GMI Agent

GMI Agent Description Document (DD)

General Management Interface Foundation

http://www.gmi-foundation.org

Program Description

The "GMI-Agent.exe" program is a general-purpose agent that executes on a managed platform. The agent program is accessed by manager programs, such as the "GMI-Cmd.exe" program (but also other programs, developed by third-parties)

The GMI Agent program provides a secure, reliable, and flexible method of managing a remote platform for a variety of purposes, in particular "end-point management" services, but also other functions such as remote control and software distribution.

Once the GMI Agent is installed, the administrator can upload GMI Applications (i.e. "GMI Apps") to the agent, thereby extending the range of agent functions. Each GMI App is certified (by an appropriate certification authority) to establish the identity of the App developer, helping to ensure that the agent software is traceable to its originator as a hedge against malicious hacking, and to promote support of third-party developers.

Overview information on the GMI system may be found in the "GMI Overview" documentation, available under a separate cover. Information on certification of applications, as well as developer libraries, may be found on the GMI Foundation website.

The document herein describes only the basic functions of the agent that exist in all installations, as well as general usage of the program.

Description of All Standard Agent Folders And Paths

The GMI-Agent program presents data to management functions as a series of virtual folders within the agent. These folders establish a "Management Information Base" (sometimes casually referred to as a MIB.) Each function is associated with a path that can be listed, set, uploaded and / or downloaded by a manager program such as GMI-Cmd.exe

The user can upload Apps to create new folders, each which may perform specialized control, performance, utility, or system functions. The precise functions of these applications are documented by a GMI Application "Description Document" (sometimes casually referred to as a "DD")

A "Description Document (DD)", such as the document herein, is a necessary part of all certified Apps, and will be available from the third-part Application developer and / or the GMI Foundation website. The "Description Document" will furnish the purpose, intent, usage, and syntax of all folders and objects supported by the application.

The following folders and paths furnish the "native" functions of the GMI Agent program, available with all releases of this version:

/control

(Folder) This folder is reserved for application developers interested in furnishing control functions to the agent, such as remote shutdown or re-initialization requests, or any application that can modify the state of the platform or a peripheral of the platform. By default, this path is empty unless a certified App has been installed in this particular path.

/install

(Folder) This folder contains information about the currently installed apps for this agent. Within this folder are various objects that an administrator can use to view the installed applications, and detect changes to the agent configuration. As new applications are uploaded an installed, references to these applications will be contained within this folder.

/install/BuildDate

(Read Only Time String) This object can be read by a management program, and indicates the build date and time of the GMI-Agent program, useful for tracking different versions and updates to the system. Note that this value applies only to the agent program, and not to individual Apps for the agent.

/install/InstallCount

(Read Only Gauge) This object can be read by a management program, and indicates the current number of installed applications for the agent. The value is useful for detecting when a change occurs in the agent. A GMI command program can periodically poll this value and determine whether the number of apps has changed, useful for managing the configuration of the agent program.

/install/LastChange

(Read Only Time String) This object can be read by a management program, and indicates the time that an application was last installed OR uninstalled for the agent. The time string is the weekday, along with time in the current locale of the platform. This object is useful for detecting when a package is installed at the agent. A GMI command program can periodically poll this value to see if an application has been installed or uninstalled at the agent. Whenever a new

application is installed or existing application is removed, this object value reflects the time of the operation.

/install/SiteIdent

(Read Only Text String) This object can be read by a management program, and provides a unique identifier of the site consisting of a checksum on the hostname, the date and time of the installation, and the installation-working directory. The value is mainly useful for licensing Apps that require a special key on a per-site basis. (The operator can send this "SiteIdent" value to a vendor, who can issue a license key for the specified site.)

/install/apps

(Folder) This folder contains a subfolder for each installed App on the system. Within the subfolder (at the relative path configured for the application) exists certification information for the application. The certification information includes (1) the original package name; (2) where the app is installed; (3) a text description of the app; (4) the certified author for the app; (5) the certified contact information for the app; (6) the app version string, and; (7) the certification date for the app. This information can be used to track which applications are installed, and where the applications reside in the hierarchy of folders.

/misc

(Folder) This folder is reserved for application developers interested in furnishing miscellaneous functions for the agent, such as file and data stores, or applications that have no well-defined category. By default, this path is empty unless a certified App has been installed in this particular path.

/perf

(Folder) This folder is reserved for application developers interested in furnishing performance monitor functions for the agent, such as network, application, and hardware monitors of any and all types. Often, these applications support only "list" functions to acquire data from the system. By default, this path is empty unless a certified App has been installed in this particular path.

/security

(Folder) This folder contains subfolders all related to the security of the agent, including the authentication mode, passkey, allowed IP access, and syslog interface for the agent program.

/security/IPAllowList

(Read Write Upload File Object) This object contains a list of IP addresses that work with the "SecurityMode" object described below. Each time the user connects to the agent, the IP address of the management program is recorded herein. Additionally, the user can "upload" a file of IP addresses to this object in standard hosts format (one IP address per line.) When the "SecurityMode" value is set to "2" or "3" (discussed below) the IP address list is no longer updated on connection. Instead, the IP address of the management program must match one of the values in the list, or the connection is silently rejected. This mechanism furnishes a simple and direct way of limiting access to the agent based upon the IP address of the connecting program.

/security/PassKey

(Write Only Text String) This object is the system passkey (i.e. password), used in conjunction with the "SecurityMode" object described below. When the "SecurityMode" value is set to either "1" or "3", a user must provide the passkey value when connecting to the agent, or the connection is rejected. Note that the passkey value can only be set and not read. If the operator forgets the passkey, or the passkey is not known (and the security mode is set to "1" or "3"), then the agent will be inaccessible and require re-installation. Therefore, normal caution should be taken when setting this value, to prevent agent lockout.

/security/PassKeyReadOnly

(Write Only Text String) This object is a second system passkey, similar to above, except the passkey permits only "read" access to the agent. If this particular passkey is used, then "set", "upload", "install", and "uninstall" functions (which modify the agent configuration) are rejected. Note that the "PassKeyReadOnly" value is only operable when the "PassKey" value is a non-zero length string, and the security mode value is either "1" or "3". Setting the "PassKeyReadOnly" value without first setting the "PassKey" value does not affect or enable authentication. (See "PassKey Data Item Description" section of this document for more information.)

/security/SecurityMode

(Read Write Integer) This object defines the security mode of the agent, ranging from 0 to 3 as follows: (0) indicates that anyone may read or write values to the agent; (1) indicates that a valid password is required to connect with this agent, where the password is set via the "PassKey" object above; (2) indicates that the connecting management program must be in the "IPAllowList", which is described above, and; (3) indicates that both the "PassKey" and "IPAllowList" objects are used to authenticate the connection. No other values are valid for a

set request. (See "Security Mode Data Item Description" section of this document for more information.)

/security/SyslogHosts

(Read Write Upload File Object) This object contains a list of IP addresses that will receive syslog messages based upon user access, and other errors. The syslog interface employs standard syslog protocol to send status information to end-users, in compliance with various security standards. The syslog interface is also available to the Agent API, so that developers can send syslog messages. By default, no syslog hosts are defined. The operator can read or set this value. Additionally, the operator can "upload" a file of IP addresses to this object in standard hosts format (one IP address per line.)

/security/stats

(Folder) This folder contains useful statistics for the agent. The folder contains a series of Counter and Gauge values that may be used to assess the current state of the agent, and detect when application programs (or malicious users) are issuing certain commands or invalid passwords.

/security/stats/BadMessageFormats

(Read Only Counter) This object counts the number of times that communication was attempted with the agent since agent startup, where the format of the received message was invalid or unrecognized. This value can increment due to port scanners, or due to attempts to hack into the agent program. If the value increments quickly, this indicates that a program that is probing the GMI-Agent TCP port. When this counter increments, an appropriate syslog message is generated and sent to the syslog hosts defined in the "SyslogHosts" file (described above.)

/security/stats/BadPasswords

(Read Only Counter) This object counts the number of times that a bad password was used with the agent since agent startup. The value is updated only if the SecurityMode setting (described above) is set to "1" or "3". If the value increments quickly, this indicates that a program is either misconfigured, or may also indicate a brute force password attack. When this counter increments, an appropriate syslog message is generated and sent to the syslog hosts defined in the "SyslogHosts" file (described above.)

/security/stats/CommandAttempts

(Read Only Counter) This object counts the total number of times that a command was received by the agent since agent startup. This value may increment quickly under high agent load. The counter provides a good indication of how busy the agent is, and how many times the agent is being accessed by command programs. Note that this object contains all command attempts, including failed attempts.

/security/stats/CommandFails

(Read Only Counter) This object counts the total number of failures in command execution, where a failure occurs for any number of reasons such as bad command syntax, improper or non-existent path references, or general issues with an application program. The value should not increment often. If the counter increments quickly, this may be caused by a GMI application being uninstalled at the agent. When the counter increments, an appropriate syslog message is generated and sent to the syslog hosts defined in the "SyslogHosts" file (described above.)

/security/stats/ConnectAttempts

(Read Only Counter) This object counts the total number of times that a connection attempt was received by the agent since agent startup. This value may increment quickly under high agent load. The counter provides a good indication of how busy the agent is, and how many times the agent is being accessed by command programs. Note that this object contains all connect attempts, including failed attempts.

/security/stats/ConnectFails

(Read Only Counter) This object counts the total number of connection failures, due to bad password, or connection attempts by IP addresses not in the "SyslogHost" file (described above.) The value should not increment often. If the counter increments quickly, this may indicate a brute force attack, or may be due to a command program that is using the wrong password to access the agent program. When the counter increments, an appropriate syslog message is generated and sent to the syslog hosts defined in the "SyslogHosts" file (described above.)

/security/stats/NumIPAllows

(Read Only Gauge) This object is the total number of IP addresses that are contained in the "IPAllowList" (described above.) A management program can determine whether new addresses are being added to the list by periodically

polling this value. The number will correspond exactly to the number of IP addresses that are allowed access to (or have accessed) the agent program.

/security/stats/NumSyslogHosts

(Read Only Gauge) This object is the total number of IP addresses that are contained in the "SyslogHost" file (described above.) A management program can determine whether new addresses are being added to the list by periodically polling this value. The number will correspond exactly to the number of IP addresses that receive syslog messages from the agent program.

/system

(Folder) This folder contains useful values that help identify the agent. The folder contains a series of Text values that can identify the agent program uniquely. Users of SNMP protocol will recognize many of these object names and values as the same found in the SNMP "system" Management Information Base.

/system/SysContact

(Read Write Text String.) This value contains the system contact information, an arbitrary string, that is frequently an e-mail address, a URL, a person or organization's name, or other information indicating who is responsible for the agent program and managed platform. The object has no value until set by a management program.

/system/SysDescr

(Read Only Text String.) This value contains a textual description of the agent platform. The value can include the full name and version identification of the system's hardware type, software operating system, and networking software. The value is useful for identifying the general type of platform.

/system/SysInfo

(Read Write Upload File Object.) This value can contain a brief or comprehensive description of the agent program configuration or platform. The value can be a single line of text, or an entire file that is uploaded to the agent. This object does not have a value until a management program sets or uploads information to the agent. If the operator uploads a non-text file, the object can be retrieved via a manager "download" command. The object is useful for storing ancillary information about the nature of the agent and managed platform of any type.

/system/SysLocation

(Read Write Text String.) This value contains the system location information, an arbitrary string, which is frequently the building, floor, grid number, rack number, or some other identification as to where the managed platform is physically located. The object has no value until set by a management program.

/system/SysName

(Read Only Text String.) This value contains the name of the platform. This is typically the DNS name, but may be any name assigned to the computer platform via its operating system. The value cannot be modified.

/system/SysTime

(Read Only Text String). This value contains the local time of the platform, consisting of the weekday followed by time in the currently set locale. This value is the time known to the platform, useful when synchronizing clocks or detecting clock errors.

/system/SysUpTime

(Read Only Integer.) This value is the number of seconds that the platform has been up. The value is set back to zero when the agent restarts. Because the agent is usually started with the platform, this value provides a reliable indication of when the platform was rebooted. In particular, a management program can poll this value, and determine when the platform has been rebooted (when the "SysUpTime" value is less than the current time.)

/util

(Folder) This folder is reserved for application developers interested in furnishing general utility functions for the agent, such as scheduler programs, database utilities, or other applications that are not specifically control and monitor applications, nor simple miscellaneous functions. By default, this path is empty unless a certified App has been installed in this particular path.

Security Mode Data Item Description

The GMI Agent program provides various features to promote secure operation within an enterprise including full encryption of transmission and data files, as well as security logging of access.

In particular, the "/system/SecurityMode" value provides several mechanism to restrict access to the agent for security purposes. The user may set the "SecurityMode" to an integer value, either "0", "1", "2", or "3", where each setting is described below.

- **0 = None** – A value of "0" is the default security mode of the agent on installation. No special security is enabled for the platform. At most sites, the user should adjust the SecurityMode to some other value for secure operation.

- **1 = Password** – Setting "SecurityMode" to "1" will restrict access to the program based upon a password. The password is configured in the "PassKey" and / or the "PassKeyReadOnly" objects. The agent rejects an access attempt unless the user supplies the correct password. The "GMI-Cmd.exe" program will prompt the user to supply a password (but some other GMI applications may take other action.) Note that the password is not recoverable, so caution should be taken to remember the configured password.

- **2 = IP List** – Setting "SecurityMode" to "2" will restrict access to the agent based upon a list of authorized IP addresses, contained in the "IPAllowList". The agent silently rejects any access attempt from an unknown address. The "IPAllowList" values can be uploaded. Also, the agent automatically builds the "IPAllowList" with IP addresses when the security mode is not "2" or "3". The client program that modifies the SecurityMode is always added to the list to prevent lockout of the program.

- **3 = Password + IP List** – Setting "SecurityMode" to "3" combines password and IP list authentication. The user must supply both a password to the agent, and the client IP address must be in the "IPAllowList" list of allowed IP addresses. This is the most secure setting for the agent program.

For more information, see the prior sections on the "/security" folder of the agent for a detailed description of the "IPAllowList", "PassKey", and "PassKeyReadOnly" values referenced above.

Note: if security of the managed platform is a consideration, the user should select one or all of the above security settings as a matter of course, to prevent unauthorized access of agent data or modification of the agent consideration. Depending upon the particular Apps installed at the agent, failure to restrict access can result in complete compromise of the managed platform.

PassKey Data Item Description

When the /system/SecurityMode is set to "1" or "3", a password is required to access the agent. Two different passkeys are supported: (a) the "PassKey" value serves as an unrestricted administrative password to the agent, and; (2) the "PassKeyReadOnly" value permits read-only operation of the agent (and blocks the "set", "upload", "install" and "uninstall" directives.)

The following behaviors apply.

1. For a passkey to be enforced, the "SecurityMode" setting must be either "1" or "3", as described previously. For example, at a GMI> prompt, issue the following command:

   ```
   GMI> set /security/securitymode = 1
   ```

2. For a passkey to be enforced, the "PassKey" value must be a non-zero length string. For example, at a GMI> prompt, issue the following command:

   ```
   GMI> set /security/passkey = mypassword
   ```

   Note: The "PassKey" value must be a non-zero length string for the "PassKeyReadOnly" value to be operable. Setting just the "PassKeyReadOnly" value, without first setting the "PassKey" value, will have no effect on authentication until the "PassKey" value is set

3. The operator can connect with the "ReadOnlyPassKey" (in a fashion identical to the regular passkey, but the operator will be blocked when attempting to issue any "set", "upload", "install" or "uninstall" GMI directive.

4. Passwords are case sensitive, can contain any letters or characters (including non-printable control characters) and can be up to 999 characters in length.

5. Leading and trailing white space is eliminated from the password value, but the password can otherwise contain embedded characters.

Note that a passkey is not recoverable. (To reset the password for the agent, the administrator can download a special utility from GMI Foundation, or can re-install the agent program.) Additionally, password values cannot be read or recovered by any installed application, and the passwords are triple-encrypted on the disk using a one-way algorithm.

GMI Foundation and its technical partners are unable to assist in determining the current value of any configured password (or other data item) used by the GMI Agent program.

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, who furnish 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: support@vallumsoftware.com