PAESSLER
the network monitoring company

Paessler PRTG with Built-in WMI Support Provides Trouble-Free, Automated Network Monitoring

Network Monitoring Specialist Provides Tips & Tricks for the Most Common Issues Experienced with Windows Management Instrumentation

LOS ANGELES, CA and NUREMBERG, Germany (August 18, 2010) – Windows Management Instrumentation (WMI) is a powerful Microsoft standard that allows system administrators to monitor and manage a whole Windows network from one central point. WMI technology is a key component of most network monitoring tools, as it provides vital and detailed information on devices and applications running on the Microsoft operating system.

To help administrators get the most out of WMI, maintain maximum network availability and optimize network resources, Paessler AG (www.paessler.com), developer of the award-winning network monitoring solution PRTG Network Monitor, released a five-point set of guidelines for reliable troubleshooting with WMI to help PRTG users more effectively monitor a network via WMI.

"With WMI support, PRTG enables administrators to easily monitor both local and remote computers, execute scheduled tasks and receive detailed information about devices and applications running on the Microsoft network, such as CPU usage and temperature or usage of RAM," said Dirk Paessler, CEO of Paessler AG. "The specific WMI sensors in PRTG Network Monitor integrate this data to enable centralized monitoring of all components and parameters from a single, easy-to-use dashboard."

However, faulty installation or configuration of WMI—or far more complex technical problems—can prevent administrators from fully exploiting the benefits of WMI technology. Effective troubleshooting is the key to using WMI effectively to support efficient monitoring.

To that end, the Paessler AG support team has identified the most common WMI problems and provided the following solutions for reliable WMI troubleshooting.

Five Steps for Troubleshooting WMI

1. **Simplify user credentials**: For each WMI query, Windows asks for user identification. To simplify complex rights management, make each user a member of the Domain Administrators group in the same Active Directory section as the target computer. Alternatively, set up a local system administrator account on the target computer to be used for login. Each user must also have remote access rights to use WMI and the appropriate Windows login data can be easily be entered individually into PRTG for each target computer.

2. **Enable WMI on the local firewall**: To ensure that all inquiries reach the target computer, it is essential to ensure that the firewall of the target computer allows incoming WMI requests.

3. **Configure firewall and group policies**: If the firewall is enabled on the basis of certain group policies, the setting "Allow Remote Administration Exception" must be activated for this policy.

4. **Open the port:** The RPC server for the target computer using WMI should be running in port 135 by default (unless configured otherwise). Ensure that this port is not blocked by another (hardware) firewall on the route to the remote computer.

5. **Check the security software:** Double-check to ensure that some local security software isn't blocking the WMI connections. Locate the specific software setting for these parameters and make sure that the connection is explicitly "allowed."

"With WMI sensors built right in, PRTG Network Monitor is one of the few monitoring solutions that include this common component at an affordable price in every license," Paessler said. "This makes for the most effective network monitoring solution at a better value than others' 'premium' versions."

To download a trial version of PRTG Network Monitor, or get more information, visit http://www.paessler.com/download.

PRESS INFORMATION

PAESSLER
the network monitoring company

PRESS INFORMATION

# # # # #

MEDIA CONTACT:
Megan Parker
SS|PR
847-415-9326
mparker@sspr.com