



## Technical FAQs for Customers

### ADVANCED SERVER 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'.

#### **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 – it 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 15 minutes, the agent sends a packet of 400-600 bytes.

### **How secure is the agent?**

The agent is only accessible through the Portal with the original password sent during the signup process.

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

A default setting of three retry attempts with an interval of 10 seconds.

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

The majority of data traffic is from the agent to the servers. The only time communications come from the servers is where the Agent is configured to auto-update or download the Critical Event Exclusion list.

### **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 to the server. This is used to display the information on the Portal.

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

It 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 servers?**

Only Tier3 has access to the data on the servers. Encrypted usernames and passwords to access these servers and access are restricted to specific IP addresses.

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

The only information it currently stores about customers is their name and contact details, the server information they have entered (server name, etc.) their login and the checks per device. Any additional information, proxy server login, etc. are stored locally on your client's server and are never sent to us. As we do not store any information on your company or server login details, the information we retain could in no way be used to gain access to your client's system.

### **How much of the 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 Agent configuration in the file settings.ini. Any passwords entered in the Agent are encrypted and stored on the local machine.

### **If our Internet connection goes down we would be unable to access the Portal. 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 server, the Agent will still attempt to send the data the 10 times. 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 our servers don't hear from any server within that time, you'll receive an email and your Portal 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 Portal, showing a complete hardware and software inventory for your Client. The scan information is also available in SQL and XML formats. From the Portal, 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).

## 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 Portal.

### 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

### How often does it run?

The Daily Workstation Health Check runs every day

## **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 us 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 we are never susceptible to bottlenecks and the Portal can be accessed via multiple servers at any time. We use 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 authorized personnel can enter the data center. There are separate monitoring systems that check the availability and correct operations of our servers from outside the hosting center on a 24x7 basis with immediate notification of any service issues. The servers are configured with the minimum possible levels of access consistent with us being able to operate the system. Your data is always safe and secure.

Feature	Server Agent Mode	Workstation Agent Mode
<b>Operating Systems</b>	Windows 2000 Windows 2003 (SBS) Windows XP Windows Vista Windows 2008 (SBS) Windows 7	Windows XP Windows Vista Windows 7
<b>24x7 Checks</b> Drive Space Check Performance Monitoring Ping check TCP Service check Web Page check Windows Service Check SNMP Check Bandwidth Monitoring Check File Size Check Event Log Check	Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes	Yes Yes No No No No Yes Yes* No Yes Yes
<b>Daily Safety Checks</b> Anti-Virus Update Check Backup Check Drive Space Change Check Exchange Check Hacker Check Physical Disk Check Critical Events Check SNMP Check File Size Check Event Log Check WSUS Check	Yes Yes Yes Yes Yes* Yes Yes Yes No Yes Yes Yes* Yes*	Yes Yes No Yes No Yes Yes Yes Yes Yes Yes No No
<b>Data Overdue Alerts</b>	Yes	No
<b>Dashboard Controls</b>	Yes	Yes
<b>Remote Agentless Scans</b>	Yes	No

\* localhost only