

IPSWITCH



Features Overview Guide

About new features in WhatsUp Gold v14



New Features in Ipswitch WhatsUp Gold v14	
Welcome to WhatsUp Gold v14!	1
About the Welcome Center	
About the Quick Setup Assistant	3
About the Discovery console	
About Device Roles	
About Alert Center	
Using Alert Center and actions	
New active monitors	
About the APC UPS Monitor	
About the Exchange Monitor	12
About the Fan Monitor	12
About the File Properties Monitor	13
About the Folder Monitor	14
About the FTP Monitor	15
About the HTTP Content Monitor	16
About the Network Statistics Monitor	17
About the Printer Monitor	
About the Process Monitor	19
About the Power Supply Monitor	20
About the Microsoft SQL and MySQL Query Monitor	21
About the Temperature Monitor	22
About critical active monitors	

New actions

About the SNMP Set action	23
About the Log to Text File action	24
About the Windows Event Log action	25

About Find Device

About the Argument field

New in Flow Monitor plug-in

New Flow Monitor reports	29
About ifIndex on the Flow Interface dialog	

Added support

For more information

New Features in Ipswitch WhatsUp Gold v14

Welcome to WhatsUp Gold v14!

Ipswitch proudly introduces the most powerful version of WhatsUp Gold to date. WhatsUp Gold v14 offers a Welcome Center and Quick Setup Assistant that aid you in easily setting up WhatsUp Gold for your network; a totally revamped Discovery console that intuitively categorizes your network devices in specific roles; an Alert Center to manage notifications for all of your WhatsUp monitors; new critical active monitors that allow you to configure the order in which monitors are polled according to the up or down state of monitors that you specify as critical; 13 new dynamic active monitors in WhatsUp Gold v14 Premium Edition; 3 new actions--2 that utilize a brand new percent variable picker; an improved and renamed Flow Monitor plug-in with new reports and support for sFlow and J-Flow; and much, much more!

Refer to the v14 Release Notes on www.WhatsUpGold.com/support for Ipswitch WhatsUp Gold product features and information.

About the Welcome Center

The first time that you open v14 console, you are greeted by the WhatsUp Gold Welcome Center. This dialog includes a variety of links to helpful, insightful information on how to use WhatsUp Gold for your network management needs. From here you can launch the Quick Setup Assistant, see what's new on the WhatsUp user community, view new Knowledge Base articles and forum threads, view product videos, and access helpful resources like the User Guide and Help system.



About the Quick Setup Assistant

You can start using WhatsUp Gold quickly by using the Quick Setup Assistant. This discovery assistant guides you through the three steps involved in discovering devices on your network. You will setup notifications, configure SNMP credentials, and run a discovery scan. After you complete the discovery scan and add devices to the WhatsUp database, you are ready to manage your network using WhatsUp Gold.



The Quick Setup Assistant is accessible on the WhatsUp Gold console from the Welcome Center (**Tools > Welcome Center**).

About the Discovery console

The new Discovery console and web interface includes a new and improved discovery engine that identifies network devices more accurately than previous versions of WhatsUp Gold. Network discovery scans each device to determine its manufacturer, model, and running software and services. WhatsUp Gold uses this information to categorize network devices into new device roles, and then uses these roles to automatically assign commonly used monitors for each device.

Progress Summary Most Name Address Brand Model Operating System Role Device Limit Unlimited atl-cisco4506.ipswitch_m 192168.3.1 Web server Existing Devices 147 192168.3.3 192168.3.3 HP HP J4121A P Switch Discovered Devices 127 192168.3.4 192168.3.4 Web server Web server Stand Devices 127 192168.3.4 192168.3.5 Web server Web server DC 192168.3.5 DC 192168.3.6 Web server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP Hp LaserJet A Printer Scan Start 6/001.06 HT 192168.3.10 HP HP LaserJet A Printer Scan Start 6/01.7/2009 327:24 PM 192168.3.10 HP HP LaserJet A Printer Scan Start 6/01.06 HT 192168.3.10 HP HP LaserJet A Printer Scan Type Range atl-																																																																																																																																																																																																																																						
Device LimitHiot NameAddressBrandModelOperating SystemRoleDevice LimitUnlimitedatl-cisco4506.jpswitch_m192168.3.1Web serverWeb serverExisting Devices147192168.3.3192168.3.3HPHP.J4121A PSwitchDiscovered Devices127192168.3.4192168.3.4HPHP.J4121A PWeb serverNetworkTaffic192168.3.4192168.3.5Web serverWeb serverSMP Bytes (in/out)419461./357524EXCH2007192168.3.6Web serverEmail serverScanned180 of 255NPID51ACD192168.3.7HPHP Laser/et FPrinterScan Start6/17/2009.327:24 PM192168.3.0192168.3.8HPhp Laser/et AWeb serverScan Start6/17/2009.327:24 PM192168.3.10192168.3.10HPHP Laser/et APrinterBapsed Time0:001.06192168.3.10192168.3.10HPHP Laser/et APrinterScan Start6/17/2009.327:24 PM192168.3.10192168.3.10HPHP Laser/et APrinterScan Start0:001.06192168.3.10192168.3.10HPHP Laser/et APrinterScan TypeRangeatl-ap1.ipswitch_mipswi192168.3.14HPLoolor LasWeb serverScan TypeRangeatl-ap2.ipswitch_mipswi192168.3.15LWeb serverWeb serverSwMP Credentials(/) //atl-ap2.ipswitch_mipswi192168.3.15LWeb server <tr <="" th=""><th>Progress S</th><th>Summary 📀</th><th></th><th></th><th>Devic</th><th>es Discovered</th><th></th><th></th><th></th><th></th></tr> <tr><th>Device Limit Unlimited atl-cisco4506.jpswitch_m 192168.3.1 Web server Existing Devices 147 192168.3.3 192168.3.3 HP HP_J4121A P Switch Discovered Devices 127 192168.3.4 192168.3.4 Web server Web server Network Traffic DC 192168.3.5 Web server Web server SMMP Bytes (in/out) 419461./357524 DC 192168.3.5 Web server Web server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327/24 PM 192168.3.0 192168.3.0 HP hp LaserJet 1 Web server Scan Start 6/001.06 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/001.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.jpswitch_mipswi 192168.3.15 Web server SvMP Credentials (1/1) atl-ap2.ipswitch_mipswi</th><th>Device</th><th>Summary</th><th>Host Name</th><th>Address</th><th>Brand</th><th>Model</th><th>Operating System</th><th>Role</th><th></th><th></th></tr> <tr><td>Existing Devices 147 192.168.3.3 192.168.3.3 HP HP J4121A P Switch Discovered Devices 127 192.168.3.4 192.168.3.4 192.168.3.4 Web server Network Traffic DC 192.168.3.4 192.168.3.4 Web server SNMP Bytes (in/out) 419461./357524 DC 192.168.3.5 Web server Scanned 180 of 255 NPIDS1ACD 192.168.3.7 HP HP Laser/let F Printer Scan Start 6/17/2009.327:24 PM 192.168.3.0 192.168.3.0 HP hp Laser/let 1 Web server Scan End </td><td>Device Limit</td><td>Unlimited</td><td>atl-cisco4506.ipswitch_m</td><td>192.168.3.1</td><td></td><td></td><td></td><td>Web server</td><td>•</td><td>com</td></tr> <tr><td>Discovered Devices 127 192.168.3.4 192.168.3.4 Web server Network Traffic DC 192.168.3.5 Web server SNMP Bytes (in/out) 419461 / 357524 DC 192.168.3.5 Web server PDU (in/out) 7600 / 7766 EXCH2007 192.168.3.7 HP HP Laserlet F Printer Scansed 180 of 255 NPID51ACD 192.168.3.7 HP HP Laserlet I Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.9 Web server Scan End 192.168.3.10 192.168.3.10 HP HP Laserlet 4 Printer Eageed Time 00.01.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192.168.3.15 Web server Stom Vpe Range atl-ap3.ipswitch_mipswi 192.168.3.15 Web server Stom Vpe Range atl-ap3.ipswitch_mipswi 192.1</td><td>Existing Devices</td><td>147</td><td>192.168.3.3</td><td>192.168.3.3</td><td>HP</td><td>HP J4121A P</td><td></td><td>Switch</td><td>•</td><td>con</td></tr> <tr><td>Netw DC 192168.3.5 Web server SNMP Bytes (in/out) 419461 / 357524 EXCH2007 192168.3.6 Email server PDU (in/out) 7600 / 7766 EXCH2007 192168.3.6 Email server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327:24 PM 192168.3.9 192168.3.9 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Web server Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.11 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap21pswitch_mipswi 192168.3.15 Web server Web server Scan Type Range atl-ap31pswitch_mipswi 192168.3.15 Web server Web server</td><td>Discovered Devices</td><td>127</td><td>192.168.3.4</td><td>192.168.3.4</td><td></td><td></td><td></td><td>Web server</td><td></td><td>con</td></tr> <tr><td>SNMP Bytes (in/out) 419461 / 357524 End of the server End of the server PDU (in/out) 7600 / 7766 EXCH2007 192.168.3.6 Email server Scanned 180 of 255 NPID51ACD 192.168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.9 Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.10 HP HP LaserJet 1 Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.10 192.168.3.10 HP HP LaserJet 4 Printer Bapsed Time 00:01:06 ATL-COLOR1 192.168.3.10 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_m.ipswi 192.168.3.15 Web server SNMP Credentials (1 / 1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server Web server Web server Web server Web server Web server</td><td>Netw</td><td>ork Traffic</td><td>DC</td><td>192 168 3 5</td><td></td><td></td><td></td><td>Web server</td><td></td><td>con</td></tr> <tr><td>PDU (in/out) 7600 / 7766 EX.RELOP 192.168.3.6 Email server Scanned 180 of 255 NPIDS1ACD 192.168.3.7 HP HP LaserJet F Printer Seasion Metrics NPID51ACD 192.168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192.168.3.9 192.168.3.9 Web server Web server Scan Start 6/17/2009 327:24 PM 192.168.3.9 192.168.3.9 Web server Web server Scan Start 6/17/2009 327:24 PM 192.168.3.10 192.168.3.10 HP HP LaserJet 1 Web server Scan Try 0.001.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap2.ipswitch_mipswi 192.168.3.15 Web server SNMP Credentials (1/1) atl-ap2.ipswitch_mipswi 192.168.3.16 Web server Windows Credentials (0/0) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server</td><td>SNMP Bytes (in/out)</td><td>419461 / 357524</td><td>ENCURRAT</td><td>10216926</td><td></td><td></td><td></td><td>Freell searce</td><td></td><td></td></tr> <tr><td>Scanned 180 of 255 NPIDS1ACD 192168.3.7 HP HP LaserJet F Printer Seasion Metrics NPID574F8 192168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 3:27:24 PM 192168.3.9 192168.3.9 Web server Web server Scan End 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Bapsed Time 00.01.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1ipswitch_mipswi 192168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2ipswitch_mipswi 192168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192168.3.16 Web server</td><td>PDU (in/out)</td><td>7600 / 7766</td><td>EXCH2007</td><td>192.108.3.0</td><td></td><td></td><td></td><td>Email server</td><td>_</td><td>com</td></tr> <tr><td>Session Metrics NPI25F4F8 192168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192168.3.9 192168.3.9 Web server Web server Scan End 192168.3.0 192168.3.0 HP HP LaserJet 4 Printer Elapsed Time 00.01.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1ipswitch_mipswi 192168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2ipswitch_mipswi 192168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192168.3.16 Web server</td><td>Scanned</td><td>180 of 255</td><td>NPID51ACD</td><td>192.168.3.7</td><td>HP</td><td>HP LaserJet F</td><td></td><td>Printer</td><td>٠</td><td>con</td></tr> <tr><td>Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 Web server Scan End 192.168.3.0 192.168.3.0 HP HP LaserJet 4 Printer Elapsed Time 00:0.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_m.ipswi 192.168.3.15 Web server Web server SNMP Credentials (1/1) atl-ap2.ipswitch_m.ipswi 192.168.3.16 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server</td><td>Sessio</td><td>on Metrics</td><td>NPI25F4F8</td><td>192.168.3.8</td><td>HP</td><td>hp LaserJet 1</td><td></td><td>Web server</td><td>•</td><td>con</td></tr> <tr><td>Scan End 192.168.3.10 HP HP Laserlet 4 Printer Elapsed Time 00:0.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192.168.3.14 Web server Web server SNMP Credentials (1/1) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server Web server Windows Credentials (0/0) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server</td><td>Scan Start</td><td>6/17/2009 3:27:24 PM</td><td>192.168.3.9</td><td>192.168.3.9</td><td></td><td></td><td></td><td>Web server</td><td>•</td><td>con</td></tr> <tr><td>Elapsed Time 00:01:06 ATL-COLOR1 192:168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192:168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2.ipswitch_mipswi 192:168.3.16 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192:168.3.16 Web server</td><td>Scan End</td><td></td><td>192.168.3.10</td><td>192.168.3.10</td><td>HP</td><td>HP LaserJet 4</td><td></td><td>Printer</td><td></td><td>Dev</td></tr> <tr><td>Session Settings att-ap1.jpswitch_m.ipswi 192.168.3.14 Web server SNMP Credentials (1/1) att-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) att-ap3.ipswitch_m.ipswi 192.168.3.16 Web server</td><td>Elapsed Time</td><td>00.01.06</td><td>ATL-COLOR1</td><td>192.168.3.11</td><td>HP</td><td>HP Color Las</td><td></td><td>Printer</td><td></td><td>com</td></tr> <tr><td>Scan Type Range airiap.ipsmitor_mapsin_ips.ipsa.103.24 intelligence SNMP Credentials (1/1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0/0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server</td><td>Sessio</td><td>n Settings</td><td>att and installed on install</td><td>102169214</td><td></td><td></td><td></td><td>Web searces</td><td>-</td><td></td></tr> <tr><td>SNMP Credentials (1 / 1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server</td><td>Scan Type</td><td>Range</td><td>an-abribanci miban</td><td>192.100.3.14</td><td></td><td></td><td></td><td>web server</td><td>_</td><td>LOI</td></tr> <tr><td>Windows Credentials (0 / 0) att-ap3.jpswitch_m.jpswi 192.168.3.16 Web server</td><td>SNMP Credentials</td><td>(1/1)</td><td>atl-ap2.ipswitch_m.ipswi</td><td>192.168.3.15</td><td></td><td></td><td></td><td>Web server</td><td>•</td><td>con</td></tr> <tr><td>· · · · · · · · · · · · · · · · · · ·</td><td>Windows Credentials</td><td>s (0 / 0)</td><td>atl-ap3.ipswitch_m.ipswi</td><td>192.168.3.16</td><td></td><td></td><td></td><td>Web server</td><td>•</td><td>com</td></tr> <tr><td></td><td></td><td></td><td>·</td><td></td><td>m</td><td></td><td></td><td></td><td></td><td>,</td></tr> <tr><td>Progress 70.59 %</td><td></td><td></td><td>Progress</td><td></td><td></td><td>70.59 %</td><td>-</td><td></td><td></td><td></td></tr> <tr><td>Device Information</td><td></td><td></td><td>-</td><td></td><td>Devic</td><td>e Information</td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>	Progress S	Summary 📀			Devic	es Discovered					Device Limit Unlimited atl-cisco4506.jpswitch_m 192168.3.1 Web server Existing Devices 147 192168.3.3 192168.3.3 HP HP_J4121A P Switch Discovered Devices 127 192168.3.4 192168.3.4 Web server Web server Network Traffic DC 192168.3.5 Web server Web server SMMP Bytes (in/out) 419461./357524 DC 192168.3.5 Web server Web server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327/24 PM 192168.3.0 192168.3.0 HP hp LaserJet 1 Web server Scan Start 6/001.06 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/001.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.jpswitch_mipswi 192168.3.15 Web server SvMP Credentials (1/1) atl-ap2.ipswitch_mipswi	Device	Summary	Host Name	Address	Brand	Model	Operating System	Role			Existing Devices 147 192.168.3.3 192.168.3.3 HP HP J4121A P Switch Discovered Devices 127 192.168.3.4 192.168.3.4 192.168.3.4 Web server Network Traffic DC 192.168.3.4 192.168.3.4 Web server SNMP Bytes (in/out) 419461./357524 DC 192.168.3.5 Web server Scanned 180 of 255 NPIDS1ACD 192.168.3.7 HP HP Laser/let F Printer Scan Start 6/17/2009.327:24 PM 192.168.3.0 192.168.3.0 HP hp Laser/let 1 Web server Scan End	Device Limit	Unlimited	atl-cisco4506.ipswitch_m	192.168.3.1				Web server	•	com	Discovered Devices 127 192.168.3.4 192.168.3.4 Web server Network Traffic DC 192.168.3.5 Web server SNMP Bytes (in/out) 419461 / 357524 DC 192.168.3.5 Web server PDU (in/out) 7600 / 7766 EXCH2007 192.168.3.7 HP HP Laserlet F Printer Scansed 180 of 255 NPID51ACD 192.168.3.7 HP HP Laserlet I Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.9 Web server Scan End 192.168.3.10 192.168.3.10 HP HP Laserlet 4 Printer Eageed Time 00.01.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192.168.3.15 Web server Stom Vpe Range atl-ap3.ipswitch_mipswi 192.168.3.15 Web server Stom Vpe Range atl-ap3.ipswitch_mipswi 192.1	Existing Devices	147	192.168.3.3	192.168.3.3	HP	HP J4121A P		Switch	•	con	Netw DC 192168.3.5 Web server SNMP Bytes (in/out) 419461 / 357524 EXCH2007 192168.3.6 Email server PDU (in/out) 7600 / 7766 EXCH2007 192168.3.6 Email server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327:24 PM 192168.3.9 192168.3.9 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Web server Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.11 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap21pswitch_mipswi 192168.3.15 Web server Web server Scan Type Range atl-ap31pswitch_mipswi 192168.3.15 Web server Web server	Discovered Devices	127	192.168.3.4	192.168.3.4				Web server		con	SNMP Bytes (in/out) 419461 / 357524 End of the server End of the server PDU (in/out) 7600 / 7766 EXCH2007 192.168.3.6 Email server Scanned 180 of 255 NPID51ACD 192.168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.9 Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.10 HP HP LaserJet 1 Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.10 192.168.3.10 HP HP LaserJet 4 Printer Bapsed Time 00:01:06 ATL-COLOR1 192.168.3.10 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_m.ipswi 192.168.3.15 Web server SNMP Credentials (1 / 1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server Web server Web server Web server Web server Web server	Netw	ork Traffic	DC	192 168 3 5				Web server		con	PDU (in/out) 7600 / 7766 EX.RELOP 192.168.3.6 Email server Scanned 180 of 255 NPIDS1ACD 192.168.3.7 HP HP LaserJet F Printer Seasion Metrics NPID51ACD 192.168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192.168.3.9 192.168.3.9 Web server Web server Scan Start 6/17/2009 327:24 PM 192.168.3.9 192.168.3.9 Web server Web server Scan Start 6/17/2009 327:24 PM 192.168.3.10 192.168.3.10 HP HP LaserJet 1 Web server Scan Try 0.001.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap2.ipswitch_mipswi 192.168.3.15 Web server SNMP Credentials (1/1) atl-ap2.ipswitch_mipswi 192.168.3.16 Web server Windows Credentials (0/0) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server	SNMP Bytes (in/out)	419461 / 357524	ENCURRAT	10216926				Freell searce			Scanned 180 of 255 NPIDS1ACD 192168.3.7 HP HP LaserJet F Printer Seasion Metrics NPID574F8 192168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 3:27:24 PM 192168.3.9 192168.3.9 Web server Web server Scan End 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Bapsed Time 00.01.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1ipswitch_mipswi 192168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2ipswitch_mipswi 192168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192168.3.16 Web server	PDU (in/out)	7600 / 7766	EXCH2007	192.108.3.0				Email server	_	com	Session Metrics NPI25F4F8 192168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192168.3.9 192168.3.9 Web server Web server Scan End 192168.3.0 192168.3.0 HP HP LaserJet 4 Printer Elapsed Time 00.01.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1ipswitch_mipswi 192168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2ipswitch_mipswi 192168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192168.3.16 Web server	Scanned	180 of 255	NPID51ACD	192.168.3.7	HP	HP LaserJet F		Printer	٠	con	Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 Web server Scan End 192.168.3.0 192.168.3.0 HP HP LaserJet 4 Printer Elapsed Time 00:0.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_m.ipswi 192.168.3.15 Web server Web server SNMP Credentials (1/1) atl-ap2.ipswitch_m.ipswi 192.168.3.16 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Sessio	on Metrics	NPI25F4F8	192.168.3.8	HP	hp LaserJet 1		Web server	•	con	Scan End 192.168.3.10 HP HP Laserlet 4 Printer Elapsed Time 00:0.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192.168.3.14 Web server Web server SNMP Credentials (1/1) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server Web server Windows Credentials (0/0) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server	Scan Start	6/17/2009 3:27:24 PM	192.168.3.9	192.168.3.9				Web server	•	con	Elapsed Time 00:01:06 ATL-COLOR1 192:168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192:168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2.ipswitch_mipswi 192:168.3.16 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192:168.3.16 Web server	Scan End		192.168.3.10	192.168.3.10	HP	HP LaserJet 4		Printer		Dev	Session Settings att-ap1.jpswitch_m.ipswi 192.168.3.14 Web server SNMP Credentials (1/1) att-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) att-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Elapsed Time	00.01.06	ATL-COLOR1	192.168.3.11	HP	HP Color Las		Printer		com	Scan Type Range airiap.ipsmitor_mapsin_ips.ipsa.103.24 intelligence SNMP Credentials (1/1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0/0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Sessio	n Settings	att and installed on install	102169214				Web searces	-		SNMP Credentials (1 / 1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Scan Type	Range	an-abribanci miban	192.100.3.14				web server	_	LOI	Windows Credentials (0 / 0) att-ap3.jpswitch_m.jpswi 192.168.3.16 Web server	SNMP Credentials	(1/1)	atl-ap2.ipswitch_m.ipswi	192.168.3.15				Web server	•	con	· · · · · · · · · · · · · · · · · · ·	Windows Credentials	s (0 / 0)	atl-ap3.ipswitch_m.ipswi	192.168.3.16				Web server	•	com				·		m					,	Progress 70.59 %			Progress			70.59 %	-				Device Information			-		Devic	e Information															
Progress S	Summary 📀			Devic	es Discovered																																																																																																																																																																																																																																	
Device Limit Unlimited atl-cisco4506.jpswitch_m 192168.3.1 Web server Existing Devices 147 192168.3.3 192168.3.3 HP HP_J4121A P Switch Discovered Devices 127 192168.3.4 192168.3.4 Web server Web server Network Traffic DC 192168.3.5 Web server Web server SMMP Bytes (in/out) 419461./357524 DC 192168.3.5 Web server Web server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327/24 PM 192168.3.0 192168.3.0 HP hp LaserJet 1 Web server Scan Start 6/001.06 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/001.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.jpswitch_mipswi 192168.3.15 Web server SvMP Credentials (1/1) atl-ap2.ipswitch_mipswi	Device	Summary	Host Name	Address	Brand	Model	Operating System	Role																																																																																																																																																																																																																														
Existing Devices 147 192.168.3.3 192.168.3.3 HP HP J4121A P Switch Discovered Devices 127 192.168.3.4 192.168.3.4 192.168.3.4 Web server Network Traffic DC 192.168.3.4 192.168.3.4 Web server SNMP Bytes (in/out) 419461./357524 DC 192.168.3.5 Web server Scanned 180 of 255 NPIDS1ACD 192.168.3.7 HP HP Laser/let F Printer Scan Start 6/17/2009.327:24 PM 192.168.3.0 192.168.3.0 HP hp Laser/let 1 Web server Scan End	Device Limit	Unlimited	atl-cisco4506.ipswitch_m	192.168.3.1				Web server	•	com																																																																																																																																																																																																																												
Discovered Devices 127 192.168.3.4 192.168.3.4 Web server Network Traffic DC 192.168.3.5 Web server SNMP Bytes (in/out) 419461 / 357524 DC 192.168.3.5 Web server PDU (in/out) 7600 / 7766 EXCH2007 192.168.3.7 HP HP Laserlet F Printer Scansed 180 of 255 NPID51ACD 192.168.3.7 HP HP Laserlet I Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.9 Web server Scan End 192.168.3.10 192.168.3.10 HP HP Laserlet 4 Printer Eageed Time 00.01.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192.168.3.15 Web server Stom Vpe Range atl-ap3.ipswitch_mipswi 192.168.3.15 Web server Stom Vpe Range atl-ap3.ipswitch_mipswi 192.1	Existing Devices	147	192.168.3.3	192.168.3.3	HP	HP J4121A P		Switch	•	con																																																																																																																																																																																																																												
Netw DC 192168.3.5 Web server SNMP Bytes (in/out) 419461 / 357524 EXCH2007 192168.3.6 Email server PDU (in/out) 7600 / 7766 EXCH2007 192168.3.6 Email server Scanned 180 of 255 NPID51ACD 192168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 327:24 PM 192168.3.9 192168.3.9 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Web server Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.11 HP HP LaserJet 4 Printer Scan Start 6/17/2009 327:24 PM 192168.3.10 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap21pswitch_mipswi 192168.3.15 Web server Web server Scan Type Range atl-ap31pswitch_mipswi 192168.3.15 Web server Web server	Discovered Devices	127	192.168.3.4	192.168.3.4				Web server		con																																																																																																																																																																																																																												
SNMP Bytes (in/out) 419461 / 357524 End of the server End of the server PDU (in/out) 7600 / 7766 EXCH2007 192.168.3.6 Email server Scanned 180 of 255 NPID51ACD 192.168.3.7 HP HP LaserJet F Printer Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.9 Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 192.168.3.10 HP HP LaserJet 1 Web server Scan Start 6/17/2009 3:27:24 PM 192.168.3.10 192.168.3.10 HP HP LaserJet 4 Printer Bapsed Time 00:01:06 ATL-COLOR1 192.168.3.10 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_m.ipswi 192.168.3.15 Web server SNMP Credentials (1 / 1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server Web server Web server Web server Web server Web server	Netw	ork Traffic	DC	192 168 3 5				Web server		con																																																																																																																																																																																																																												
PDU (in/out) 7600 / 7766 EX.RELOP 192.168.3.6 Email server Scanned 180 of 255 NPIDS1ACD 192.168.3.7 HP HP LaserJet F Printer Seasion Metrics NPID51ACD 192.168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192.168.3.9 192.168.3.9 Web server Web server Scan Start 6/17/2009 327:24 PM 192.168.3.9 192.168.3.9 Web server Web server Scan Start 6/17/2009 327:24 PM 192.168.3.10 192.168.3.10 HP HP LaserJet 1 Web server Scan Try 0.001.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap2.ipswitch_mipswi 192.168.3.15 Web server SNMP Credentials (1/1) atl-ap2.ipswitch_mipswi 192.168.3.16 Web server Windows Credentials (0/0) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server	SNMP Bytes (in/out)	419461 / 357524	ENCURRAT	10216926				Freell searce																																																																																																																																																																																																																														
Scanned 180 of 255 NPIDS1ACD 192168.3.7 HP HP LaserJet F Printer Seasion Metrics NPID574F8 192168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 3:27:24 PM 192168.3.9 192168.3.9 Web server Web server Scan End 192168.3.10 192168.3.10 HP HP LaserJet 4 Printer Bapsed Time 00.01.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1ipswitch_mipswi 192168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2ipswitch_mipswi 192168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192168.3.16 Web server	PDU (in/out)	7600 / 7766	EXCH2007	192.108.3.0				Email server	_	com																																																																																																																																																																																																																												
Session Metrics NPI25F4F8 192168.3.8 HP hp LaserJet 1 Web server Scan Start 6/17/2009 327:24 PM 192168.3.9 192168.3.9 Web server Web server Scan End 192168.3.0 192168.3.0 HP HP LaserJet 4 Printer Elapsed Time 00.01.06 ATL-COLOR1 192168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1ipswitch_mipswi 192168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2ipswitch_mipswi 192168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192168.3.16 Web server	Scanned	180 of 255	NPID51ACD	192.168.3.7	HP	HP LaserJet F		Printer	٠	con																																																																																																																																																																																																																												
Scan Start 6/17/2009 3:27:24 PM 192.168.3.9 Web server Scan End 192.168.3.0 192.168.3.0 HP HP LaserJet 4 Printer Elapsed Time 00:0.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_m.ipswi 192.168.3.15 Web server Web server SNMP Credentials (1/1) atl-ap2.ipswitch_m.ipswi 192.168.3.16 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Sessio	on Metrics	NPI25F4F8	192.168.3.8	HP	hp LaserJet 1		Web server	•	con																																																																																																																																																																																																																												
Scan End 192.168.3.10 HP HP Laserlet 4 Printer Elapsed Time 00:0.06 ATL-COLOR1 192.168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192.168.3.14 Web server Web server SNMP Credentials (1/1) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server Web server Windows Credentials (0/0) atl-ap3.ipswitch_mipswi 192.168.3.16 Web server	Scan Start	6/17/2009 3:27:24 PM	192.168.3.9	192.168.3.9				Web server	•	con																																																																																																																																																																																																																												
Elapsed Time 00:01:06 ATL-COLOR1 192:168.3.11 HP HP Color Las Printer Scan Type Range atl-ap1.ipswitch_mipswi 192:168.3.14 Web server Web server SNMP Credentials (1 / 1) atl-ap2.ipswitch_mipswi 192:168.3.16 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_mipswi 192:168.3.16 Web server	Scan End		192.168.3.10	192.168.3.10	HP	HP LaserJet 4		Printer		Dev																																																																																																																																																																																																																												
Session Settings att-ap1.jpswitch_m.ipswi 192.168.3.14 Web server SNMP Credentials (1/1) att-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) att-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Elapsed Time	00.01.06	ATL-COLOR1	192.168.3.11	HP	HP Color Las		Printer		com																																																																																																																																																																																																																												
Scan Type Range airiap.ipsmitor_mapsin_ips.ipsa.103.24 intelligence SNMP Credentials (1/1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0/0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Sessio	n Settings	att and installed on install	102169214				Web searces	-																																																																																																																																																																																																																													
SNMP Credentials (1 / 1) atl-ap2.ipswitch_m.ipswi 192.168.3.15 Web server Windows Credentials (0 / 0) atl-ap3.ipswitch_m.ipswi 192.168.3.16 Web server	Scan Type	Range	an-abribanci miban	192.100.3.14				web server	_	LOI																																																																																																																																																																																																																												
Windows Credentials (0 / 0) att-ap3.jpswitch_m.jpswi 192.168.3.16 Web server	SNMP Credentials	(1/1)	atl-ap2.ipswitch_m.ipswi	192.168.3.15				Web server	•	con																																																																																																																																																																																																																												
· · · · · · · · · · · · · · · · · · ·	Windows Credentials	s (0 / 0)	atl-ap3.ipswitch_m.ipswi	192.168.3.16				Web server	•	com																																																																																																																																																																																																																												
			·		m					,																																																																																																																																																																																																																												
Progress 70.59 %			Progress			70.59 %	-																																																																																																																																																																																																																															
Device Information			-		Devic	e Information																																																																																																																																																																																																																																

For more information, see Discovering network devices in Help.

About Device Roles

When WhatsUp Gold discovers devices, it tries to determine the type of device so that it can monitor the device appropriately. To determine the type of device, WhatsUp Gold compares the discovered attributes of the device to a set of criteria called a *device role*.

Device roles do two things:

- Specify the criteria that a device must match to be identified as the device role.
- Specify the monitoring configuration that is applied to the device when it is added to WhatsUp Gold.

WhatsUp Gold provides several default device roles that are used to identify most common network devices. If your network includes devices that are not identified by this default set, you can create custom device roles.

Device roles are configured on the Device Role Settings dialog which can be accessed from the Discovery Console's Advanced menu. This dialog allows you to specify device characteristics that WhatsUp will use during discovery to categorize the devices in your network by specific device roles.

Device Role Settings	
This dialog allows you to spe going to be configured after	JS cify the default configuration behavior of the WhatsUp discovery, how a device is its role has been identified.
Device	
DHCP Server	A device that provides automatic host configuration through the Dynamic
Content of the server s	Host Configuration Protocol (DHCP).
🚦 Firewall	🖗 Performance monitors
FTP server E	Sping Latency and Availability
Printer	Configure
😁 Router	Active monitors
SAN device	
Switch	i ⊂g Ping ¥ Fan
Signature Telnet server	Temperature Versupply
UPS 🗸	Configure
Configure Add 🚳	J.+
	Help Close

For more information, see Using Device Roles in Help.

About Alert Center

WhatsUp Gold Alert Center handles alerting on performance monitors, passive monitors, WhatsUp Gold system health, and WhatsUp Gold Flow Monitor plug-in through user-configured thresholds and notification policies.

Thresholds

Thresholds are the benchmark mechanisms Alert Center uses to check against the database. If WhatsUp Gold finds that an aspect has exceeded or fallen below the parameters you set in a threshold, it is considered *out of threshold*. These out of threshold aspects are logged as *items*.

You can find data for Alert Center items on the Alert Center Home page and in Alert Center reports. For more information, see *Configuring Alert Center thresholds* in Help.

lame 🔺	Description New	
Flow Monitor Conversation Partners Exceeds 1000	Hosts that sent or received data with more than 1000 conversation partner	
Flow Monitor Failed Connections Exceeds 1000	Hosts that have sent or received more than 1000 failed connections in the	
Flow Monitor Interface Traffic Exceeds 90%	Average incoming or outgoing NetFlow interface traffic during the past 60 Delete	
Flow Monitor Top Sender/Receiver Exceeds 500 N	B Hosts that have sent or received more than 500 MB in the last 15 minutes	
Performance CPU Utilization Exceeds 90% 👰 E	dit WhatsUp Health Threshold	
Performance Disk Utilization Exceeds 95%	ne	
Performance Interface Utilization Exceeds 90	atsUp Health	
Performance Memory Utilization Exceeds 95	Thrashold	
Performance Ping Availability Falls Below 95 T	his threshold will alert when:	1
Performance Ping Response Time Exceeds	☑ Database size exceeds 80 % ▼ (Size limit: 4 GB)	
WhatsUp Health	3000	
L'e source article contraction of the second s	I total genormance monitors exceed 3000	
	Total performance monitor records exceed 2000000	
	Total passive monitor records exceed 1000000	
	Tatal avaired records avceed 500000	
	Total devices being monitored exceeds 90 % of license limit	
	The second second	
	View WhatsUp database	
×	🥥 Database 🛛 🔍 Services 🚽 🍓 Flow Monitor	-
	Natification	
	mail Boh and Sue	
	Threshold Check	1
c	heck threshold every 5 minutes.	
		OK
	Automatically resolve items no longer out of threshold	Cancel

Notification policies

When an aspect goes out of threshold and is logged as an item, associated notification policies begin sending notifications to alert users of the problem. These policies can include multiple steps that begin at user-specified intervals to notify multiple people of persisting problems. After you have fixed a problem, you can notify other users of the fix and stop subsequent steps of a running notification policy. For more information, see *About notification policies* and *About running notifications* in Help.

Alert Center Home

Alert Center Home is the Alert Center control page. Similar to the WhatsUp Gold Home page, Alert Center Home displays threshold data in workspace reports. From these threshold workspace reports, you can update out of threshold items. For more information, see *About Alert Center Home* and *Updating Alert Center items* in Help.

	View: All	• Eilter	by: No Filter	Sort by: Items ou	t of threshold		
Running Notification Policies							
Policy Name		Notification	Progress	Triggered by			Time Creat
		Th	ere are currently no Ri	unning Notification Policies			
Performance Ping Availability Falls I	3elow 95% (36 it	ems)	.	Performance CPU Utilization Exceeds 9	0% (7 items)		8) (D) (
Le Description: Average Ping Availability	during the past 30	minutes fails below 95%		Pescription: Average CPU Utilization durin	ng the past 30	minutes exceeds 90%	
evice	Interface	Percent nacket Loss	Time Alerted	Device	CPU	Average Ottligation	Time Alerti
spreacoff inswitch in inswitch com	192 168 3 133	65.7%	Mon 06/01 2:58 PM	all-ibenton-lan inswitch im inswitch com	Intel (1)	97.7 %	Tue 06/02 2:00 F
-build inswitch minswitch com	192 168 3 42	66.7 %	Bat 05/30 12:26 PM	att-ibenton-lap inswitch im inswitch com	intel (2)	947%	Tue 06/02 2:00 F
-build inswitch m inswitch com	192 168 1 39	667%	Sat 05/30 12:26 PM	IB-XP-VEEM	Intel (1)	91.0 %	Eti 05/29 1/35 P
wiki servers inswitch com	192 168 3 48	66.7 %	Sat 05/30 11:37 AM	ATL 132	intel (1)	927%	Tue 05/25 11:08 A
CH2007	192 168 3.6	667%	Set 05/30 3 18 AM	aff-rdp1 ipswitch mipswitch com	intel (1)	01.0 %	Fit 05/15 8:21 F
G	192 168 3.5	66.6 %	Sat 05/30 3 18 AM	all-savion3 ipswitch m ipswitch com	Intel (T)	100.0 %	Fri 05/15 9 50 A
I-Install-v14 ipswitch m leswitch.com	192,168,3,253	66.6 %	Sat 05/30 3:18 AM	ARENAMEDXPPRO	Intel (1)	100.0 %	Fri 05/15 9:20 /
STALLWIN03	192 168 3 69	66.6 %	Sat 05/30 3:18 AM				
-ci-main lpswitch mipswitch.com	192,168,3.52	66.6 %	Sat 05/30 3.18 AM				1.000
WIN03	192.168.3.204	65.7 %	Sat 05/30 3:18 AM	Performance Disk Utilization Exceeds 9	5% (4 items)		
134.ipswitch_mipswitch.com	192.168.3.134	66.7 %	Fri 05/29 1:07 PM				
Fighao3.ipswitch_m.ipswitch.com	192,168.3.131	66.7 %	Fri 05/29 10:29 AM	Description: Average Disk Utilization during	g the past 1 d	ays exceeds 95%	
KS116TEST	192.168.3.187	65.7%	Wed 05/27 11:15 AM	The second se	mark.	Looper of the sector	The state
TL-QA64bit	192,168.3.30	66.6 %	Fri 05/22 1:35 PM	Device	Utsk	Average utilization	Lime Alerti
L-QA2K8-64bit	192.168.3.214	0.0 %	Fri 05/22 9:05 AM	att-torancheau.ipswitch_m.ipswitch.com	C.1	90.0 %	Sat 05/23 6.44 /
L132	192.168.3.132	65.7 %	Thu 05/21 8:18 AM	an-sayton3 ipswitch_m ipswitch.com	Ch	95.0 %	Sat 05/16 6 41 4
TL103	192.168.3.103	66.7 %	Wed 05(20 5:07 PM	JJ-1E31	61	90.0 %	Sal 00/10 0.41 A
Hbrancheau ipswitch_m ipswitch.com	192.168.3.142	66.6%	Wed 05/20 4:27 PM	an ob observer unbawter com	u)	90.2 %	341 00/10 5/41 /
500-1.ipswitch_m.ipswitch.com	192.168.3.219	66.7 %	Wed 05/20 9:48 AM				
TL-JZH402-W2K8	192,168,3,114	66.6 %	Wed 05/20 9:18 AM	NetFlow Conversation Partners Exceeds 100	0		A 1
I-findemann.ipswitch_m.ipswitch.com	192.168.3.99	66.7 %	Tue 05/19 7:45 AM				
I-Jindemann2.ipswitch_m.ipswitch.com	192,168.3.100	65.7 %	Tue 05/19 7:45 AM	Description: Hosts that sent or received d	ata with more	than 1000 conversation	partners in the last 15
ERVER03INSTALL	192,168,3.93	66.7 %	Mon 05/18 11:57 AM	minutes			
L-QA2K3-64BIT	192.168.3.246	55.5%	Mon 05/18 10:57 AM	the second			1/2/07+08/0
WUGSQL	192.168.3.224	65.7 %	Mon 05/18 10:36 AM	Host Conversation	Partners		Time Alerta
6-tphung ipswitch_m.ipswitch.com	192.168.3.82	66.7 %	Mon 05/18 10:05 AM	The second s	1291354S	0.07080-00028	
B-XP-VEEM	192.168.3.213	65.7%	Mon 05/18 9:17 AM	No Conversatio	in Partner ale	rt detail records.	

Alert Center reports

Alert Center reports can be used to monitor and troubleshoot Alert Center data. You can access Alert Center reports from the web interface's Reports tab. For more information, see *Using Alert Center reports* in Help.

- Home	U Devices Report	s Alert Center	
	Alert Center Log entries during	Sunday, June 14, 2009 12:00:00 AM - Friday, June 26, 2009 08:49:00 AM	
	Filter by severity: No Filter ←	Date range: Custom Go Start time: 06/14/2009 12:00 AM • End time: 06/26/2009 8:49 AM •	
	Date +	Message	Severity
	Sunday, June 14, 2009 01:52:47 PM Sunday, June 14, 2009 01:28:52 PM	Stopping the Alert Center.	Information
	Sunday, June 14, 2009 01:26:31 PM	Stopping the Alert Center.	Information
	Sunday, June 14, 2009 01:13:36 PM Sunday, June 14, 2009 01:12:38 PM	Stopping the Alert Center.	Information
	Sunday, June 14, 2009 01:10:57 PM Sunday, June 14, 2009 01:10:34 PM	WugHealth threshold check failed. Error An error occured while performing the quer Started the Alert Center.	Error Information
	Sunday, June 14, 2009 01:09:26 PM Sunday, June 14, 2009 01:09:10 PM	Stopping the Alert Center. WugHealth threshold check failed. Error An error occured while performing the quer	Information Error
	Sunday, June 14, 2009 01:04:10 PM Sunday, June 14, 2009 01:03:47 PM	WugHealth threshold check failed. Error An error occured while performing the quer Started the Alert Center.	Error Information
	Sunday, June 14, 2009 12:52:09 PM Sunday, June 14, 2009 12:51:37 PM	Stopping the Alert Center. Started the Alert Center.	Information
	Sunday, June 14, 2009 12:51:37 PM Sunday, June 14, 2009 12:51:28 PM	Failed to find an assembly for the plugin for WhatsUp Health. GUID=7dde30a0-2015 Stopping the Alert Center.	Error
	Sunday, June 14, 2009 12:48:12 PM Sunday, June 14, 2009 12:45:48 PM	Failed to find an assembly for the plugin for WhatsUp Health. GUID=7dde30a0-20f5	Error
	Sunday, June 14, 2009 12:45:48 PM Sunday, June 14, 2009 12:45:48 PM	Failed to find an entropy of the plugin for WhatsUp Health. GUID=7dde30a0-20f5	Error
	Sunday, June 14, 2009 12:43:59 PM Sunday, June 14, 2009 12:43:29 PM	Storpping the Avent Center. Started the Alert Center.	Information

Using Alert Center and actions

In previous versions of WhatsUp Gold, you could only receive alerts on active and passive monitors. Alert Center brings alerting in WhatsUp Gold full-circle, by introducing alerts for performance monitors, the WhatsUp Gold system, and WhatsUp Gold Flow Monitor plug-in.

	Actions	Alert Center
Alerts on active monitors	•	
Alerts on passive monitors	•	•
Alerts on performance monitors		•
Alerts on the WhatsUp Gold database		•
Alerts on WhatsUp Gold services		•
Alerts on WhatsUp Gold Flow Monitor		•

The table below illustrates the feature you use to receive alerts of a particular type.

Though Alert Center is a powerful component of your network management solution, you will still leverage traditional alerting. The two features do not mirror one another and operate differently. While Alert Center relies on visual cues and email notifications, there are many different types of tasks you can perform using actions, such as service restarts, system reboots, sending text messages, and more. Neither feature is meant to be used exclusively, but rather should be used strategically to support your network management requirements. Together, Alert Center and actions complete alerting in WhatsUp Gold.

For more information on alerting through actions, see Using Actions in Help.

For more information on alerting through Alert Center, see About notification policies in Help.

New active monitors

WhatsUp Gold v14 Premium Edition includes 13 exciting new active monitors that greatly extend your monitoring and alerting capabilities:

- APC UPS Monitor
- Exchange Monitor
- Fan Monitor
- File Properties Monitor
- Folder Monitor
- FTP Monitor
- HTTP Content Monitor
- Network Statistics Monitor
- Printer Monitor
- Process Monitor
- Power Supply Monitor
- SQL Query Monitor
- Temperature Monitor

About the APC UPS Monitor

This monitor watches your American Power Conversion Uninterruptible Power Supply (APC UPS) device and alerts you when selected thresholds are met or exceeded, output states are reached, and/or abnormal conditions are met. For example, an alert can be sent when the UPS battery capacity is below 20%, when the battery temperature is high, when the battery is in bypass mode due to a battery overload state, and many other UPS alert conditions.

Add APC UPS Monitor			
<u>l</u> ame:			
APC UPS Monitor			
Degcription:			
Monitors APC UPS (Unive	rsal Power Supply) devices		
Thresholds:			
Parameter	Fail If		Configure
Battery Status	Battery status not 'normal'		
Battery Capacity	Battery capacity below 20%		
Battery Runtime	Battery runtime left below 5 minutes		
Output Load	Load above 95%		
Output State		Í	
Abnormal Condition F	Present		
AVR Boost Active			
Red Outer & Voltage			
Bad Output Voltage			
donitor the following abnor	mal conditions.		
Abnormal Condition		-	
Backfeed Protection	Relay Opened		
Battery Failure			Advanced.
Battery Voltage High			OK
Bypass Contactor St	uck in Bypass Condition	1	Cancel
	1.1.4.11.4.11		Composi

For more information, see Using the APC UPS Monitor in Help.

APC UPS Performance Monitor

In addition to the active APC UPS monitor, you can also set up an APC UPS performance monitor. This monitor collects statistical output power usage information and graphs APC UPS power utilization over time. This monitor detects when UPS devices are close to maximum performance level, and what time of day networking devices connected to UPS devices are using the most power--both indicating the need to equally distribute the load across several UPS devices.



About the Exchange Monitor

A new Exchange Monitor has been added that includes support to monitor Microsoft Exchange 2007 and 2010 Beta1. Use this version of the monitor to check Exchange roles and services, and performance thresholds.

New Exchange Monitor		7 . *
Name:		
Exchange 2007 Monitor		
Description:		
Exchange active monitor		
Performance aspects to monitor:		
Category		Configure
Hub Transport Server		
Mailbox Server		
Outlook Web Access		
Services to monitor: Service Name		
Active Directory Topology Service	E	
Anti-spam Update		
EdgeSync		
E File Distribution		
IMAP4		
Information Store	*	OK
♥ Use in rescan		Cancel

For more information, see *Monitoring Microsoft Exchange Servers in Help*.

About the Fan Monitor

The Fan Monitor checks select Cisco, Dell, and HP device fans and cooling devices, such as active and passive cooling components, to see that they are enabled and return a values that signal they are working properly. The monitor first checks to see if a device is a Dell, Cisco, or HP device, then checks any enabled fans and other cooling devices. If a fan is disabled, the monitor ignores it; if a fan does not return a value of 1 - Normal (for Cisco devices), 3 - OK (for Dell Servers), 1 - Normal (for Dell PowerConnect switches and routers), devices), 4 - OK (for HP ProCurve Servers), 2 - OK (for ProLiant switches and routers) the monitor is considered down.

Note: Not all types of device fans and cooling components may be able to be monitored using the Fan Monitor. Check the make and model of your device fan or cooling component before attempting to monitor.

🤣 Edit Fan Monitor	? 🔀
<u>N</u> ame: Fan	Advanced
Des <u>c</u> ription: Fan active monitor	OK Cancel

For more information, see Using the Fan Monitor in Help.

About the File Properties Monitor

This monitor checks to see if a file in a local folder, or on a network share, meets the conditions specified in the monitor's configuration. With this monitor you can check to see that a file is less or more than a specified number of megabytes, that a file has not been modified after a certain date, and more.

Vew File Properties Monitor	? 🔀
Name:	
Description:	
File Properties active monitor	
Path of the file to monitor:	
Monitor is up if	
<u>F</u> ile exists ▼	
✓ File size is less than bytes ≥	
✓ Last modified date is	
✓ File checksum using SHA1 v is	OK
	Cancel

For more information, see Using the File Properties Monitor in Help.

About the Folder Monitor

This monitor checks that a local or network share folder meets the conditions specified in the monitor configuration. For example, you can monitor folders for the existence of specific files, whether a folder exists, when a folder size is greater than or less than a specified size, when the number of files in a folder is greater than or less than a specified number of files, and more.

🤣 New Folder Monitor				? 💌
<u>N</u> ame:				
Des <u>c</u> ription:				
Folder active monitor				
Path of the folder to monitor:				
Include sub-folders				
- Files to include				
 Include all files 				
Include files with name	es matching following wildcard	expression		
— Monitor is up if				
<u>Folder</u> exists	•			
Actual folder size is	less than 👻		bytes 👻 🥵	
Folder size on disk is	less than 👻		bytes 👻 🕼	
☑ N <u>u</u> mber of files is	less than 👻		6	ОК
				Cancel
Mote: The Folder M	onitor only checks folde	rs local to a mac	ning on which	Whatsi in Gold

Note: The Folder Monitor only checks folders local to a machine on which WhatsUp Gold is installed, or folders on a network share accessible from the WhatsUp Gold device.

Note: This monitor uses the Windows credentials assigned to the device.

For more information, see Using the Folder Monitor in Help.

About the FTP Monitor

This active monitor performs upload, download, and delete tasks on designated FTP servers to ensure that the FTP servers are functioning properly. You can configure a single monitor to perform all three tasks, but note that if any one of the tasks fails, the entire monitor is considered down.

Add FTP Monitor		
<u>N</u> ame:		
Description:		
FTP Active Monitor		
Server settings		
ETP server:	Port:	
%Device.Address	21	
Usemame:		
P <u>a</u> ssword:		
Vse passive mode		
File actions		
Vpload V Download	Delete	
Timeout (seconds):		
3		
		OK
Use in rescan		Cancel

For more information, see Using the FTP Monitor in Help.

m

About the HTTP Content Monitor

This monitor requests a URL and checks the HTTP response against the expected content. If the response does not return the expected content, the monitor fails. You can use this monitor to ensure that your web pages are available for viewing or that they are rendering on certain browsers. For example, you can check to see that a web page contains specific content that is to be listed after a certain date, such as "Ipswitch introduces its newest release, WhatsUp Gold v14." If the monitor does not find the content that you request it to find, the monitor fails and you know to update your web page.

Note: You can access some HTTPS sites, such as Gmail's login screen, using the HTTP Content Monitor.

Add HTTP Content Monitor			
<u>l</u> ame:			
Description			
HTTP Content Monitor			
HTTP server settings			
URL:		~	
http://%Device.Address/Nm	Console/		
Authentication username:	Authentication password:		
Proxy server:	Proxy port:		
Timeout (seconds):			
Web page content			
Use regular expression			
Request URL contents			
		*	
			Advanced,
		-	
			OK
Use in resgan			Cancel

For more information, see Using the HTTP Content Monitor in Help.

About the Network Statistics Monitor

This monitor uses Simple Network Management Protocol (SNMP) to query a device to collect data on three device protocols, Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP), and alerts you when the thresholds you specify are met or exceeded. For example, you can use the *IP received discarded* threshold monitor to watch for situations where a router with Quality of Service (QOS) has priorities set for Voice over IP (VoIP).

Name:			
Description:			
Network Statistics Monitor			
Thresholds to monitor:			
Parameters 🔺	Down If	*	Configure
IP deliveries	Datagrams delivered exceeds 0	E	
IP receive errors	Received datagram errors exceeds 0		
P received	Received datagrams exceeds 0		
IP received discarded	Datagrams discarded exceeds 0		
P requests	Datagram requests exceeds 0		
4		•	
bject ID: 1.3.6.1.2.1.4.9 (iplr	Delivers)		
escription:			Advanced
he total number of input data	grams successfully delivered to IP user-		
rotocols (including ICMP).			OK
			Cancel

For more information, see Using the Network Statistics Monitor and Using a Network Statistic Monitor to check for IP data received and discarded in Help.

About the Printer Monitor

This monitor uses SNMP to collect data on SNMP-enabled network printers. If a failure criteria is met, any associated actions will fire. For example, you can monitor printer ink levels, for a paper jam, for low input media (paper), for a fuser that is over temperature, and more.

ame:		4
es <u>c</u> ription:		5
rinter active monitor		
Failure Criteria		
	148	
If the ink level in any of the cartridges falls below	%	
If the ink level in any of the cartridges falls below	%	
 If the ink level in any of the cartridges falls below If the printer registers any of the following alerts: 	%	
If the ink level in any of the cartridges falls below If the printer registers any of the following alerts: Alert Description	%	
If the ink level in any of the cartridges falls below If the printer registers any of the following alerts: Alert Description General Alerts	% 	
If the ink level in any of the cartridges falls below If the printer registers any of the following alerts: Alert Description General Alerts If Other	9%	
 If the jnk level in any of the cartridges falls below If the printer registers any of the following alerts: Alert Description General Alerts Other Unknown 	9%	Advanced
 If the ink level in any of the cartridges falls below If the printer registers any of the following alerts: Alert Description General Alerts Other Unknown Cover Open 	 	Advanced
 If the jink level in any of the cartridges falls below If the printer registers any of the following alerts: Alert Description General Alerts Other Unknown Cover Open Cover Closed 	_%	Advanced.

For more information, see Using the Printer Monitor in Help.

Printer Performance Monitor

m

In addition to the active printer monitor, you can also set up a printer performance monitor. This device-level performance monitor watches the ink and/or toner levels of a single printer cartridge. In order to monitor all cartridges on a single printer, you must create separate instances of the Printer Monitor for each cartridge.

Note: Because the monitor applies to a device-specific attribute (a specific printer cartridge), you must configure the monitor from the device's Device Properties dialog.

About the Process Monitor

This monitor uses SNMP to monitor the status of device processes and issues state changes as needed. The Process Monitor can detect whether a process is running. You can use this monitor to verify that anti-spyware or antivirus software is running of a device. If the monitor does not find the specified program running, an associated action will notify you of this potentially harmful vulnerability.

Add Process Monitor				
<u>N</u> ame:				
Description:				
Process Monitor				
Process Name:				
			210	Advanced
Threshold To Monitor				
Down if the process is	not loaded	•		ОК
				Cancel

For more information, see Using the Process Monitor and Using the Process Monitor to check for antivirus software in Help.

m

About the Power Supply Monitor

The Power Supply Monitor checks Cisco switches/routers, Dell servers, Dell Power Connect switches/routers, and HP ProCurve and switches/routers, HP ProLiant servers, and other device power supplies to see that they are enabled and return a value that signals they are in an up state. The monitor first checks to see if a device is a Cisco, Dell, or HP device, then checks any enabled power supply devices. If a power supply is disabled, the monitor ignores it; if a power supply does not return a value of 1 - Normal (for Cisco switches/routers), 3 - OK (for Dell server devices), 1 - OK (for Dell switches/routers), 4 - Good (for HP ProCurve switches/routers), or 2 - OK (for HP ProLiant servers), the monitor is considered down.

Note: Not all types of device power supplies may be able to be monitored using the Power Supply Monitor. Check the make and model of your device power supply before attempting to monitor.

New Power Supply Monitor	
Name:	Advanced
Description:	ОК
Power supply active monitor	Cancel

For more information, see Using the Power Supply Monitor in Help.

About the Microsoft SQL and MySQL Query Monitor

This monitor lets you check that certain conditions exists in a Microsoft SQL or MySQL database, based on a database query. You can define the criteria you want to exist in the database and as long as the specified conditions are present, the SQL Query Monitor is in an up state. If the database data changes outside the boundaries of the query criteria, the monitor triggers to a down state.

ame:		
escription		
QL Query active monit	or	
Server Properties		
Server type:		
Microsoft SQL Server	•	
Server Address:	Port (optional):	
ServerName\Instance		
SOL Query To Run		
sate doors to that		
		<u>Build</u>
		<u>Build</u>
		<u>Build</u>
Monitor is Up If		<u>Build</u>
Monitor is Up If	turned is equal to - 0	<u>Build</u> Verify
Monitor Is Up If	turned is equal to - 0	<u>B</u> uild Verify
Monitor Is Up If Number of rows rel Content of each re 	turned is equal to - 0 trieved row matches the following critieria:	<u>B</u> und
Monitor Is Up If Number of rows rel Content of each re Value of	turned is equal to - 0 trieved row matches the following critieria: Condition	<u>B</u> uild Verify
Monitor Is Up If Number of rows ref Content of each re Value of	turned is equal to - 0 trieved row matches the following critieria: Condition	<u>Build</u> <u>V</u> erify <u>Add</u> Edit
Monitor Is Up If Number of rows rel Content of each re Value of	turned is equal to - 0 trieved row matches the following critieria: Condition	Add. Edit. Dejete
Monitor Is Up If Number of rows ref Content of each re Value of	turned is equal to - 0 trieved row matches the following critieria. Condition	Add Edit Dejete
Monitor Is Up If Number of rows rel Content of each re Value of	turned is equal to - 0 trieved row matches the following critieria: Condition	Build Verify
Monitor Is Up If Number of rows ref Content of each re Value of Monitor is up if	turned is equal to - 0 trieved row matches the following critieria: Condition	Add_ Edit_ Dejete

For more information, see Using the SQL Query Monitor in Help.

About the Temperature Monitor

The Temperature Monitor checks select Cisco switches/routers, Dell servers, HP ProCurve switches/routers, and Ravica temperature probes to see that they return a value that signals they are in an up state. The monitor first checks to see if a device is a Cisco, Dell, HP, or Ravica device, then checks any enabled temperature monitor devices. If a temperature probe is disabled, the monitor ignores it; if a temperature probe does not return a value of 1 - Normal (for Cisco switches/routers), 3 - OK (for Dell server devices), 4 - Good (for HP ProCurve switches and routers), 2 - OK (for HP ProLiant servers), or 2 - normal (for Ravica temperature probes) the monitor is considered down.

New Power Supply Monitor	
Name:	Advanced
Description:	ОК
Temperature active monitor	Cancel

For more information, see Using the Temperature Monitor in Help.

About critical active monitors

Critical active monitors allow you to define a specific polling order for a device's active monitors; you can make one monitor dependent on another monitor on the same device, such as making an HTTP monitor dependent on the Ping monitor, so that you are not flooded with multiple alerts on the same device if network connectivity is lost.

In a critical monitor polling path, critical monitors are polled first. If you specify more than one critical monitor, you also specify the order in which they are polled. Critical monitors are "up" dependent on one another; if critical monitors return successful results, non-critical monitors are polled. If any of the critical monitors go down, all monitors behind it in the critical polling order are no longer polled and are placed in an unknown state for the duration of the polling cycle. If at the start of the next polling cycle, the critical monitors returns successful results, polling of successive critical monitors and non-critical monitors resumes.

When critical monitoring is enabled, and you specify a critical polling order, you now receive only one alert when a device loses its network connectivity.

Only monitors that you specify as critical follow a specific polling order; non-critical monitors are not polled in any specific order. Additionally, if multiple non-critical monitors fail, all associated actions fire.

Critical active monitors can be viewed and configured from the Device Properties - Active Monitors dialog (In Device or Map View, right-click on a device, then select **Properties**).

Critical Active Monitors to	o poll on Devi	ce:ATL-VMS1		7 💌
Enable critical mo	nitor polling fo	or this device		
Critical monitors (polling	ng order):			
Monitor Name	Argument	Network Interface	Comment	
HTTP		(Default)		🚹 Up
				▲ nomu
in <u>O</u>	tical	<u> Non-critical </u>	J	
Non-critical monitors:				
Monitor Name	Argument	Network Interface	Comment	
1 Ping		(Default)		
% Ping		(Default)		
No Ping		(Default)		
N Ping		(Default)		
N Ping		(Default)		
The polling of ATL-VMS1's	non-critical n	(Default)	'Uo'state of	
The polling of ATL-VMS1's each its critical monitors (f	non-critical n HTTP). If any	(Default) nonitors depends on the one of the critical monitor	'Up' state of ors go 'Down',	
The polling of ATL-VMS1's each its critical monitors (t polling will not continue.	non-critical n HTTP). If any	(Default) nonitors depends on the one of the critical monitor	'Up' state of ors go 'Down',	ОК

For more information, see *Configuring a critical polling path* in Help.

New actions

About the SNMP Set action

This action sends an SNMP Set to a device in order to change a specific SNMP action. You can configure SNMP Set Actions perform a number of tasks, including rebooting a device, changing the state of a network remotely, disabling or enabling a device feature, etc.

The SNMP Set Action can use any SNMP credential defined in the WhatsUp Gold Credential Library and supports all types of writable objects (strings, integers, timeticks, etc.).

If the action's operation fails, errors are reported to the Action Log.

New SNMP Set Action		
Name:		-
Description:		
SNMP Set Action		1
Device Settings		
IP address or host name:		
SNMP v1/v2/v3 credential	S	
public (SNMPv1)	• (21)	
Object Details		
Object identifier:	Instance:	
Value type:		
Unsigned Integer	•	Advanced
<u>V</u> alue to set:		
		OK

For more information, see Using an SNMP Set Action in Help.

About the Log to Text File action

The Log to Text File Action uses Percent Variables to gather information about your network devices and logs a custom message to a specified text file with the Percent Variable results. You can specify the name and location of an existing text file or create a new file and location to which the message will be written.

This action is useful if you would rather receive network messages in a text file that can be saved, as an alternative to receiving an email or SMS alert.

Vew Log To Text File Action		7 🗙
Name:		
Description:		
Log To Text File Action		
Log file:		
Log file write mode:		
Append -		
Log Message:		
<pre>%Device.ActiveMonitorDownNames is %Device.State on % Device.Tune: %Device.HostName (%Device.Address)</pre>	*	
bevice.rgper absvice.nostinane (absvice.nadress)		
Details:		
Monitors that are down include: %Device.ActiveMonitorDownNames Monitors that are up include: %Device.ActiveMonitorUpNames	Ξ	
Notes on this device (from device property page): Device.Notes		
This message was logged on %System.Date at %System.Time	- [ок
Right-click in the 'Log message' area to add a WhatsUp percent variable.	ľ	Cancel

For more information, see Using the Log to Text Action in Help.

About the Windows Event Log action

The Windows Event Log Action uses Percent Variables to gather information about your network devices and logs messages to the Windows Event Viewer dependent on the Percent Variable results. You can select to have messages logged as error, warning, or informational messages. You can easily sort messages in the Windows Event Viewer by the source that you specify in the action.

This action is useful to use if you typically check the Windows Event Viewer for network messages, as an alternative to receiving an email or SMS alert.

New Windows Event Log Action	1					7 🗙
Name:						
Description:						
Windows Event Log Action						
Source:	Event ID:	Level:				
Ipswitch WhatsUp Log Action	1000	Error	•			
Log Message:						
<pre>%Device.ActiveMonitorDow Device.Type: %Device.Hos</pre>	nNames is tName (%I	<pre>%Device evice.Ad</pre>	.State dress).	on %	-	
Details: Monitors that are down i Monitors that are up inc	nclude: % lude: %De	Device.A	ctiveMo iveMoni	nitorDownNa torUpNames	ime a E	
Notes on this device (fr %Device.Notes	om device	property	y page)	:		
This message was logged	on %Syste	m.Date a	t %Syst	em.Time	- 1	ок
Right-click in the 'Log message' a	rea to add a	WhatsUp p	ercent va	riable.		Cancel

For more information, see Using the Windows Event Log Action in Help.

The Log to Text and Windows Event Log actions now use an improved Percent Variable Picker that allows you to select the Percent Variables you would like to use in an action's code. Percent Variables help you customize notification and log message information.

Percent Variables	•	System	► wn.▶an
		Active Monitor	Payload
	0.2	Passive Monitor	State
			Name
			Argument
			Comment
			Network interface address

For more information, see *Using the Windows Event Log Action* or *Using the Log to Text Action* in Help.

About Find Device

The new Find Device feature allows you to easily find the device group(s) to which a network device belongs by performing a simple search. After finding the device groups in which a devices resides, you can open the device group that contains the device, edit the device, remove the device from a selected group, or remove it from the WhatsUp Gold database.

Find Device					7 ×
Search:					
Display Name			•		
Eor:					
ATL					
Exact match			Find		
Display Name	Hostname	IP Address	Device Group	-	
BATL103	ATL103	192.168.3.103	RangeScan (5/12/2009 10:	E	View Group
ATL105	ATL105	192.168.3.105	RangeScan (5/12/2009 10:		
BATL106	ATL106	192.168.3.106	RangeScan (5/12/2009 10:		
BATL107	ATL107	192.168.3.107	RangeScan (5/12/2009 10:		Edit
ATL132	ATL132	192.168.3.132	RangeScan (5/12/2009 10:		Delete
Batl134.ipswitch_m.ipswitch	atl134.ipswitch_m.ipswitch	192.168.3.134	RangeScan (5/12/2009 10:		
ATL136	ATL136	192.168.3.136	RangeScan (5/12/2009 10:		
B ATL140	ATL140	192.168.3.51	RangeScan (5/12/2009 10:		
Batl160.ipswitch_m.ipswitch	192.168.169.1	192.168.169.1	RangeScan (5/12/2009 10:		
Batl160.ipswitch_m.ipswitch	192.168.174.1	192.168.174.1	RangeScan (5/12/2009 10:		
📕 atl160.ipswitch_m.ipswitch	atl160.ipswitch_m.ipswitch	192.168.3.160	RangeScan (5/12/2009 10:	-	Close

The Find Device feature is accessible from the web interface from GO menu at **Device > Find Device**. For more information, see *Performing a device search using Find Device* in Help.

About the Argument field

An **Argument** field has been added to the Device Properties - Active Monitors dialog to help you differentiate between interfaces on devices with more than one interface by automatically including the ifIndex interface number. You will also find the Argument field in the Up and Down dependency dialogs (Device Properties - Polling dialog), and the Critical Active Monitors dialog.

Properties	Active Monitors					
General	Active Monitors attack	ned to this device:				
Performance Monitors	Monitor Name	Argument	Critical	Network Interface	Comment	Add
	44 Dell / Cisco Fa	an	No	(default)		Edit
Active Meeiter	THTTP		No	(default)		
Active Monitors	Interface	3	No	(default)	GigabitEthemet 1/2	Remove
0	J# Interface	4	No	(default)	GigabitEthernet2/1	
Passive Monitors	J# Interface	5	No	(default)	GigabitEthemet2/2	Contract
9	J# Interface	6	No	(default)	GigabitEthernet2/3	Critical
Actions	J Interface	7	No	(default)	GigabitBhemet2/4	
N	J Interface	8	No	(default)	GigabitEthernet2/5	Dicable
Containt.	Minterface	9	No	(default)	GigabitEthemet2/6	Disable
Credentials	Interface	10	No	(default)	GigabitEthemet2/7	Enable
	Interface	11	No	(default)	GigabitEthemet2/8	
Poling	Interface	12	No	(default)	GigabitEthernet2/9	
	Minterface	13	No	(default)	GigabitEthemet2/10	Denne
Notes	JIII Interface	14	No	(default)	GigabitEthernet2/11	Rescan
30	J Interface	15	No	(default)	GigabitBhemet2/12	
aton	James e	**		(1.6. 2)	C 1101 10.00	
Menu	* Click the 'Critical'	button to select critical m	nonitors and se	t their polling order.		

New in Flow Monitor plug-in

New Flow Monitor reports

The Interface Usage report provides you with a view of the total amount of incoming and outgoing traffic for Flow Monitor source interfaces over the selected time period. Interfaces can be displayed separately, or grouped together by interface name. When you group together by interface name, all interfaces under a single display name are added together, and all data displayed is a total for those interfaces.

Interlace Name	Incoming Bytes	Outgoing Bytes	Total Bytes -	1.5
0 exector - Cisco 4510R) Production	3.34.68	3.62 GR	6.86.GB	
(Atlanta Laver 3 Switch - Cisco 4506) VLAN To the 3 N	146 GB	131 G8	277 G8	
(Augusta TS & QA) External	1.05 GB	149.57 MB	1.20 GB	
(Augusta TS & QA) Internal 6	145.56 MB	1.05 G8	1.19 G8	
(Lexington - Cisco 4510R) VOIP traffic	592 97 MB	395 83 MB	992 80 MB	
(Atlanta Layer 3 Switch - Cisco 4506) VLAN To QA Te	211.91 MB	328.75 MB	540.66 MB	
(Atlanta Data) External	308.61 MB	152.08 MB	460.70 MB	
(Atlanta Data) Internal 3	152.08 MB	308.61 MB	460.69 MB	
(Atlanta Gateway Router) connection to customer LAN	128.70 MB	320.75 MB	449.45 MB	
(Atlanta Gateway Router) Multiink1	320.75 MB	128.70 MB	449.45 MB	
(Atlanta Layer 3 Switch - Cisco 4506) VLAN To DEV T	3.02 MB	40.84 MB	43.86 MB	
(QA Test) 201.x Network	1.82 MB	37.47 MB	39.29 MB	
(QA Test) 199 x Network	37.47 ME	1.82 MB	39.29 ME	
(Atlanta Layer 3 Switch - Cisco 4506) 254	22.67 MB	4.67 MB	27.24 MB	
(Atlanta VOIP) Connection to Paetec	4.23 MB	4.20 MB	8.43 MB	
(Atlanta VOIP) Connect to Port Gi5/12 on Cisco 4506	4.20 MB	4.23 MB	8.43 MB	
(DEV Test) 203.x Network	4.63 MB	1.12 MB	5.75 MB	
(Lexington - Cisco 4510R) SAN Management	2.45 MB	2.96 MB	5.40 MB	
(DEV Test) 204 x Network	1.12 MB	1008.B1 KB	2.10 MB	
(Atlanta Layer 3 Switch - Cisco 4506) 256	228.61 KB	224.23 KB	452.84 KB	
(Juniper device) ge-0/0/0.0	39.01 KB	24.02 KB	63.03 KB	
(Juniper device) ge-0/0/1.0	2.05 KB	0 Bytes	2.05 KB	

For more information, see About the Interface Usage report in Help.

This workspace report displays a summary graph of the top Internet Control Message Protocol (ICMP) errors occurring on the selected interface during the time period selected for the Interface Details report. This information helps identify the top ICMP errors experienced on the network during the selected time period. For example, routers that cannot be reached or unavailable services.



For more information, see *ICMP Types* in Help.

This workspace report displays a bar chart where each bar represents the percentage of packets that fall within a given size range in bytes. The data used in this report is based on the packets being transmitted over the network during the time period selected for the Interface Details report.

Packet Size Dis	stribution		2 D D
7	16.08%	. 03190 86%1 2518 28%0 53%1 39%1 .64	37.77% 23.84%
Packet Size	Packets	Bytes	Percentage of Packets
0-100	51346	3228933	7.86 %
100-200	105041	18045896	16.08 %
200-300	10652	2612346	1.63 %
300-400	5326	1911126	0.82 %
400-500	6718	3031487	1.03 %
500-600	5630	3129333	0.86 %
600-700	8156	5257064	1.25 %
700-800	8360	6206321	1.28 %
800-900	4135	3544525	0.63 %
900-1000	9064	8586474	1.39 %
1000-1100	10731	11188745	1.64 %
1100-1200	5862	6847092	0.9 %
1200-1300	4033	5043931	0.62 %
1300-1400	15666	21417966	2.4 %
1400-1500	246735	369231680	37.77 %
1500-1600	155722	233583008	23.84 %

For more information, see *Packet Size Distribution* in Help.

70m

Added improved Flow Monitor report configuration to allow fields in the Top Sender and Receiver workspace reports to sort by Bytes, Packets, and Flows.



Flow Monitor now supports user permissions that allow WhatsUp Gold admins to configure which user accounts can view and manage Flow Monitor data. This keeps unwanted user accounts from viewing or manipulating information on certain Flow Monitor sources.

Note: In order for a user to be able to block access for other WhatsUp Gold users, the user must have the Manage Users access right (From the **WhatsUp** section of the **GO** menu, **Configure > Manage Users**). Additionally, the user for which you are trying to block access should not have this right, as this will allow them to block access for other users.

Name 🔺	IP	Enabled	Protocol	Edit			
Atlanta Data	and the second	Yes	NetFlow	Access rights			
Atlanta Gateway Router		Yes	NetFlow				
Atlanta Layer 3 Switch - Cisco 4506	100.000	Yes	NetFlow				
Atlanta VOIP	100.000.00	Yes	NetFlow		Flow Source Access Rights		
atl-rmiller.ipswitch_m.ipswitch.com	100.000	No	NetFlow		Atlanta Data ()		
atl-tphung.ipswitch_m.ipswitch.com	10.000.000	No	NetFlow		User name 🔺	Block Access	Select Al
Augusta TS & QA	10.000	Yes	NetFlow		& Bob	27	Degelect A
CROBLES-DELL (Probe) ?????	10.001-00	Yes	NetFlow		a claudio	13	
DEV Test	10.000	Yes	NetFlow		a guest	1	
HP Procurve switch (sFlow)	10.000.000	Yes	sFlow		🚄 jwilliams	10	
Juniper device	10.000.00	Yes	NetFlow		🚨 mneuburger	121 121	
Lexington - Cisco 4510R	100101-01	Yes	NetFlow		🚑 mswimm	13	
QA Test	10.00	Yes	NetFlow		a netflow	23	
uslec-63-243-52-90 cust uslec net	1010010-000	No			a sayton	10	
				Close			

For more information, see Flow Source Access Rights in Help.

About ifIndex on the Flow Interface dialog

The Flow Interface dialog now includes the ifIndex number of an interface to help you differentiate between network interfaces.

Flow Interface		2 💌
Interface:	Unnamed	
ifIndex:	3	
Type:	J Unknown	
Status:	Unknown	
Last incoming:	Mon Jun 22 09:27:51 2009	
Last outgoing:	Mon Jun 22 09:27:51 2009	
Speed: (bps)	Undefined	
Hide this inter Home page ar properties.	face from the Flow Monitor ad related configuration	
Specify a cust	om speed for this interface	
In 0	bps	ОК
Qut 0	bps	Cancel

This number is included in parenthesis next to the interface's name on the Flow Source dialog.

Flow Source				? X
Source 114.21.3.101				
Flow Protocol:NetFlow v5				
Display Name:				
116-21.3 101				
Collect data from this source				
Poll source for total interface traffic				
SNMP credentials				
(None)	Adv	anced] Quer	ry]	
Access rights				
Interfaces				
Name		Туре		
Junnamed (3)		Unknow	m	
)= Null(0)		Unknow	//n	5.0
				Edit
			Ē	OK]
	-		, [Cancel
N.				

The ifIndex number represents a unique value for each Flow Source interface. You can assign a name for the interface ifIndex value to make the interface more easily identifiable.

For more information, see Flow Interface Properties in Help.

Added support

WhatsUp Gold v14 has added support for the following applications and devices:

- Cisco and Juniper Netscreen CPU and Memory Performance Monitors
- 64 bit OSs Microsoft Windows XP Pro, Vista, and Windows Server 2008
- Microsoft SQL Server 2008
- VmWare ESXi 3.0 or later
- Microsoft Hyper-V Server 2008

For more information

Following are information resources for WhatsUp Gold. This information may be periodically updated and available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/support/index.aspx).

- Release Notes. The release notes provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for installing, upgrading, and configuring WhatsUp Gold. The release notes are available at Start > Programs > Ipswitch WhatsUp Gold > Release Notes or on the WhatsUp Gold web site (http://www.whatsupgold.com/wug14reInotes).
- Application Help for the console and web interface. The console and web help contain dialog assistance, general configuration information, and how-to's that explain how to use the features. The Table of Contents is organized by functional area, and can be accessed from the main menu or by clicking Help in the console, or the ? icon in the web interface.
- Additional WhatsUp Gold guides. For a listing of current and previous guides and help files available for WhatsUp Gold's multiple versions, see the WhatsUp Gold web site (http://www.whatsupgold.com/wug14guides).
- WhatsUp Gold optional plug-ins. You can extend the core features of WhatsUp Gold by installing plug-ins. For information on available plug-ins and to see release notes for each plug-in, see WhatsUp Gold plug-ins documentation (http://www.whatsupgold.com/wug14guides).
- Licensing Information. Licensing and support information is available on the Mylpswitch licensing portal (http://www.myipswitch.com/). The web portal provides enhanced web-based capabilities to view and manage lpswitch product licenses.

- **Knowledge Base**. Search the Ipswitch Knowledge Base of technical support and customer service information. The knowledge base is available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wugTechSupport).
- Support community. Use the WhatsUp Gold community site to interact with other WhatsUp Gold users and share helpful application information on the forums, view KBs and documentation, submit new product ideas, access the script library, and keep up with the latest news on the blog. The wugSpace support community for WhatsUp Gold is available on the WhatsUp Gold community site (http://www.whatsupgold.com/wwc14forumsmore).