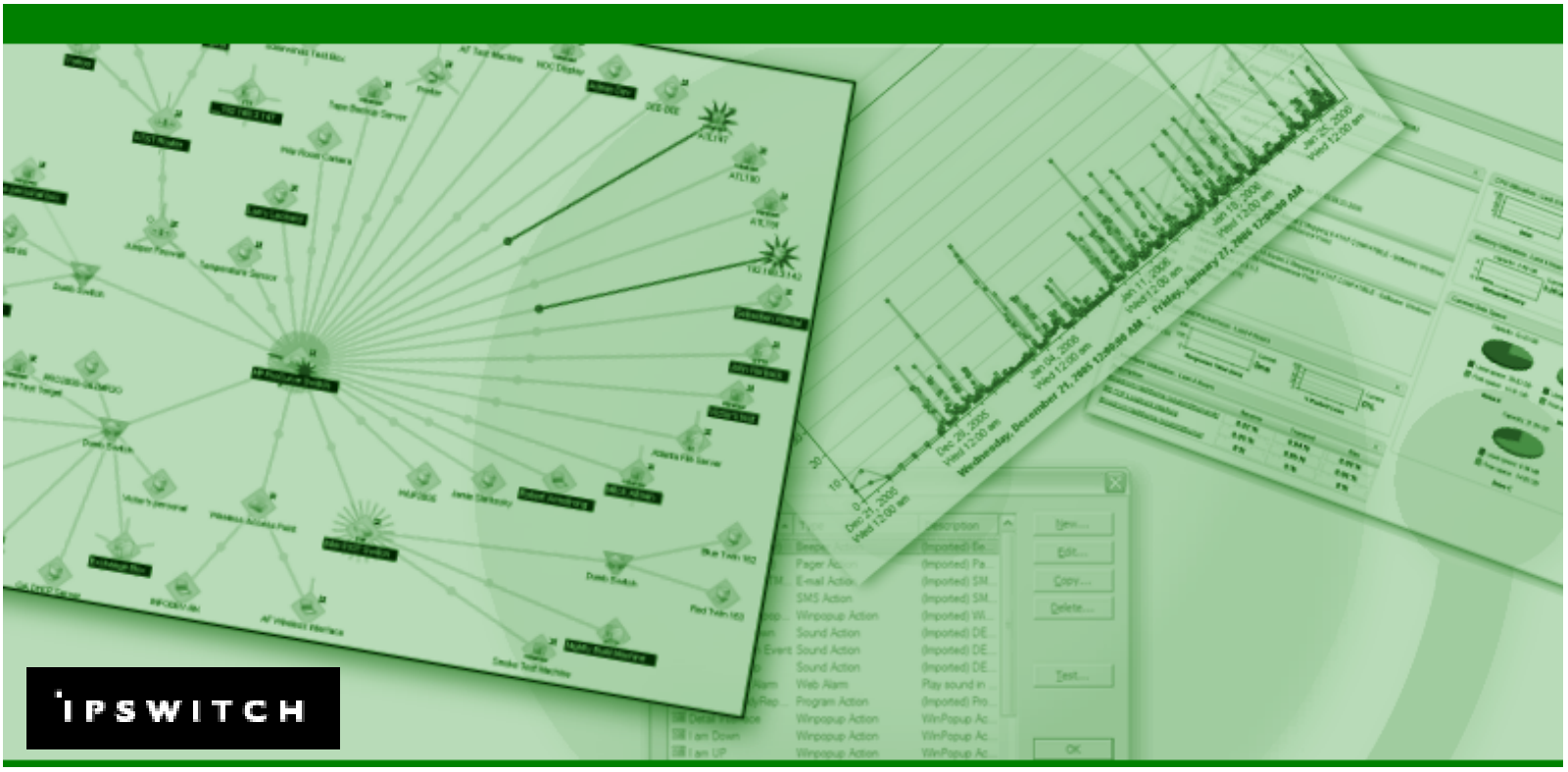


Configuring WMI Performance Monitors

With WMI, WhatsUp Gold Premium Edition monitors and sends alerts based on performance counters that are reported from Microsoft Windows® devices. The data collected is displayed in graphical reports that show historical trends and provides highly visible network status information.

IPSWITCH WhatsUpGold

Introduction

Windows Management Instrumentation (WMI) is a Microsoft® Windows® standard for retrieving information from computer systems running Windows. WMI comes installed by default on Windows 2000, 2003, and XP systems.

How is WMI used in WhatsUp Gold v11Premium Edition?

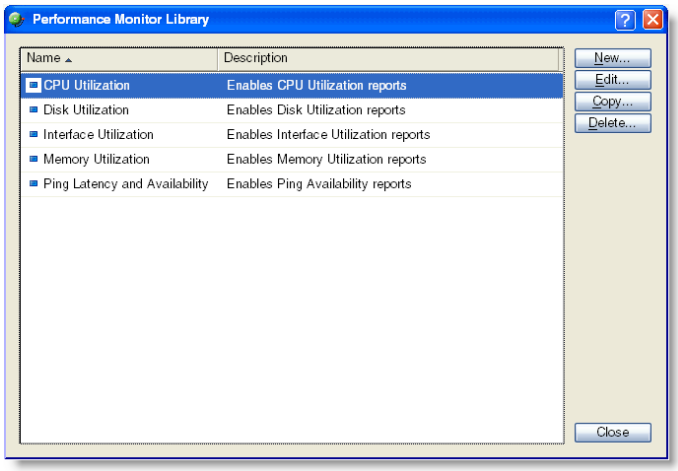
WhatsUp Gold v11 uses WMI in two ways; to gather historical data on device performance counters and to monitor the counters and then alert you when the counters do not match the criteria you establish. These two features act independently, but can be used in together to ensure the ongoing health and availability of your network.

If you are familiar with the way Microsoft® Management Control (MMC) (or Perfmon) operates, you should recognize the WMI implementation in WhatsUp Gold. There is a 1 to 1 correspondence in the performance counters available in each of the two applications. If you can use MMC to access the performance counter, you can perform historical charting of those counters in WhatsUp Gold.

Performance Monitoring

WhatsUp Gold is installed with five default Simple Network Management Protocol (SNMP) performance monitors that monitor specific types of performance data on your network devices:

- CPU Utilization
- Disk Utilization
- Interface Utilization (Bandwidth)
- Memory Utilization
- Ping Latency and Availability



Performance Monitor Library

Since performance monitoring was designed to be available to a wide variety of devices, these monitors use SNMP to gather performance data instead of WMI. On Windows devices, the same data can be gathered through WMI. However, it is not necessary to use WMI to gather performance data, unless the Windows device is not SNMP enabled.

If you want to collect performance data on a non-SNMP manageable device through WMI, or if you need to gather data on a performance counter other than the default monitors, you can create a custom WMI performance monitor in the Performance Monitor Library.

Example of Configuring a Custom Performance Monitor

One of your devices that runs overnight processes is consistently failing attempts to do the processing. When you try to troubleshoot the device, you notice that everything seems to be running correctly, and you are able to manually process the job without any errors. You determine that something occurs during non-business hours on the device that is causing it to fail.

After some investigation, you find that the process may have a memory leak. You need to see when the spike occurs and how it correlates with other things that are going on with the device and other processes running on the device. To do this, you can create a custom performance monitor for the process you're troubleshooting.

To create a custom performance monitor for the process in question:

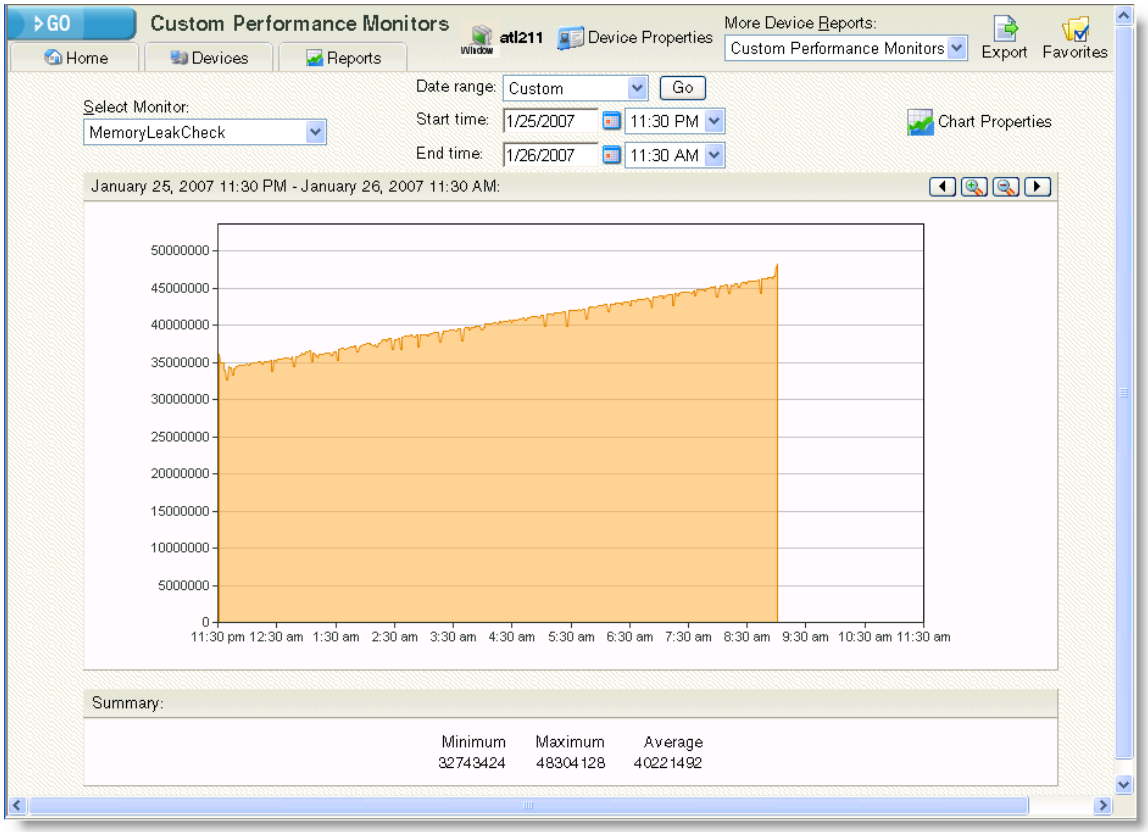
1. In the web interface Device View, select a device from the device list.
2. Right-click the device, click **Properties** from the right-menu to view the Device Properties for the selected device, then click **Credentials**.
3. Select a credential from the **Windows credentials** list or the **SNMP v1/v2/v3 credentials** list, then click **OK**.
   - or -
   To access the Credentials Library and create a new credential, click the **Browse (…)** button, next to the Windows credentials list.
   a. Click **New** to create a new credential. The Select Credential Type dialog opens.
   b. Complete the dialog, click **OK**, then click **Close**.
   c. Select a credential from the **Windows credentials** list or the **SNMP v1/v2/v3 credentials** list, then click **OK**.
   Note: Refer to the Help for more information about the credentials set up.
4. In the Device Properties dialog, click **Performance Monitors**.
5. In the **Enable individual performance monitors (for this device only)** section, click **New**. The Select Performance Monitor Type dialog opens.
6. In the **What type of monitor would you like to create?** list, select **WMI Performance Monitor**, then click **OK**. The Add WMI Performance Monitor dialog opens.
7. In the **Name** box, enter the name **MemoryLeakCheck** and enter a **Description** for the monitor.
8. Click the **Browse (...)** button next to the **Instance** box. The Performance Counters dialog opens.
9. In the **Performance Object** list, select **Process**. The Process **Performance Counters** displays a list of options.
10. Select the **Private Bytes** performance counter.
11. In the **Performance Instances** list, select the specific application process you want to monitor.
12. Click **OK** to add the counter and instance to the Performance Counters dialog. The Add WMI Performance Monitor dialog opens.
13. Adjust the Collection interval (polling intervals) and Timeout for the monitor. This setting is independent of the default polling frequency setting in WhatsUp Gold.
14. Verify the configuration, then click **OK** to begin collecting statistics on this monitor.

Performance Reports

After a few polling cycles, you will have enough data to view in the Performance Reports. In the Private Bytes example, we were looking at data during off-hours, so the following day, you should have interesting results to look through.

To view the historical data of the custom performance monitor:

1. From the web interface, click **Reports > Device.** The Device Reports list appears in the web interface Reports View.
   - or -
   From the console, click **Reports** > **Device**. The web interface opens in the Reports View.
2. Select the Custom Performance Monitor report from the Performance Monitor section.
   Note: Make sure you have the device that you set up the custom performance for selected. Click the **Devices** tab, right-click the device you want to view, then click **Device Reports**.
3. On the Custom Performance Monitors report, in the **Select Monitor** list, click the custom monitor to view historical data. In this example, select **MemoryLeakCheck**. The data displays.



WMI Active Monitor

Active Monitors query network services installed on a device and wait for the value (response) to be returned. If the returned value does not match what is expected, or the returned value's rate of change is higher than the configured threshold, the active monitor can be set to fire an action based on the state change that occurs.

Beyond the basic active monitors installed with WhatsUp Gold, you can configure custom active monitors in the Active Monitor Library. One of the available active monitor types is the WMI Monitor (available in WhatsUp Gold Premium Edition v11). This type of monitor uses WMI to poll the performance counters reported on a Windows device.

Example of Configuring a Custom WMI Active Monitor

A device on your network has been illegally logged into through a 'brute force' attack where someone used a script to try random usernames and passwords on a range of IP addresses on your network. These types of attacks are extremely dangerous if the device that is accessed is on your domain or has sensitive information stored on it. To keep this from happening again, you decide that you need to know immediately when such attacks are attempted.

By creating a custom WMI Active Monitor that checks on the Windows device performance counters, you can have WhatsUp Gold notify you when this type of attack occurs. This monitor will help raise the visibility of such attacks on your network, so you can react to prevent an intruder from accessing your critical network data.

To configure a WMI Active Monitor to check Windows device performance counters:

1. In the web interface Device View, select a device from the device list.
2. Right-click the device, click **Properties** from the right-menu to view the Device Properties for the selected device, then click **Credentials**.
3. Select a credential from the **Windows credentials** list or the **SNMP v1/v2/v3 credentials** list, then click **OK**.
   - or -
   To access the Credentials Library and create a new credential, click the **Browse (…)** button, next to the Windows credentials list.
   a. Click **New** to create a new credential. The Select Credential Type dialog opens.
   b. Complete the dialog, click **OK**, then click **Close**.
   c. Select a credential from the **Windows credentials** list or the **SNMP v1/v2/v3 credentials** list, then click **OK**.
   Note: Refer to the Help for more information about the credentials set up.
4. In the Device Properties dialog, click **Active Monitors**.
5. In the Active Monitors section, click **Add**. The Select Active Monitor Type dialog opens.
6. Since you do not have an active monitor of this type configured in the Active Monitor Library, click **Browse (…)**. The Active Monitor Library opens.
7. Click **New**. The Select Active Monitor Type dialog opens.

8. In the **What type of Active Monitor would you like to create?** list, select **WMI Monitor**, then click **OK**. The Add WMI Monitor dialog opens.
9. In the **Name** box, enter the name **ErrorsLogon** and enter a **Description** for the monitor.
10. Click the **Browse (…)** button next to the **Instance** box. The Performance Counters dialog opens.
11. In the **Computer name** box, enter the name of the computer, the **User name**, and **Password** for the computer that set up the WMI monitor for, then click **OK**. **Note**: If a domain account is used, then the expected user name is entered in the form of domain\user. If the device is on a workgroup, there are three possible user name formats: workgroup name\user, machine name\user, or \user. The target computer requires user account administrative privileges.
15. In the **Performance Object** list, select **Server**. The Server **Performance Counters** displays a list of options.
16. Select the **Errors Logon** performance counter, then click **OK** to add the counter and Instance to the Performance Counters dialog. The Add WMI Monitor dialog opens.
17. In the Check Type drop-down list, select **Rate of Change**.
18. In the **Rate of Change** box, enter the number of logon errors you feel is acceptable. This is the number of failed logon attempts between polls.
19. In the **If the value is above the rate, then the monitor is:** box, select **Down**.
20. Verify the configuration, then click **OK** to add the Performance counter to the Active Monitor Library.
21. Click **Close**. The Active Monitor Properties dialog opens.
22. Click **Next**. The Set Polling Properties dialog opens.
23. Click to select **Enable polling for this Active Monitor**.
24. Click **Next**. The Setup Actions for Monitor State Changes dialog opens.
25. Select the type of action scenario you want to use for the monitor.
    - **Apply this Action Policy** list. Select an action profile that you have configured through the Action Profile Library, or
    - **Apply individual actions**. Select to build a list of actions that you select from the Action Library.
26. Click **Finish** to begin using this active monitor on the device.

You may want to consider creating several levels of the active monitor, each with a higher threshold than the other, and with more severe actions associated with it.

For example, create a monitor with 30 as the threshold that sends you an email to notify you that at least 31 attempts have been made. Next, create another monitor that uses 60 as the threshold. This monitor may have an SMS action associated with it that sends a text message to you when at least 61 attempts are made. For the most severe level you could create a 100 threshold and have the action send messages to several people who may be able to block the IP or take the device off the network while the attack is addressed.