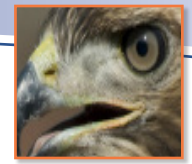




Speed Access



Enable Business



Extended Enterprise



The Last Strong Authentication Software You Will Ever Need To Buy

v-GO® Universal Authentication Manager™

Many organizations want to deploy stronger two-factor authentication for Windows logon to improve security and support regulatory compliance efforts, but are deterred by the cost and complexity of most solutions that often times locks-them into a single form of strong authentication. v-GO Universal Authentication Manager (v-GO UAM) eliminates these concerns with an open architecture that supports any authentication device, use of the organization's existing back-end network infrastructure, and easy end user logon.

v-GO Universal Authentication Manager quickly and securely authenticates users to the Windows network (and, optionally, to v-GO Single Sign-On) with any authentication device from any vendor. Organizations that are already using building access badges, government-issued citizen identity cards, OTP tokens or laptop biometric readers can now use those same devices – or any combination - for Windows logon. Organizations without existing strong authentication technology can choose the best device or devices for their environment with assurance that they can be used for network access.

How it Works:

To authenticate to Windows with v-GO Universal Authentication Manager, a user simply presents their authentication device to the workstation and v-GO Universal Authentication Manager does the rest. For example, a user who has a door access badge simply taps the badge on a badge reader attached to their computer and enters a PIN code. v-GO Universal Authentication Manager retrieves the user's logon credentials from Microsoft Active Directory and compares them on the client. If they match, v-GO Universal Authentication Manager provides Windows with the information needed to log that user on. Another tap of the badge locks the workstation or logs the user off.

The use of Microsoft Active Directory for data storage and administrative policies eliminates the need for proprietary authentication servers. This lowers costs as well as avoiding the administrative overhead associated with managing a separate strong authentication infrastructure.

v-GO Universal Authentication Manager Benefits:

Fast, Secure Windows Authentication

Many organizations want to increase the security of their Windows networks by replacing Windows passwords with two-factor authentication. The problem is that increased security usually slows and complicates authentication, leading to frustrated end users and failed deployments. v-GO Universal Authentication Manager overcomes this barrier with a fast and simple user logon process that also increases data protection for organizations that must comply with regulations such as HIPAA, PCI DSS and FISMA.

Leverage Existing Authentication Devices

Many organizations already have authentication devices such as door access badges, government-issued ID cards, and built-in laptop biometric readers. However, Windows doesn't natively accept these devices for logon. v-GO Universal Authentication Manager solves the problem by allowing virtually any authentication device to be used for accessing Windows. This allows organizations to deploy strong authentication to Windows without incurring the expense of buying and issuing new authentication devices for every user.

Use Multiple Device Types Simultaneously

No single form of strong authentication will meet the needs of all users in an organization. Fingerprint authentication might be a great solution for many departments, for example, but it would not work for employees who wear gloves. v-GO Universal Authentication Manager is able to utilize and manage all forms of authentication through one framework. This allows organizations to choose the right authentication technology for each user environment. It also provides a way to audit all authentication events, regardless of the technology used, from one resource.

Reduced Cost and Administration

Most strong authentication deployments require a separate infrastructure with proprietary servers. Disaster recovery and failover plans are also required to ensure that users are able to gain access to their workstations at all times. v-GO Universal Authentication Manager removes both the cost and administrative burden of a proprietary server by leveraging the organization's existing Active Directory for data storage. This provides a highly scalable solution without the need to manage another authentication infrastructure.

v-GO Universal Authentication Features

- Logon
 - Simple steps to logon: insert, swipe or tap, and type PIN
 - Same card used to authenticate to v-GO SSO and all applications
- Workstation Auto-Lock
 - Remove or tap card to lock workstation
 - Inactivity timer locks workstation
- Enrollment
 - Client side “in the flow” user enrollment
 - Enforce enrollment during computer logon
- Security Policies and Settings
 - Configure allowed authentication methods
 - Enforce enrollment in any logon method
 - Manage and configure client settings and behavior
- Credential Management
 - Centrally view and manage user credentials
 - PIN policy management
 - Leverage existing Active Directory for centralized data storage
- Auditing
 - Capture detailed authentication events
 - Workstation Logon
 - Workstation Unlock
 - SSO Authentication
 - Redirect events to other systems
- Seamless Integration with v-GO SSO

v-GO Universal Authentication Manager System Requirements

- v-GO Universal Authentication Manager Client
 - Microsoft® Windows® XP Professional (SP3)
 - RAM and Processor - Minimum: 256 MB RAM and 1 Ghz processor
- v-GO Universal Authentication Manager Administrative Console
 - Microsoft® Windows® XP Professional (SP3)
 - Microsoft Windows Vista Business Edition SP1
 - Microsoft Windows 7 Enterprise Edition
 - Microsoft Windows Server 2008, 2003 SP2
 - 100 MHz Pentium-compatible processor and 64 MB RAM
 - .NET Framework 2.0
 - 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 Support
 - Microsoft Active Directory

