General Management Interface

System Overview and Description.

General Management Interface Foundation

http://www.gmi-foundation.org

Introduction to the GMI System

The GMI (General Management Interface) system is a protocol, agent system, API, and standard set of command line utilities that permits a user to query and control a remote platform. The system includes a simple but effective security model based upon passwords and "IP Allow Lists". Agent functions are provided by remotely uploading and installing new software modules herein called "Apps" or "Applications") to extend the range of functions.

The GMI system is intended to satisfy several chronic problems within industry.

- The GMI system permits a single "master" agent to be responsible for all control and monitor functions of a platform, reducing the proliferation of different agent interfaces and consoles to a single slim agent.

- The GMI system provides a very simple API that allows other developers and organizations to create and deploy new application software to the agent.

- The GMI system provides a secure way of managing and monitoring a platform based upon verifiable security algorithms (such as AES-256, or user supplied encryption methods.)

- The GMI system reduces system complexity and cost of ownership by enforcing a consistent and simple command set, API, and operating principles that do not restrict the flexibility of the system to perform complete infrastructure management.

- The GMI system provides an open-source community of developers that extend the usefulness of the agent program without sacrificing security, promoting alternatives in implementation designs and styles that are necessary for conformance to a wide range of user needs.

In brief, GMI is intended as a full featured "end-point management" system, furnishing to users a simple method of managing all activities that may be necessary by an organization (given proper support by existing or new Apps, available as open source or for profit software.) The above concepts are discussed in more detail within the paragraphs that follow.

GMI Agent Program

The GMI interface is completely contained within a single agent program that operates as a service on Windows platforms. The agent accepts signed Apps from an end-user. This capability extends the range of agent functions to include any program that can be executed by the platform.

Typical functions of the agent may include:

- **Control Functions.** The agent permits the end-user to issue control functions with authentication, such as starting and stopping processes, installing software, running specific (or general) programs. The particular control functions are provided by Apps that are uploaded by the end-user.

- **Performance Monitor Functions.** The agent permits the end-user to query performance parameters of any type with authentication. This permits the agent to serve in a capacity similar to traditional SNMP agents or other performance monitor agents.

- **Software Deployment Functions.** The agent permits the end-user to upload and install third-party software, issue remote commands, and perform those functions typically executed by remote software installation and deployment.

- **Scan Support Functions.** The agent is designed to permit fast scanning operations by a central manager, such as to determine the platform with the highest CPU, most disk space, or support system wide search and control functions.

- **Alerting Functions.** The agent includes an alerting function that permits Apps to send alerts via syslog, run applications at scheduled intervals and log the success or failure of scheduled operations. The particular alerting functions are arbitrary, and supplied by Apps that are upload by the end-user.

- **Other Functions.** The agent provides many other applications for both general purpose and highly specific use cases. Any process or service can be interfaced rather simply to the agent program via a simple wrapper. In some cases, many different Apps may be available for selection by the end-user. Other functions may include asset management, user management, change management, security monitoring, power management, etc.

The actual GMI Agent itself is specifically designed for ease of deployment, small footprint, low network bandwidth, low-memory utilization, low-CPU utilization, and high security. The agent is designed to be as simple and non-intrusive as possible, consisting of a single executable program and service entry.

GMI Apps

Once the agent is installed at a site, the end-user can upload and install applications (referred to in the context of GMI as "GMI Apps" or simply "Apps".) Each application opens additional directories and controls for a specialized purpose necessary for the end-point management strategy.

GMI Apps conform to certain strong principles that promote ease-of-use and security, as follows:

- **Remote Installation and Uninstallation.** Apps can be remotely installed, updated, or uninstalled from the centralized manager. Therefore, each GMI Agent contains just those functions that may be necessary for the management strategy, and each App is easily maintained and upgraded over its entire life cycle. This promotes good ROI for any site that installs the agent.

- **Consistency in Usage.** All GMI Apps are interoperable with all GMI command programs, permitting easy scanning, alerting, monitoring, and control of a managed infrastructure in a manner consistent with the entire GMI program philosophy. This shortens the learning time for any App, and leverages existing knowledge base of any organization supporting GMI.

- **Description Document.** The GMI specification requires all GMI Apps to have a "Description Document" (often referred to as a "DD"), which consistently documents all virtual folders, paths, functions, data types needed to fully document the agent. This consistency of design and documentation makes it easy to understand the purpose and intent of an application necessary for the end-user to deploy the application across possibly thousands of agents.

- **App Certification.** The GMI specification promotes a "Certification" principle, where each App must be given to a certifying authority, so that the responsible developer of the application can be tracked back. Not only does certification enforce a minimum quality and conformance standard, but also greatly contributes to the security of the application's usage (since the developer cannot be an anonymous hacker.) The result is more reliable and secure operation.

The precise functions of any GMI App is documented by the GMI Application "Description Document" (sometimes casually referred to as a "GMI DD") This document is required for the GMI certification process, and furnishes a description of all folders and objects supported by the application, and is a good starting point when considering a GMI App for deployment.

A variety of GMI Apps are free for general usage, with more Apps developed every day through open source initiatives. Additionally, fully supported and commercial Apps are available through a variety of vendors and independent developers.

GMI Application Program Interface (API)

What makes the GMI agent philosophy so viable is that it is extremely easy to get started with, due to a straightforward API. The agent program creates a series of "Virtual Directories", where each directory is traversed using traditional and familiar "cd" commands, and accessed by "ls" or "set" commands. The GMI Application Program Interface simply connects to the agent (with possible authentication required) and issues this basic command set to get values, fetch values, or initiate tasks.

The API includes elements such as a command line tool, an XML tool (for easy integration into web pages using AJAX) as well as elements to support C / C++ programmers. In most cases, a developer can tap the data in the agent through any number of techniques. Some Apps, such as the "rshell" application, include additional APIs (in this case the "rshell.exe" program) These stand-alone programs further extend the range of usable functions provided by the installed agent.

GMI System Security

The GMI agent includes multiple features to support and promote good security, as is required given the substantial power over and end-point device that the agent provides. These security features include the following.

- **Encryption of Transmission.** All agent transmissions are encrypted using a high security algorithm. The agent comes standard with a pseudo-one-time pad type algorithm. This encryption capability can be substituted by the end-user for other encryption methods, depending on the user locale.

- **Encryption of Data Files.** The agent program writes any data to the disk using a separate encryption algorithm, completely encrypting any data that may be uploaded or added to the agent program.

- **IP Allow List,** The agent uses an "IP Allow List" that restricts communication with the agent program to a small set of devices. Any device that attempts to communicate with the agent, and which is not in the include list, is silently rejected. The IP Allow List is automatically built based upon access to the agent prior (prior to setting a security mode, described below.)

- **Support for Passkeys.** The agent employs a single encrypted passkey, executed in a "challenge / response" authentication system, which limits communications with the agent to end-users that know the passkey. Any end-user that does not know the passkey is silently rejected.

- **Support for Different Security Modes.** The agent permits three types of security based upon the above to capabilities: no security (for those sites working in a trusted environment); IP Allow List (to restrict access to a small set of devices); Passkey Access (to limit access to users with a passkey); Both IP Allow

List and Passkey authentication (the highest level of security provided by the agent.)

- **Log Capability.** The GMI agent program includes full support for standard syslog, permitting security managers to monitor access and issues related to each agent installation.

- **App Signing and Certification Process.** Fundamental to the GMI system is the concept of "signed applications", where only applications that have been certified by an authority can be uploaded to the agent. This provides a way to ensure that applications are supported, and that security issues that may arise can be easily traced back to a supporting organization. The user cannot upload an application that has not been signed. (See next section.)

GMI Application Certification Process

As a means of promoting further security, all GMI Apps must be digitally signed by a GMI certifying authority in order for these applications to be used at an agent site. (The agent, and command programs will reject any package that does not have a valid GMI signature.) Once an application is certified, it may be used at any GMI installation (given the conditions of the application itself.)

To certify a GMI App, the following elements are required:

- **Independent Verification of Identity.** The certifying authority verifies the author of the software, and verifies that the author's contact information is valid. Failure to provide a valid and verifiable identity prevents certification from going forward.

- **Verification of Basic Functionality.** The certifying authority verifies that the package will install correctly in the agent and will not cause obvious conflict with the agent performance and functionality. Generally, this is just a superficial test of the agent (but may be more rigorous at the request of the software author.)

- **Valid App Description Document.** The certifying authority verifies that the Application DD is valid, accurately accounts for all data items, and the basic functionality described by the agent is valid.

The above items are acquired by the certifying authority. Although the certification process does not necessarily ensure that the application will perform without fault, the certification system DOES verify the identity of the author, which prevents anonymous (and potentially malicious) insertion of software into a managed platform. Additionally, the certification process prevents gross conflicts, and ensures a consistent level of quality and conformality to the GMI system.

The GMI Foundation certifies GMI apps at no cost. Additionally, GMI partners are capable of certifying Apps for themselves and others. Users should contact the GMI Foundation for details.

Simplicity and Cost of Ownership

A chronic issue with industry is the proliferation of agent programs, and required background services. Often, to accomplish multiple activities, the end-user must resort to multiple agents and consoles, different management techniques, each with a high cost of ownership.

A typical example may include, executing on the same platform, a WMI agent, an SNMP agent, Anti-Virus protection, Application Services of different types, special software for remote updating and deployment of the system.

The GMI agent can both eliminate and consolidate existing agents into a central console that manages the installation, access, security and functionality of the platform. The end-user of the system manages the entire system with a small and uniform set of intuitive commands.

Importantly, the GMI system provides very easy entry into full "End Point Management" (EPM) and all the capabilities that includes. The end-user can quickly add or delete management and monitor applications, experiment with these applications, exchange old functions for new functions, upgrade modules, and architect full-blown strategies that may be highly specific to the organization.

Open Source Community

Finally, the GMI system provides a simple way for third-party users to add a wrapper to their existing service, so that a secure and flexible management interface, available to a wide variety of open source tools, is available for their product or service. This technique, which has been widely accepted for Mobile Devices, is generalized to the system infrastructure components of the organization.

About The GMI Foundation

The GMI Software consists of agents, utilities, documentation and API's intended to promote secure and flexible management of end-points. GMI fully supports Open Source Initiatives, and views its role as one of not-for-profit promotion of software to correct the endemic problems associated with system and software management. More information on the GMI Foundation is available at the following location:

GMI Foundation
http://www.gmi-foundation.org
mailto: info@gmi-foundation.org

About Our Technical Partners

Additional information on the GMI Software, including a selection of useful GMI Apps, as well as professional and support services, is available from various members of the GMI Foundation.

A central clearinghouse for GMI applications is provided by Vallum Software, LLC, which provide support, certification, and development solutions, as well as the "Halo Management System", based on the GMI agent. Visit the link below.

Vallum Software, LLC
http://www.vallumsoftware.com
mailto: info@vallumsoftware.com