



General Management Interface

GMI FAQ – Frequently Asked Questions

Published: Sept 2013

<http://www.gmi-foundation.org>

Question: What is GMI?

GMI stands for "General Management Interface", and is intended to be a new and improved way of implementing all types of end-point management, including control, monitor, remote installation, audit, and security functions. Specifically, GMI is an agent program, a protocol, and a simple but effective support system for all types of network management, remote control, auditing, and remote software distribution.

Question: Why do I need "yet another" agent?

This question is at the heart of the GMI project; you need just this one more agent program, the "GMI-Agent.exe" program, so that you don't have to manage the other agents on your platform. The GMI agent is intended to be the single interface to all agent activities. Once you have installed the GMI agent program, you can upload other agent functionality, control existing agents, and upgrade the GMI agents across your network and infrastructure.

Question: How is the GMI software normally used?

The fast answer is: you install "GMI-Agent.exe" programs on one or more platforms on your network (which are subsequently referred to as "managed platforms" or "managed devices"). You remotely control the agents through the "GMI-cmd.exe" program (or other command program) to effect control and monitoring of the managed platform.

A more complex and abstract answer is that GMI software is a general-purpose "end-point management" system. Try web resources for a definition of what all that really means (and be aware that "end-point management" is MUCH more than "security end-point management", such as AV programs, which is a small subset of end-point management in general.)

Question: What is your licensing model for your software?

In brief – any software from this particular site is totally free. You may download and use the GMI agent, and related software without limit, for any purpose, including redistribute the agent with your software. See the LICENSE.txt file that

accompanies our packages for a description of the terms and waivers that apply to usage of GMI software.

Question: How secure is the agent program?

GMI Foundation has taken care to make the agent secure through a variety of techniques. However, the user should consult the "GMI Security Guide" before deploying the agent to a production environment. Specifically, the default "/security/SecurityMode" value for GMI Agent permits access by any user to all types of information, and this value should be set to "non-zero" for any non-test environment. (The "GMI Security Guide" document is available in the "Resources" section of the GMI Foundation website, and should be read carefully by new users.)

Question: What are "GMI Apps"?

A GMI "App" is a package that is uploaded to an agent program to add new functions and capabilities to the agent program. Each "App" will add new folders and "managed objects" to the system that can be set, fetched, uploaded, downloaded, or otherwise accessed, given proper permissions. You install a GMI App via the "install" command of the GMI-cmd.exe (or other) control program.

Question: How do I use GMI Apps?

You can remotely install, uninstall, and upgrade Apps at an agent program. Each GMI App includes a standard document called the Application "Data Description", which provides specific notes on usage for the App. Apps range from simple monitor programs to more complex, multi-threaded, multifunction control programs.

Once an App is installed, you can "set", "list", "download", and "upload" values to the agent to effect changes or receive information from the remote platform, as discussed in the particular App DD.

Question: What is an Application "DD"?

The term "DD" is short hand for a "Data Description" document. This is just a PDF or other document, which completely lists all the folders and data items that are created at the agent when you install a new application. It is a compact user guide to the App, so that the end-user knows whether the App is worth installing. A valid DD is required before an App can be certified and uploaded to the agent.

Note that, in the SNMP world, the "MIB Definition" document is similar to the "DD" in the GMI world (except that the SNMP MIB is written in a much more obtuse ASN.1 format, as opposed to the Agent DD which is just a PDF or text

file.) Unlike with SNMP, there is no need to compile the DD into the manager or agent.

Question: What is "GMI Certification"?

"Certification" applies only to App developers, not necessarily to GMI users. Before an App can be uploaded to the agent, it must be "Certified". This involves verifying the identity of the author, performing minimal tests on the application, and then digitally signing the App. This prevents insertion of malicious Apps by anonymous software developers. It also guarantees a minimal level of quality for an App (such as the App will not immediately crash the agent program.)

The "Certification" process is a free service offered to App developers, but requires you (as a developer) to identify yourself with a real name, contact information. GMI Foundation and its partners will not certify anonymous Apps, hence it is not possible for an end-user upload an App that has is not traceable back to the software author.

Question: Are GMI Apps Free?

There are many free Apps for GMI, with more free Apps being created each day. However, some Apps may have a license agreement independent of the GMI license. In particular, some Apps may be "for-profit" by a software vendor. Check the documentation for the App to determine whether the App is free, and what the terms of usage are.

Note that, unlike GMI Apps, the GMI Agent and GMI Cmd programs (as well as the GMI API, in short all software available from GMI-Foundation.org) are completely free. See earlier question or refer to the LICENSE.txt file that comes with the "Quickstart" package.

Question: What platforms and operating systems do you support?

Currently, GMI supports all versions of the Windows operating system: 2000, 2003, 2008, 2012, XP, Vista, and Windows 7. The GMI Agent and GMI command line manager do not require Java, .NET, or other supporting software to fully operate.

Question: Do you support other platforms, aside from Windows?

A Linux version of the GMI agent is currently in development, and may be announced later this year. Following that, agents will be available for other types of systems.

Question: How "heavy" is the agent program?

The GMI Agent program is designed to be as lightweight as possible. It uses minimal CPU and disk space. It requires no supporting software (such as Java, .NET) nor does it require any DLLs or third-party software of any kind.

Question: Can I remotely deploy the GMI Agent?

The GMI Agent can be remotely deployed by an MSI file, or some other mechanism (such as a silent installer.) Once the agent is installed on a managed platform, it can be upgraded without further need of a software distribution system.

Note that the GMI Agent has many software deployment features that permit software to be remotely installed (once the agent is installed for the first time.) For example, you can simply remotely install a new version of a GMI App at one or more agents to obtain new features or fix bugs.

Question: What is the difference between GMI-Agent.exe and GMI-Command.exe?

Both of these programs are provided in the GMI "Quickstart" program, and complement each other. But they do quite different things: (1) The "GMI-Agent.exe" program runs as a persistent process on a managed platform, awaiting requests from a control program; (2) The "GMI-command.exe" program is a control program that acts as a "client" for one or more agents.

You install the "GMI-Agent.exe" program as a service on Windows platforms. Then, you launch the "GMI-Command.exe" program on any computer with access to that platform (through TCP port 6441) and you can then issue "list", "set", "upload", "download", "install", and "uninstall" directives to communicate with the platform. This is well documented in the PDF files that come with the GMI "Quickstart" package.

Question: How do I install a new agent?

After extracting files from the "Quickstart" (or other) package, you simply issue the following two commands at a command prompt: (1) "GMI-Agent.exe -install", followed by; (2) "GMI-Agent.exe -start".

Once the program is installed, you can also control the GMI-Agent.exe program through the standard Windows Service Manager, or via the "net start GMI" or "net stop GMI" commands at a command prompt.

Question: How do I install or update new GMI Apps?

Launch the "GMI-cmd.exe" program. At the "GMI>" prompt, you simply issue the command: "install (package.gmi)". This will remove any existing GMI App, and install the new App.

Certification information for the new App will appear in the "/install/apps" folder of the agent, and new files and folders will be created at the agent. You should also read the Agent DD to determine the features and capabilities of the agent.

Question: How do I install and use the "GMI-cmd.exe" program?

Just copy the "GMI-cmd.exe" program from the "Quickstart" package to a location anywhere in your path. This utility requires no DLL or support files or any special environment. It is a completely stand-alone program.

Question: What kind of encryption do you use?

The standard encryption uses a 500-character key, which is convolved with the time of the request to create a pseudo-one-time pad encryption method. This is a highly effective and secure encryption method that rivals AES-256 in terms of its difficulty to break.

For those sites that wish to swap the native encryption with AES-256 (or some other encryption standard) this can be accomplished using the "security/upgrade" package, which will double encrypt the data using a second encryption standard. Experience shows that some users may be paranoid enough to do this, but it is really not necessary, because the native pseudo-one-time pad encryption standard is quite secure.

Question: What kind of authentication do you use?

GMI Agent employs three different authentication modes, adjustable via the "/security/SecurityMode" folder. The user can: (1) authenticate against a password, or; (2) authenticate against an approved list of client addresses, or; (3) authenticate using both a password and list of client addresses. Refer to the GMI Agent-DD for a complete description of agent security modes. Other features also exist, documented in the Agent DD, such as a syslog interface, and read-only password.

Question: What port number(s) do you communicate on?

The GMI Agent listens on TCP port 6441. It requires no other port number. The port number cannot be changed in this version (for security reasons.) On the platform executing the GMI Agent, you will need to open up TCP port 6441 (if it is not already opened.)

Note that failure to open a TCP port 6441 to the agent is the MOST COMMON reason that you cannot connect to the agent program. This is especially true with new Windows 2008 implementations, which lock down the Advanced Firewall settings on startup, forcing the administrator to modify the firewall policies before the GMI Agent program can be used on a platform.

Question: Why can't I connect to the agent using GMI-cmd.exe?

This is a common problem when first getting started. First, on the native platform, verify that TCP Port 6441 is listening for requests, and the "GMI-Agent.exe" program is actually running. If it is not, you need to start the agent program via the Windows Service Manager.

If the GMI-Agent.exe program is running, and you still can't connect, the issue is either: (1) The Windows Firewall is blocking TCP Port 6441; (2) Some other firewall between the GMI-cmd.exe program and the agent program is blocking TCP Port 6441; (3) The GMI-Agent.exe is rejecting the request because the client program is not in the "/security/IPAllowList" of the agent. Each of the above items should be investigated.

Question: How do I determine the configured password for the agent?

The password for the agent is not recoverable by GMI or any technical partner. If you lock yourself out of the agent, you will need to remove and re-install the agent program. Additionally, it is not possible for an installed App to get the password information, nor is it possible to decode the agent password from disk storage or from the computer registry.

A method of resetting the Agent "SecurityMode" is under investigation, but the inevitable security issues that this entails has made this a big internal issue at GMI Foundation. (For the time being, the best policy is to remember your password.)

Question: How do I query a value from the agent?

The "ls" command lists the contents of an agent folder. This can be a single scalar value, or can be a large listing of values. In either case, you you can redirect information to a file and operate on the listing with an external program.

Note that the "ls" command is quite similar to the same command found on UNIX systems; there exists an "ls -r" option to list all paths, and an "ls -b" option to list brief mode (without header information.)

The "download" command is an alternate way of querying data, where a file (that was previously uploaded to the agent) can be downloaded to a file. Note that you

can use the "ls" value on uploaded files if they are text files, but you can only "download" a file that was previously uploaded (and not a value that was "set".)

Question: What is the GMI-cmd.exe "parse" function do?

Because a lot of GMI data resides in regular text listings, it has been useful to incorporate a built-in parser into the "GMI-cmd.exe" program. The parser is a simple utility highly reminiscent of "awk", which lets you match values in a listing and parse out individual lines. The "parse" function is simple to use; an understanding is not strictly necessary, but typically quite useful.

A complete discussion of the GMI Parser usage is available from the "Resource" center of the GMI Foundation website. Note that users familiar with "awk" can simply pipe data to that program instead of using the built-in GMI-cmd.exe parser.

Question: What is the difference between an "ls" and "download" command?

Both GMI commands are similar in that they fetch data and values from the GMI Agent program. The "ls" command can be used for any text listing. The "download" command is useful if the agent object contains binary data (such as an image file, a PDF file, an executable program, etc.) You can only download a program that has been "uploaded" to the agent. You cannot download a value that has been "set" by the GMI-cmd.exe or other command program.

Question: What is the difference between a "set" and "upload" command?

Both GMI commands are similar in that they set an agent value. The "set" command will set a value that is a scalar (one-line) value, such as the "/system/SysContact" folder. The "upload" command will allow you to set a value consisting of any arbitrary multi-line text or binary data, such as "/system/SysInfo" folder.

When you "upload" a file to the agent, you may list the contents with the "ls" command. If you want to acquire a binary file from the agent you must use the "download" command.

Note that, if the object is both settable and uploadable, this is identified in the GMI agent folder listing with a "W+" notation. This means the object is writable (settable) as well as uploadable. If the object is not uploadable, the notation will be "W" rather than "W+". This provides a simple method of identifying the characteristics of the folder.

Question: What does "Invalid Agent Path" mean?

This message is displayed when the user attempts to "cd" or "ls" or perform some operation on an agent object, but the pathname is misspelled or non-existent. This generally means you have typed in an invalid pathname to an agent program object, and are attempting to access an invalid agent folder.

Question: What does "Invalid Security Mode" mean?

Some Apps require a "/security/SecurityMode" setting of non-zero before they execute, as an extra security check. This message indicates you should set the "SecurityMode" value to something other than zero, and optionally apply a password (if the security mode is set to "1" or "3").

This is intended to prevent against mistakes in the agent configuration that might compromise platform security (such as permitting end users to access certain Apps without any authentication or protection.) See the "GMI Security Guide" for more information, or refer to the GMI Agent DD for an explanation of GMI security features.

Question: What does "Agent path is not uploadable" mean?

This message is displayed when the operator uses the "download" command and specifies an agent path (as the second argument to the command) that is not downloadable. For a path to be downloadable, it must have been previously "uploaded." Note that not all paths can be uploaded.

Only a path that contains an access flag of "W+" (in the second column of the "ls" command output) can be uploaded. Also note that, some paths are both "uploadable" and "settable", and you can only download a value if it was previously uploaded.

Question: What does "Upload rejected by agent" mean?

This message is displayed when the operator uses the "upload" command and specifies an agent path (as the second argument to the command) that is not uploadable.

Only paths that contain an access flag of "W+" (in the second column of the "ls" command output) can be uploaded. Once a path is uploaded with data, you can issue the "ls" command or the "download" command to fetch data.

Question: Where does the directory structure of the Agent exist on the disk?

The Agent directory structure is a completely virtual system, contained in the memory space of the running agent, derived from the contents of the package

files that are uploaded to the agent. There is no actual directory of values that is accessible from the file system or outside the agent construct.

Question: Where do I find GMI Apps?

GMI Apps are available from various locations. Vallum Software, LLC, furnishes an "App Exchange" that offers a wide selection of free apps. See the footnote to this document for links and more information.

More information on how to acquire and / or write a GMI App is available from the GMI Foundation website. Note that new GMI Apps are being written every day, and you can also request the creation of a new GMI App from GMI Foundation and / or one of its technical partners.

Question: How do I request a new GMI App?

The best place to request a new App is to contact Vallum Software, who furnish a central clearing house for GMI Apps, and run the VAX (Vallum App Exchange) resource center from their website.

This company is currently best positioned to handle change requests to existing Apps, and requests for completely new Apps. You may also contact GMI Foundation or one of its technical partners, but they will likely refer you back to Vallum Software LLC. The contact information for Vallum Software is provided at the end of this document.

Question: How do I script a GMI command program?

The "GMI-Cmd.pdf" file, available from the "Resources" section of the GMI Foundation website, provides some brief information on this. (This file is also included as part of the GMI Foundation "Quickstart" package.)

The GMI-Cmd.exe program accepts input redirected from standard input. As per the PDF documentation, The "GMI-cmd.exe -q" option will execute the program in "quiet" mode to de-clutter the display.

Note that GMI-Cmd.exe is not intended as a full-featured scripting language. However, some creative users have invented various systems to fetch data from the GMI-Cmd.exe using powershell, cscript, and other high-level languages. For example, a script can create an "input" file which is then redirected into the "GMI-cmd.exe -q" command to perform complex operations.

Question: I am a programmer. Where is the API?

GMI Foundation provides two different APIs: (1) The GMI-Agent-API package allows developers to create new applications for agents, which can be sent to

GMI Foundation or a technical partner for "certification"; (2) The GMI-Cmd-API package allows developers to create new command programs that communicate with agent programs. Both of these API packages are fairly well documented, and available from the "Resources" section of the GMI Foundation website.

Question: Do you have PHP, Perl, Ruby bindings available?

GMI Foundation currently has a package under development for PHP, with Perl and Ruby soon to follow. Ambitious developers can craft their own bindings from the GMI-Cmd-API package discussed above with just a little bit of investigation and effort. (The GMI bindings, when released, will essentially use the info from the GMI-Cmd-API package, and include some examples and user documentation.)

Question: Can I consult with you about our requirements?

GMI Foundation is pleased to consult via e-mail on any subject related to our technology. Note that we may refer you to one or more of our technical partners as part of the discussion, who may be better positioned to support conversations on detailed interface requirements and system architectures. Contact us today to kick things off.

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: info@vallumsoftware.com