

App Note: Installing the WMI Agent

Operation:

Monitoring a Microsoft Windows based desktop or server using Pandetix MSOWare requires an agent on each monitored system enabling the Windows Management Instrumentation (WMI). WMI allows remote monitoring of services and various statistics on remote servers and workstations. The WMI interface is accessed by the Common Information Model (CIM), a web services model using this mapper agent. WMI to CIM mapper is a web services interface with a mapping agent available for remote queries. The MSOWare model can use either HTTP or HTTPS protocols but defaults to HTTPS.

Installation and setup:

The setup process is as follows:

Download the WMI Mapper from the Pandetix support web site. This is an open source program written by the Pegasus project and modified by HP for Windows installation.

Install the downloaded WMI agent on the system to be monitored by following the on screen instructions.

The WMI agent will create a file on the monitored system in the following location:

```
\program files\the open group\wmimapper\cimserver_planned.conf
```

Locate the file and REMOVE two lines for the SSL Certificates:

```
_sslCertificateFilePath=C:\hp\sslshare\cert.pem  
_sslKeyFilePath=C:\hp\sslshare\file.pem
```

Restart the Pegasus WMI Mapper service (Control Panel/Administrative tool/Services/Pegasus WMI Mapper)

Note:

The assigned computer name of the computer being monitored must be

Microsoft-acceptable format, using alphanumeric characters only [a-z, 0-9].

For example, the computer name of 'computer one' is not compatible where computer1 would be compatible.