



Speed Access



Enable Business



Extended Enterprise



Increase security • Demonstrate compliance • Improve operation efficiency

v-GO® Shared Accounts Manager™

v GO SAM provides quick and secure access to systems and applications for administrators, temporary workers, and others who must share account IDs. v GO SAM plugs a significant security and compliance hole commonly found with shared accounts—accountability. Because v GO SAM automatically ties actual users to shared IDs, enterprises, for the first time, know who is using what shared account and when.

Improve Security and Compliance Demonstration

Managing shared IDs—including system-defined accounts for operating systems, network devices, and databases—is a security and compliance challenge. It is impossible to account for who is using the shared ID and when, exposing the enterprise to security breaches, privacy risk, and compliance risk. Privileged account passwords are routinely shared by system administrators. Users can steal, change, or delete data, and it is impossible to pinpoint the culprit. Even an inadvertent act can cost an enterprise millions in damages and brand reputation.

v GO SAM enables users to check out shared IDs, each of which is uniquely associated to a specific user for its duration of use. Shared credentials can be securely stored and retrieved, with the needed authorization and usage tracking to improve security, increase accountability, and reduce compliance exposure.

Authorized administrators can set policies to control usage of shared IDs (for example, IDs can only be used to log on once.) And because users never see shared IDs or passwords, there is nothing to share—inadvertently or maliciously.

Only v GO SAM provides this level of security, accountability, and tracking, previously unattainable for shared accounts.

Demonstrate Compliance More Effectively

Using shared IDs presents a significant compliance challenge. Most regulations either prohibit or strongly discourage the use of shared IDs, yet many systems and databases force you to use them (for example, “root” accounts in Unix.) v GO SAM meets this challenge head-on, enabling you to assign shared IDs to each user and track their use. With credit card processing, for example, merchants and service providers can now easily demonstrate that each user accessing system components or cardholder data is identified by a unique user name (the user using the shared ID) —a key requirement of PCI DSS.

Improve Operational Efficiency

Managing shared accounts impacts operational efficiency as well. Ensuring that all hard-coded passwords are changed in a coordinated fashion places undue burden on the IT staff. And, with error-prone manual processes, the risk of operational failure increases significantly.

v GO SAM enables organizations to manage conventional and shared credentials with one strategy and infrastructure, improving operational efficiency. v GO SAM allows organizations to use their existing enterprise single sign-on (ESSO) infrastructure, and optionally an identity management system, to address the challenge of privileged account password management and compliance, rather than buying a separate hardware or software vault system to administer shared accounts.

Provide Fast, Secure Application Access for Temporary Workers

Many organizations keep a pool of IDs and passwords available for temporary workers. With no realistic way to track which shared ID is used by whom and when, the enterprise is exposed to significant security and compliance risk.

v GO SAM provides quick and secure application access for temporary workers and contractors who must use shared IDs. Just as it does for internal shared account users, v GO SAM allows temporary workers to check out IDs, each of which is uniquely associated to a specific user for its duration of use. Authorized administrators can set policies to control usage of shared IDs (for example, IDs can only be used to log on during a specified period.) And because users never see shared IDs or passwords, there is nothing to share—inadvertently or maliciously.

Because v GO SAM automatically ties and tracks each temporary worker to applications usage, enterprises, for the first time, know which contractor is using what shared account and when, delivering the accountability, security, and audit trail previously unattainable.

How it Works

A user requiring access to a privileged account makes an online request to check out a specific username and password. The request is approved or denied based on the user's role and group membership in the corporate directory (for example, Active Directory) or an approval workflow in the enterprise's identity management system. The system then issues the username and password to the user subject to policy-based usage controls, such as a two-hour credential expiration or a one-time use of the credential.

The ID and password, the associated authorization profile, and expiration information are all granted and tracked by v GO SAM. When the user accesses the desired system, v GO SAM automatically logs the user on. When the defined usage period expires, the username and password are automatically deleted from the user's credential store and checked back in to v GO SAM. Usernames and passwords can only be checked out to one user at a time, establishing a single point of accountability for all activity on the target application.

v-GO Access Accelerator Suite

v GO SAM is part of the Passlogix v GO Access Accelerator Suite. The v GO Access Accelerator Suite speeds access to systems and applications for users throughout the extended enterprise and drives out complexity at critical points in sign-on, authentication, and provisioning processes.

v-GO SAM enables organizations to manage shared credentials without needing a dedicated vault system. V-GO SAM leverages Passlogix's proven technology so that application passwords can be securely shared by multiple users, such as system administrators who must access privileged accounts, workgroup members who must share a pool of generic accounts, and temporary worker or contractors who must be issued temporary, generic accounts. v-GO SAM works in conjunction with v-GO Single Sign-ON (v-GO SSO) and v GO Provisioning Manager (v-GO PM).

Administration

Use v-GO SSO to create shared account templates for applications

Use the v-GO SAM interface to:

- create shared accounts
- create strong policies to govern use of the accounts
- change shared account passwords
- force check out and check in shared accounts for users

Command Line Interface

v-GO SAM offers a CLI that enables administrators to:

- check out shared accounts
- check in shared accounts
- request changes to shared account password

Repository Support

v-GO SAM works with Microsoft Active Directory and Microsoft Active Directory Application Mode.

Deployment

- v-GO SAM utilizes Windows installer technology.
- The v-GO SAM Client can be deployed using v-GO On Demand Edition (v-GO ODE). (The v-GO SSO Agent and the v-GO PM Client can also be deployed using v-GO ODE.)

System Requirements

v-GO SAM Server

Minimum Configuration:

- Microsoft Windows Server 2000 (SP4), Windows 2003 Server (SP1)
- 512 MB RAM (minimum) and 1 GHz processor; 2 GB RAM or greater and 2 GHz or faster process (recommended)
- Disk Space: a complete installation requires up to 10 MB
- Microsoft Internet Information Server (IIS) 5.0 or later (6.x is recommended)
- Microsoft .NET Framework 2.0
- Microsoft Active Directory or Microsoft ADAM
- Internet Explorer 6.0 or higher with 128-bit encryption
- Installation via an MSI package that requires Windows Installer 2.0
- v-GO SSO 6.0 Rollup G
- v-GO PM Server 7.0

v-GO SAM Client

Minimum Configuration:

- Microsoft Windows 2000 (SP4), XP (SP2), Vista
- 256 MB RAM and 1 GHz (minimum); 512 MB RAM and 2 GHz processor (recommended). For Microsoft Vista, minimum RAM is 512 MB; recommended RAM is 1 GB.
- Disk Space: a complete installation requires up to 1 MB
- v-GO SSO 6.0 Agent
- v-GO PM 7.0 Client



75 Broad Street, Suite 815, New York, NY 10004

Tel: 212.825.9100 x 2 or 866.727.7564 x 2

Web: www.passlogix.com

Fax: 212.825.0326 Email: sales@passlogix.com

Copyright. © 2008 Passlogix, Inc. All rights reserved. All trademarks, trade names, service marks and logos herein belong to their respective companies. SAM100608