



**GFIMAX**<sup>™</sup>

Easy, Affordable Tools for IT Support & Managed Services<sup>™</sup>

# Technical FAQs

The purpose of this document is to provide overview information about how **GFI MAX** aka HoundDog works. It answers questions on:

ADVANCED MONITORING AGENT TECHNICAL INFORMATION .....	3
ASSET TRACKING .....	5
DAILY WORKSTATION HEALTH CHECK.....	6
GFI MAX'S CENTRAL SERVERS.....	7
THE DASHBOARD .....	7

*Note that it does not provide details on a check-by-check basis. If you have queries about how to set up any one check, or about the limitations of any one check, please refer to the GFI MAX User Guide.*

# Technical FAQs

## ADVANCED MONITORING AGENT TECHNICAL INFORMATION

### What operating systems does the Agent support?

The agent can be used on Microsoft NT4 or higher server operating system. It can also be used on any Windows 2000 or higher desktop operating system.

### Can the agent be used on Linux or MAC servers?

Not at this time.

### How does the Agent run?

The agent runs as a service under Windows. The Agent service name is 'Advanced Monitoring Agent' and there is also the update service 'Advanced Monitoring AutoUpdate'. So if your client ever stumbles across them, there is no reference to GFI MAX.

### How does the agent do its job?

The Agent accesses a wide range of systems on the server to collect information that would otherwise be discarded. By selectively accumulating this information – and discarding the rest – GFI MAX is able to alert you when there is an issue that needs your attention.

### Can you give us the vital stats on the Agent?

5MB memory is used when running. It requires 5MB of disk space. Its load on the server barely registers on Task Manager.

### How does the agent communicate with the central server?

All agent communications to the server are encrypted via SSL. Proxy servers (SOCKS5 and HTTP) are accommodated. The agent makes use of NTLM or basic authentication. The agent uses multiple servers for upload so that it can continue to operate if any server fails.

### Do I need to make changes to the firewall?

Not unless the firewall is currently restricting HTTPS communications.

### How much data is pushed out?

Every five or 15 minutes, the agent sends a packet of 400-600 bytes, depending on the checks you have selected.

### How secure is the agent?

The agent is only accessible to those with a 'key', that is, the original password sent during the sign-up process.

## Technical FAQs

### **How long are connections held open for?**

A default setting of three retry attempts with an interval of 10 seconds. This is easily configurable via the Agent.

### **Does the GFI MAX software service any inbound connections?**

The majority of data traffic is from the agent to the GFI Software servers. The only time communications come from the GFI MAX is where the Agent is configured to auto-update or download the Critical Event Exclusion list. To prevent these downloads simply disable the Advanced Monitoring AutoUpdate service.

### **What type of data do you collect?**

The only data collected from your servers is some basic configuration information, operating system etc, some data about the checks performed (e.g., disk size, AV version, or a 1 or 0 for check pass or fail) and the unique ID assigned by GFI to the server. This is used to display the information on the DashBoard.

### **How long is it held for?**

GFI currently stores the failure information for the historical reporting but the data packets themselves are discarded once a new one is received.

### **Who has access to the data on the GFI servers?**

Only GFI has access to the data on the servers. Encrypted usernames and passwords to access these servers and access is restricted to specific IP addresses.

### **What protection is in place to prevent other companies/institutions/individuals gaining unauthorized access to the data?**

The only information GFI currently stores about customers is their name and contact details, the server information they have entered (server name, etc.) their GFI MAX login and the checks configured per device.

Any additional information, proxy server login, etc. are stored locally on your client's server and are never sent to GFI.

As GFI does not store any information on your company or server login details, the information GFI does retain could in no way be used to gain access to your client's system.

### **How much of GFI MAX's collected data is held on the local client server?**

The software on the client's server stores the check configuration XML files, the check log files, the upload log files, a list of the services found on the server in the file services.ini and the GFI MAX Agent configuration in the file settings.ini. Any passwords entered in the Agent are encrypted and stored on the local machine.

## Technical FAQs

### **If our Internet connection goes down we would be unable to access the GFI MAX Dashboard. But what happens to the data being accumulated on the server (or any other server on a client site for that matter) during an extended loss of internet connection?**

Each time the Agent sends or attempts to send a data packet, the previous data packets are overwritten on the client's server. Where a connection cannot be made to the GFI server, the Agent will still attempt to send the data the specified number of times (a threshold set by you). Once this figure is achieved, the Agent will not attempt to send a data packet until the next scheduled cycle.

Note: You will be alerted to the fact that the client's server cannot send its information. If GFI's servers don't hear from any server within a specific time (that you set), you'll receive an email or SMS, and your Dashboard will be updated to clearly show that that server has not reported in.

## ASSET TRACKING

### **How it works**

The Agent contains two methods to extract the required information from your client's remote devices, the **Agentless Scan** and **MiniAgent**.

The **Agentless Scan** is performed from a single Advanced Monitoring Agent interrogating a specified IP or Domain range to identify all of the attached devices and their configuration. The scan authentication information as well as the scan schedule is entered into the Advanced Monitoring Agent and stored locally.

The **MiniAgent** is installed on each target device. When the user logs on to the system the MiniAgent scans the local device, uploading the configuration information to its parent Advanced Monitoring Agent where its schedule information is contained.

For both methods, the results of the scan are displayed on your Dashboard, showing a complete hardware and software inventory for your Client. The scan information is also available in SQL and XML formats.

From the Dashboard, you can run Asset Tracking reports such as the Inventory Report and the Modification Report (which could make you aware of additional hardware or software installed on the network). You can also define information fields of your own, for example to record care pack numbers, contract renewal and warranty expiry dates, making your asset administration easier.

## Technical FAQs

### DAILY WORKSTATION HEALTH CHECK

Like Asset Tracking there are two methods to extract the required information from the workstations, the **Agentless Scan** and **MiniAgent**.

The **Agentless Scan** allows you to monitor all of the workstations on a network remotely by installing the Agent onto just one networked device. The scan authentication information as well as the scan schedule is entered into the Advanced Monitoring Agent and stored locally.

The **MiniAgent** is installed onto each workstation; when the user logs on to the system the checks run on the local machine. This information is then uploaded to the MiniAgent's parent Advanced Monitoring Agent where its schedule information is contained.

#### How are they configured?

The Daily Workstation Health Checks for both the Agentless Scan and MiniAgent are configured via the Dashboard.

#### What does it check?

The Daily Workstation Health Checks:

- Anti virus Update Check
- Disk Space Check
- Hacker Check
- Physical Disk Health Check
- Windows Service Check\*
- Critical Events Check
- SNMP Check – RAID Array Check\*\*

\*Windows Service Check: This check will fail where a service configured to automatically start is in the stopped state.

\*\* SNMP – RAID Array Check: For this check we use our default Dell and HP OIDs.

#### How often does it run?

The Daily Workstation Health Check runs as often as you wish from every day to once a week.

Simply log onto the Advanced Monitoring Agent, choose **Settings** in the **Workstation Monitoring** section and select the **Days to Run**.

## Technical FAQs

### GFI MAX'S CENTRAL SERVERS

#### Where are the central servers? How secure are they?

The company's fully redundant central servers are located in three of the world's most advanced hosting facilities. Even the fail-safes have fail-safes. Backup generators, multiple hard drives, dual routers, cooling systems and gel battery power banks give GFI real redundancy so the fleet of high-end servers will continue to operate regardless of external conditions.

Industry-leading 18,000 MBit connectivity to the Internet via different carriers allows for no-nonsense, fast transfers at all times. The result is that GFI MAX is never susceptible to bottlenecks and the website and DashBoard can be accessed via multiple servers at any time.

GFI uses multiple servers in our central infrastructure at all levels and these are protected by 24/7 monitoring, 150+ permanently recording video cameras, safety locks and more to ensure that only authorised personnel can enter the data centre. There are separate monitoring systems that check the availability and correct operations of our servers from outside the hosting centre on a 24x7 basis with immediate notification of any service issues. The servers are configured with the minimum possible levels of access consistent with GFI being able to operate the system.

Your data is always safe and secure.

### THE DASHBOARD

#### Does the DashBoard require any software?

No. The DashBoard runs under Internet Explorer or Firefox. A plug-in may be required to play the alert sound.

#### Does the DashBoard refresh?

No. The DashBoard doesn't refresh, however the Wallchart refreshes every five minutes so that you can always be on top of your clients' problems.

#### Do I need any special software to access the MiniDash on my phone or PDA?

No. The MiniDash runs on any browser or WAP enabled phone or PDA. You can login at <http://dashboard.systemmonitor.co.uk/minidash> or **dashboard.yourname.com/minidash** where your DNS is customised. Simply use your usual DashBoard login for access.

#### How can we login to our customised DashBoard without going near GFI MAX?

You can set up a DNS CNAME entry to access the DashBoard directly. The system will respond to **http://dashboard.yourname.com** by serving up the DashBoard.

Any domain name may be used as long as it is in the format **dashboard.yourname.com** and the CNAME record points to **dashboard.systemmonitor.co.uk**

## Technical FAQs

For resilience, there is also the option to create a second DashBoard DNS CNAME entry for **<http://dashboard2.yourname.com>** pointing to **[dashboard2.systemmonitor.co.uk](http://dashboard2.systemmonitor.co.uk)**

Please be aware that some domain reseller/agent's DNS servers may take up to 24 hours to reload the new DNS address.

There should be no other set-up required, unless you are using a domain name which is under a different top-level domain than the ones specified above. If this is the case, contact GFI and we can accommodate your requirements.

For additional technical information, please contact [MAXcares@gfi.com](mailto:MAXcares@gfi.com).