2/v3 compliant directory

Zvetco Biometrics; 6820 Hanging Moss Rd. Orlando FL, 32807
www.zvetco.com; 407-681-0111