ipswitch

WhatsUp® Gold
Evaluation Guide

Table of Contents

This guide provides and overview of WhatsUp Gold. Refer to our Online Help for more details.

Getting Started

Prior to installation

- Consult the release notes to ensure your system meets the minimum requirements. If you plan on discovering over 500 devices.

Have Credentials Ready

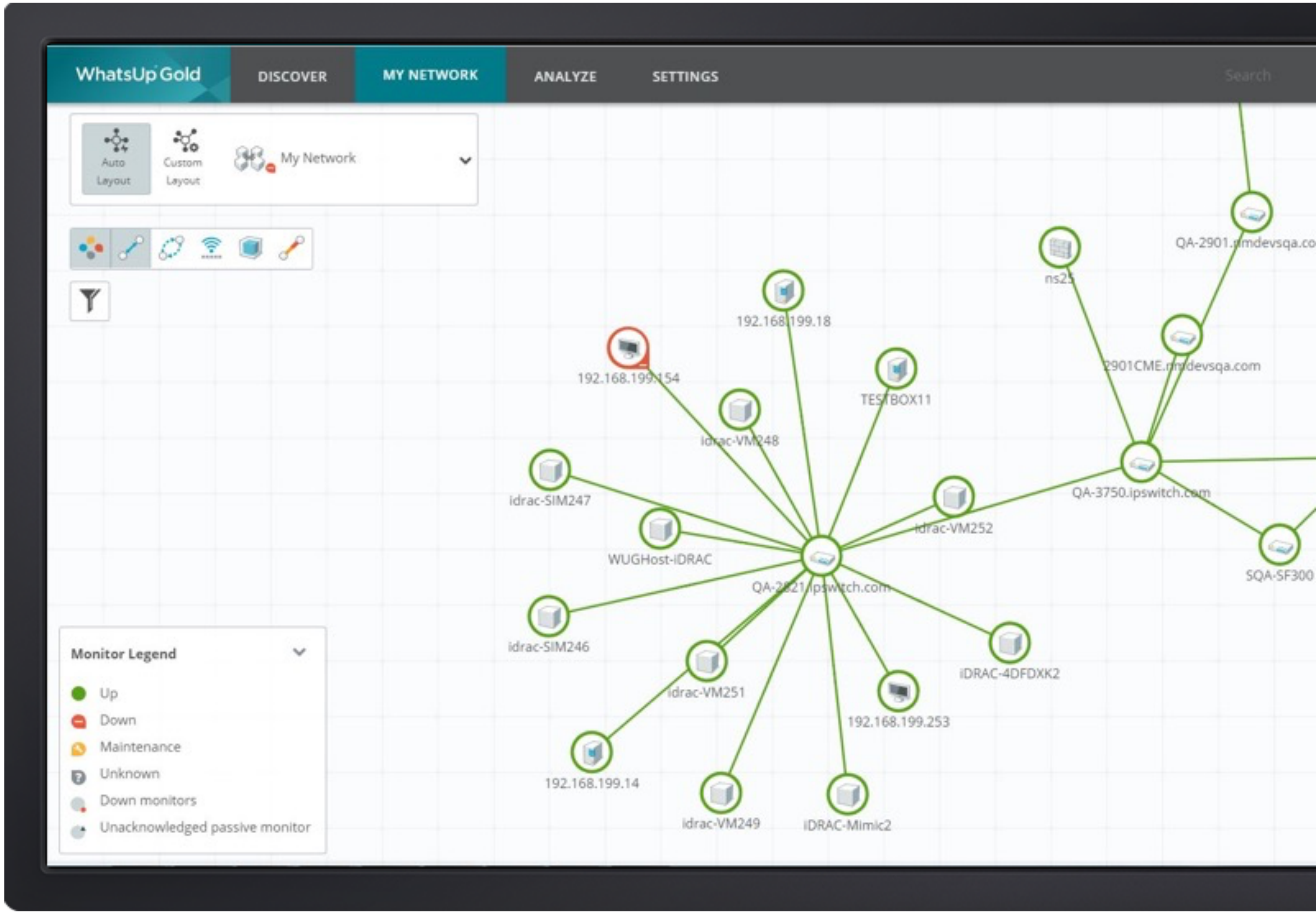
- WhatsUp Gold requires credentials to get the most information out of the devices on the network. Be sure your devices are configured correctly and you have proper access prior to running a discovery. See the credentials section for more details.

Review additional resources

- Our Online Help section provides additional detail on setup and configuration
- Our Ipswitch Community provides questions, answers and scripts

Discovery

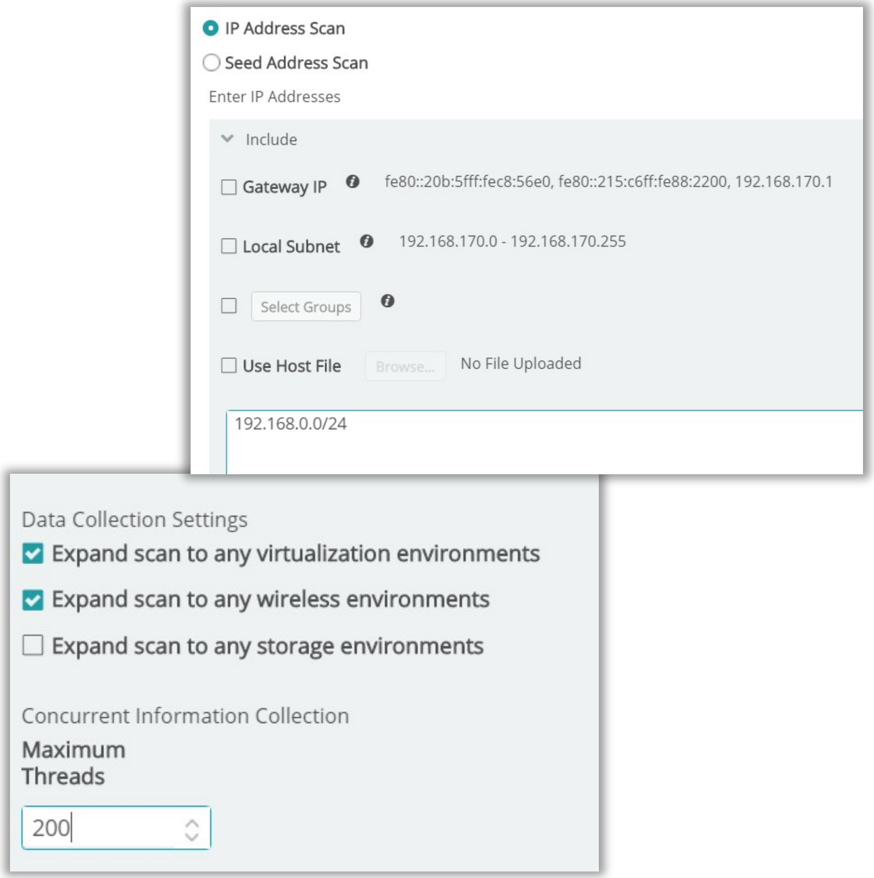
Discovery
New Scan Settings
New Scan Credentials
New Scan Schedule
Discovered Network Map
Filter Devices
Hide Devices
Device Roles



Discovery: New Scan Settings

- Launch a new discovery
  - From the main page, select Discover > New Scan
- Determine discovery scope
  - You can discover Individual IPs, ranges, or subnets with the IP range scan. The Seed discovery relies on SNMP to find connected devices. You can select a discovery depth with this method (to discover neighbors of neighboring devices)
- Provide discovery limits
  - Be sure to limit the discovery. Consider limiting it to private networks, or set a maximum number of discovered devices
- Review advanced settings
  - Set your data collection settings accordingly. If you are discovering wireless or virtualization environments, be sure those are selected. To have the discovery complete faster, you can increase the maximum thread count.

[Discovery Video]



● IP Address Scan
○ Seed Address Scan

Enter IP Addresses

Include

□ Gateway IP fe80::20b:5fff:fec8:56e0, fe80::215:c6ff:fe88:2200, 192.168.170.1

□ Local Subnet 192.168.170.0 - 192.168.170.255

□ Select Groups

□ Use Host File No File Uploaded

192.168.0.0/24

Data Collection Settings

☑ Expand scan to any virtualization environments

☑ Expand scan to any wireless environments

□ Expand scan to any storage environments

Concurrent Information Collection

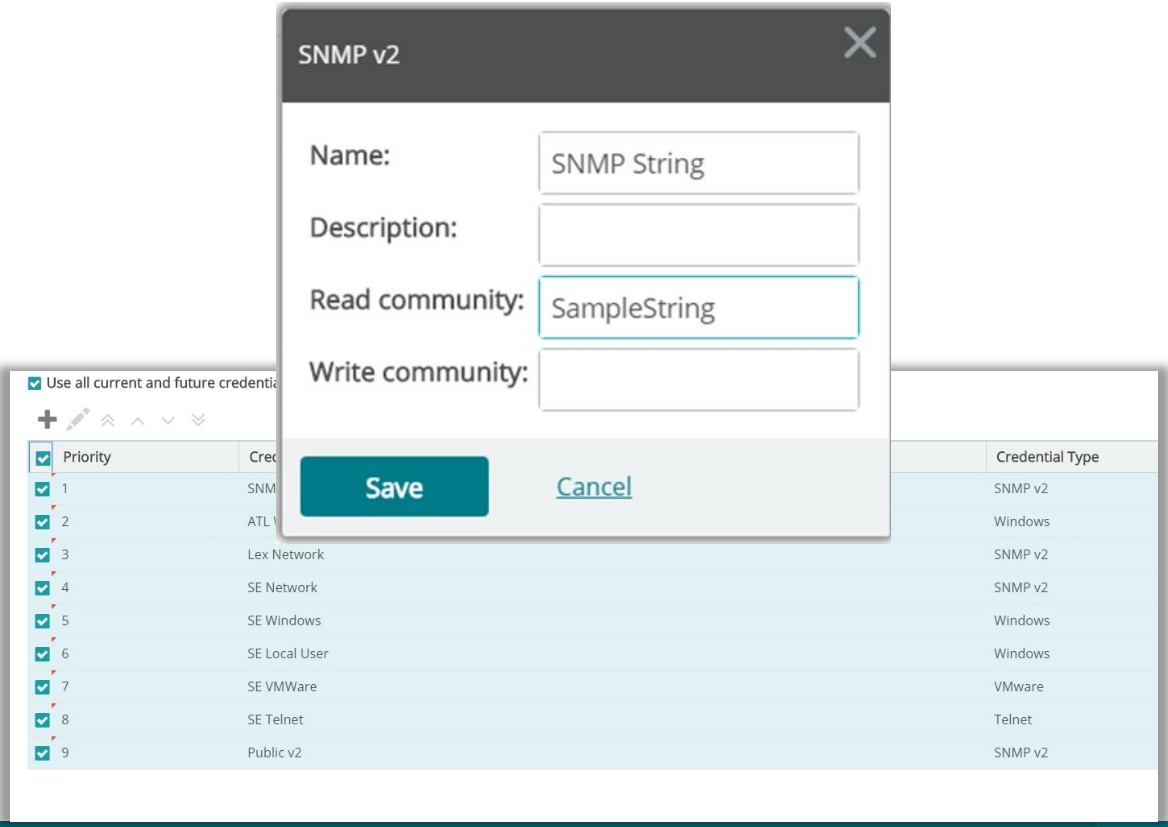
Maximum Threads

200

Discovery: Add Credentials

- In credentials tab click plus mark to select type:
  - SNMP – Most default monitors require SNMP RO access
  - Windows – Used to create WMI monitors and gather data from Hyper-V virtualization environments
  - ADO - Database Connection string information to create query monitors for SQL or Oracle DB server
  - Telnet/SSH – Command line monitors for expected results or to backup configurations
  - VMware – Access vCenter or VMware hosts for mapping and performance statistics
  - JMIX – Creating JMX monitors
  - SMIS – Required for NetApp storage devices

Helpful Tip: Be sure to select the credentials you want WUG to try against the devices during this discovery. Choices will be saved to the credential library for later use.



SNMP v2

Name:	SNMP String
Description:	
Read community:	SampleString
Write community:	

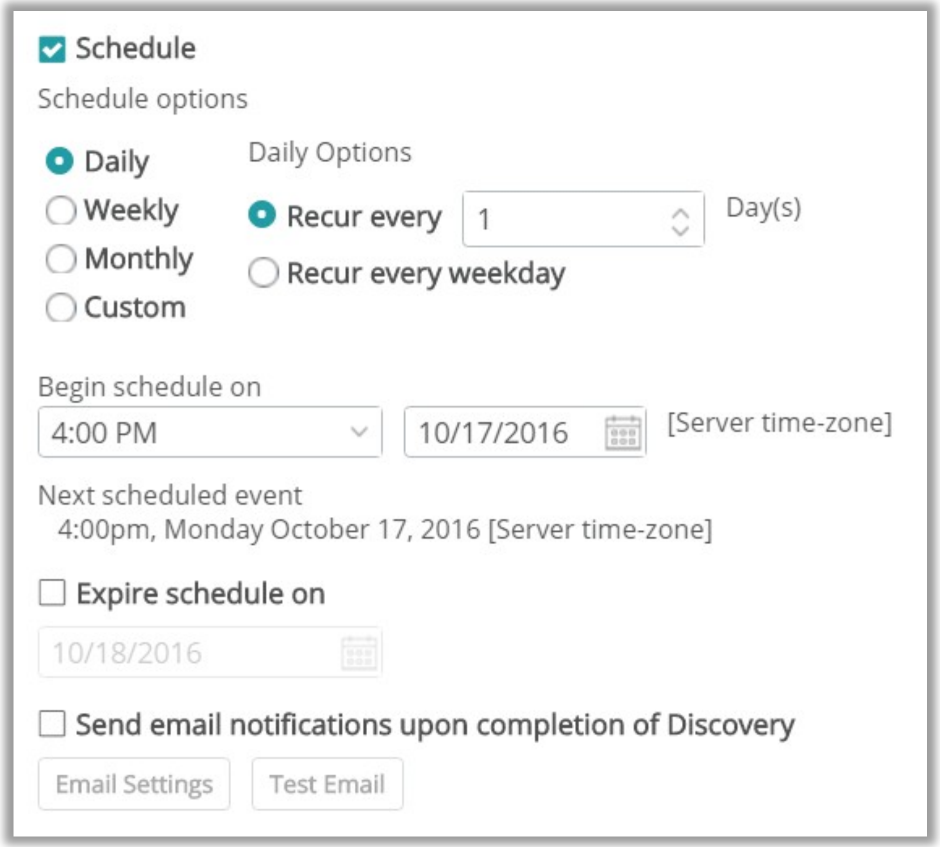
☑ Use all current and future credentia

☑	Priority	Cred	Credential Type
☑	1	SNM	SNMP v2
☑	2	ATL \	Windows
☑	3	Lex Network	SNMP v2
☑	4	SE Network	SNMP v2
☑	5	SE Windows	Windows
☑	6	SE Local User	Windows
☑	7	SE VMWare	VMware
☑	8	SE Telnet	Telnet
☑	9	Public v2	SNMP v2

Discovery: Scan Schedule

- Regularly scheduled discoveries
  - Schedule discoveries to occur on a regular basis to refresh monitors or find new devices on the network.
  - Prior to selecting this option be sure to double check your scan settings
  - Check off 'schedule' to reveal discovery schedule options. Consider running scheduled discoveries during non-peak business hours.
  - You can also setup notifications when the discovery finds new devices
- Unscheduled discoveries
  - You can also run ad hoc discoveries
  - The summary tab provides details about the discovery you are about to run. When you are ready, select "run" to kick it off.

Helpful Tip: You can schedule multiple discovery scans at different intervals for different subnets



☑ Schedule

Schedule options

● Daily
○ Weekly
○ Monthly
○ Custom

Daily Options

● Recur every 1 Day(s)
○ Recur every weekday

Begin schedule on

4:00 PM 10/17/2016 [Server time-zone]

Next scheduled event
4:00pm, Monday October 17, 2016 [Server time-zone]

□ Expire schedule on

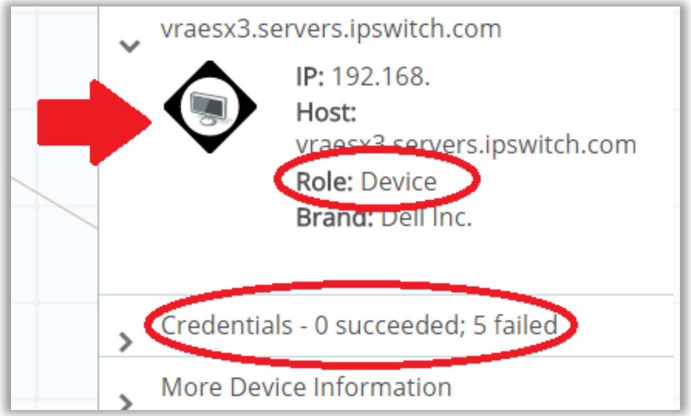
10/18/2016

□ Send email notifications upon completion of Discovery

Discovery: Discovered Network Map

- Discovery results
  - If the Role appears as “device” no credentials worked against it. Check for credential typos or bad device configurations. Rediscovery with working credentials will correct classification
- Add monitoring to devices
  - Choose a single unmonitored device or use the ‘selector tool’ to chose multiple unmonitored devices
  - Select ‘start monitoring’ (top right)
  - Confirm ‘Start/Update’ monitoring by selecting Start

Helpful Tip: WhatsUp Gold has built-in device roles that apply monitors based on device type. The device role will only apply a ping monitor to unclassified devices. Be sure that your devices are classified correctly before monitoring them



vraesx3.servers.ipswitch.com

IP: 192.168.

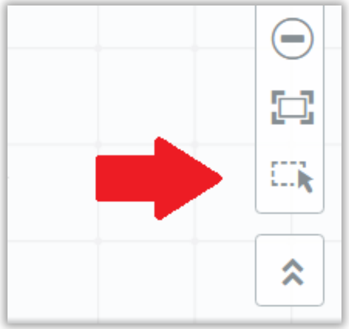
Host: vraesx3.servers.ipswitch.com

Role: Device

Brand: Dell Inc.

Credentials - 0 succeeded; 5 failed

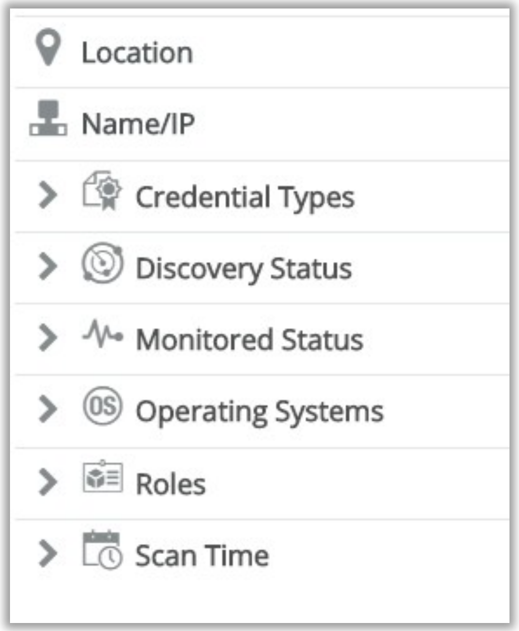
More Device Information



Discovery: Device Filters

- Use Filters to group devices
  - Filters provide an easy way to group devices by criteria. The devices that do not fit the criteria will be greyed out and are unable to be selected
  - Choose a filter and use the selector tool to begin monitoring selected devices

Examples: Use the Roles Filter to select all devices with device role of switch. Use the credential filter to select all SNMP devices. Use the scan time filter to select recently discovered devices.

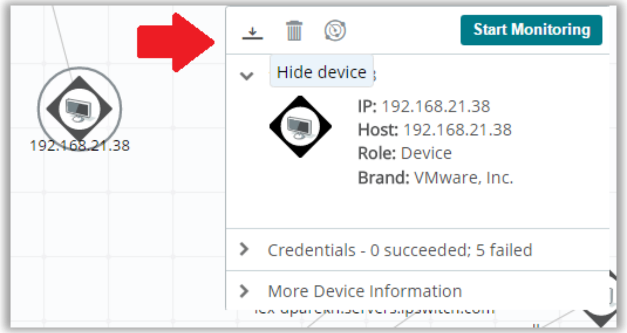


Location
Name/IP
› Credential Types
› Discovery Status
› Monitored Status
› Operating Systems
› Roles
› Scan Time

Discovery: Hiding Devices

- When and how to hide devices
  - Hidden devices are removed from the discovered network map
  - Once hidden they are not added back to the discovered map on subsequent discoveries.
  - Consider hiding devices that you do not want monitored. workstations or printers.
  - Click on a device on the map to hide it. Select ‘Hide’ from the Device Card that pops up.
  - Select “Hidden Devices” from the icon on the top left of screen to validate selection

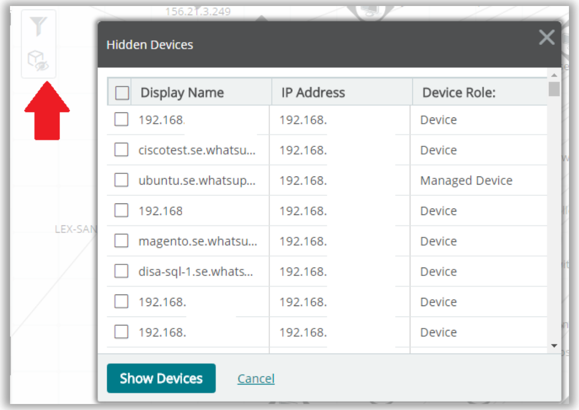
Helpful Tip: Take advantage of the selector tool and Filters to hide devices in bulk. Many users will hide Role: Device or Credentials Types: None.



IP: 192.168.21.38
Host: 192.168.21.38
Role: Device
Brand: VMware, Inc.

Credentials - 0 succeeded; 5 failed

More Device Information



Hidden Devices

□ Display Name	IP Address	Device Role:
□ 192.168.	192.168.	Device
□ ciscotest.se.whatsu...	192.168.	Device
□ ubuntu.se.whatsup...	192.168.	Managed Device
□ 192.168	192.168.	Device
□ magento.se.whatsu...	192.168.	Device
□ disa-sql-1.se.whats...	192.168.	Device
□ 192.168.	192.168.	Device
□ 192.168.	192.168.	Device

Show Devices   Cancel

Discovery: Device Roles

About Device Roles

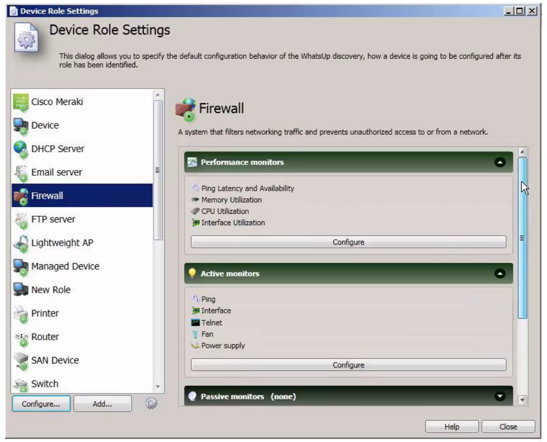
- Devices are assigned roles and sub roles automatically after the discovery which determines which monitors get assigned to the devices. Users can customize the existing device roles or create new ones.

Customization

- From the Admin Console located on your WhatsUp Gold server select Tools -> Device Role Settings. From here, you can customize existing device roles (add monitors or action policies) or create new device roles. The Role identification determines how this role will be applied to discovered devices

Helpful Tip: Be sure to make customizations prior to the discovery. Changing a device role will not edit the monitors applied to a device if it has already been discovered.

Device Roles Video

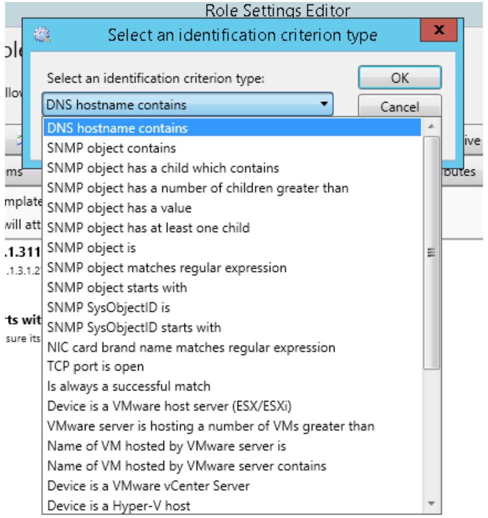


Device Role Settings

This dialog allows you to specify the default configuration behavior of the WhatsUp discovery, how a device is going to be configured after its role has been identified.

Firewall

A system that filters networking traffic and prevents unauthorized access to or from a network.



Role Settings Editor

Select an identification criterion type

Select an identification criterion type: DNS hostname contains

OK
Cancel
DNS hostname contains
SNMP object contains
SNMP object has a child which contains
SNMP object has a number of children greater than
SNMP object has a value
SNMP object has at least one child
SNMP object is
SNMP object matches regular expression
SNMP object starts with
SNMP SysObjectID is
SNMP SysObjectID starts with
NIC card brand name matches regular expression
TCP port is open
Is always a successful match
Device is a VMware host server (ESX/ESXi)
VMware server is hosting a number of VMs greater than
Name of VM hosted by VMware server is
Name of VM hosted by VMware server contains
Device is a VMware vCenter Server
Device is a Hyper-V host

Mapping

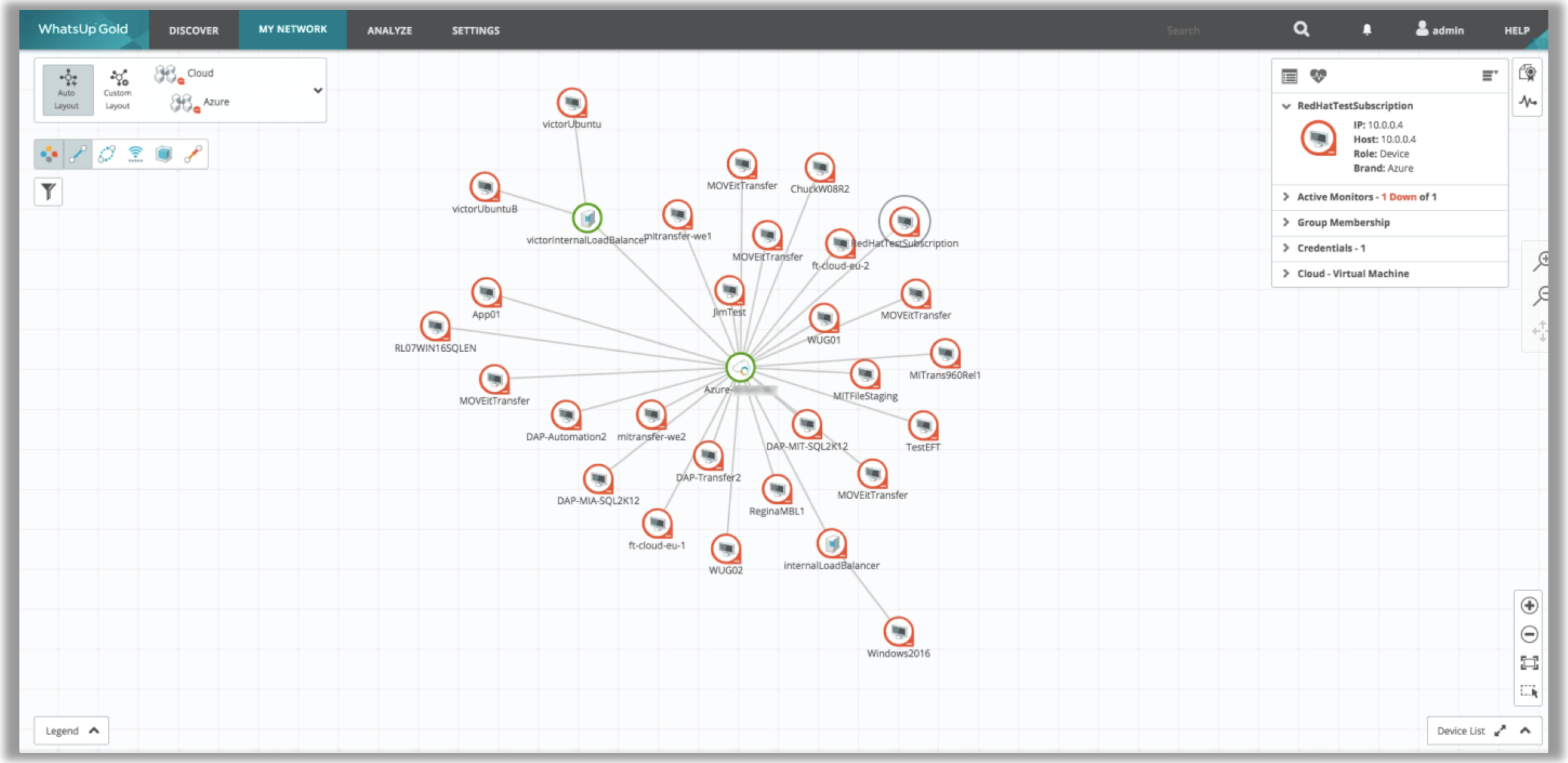
Mapping

[Monitored Network Map]

[Device Groups]

[Customizing Maps]

[Device Dependencies]



RedHatTestSubscription

IP: 10.0.0.4
Host: 10.0.0.4
Role: Device
Brand: Azure

- Active Monitors - 1 Down of 1
- Group Membership
- Credentials - 1
- Cloud - Virtual Machine

Mapping: Monitored Network Map

About the Map

- After adding monitoring to devices from the discovered map they appear on the "My Network" tab.

Navigation

- Selecting a device on the map reveals its device card from which you can 1) assign credentials, 2) navigate to device properties, 3) review status and 4) navigate to the monitor setup page

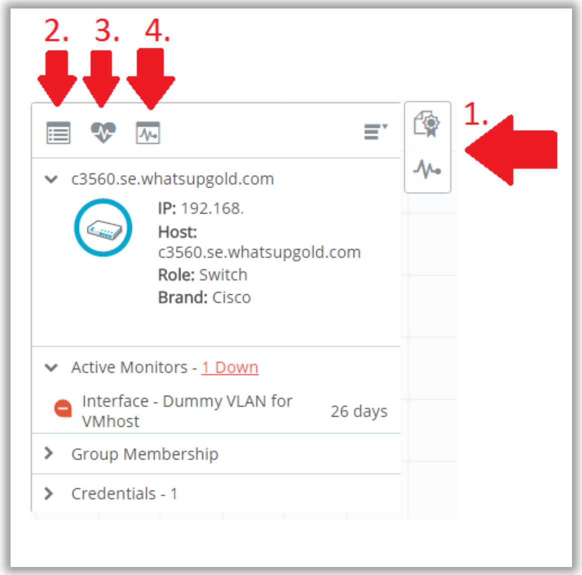
Overlays

- Map overlays add additional information to the network map. Overlays exist for connectivity, dependencies, link status and utilization, wireless networks and virtual machine and host relationships

Helpful Tip: The majority of tasks can be initiated directly from the map itself. If list view is preferred, you can click the list view button on the bottom right of the map.

.

Topology Video



c3560.se.whatsupgold.com

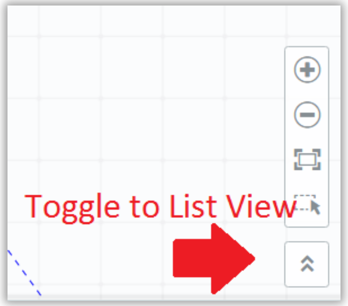
IP: 192.168.
Host: c3560.se.whatsupgold.com
Role: Switch
Brand: Cisco

Active Monitors - 1 Down

Interface - Dummy VLAN for VMhost 26 days

Group Membership

Credentials - 1


Toggle to List View

Mapping: Device Groups

Creating Groups

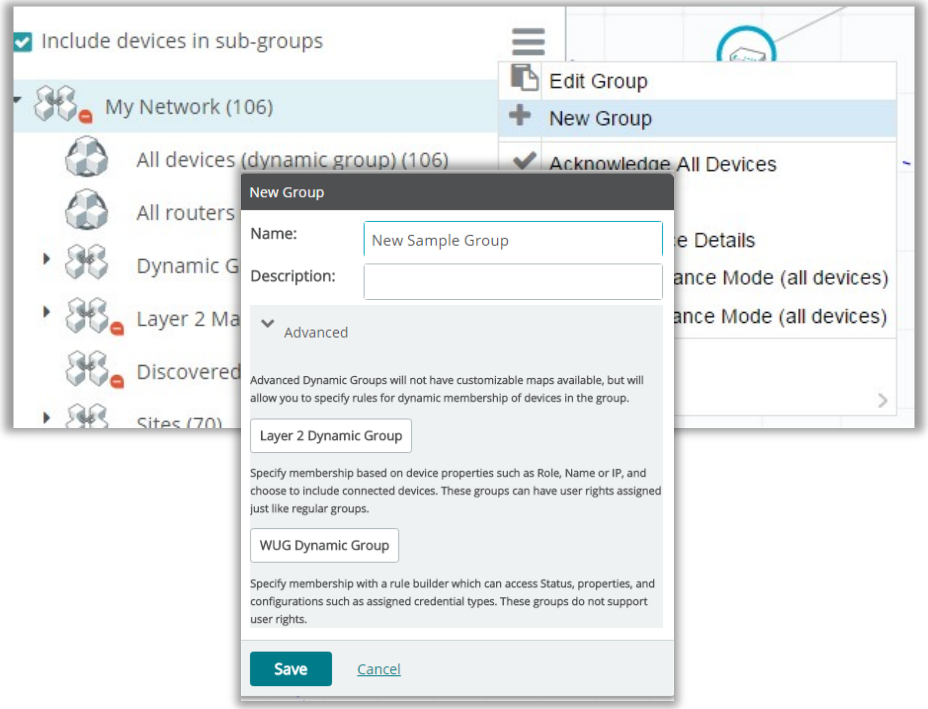
- Many dynamic and layer two groups are populated automatically
- Create additional device groups, layer two groups, or dynamic groups by selecting “New Group” from the device group menu.

Group Types

- Regular Device Groups are created manually using “Copy Device To…” to include selected devices. Device groups can leverage custom maps.
- Dynamic Device Groups are populated according to attributes like hostname, device type, or IP address.
- Layer Two Device Groups can be populated based on a number of different properties, and provides the ability to include connected devices.

Helpful Tip: You can limit user access to device groups via user access rights to ensure users view only the devices they manage.

Device Groups Video



New Group

Name: New Sample Group

Description:

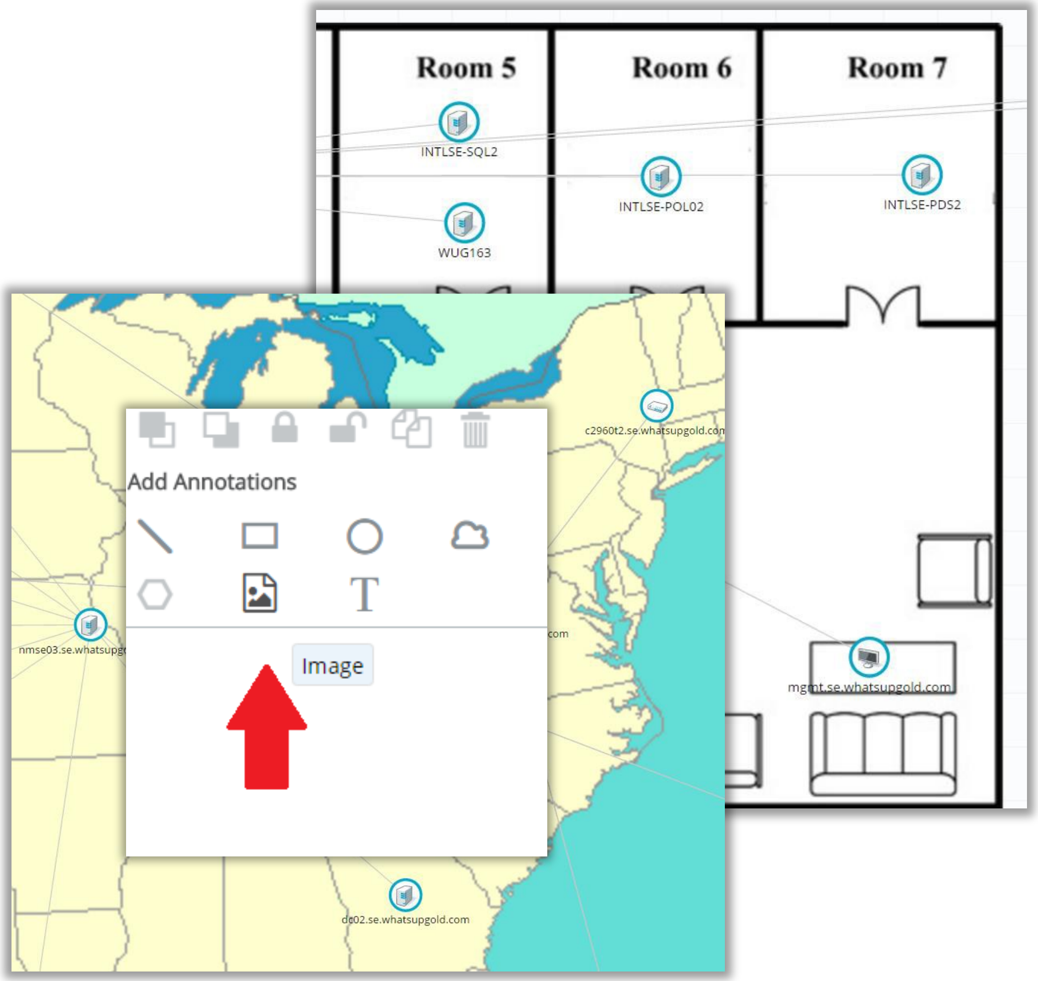
Advanced Dynamic Groups will not have customizable maps available, but will allow you to specify rules for dynamic membership of devices in the group.

Specify membership based on device properties such as Role, Name or IP, and choose to include connected devices. These groups can have user rights assigned just like regular groups.

Specify membership with a rule builder which can access Status, properties, and configurations such as assigned credential types. These groups do not support user rights.

Mapping: Customization

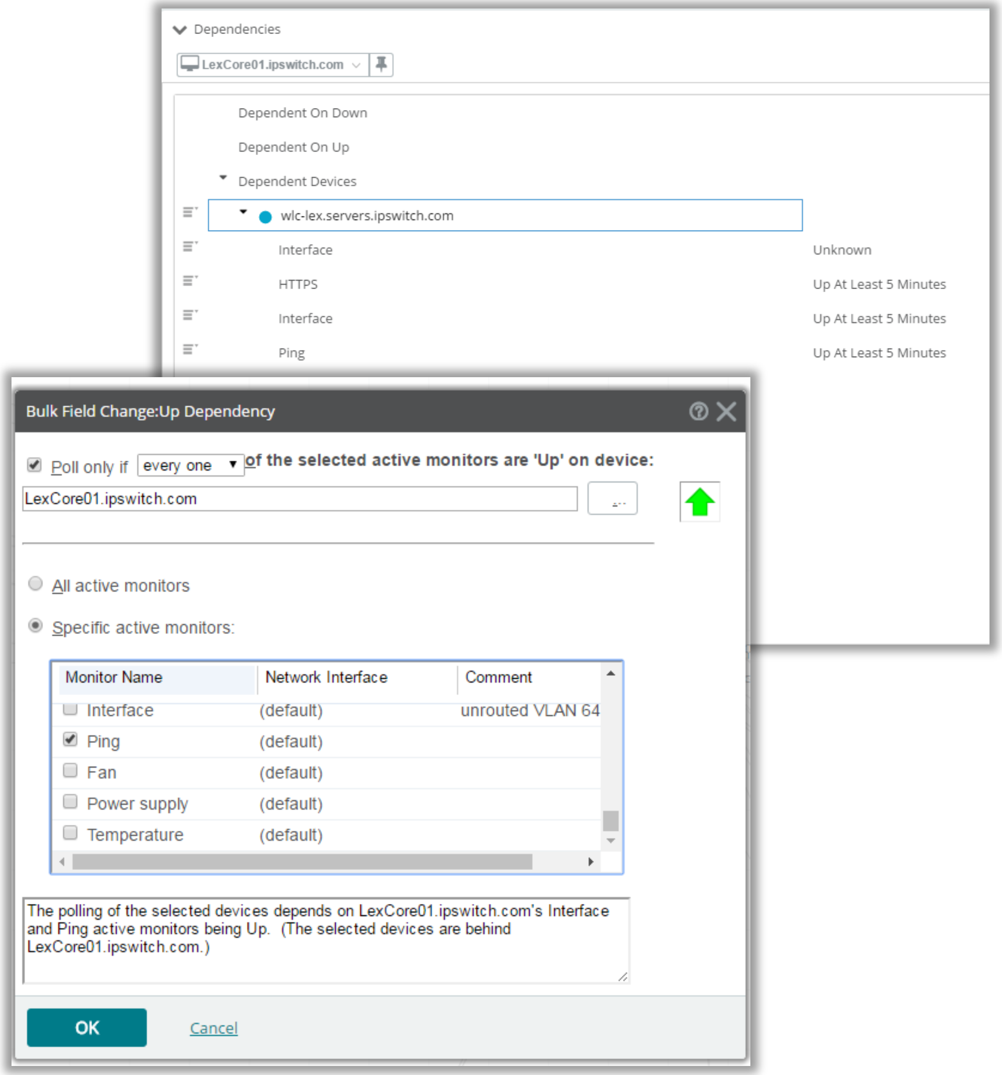
- Creating Custom Maps
  - Upload image files and arrange the devices on the image in a way that is meaningful to your organization.
  - Select a device group, and select “Custom Layout” from the top left of the screen.
  - Select the pencil icon (bottom right of screen) to arrange devices or add text and images
  - Select the image icon to upload an image, and drag and drop it on the custom map..



Mapping: Device Dependencies

How they work

- Reduce polling overhead by eliminating devices whose state can be assumed based on the status of another device
- Up dependency - device is polled only if the selected active monitors on another device are up
- Down dependency - device is polled only if the selected active monitors on another device are down
- Configuring device dependencies can help reduce alert storms with minimal configuration
- Discover devices – Be sure to apply monitoring to devices before attempting to set dependencies
- Apply up/down dependencies – On the discovered network map, select devices and navigate to “set up/down dependencies
- Review using device dependencies dashboard (Device->Dependencies). On the report, select an individual device to view the dependencies



Dependencies

LexCore01.ipswitch.com

- Dependent On Down
- Dependent On Up
- Dependent Devices
  - wlc-lex.servers.ipswitch.com

Interface	Unknown
HTTPS	Up At Least 5 Minutes
Interface	Up At Least 5 Minutes
Ping	Up At Least 5 Minutes

Bulk Field Change:Up Dependency

☑ Poll only if every one of the selected active monitors are 'Up' on device:

LexCore01.ipswitch.com

○ All active monitors

● Specific active monitors:

Monitor Name	Network Interface	Comment
□ Interface	(default)	unrouted VLAN 64
☑ Ping	(default)	
□ Fan	(default)	
□ Power supply	(default)	
□ Temperature	(default)	

The polling of the selected devices depends on LexCore01.ipswitch.com's Interface and Ping active monitors being Up. (The selected devices are behind LexCore01.ipswitch.com.)

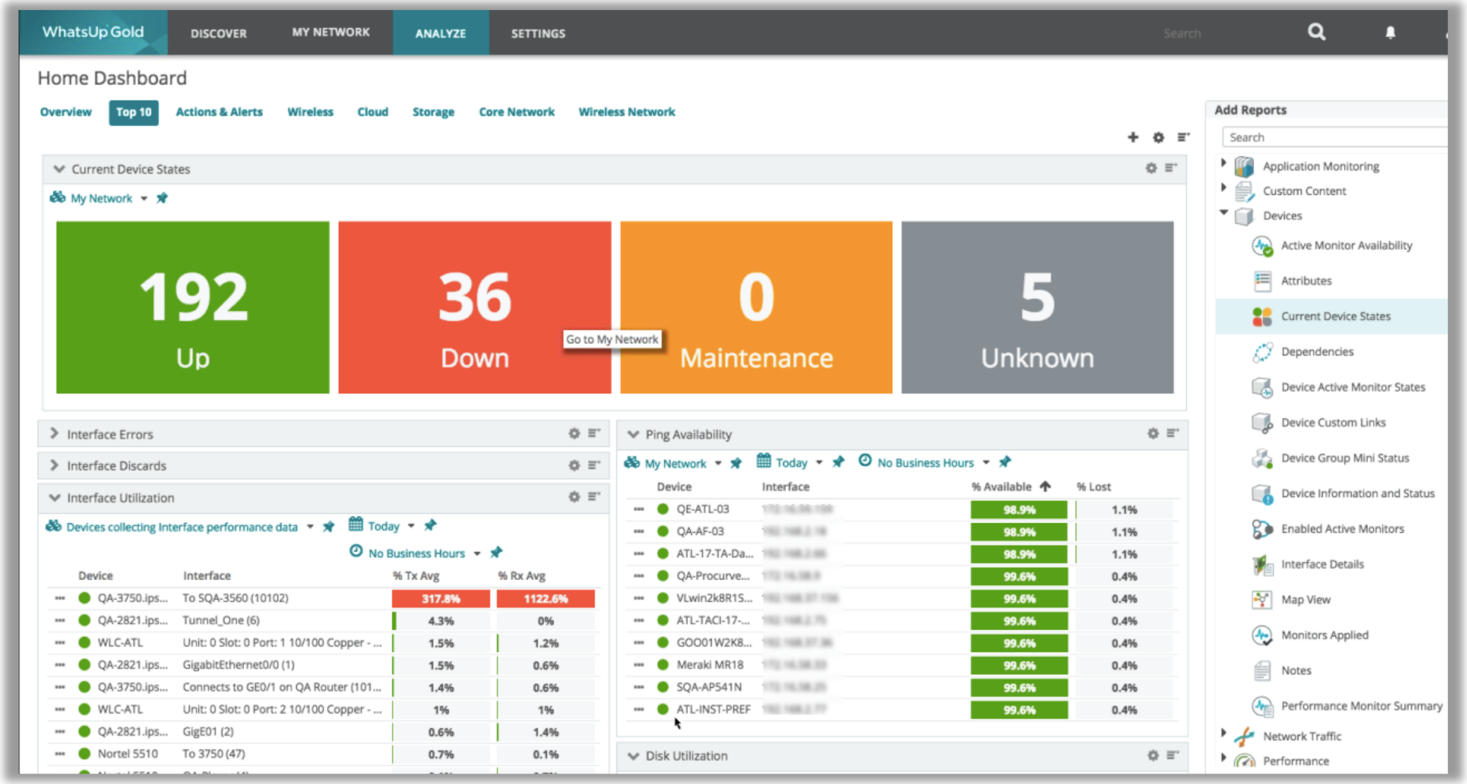
Monitoring

Basic Monitoring

- Active Monitors
- Passive Monitors
- Performance Monitors
- Applying Monitors
- Action Policies
- Alert Center
- Maintenance Mode

Advanced Monitoring

- Configuration Management
- Network Traffic Analysis
- Virtual Monitoring
- Application Monitoring



Interface Utilization

Device	Interface	% Tx Avg	% Rx Avg
QA-3750.ips...	To SQA-3560 (10102)	317.8%	1122.6%
QA-2821.ips...	Tunnel_One (6)	4.3%	0%
WLC-ATL	Unit: 0 Slot: 0 Port: 1 10/100 Copper - ...	1.5%	1.2%
QA-2821.ips...	GigabitEthernet0/0 (1)	1.5%	0.6%
QA-3750.ips...	Connects to GE0/1 on QA Router (101...	1.4%	0.6%
WLC-ATL	Unit: 0 Slot: 0 Port: 2 10/100 Copper - ...	1%	1%
QA-2821.ips...	GigE01 (2)	0.6%	1.4%
Nortel 5510	To 3750 (47)	0.7%	0.1%

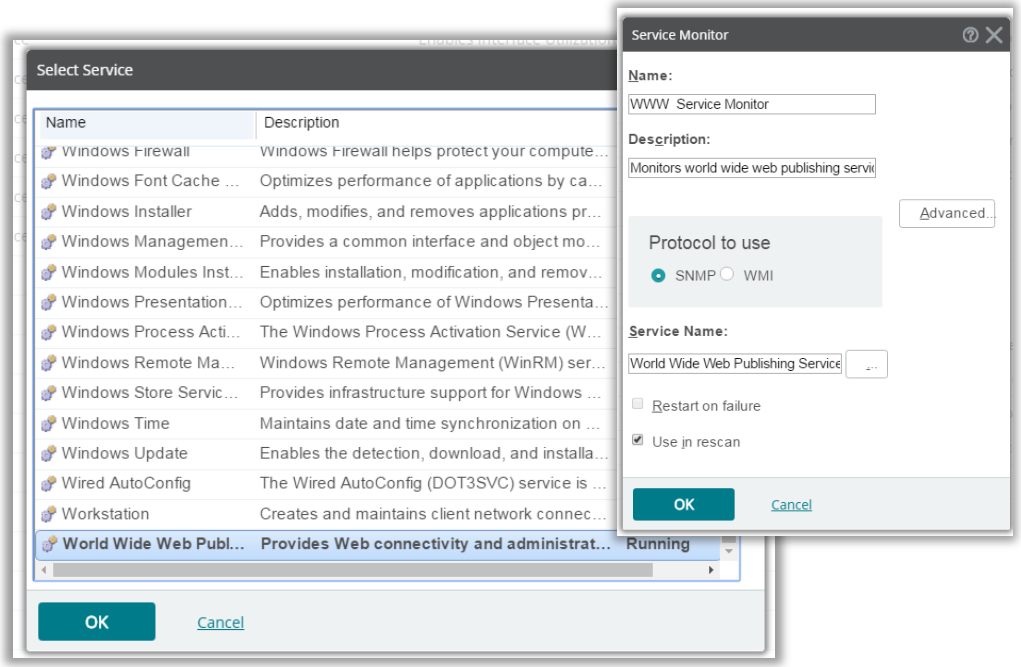
Ping Availability

Device	Interface	% Available	% Lost
QE-ATL-03	[redacted]	98.9%	1.1%
QA-AF-03	[redacted]	98.9%	1.1%
ATL-17-TA-Da...	[redacted]	98.9%	1.1%
QA-Procurve...	[redacted]	99.6%	0.4%
VLwin2k8R1S...	[redacted]	99.6%	0.4%
ATL-TACI-17-...	[redacted]	99.6%	0.4%
GOO01W2K8...	[redacted]	99.6%	0.4%
Meraki MR18	[redacted]	99.6%	0.4%
SQA-AP541N	[redacted]	99.6%	0.4%
ATL-INST-PREF	[redacted]	99.6%	0.4%

Monitoring: Active Monitors

- How they work
  - Active Monitors poll devices for an up/down or yes/no response.
  - The active monitor library includes built-in, configurable monitors including ping, port checks, file and folder monitoring, HTTP content monitors and SSL certificate monitors
- Configuring an Active Monitor (example)
  - From the main page, navigate to Settings->Libraries->Monitors.
  - Click on the plus mark, select active monitor and add “NT Service Monitor.”
  - Select a protocol to use, and select “…” to enter WMI/SNMP credentials
  - Provide a name and description and save to library
  - After the service monitor is created, you can apply the monitor to devices

Helpful Tip: Active monitors poll devices every 60 seconds by default. The polling interval can be customized.



Select Service

Name	Description	
Windows Firewall	Windows Firewall helps protect your compute…	
Windows Font Cache …	Optimizes performance of applications by ca…	
Windows Installer	Adds, modifies, and removes applications pr…	
Windows Managemen…	Provides a common interface and object mo…	
Windows Modules Inst…	Enables installation, modification, and remov…	
Windows Presentation…	Optimizes performance of Windows Presenta…	
Windows Process Acti…	The Windows Process Activation Service (W…	
Windows Remote Ma…	Windows Remote Management (WinRM) ser…	
Windows Store Servic…	Provides infrastructure support for Windows …	
Windows Time	Maintains date and time synchronization on …	
Windows Update	Enables the detection, download, and installa…	
Wired AutoConfig	The Wired AutoConfig (DOT3SVC) service is …	
Workstation	Creates and maintains client network connec…	
World Wide Web Publ…	**Provides Web connectivity and administrat…**	**Running**

Service Monitor

Name: WWW Service Monitor

Description: Monitors world wide web publishing servic

Protocol to use

● SNMP ○ WMI

Service Name: World Wide Web Publishing Service

□ Restart on failure

☑ Use in rescan

Monitoring: Passive Monitors

How they work

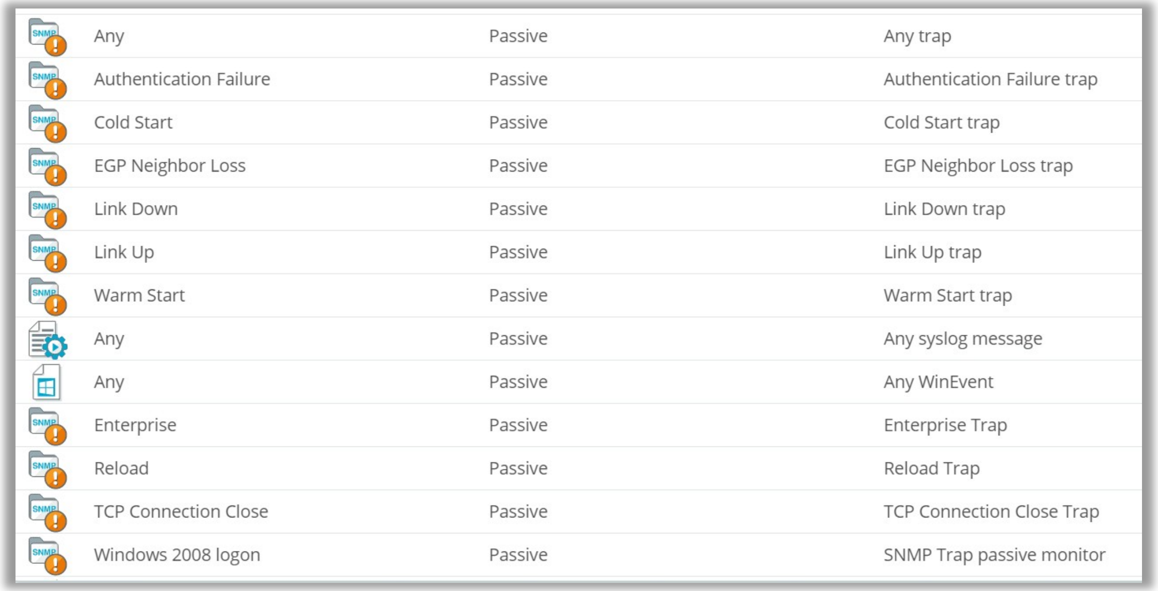
- User configure devices to send SNMP traps, Syslog or Windows Event logs to Passive Monitors on WhatsUp Gold server and alert when a specific message is received

Creating a Passive Monitor

- From Settings->Libraries->Monitors click on the plus mark and select passive monitor

Use case examples

- Set a trap to fire when a device configuration changes - set an action to backup the new config
- Use the Alert Center to get notified when a predefined number of traps are received in specified timeframe
- Get notified whenever a ‘critical’ or ‘emergency’ syslog message is received.



Any	Passive	Any trap
Authentication Failure	Passive	Authentication Failure trap
Cold Start	Passive	Cold Start trap
EGP Neighbor Loss	Passive	EGP Neighbor Loss trap
Link Down	Passive	Link Down trap
Link Up	Passive	Link Up trap
Warm Start	Passive	Warm Start trap
Any	Passive	Any syslog message
Any	Passive	Any WinEvent
Enterprise	Passive	Enterprise Trap
Reload	Passive	Reload Trap
TCP Connection Close	Passive	TCP Connection Close Trap
Windows 2008 logon	Passive	SNMP Trap passive monitor

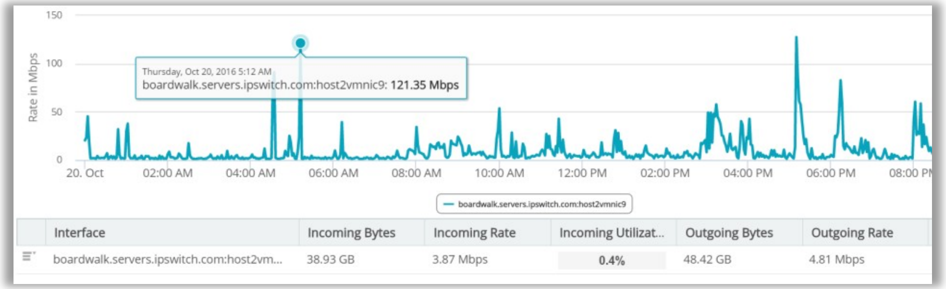
Monitoring: Performance Monitors

How they work

- Performance monitors track integers metrics like CPU, memory, disk or interface utilization over by polling devices on regular intervals (10 min default and configurable).

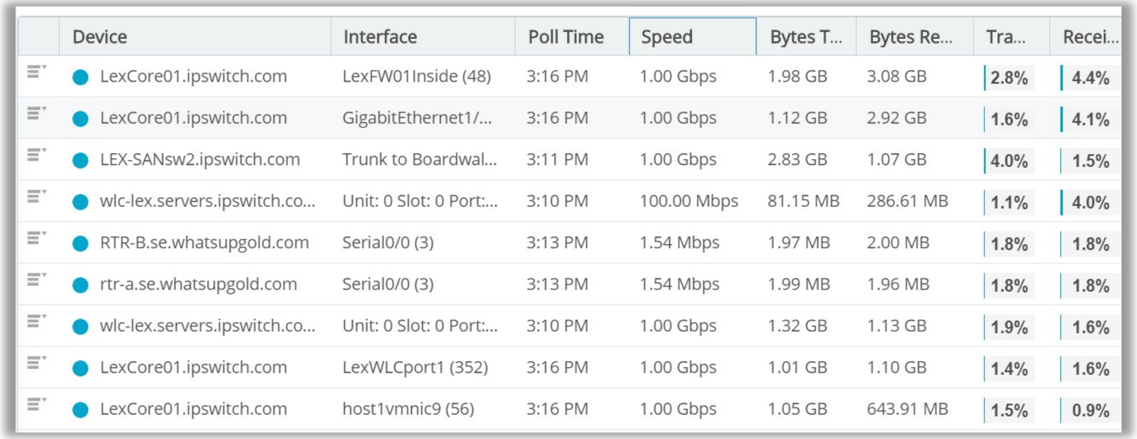
Creating a Passive Monitor

- From Settings->Libraries->Monitors click plus mark, select performance monitor.
- You can create performance monitors using a number of different protocols including SSH, SNMP, or WMI.
- You can use the Alert center to create threshold based alerts for performance monitors.



Thursday, Oct 20, 2016 5:12 AM
boardwalk.servers.ipswitch.com:host2vmnic9: **121.35 Mbps**

	Interface	Incoming Bytes	Incoming Rate	Incoming Utilizat...	Outgoing Bytes	Outgoing Rate
≡	boardwalk.servers.ipswitch.com:host2vm...	38.93 GB	3.87 Mbps	0.4%	48.42 GB	4.81 Mbps

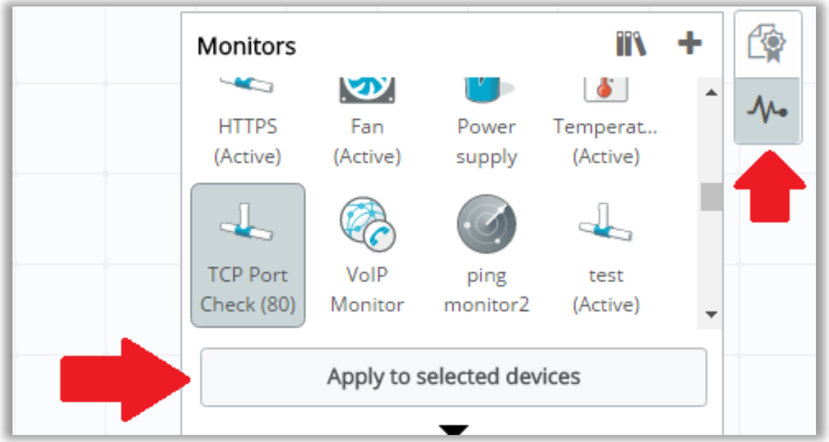


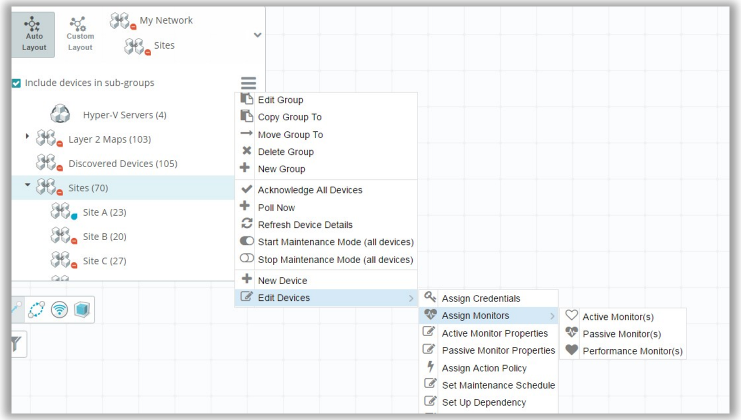
	Device	Interface	Poll Time	Speed	Bytes T...	Bytes Re...	Tra...	Recei...
≡	● LexCore01.ipswitch.com	LexFW01Inside (48)	3:16 PM	1.00 Gbps	1.98 GB	3.08 GB	2.8%	4.4%
≡	● LexCore01.ipswitch.com	GigabitEthernet1/...	3:16 PM	1.00 Gbps	1.12 GB	2.92 GB	1.6%	4.1%
≡	● LEX-SANsw2.ipswitch.com	Trunk to Boardwal...	3:11 PM	1.00 Gbps	2.83 GB	1.07 GB	4.0%	1.5%
≡	● wlc-lex.servers.ipswitch.co...	Unit: 0 Slot: 0 Port:...	3:10 PM	100.00 Mbps	81.15 MB	286.61 MB	1.1%	4.0%
≡	● RTR-B.se.whatsupgold.com	Serial0/0 (3)	3:13 PM	1.54 Mbps	1.97 MB	2.00 MB	1.8%	1.8%
≡	● rtr-a.se.whatsupgold.com	Serial0/0 (3)	3:13 PM	1.54 Mbps	1.99 MB	1.96 MB	1.8%	1.8%
≡	● wlc-lex.servers.ipswitch.co...	Unit: 0 Slot: 0 Port:...	3:10 PM	1.00 Gbps	1.32 GB	1.13 GB	1.9%	1.6%
≡	● LexCore01.ipswitch.com	LexWLCport1 (352)	3:16 PM	1.00 Gbps	1.01 GB	1.10 GB	1.4%	1.6%
≡	● LexCore01.ipswitch.com	host1vmnic9 (56)	3:16 PM	1.00 Gbps	1.05 GB	643.91 MB	1.5%	0.9%

Monitoring: Applying Monitors

› How it works

- Select a device on your monitored network map and select “Monitors” (Top right of Map)
- Pick the monitor to be added and select “Apply to selected Devices”
- For multiple devices use the selector tool to highlight multiple devices on a map and navigate to Edit Devices >Assign Monitors
- For groups of devices use the group selector menu. Navigate to Edit Devices->Assign Monitors to add monitors to all devices in a group



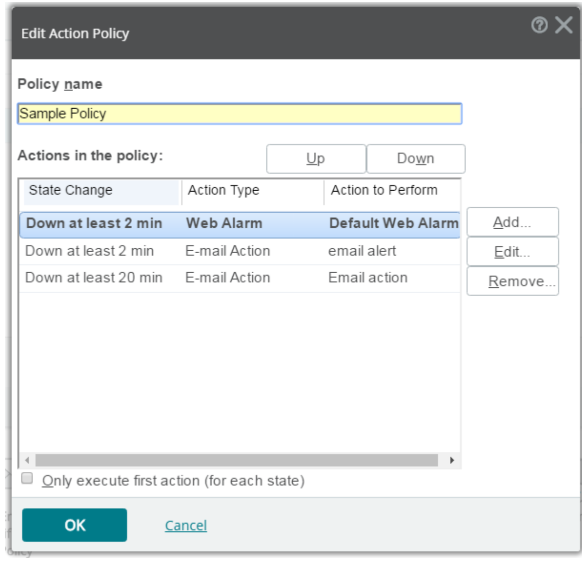


Monitoring: Action Policies

- How they work
  - They determine actions to initiate upon active monitor state changes and can be assigned to individual monitors or on the device level
  - Actions include: email alerts, SMS alerts, service restarts, and web alarms
- Creating Action Policies
  - From Settings > Actions & Alerts > Action & Policies create actions in the action library
  - Create an action policy from the actions from the library.
- Applying Action Policies
  - From the monitor setup page you can assign to individual monitors or on the device level under the actions and action policies section

Helpful Tip: Change action initiated times in the admin console under Configure > Program Options > Device States

Action Policies Video



Policy name

Sample Policy

Actions in the policy:

State Change	Action Type	Action to Perform
Down at least 2 min	Web Alarm	Default Web Alarm
Down at least 2 min	E-mail Action	email alert
Down at least 20 min	E-mail Action	Email action

□ Only execute first action (for each state)

Monitoring: Alert Center

Helpful Tip: Use blackout policies to suspend notifications during specific times such as assuring management do not receive notification on weekends.

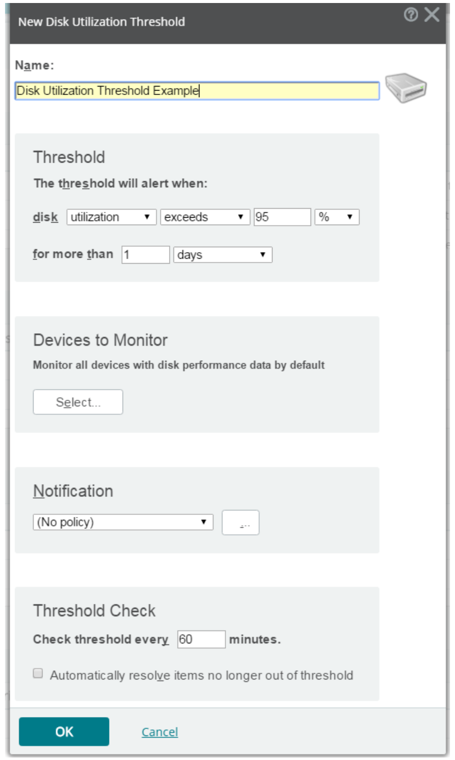
About

- The alert center provides a centralized view of device thresholds and policies applied and lets you create threshold based alerts and notifications

Creating & Viewing Alert Thresholds

- From Settings > Actions & Alerts > Alert Center Libraries click the plus icon under threshold library.
- You can customize multiple thresholds and select which devices they apply to.
- The notification policy library lets you setup notifications
- From Analyze > Dashboards > Alert Center to view all the configured thresholds and filter options

▶ [Alert Center Video]



New Disk Utilization Threshold

Name: Disk Utilization Threshold Example

Threshold

The threshold will alert when:

disk utilization ▾ exceeds ▾ 95 % ▾

for more than 1 days ▾

Devices to Monitor

Monitor all devices with disk performance data by default

Notification

(No policy) ▾

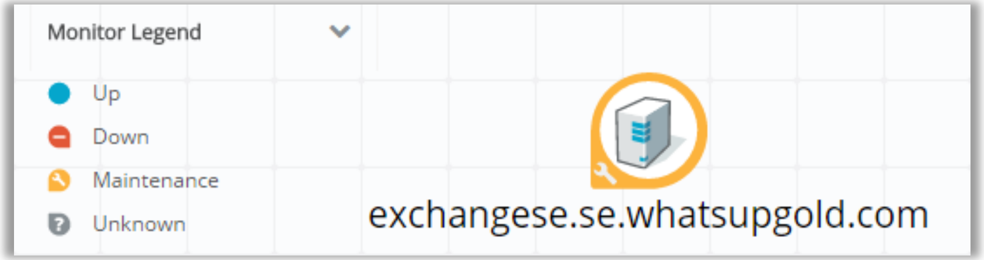
Threshold Check

Check threshold every 60 minutes.

□ Automatically resolve items no longer out of threshold

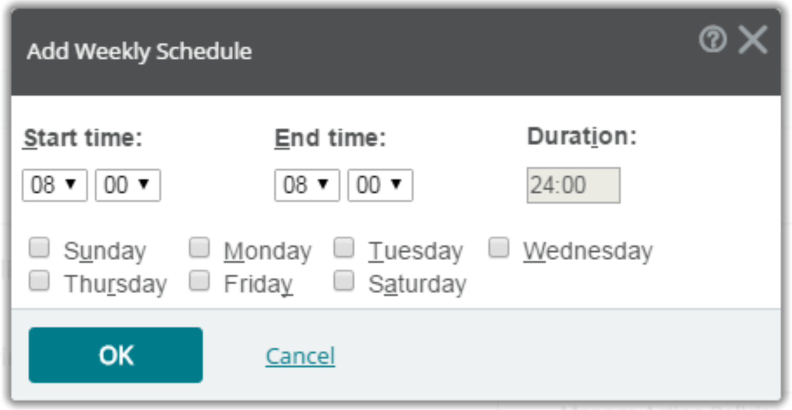
Monitoring: Maintenance Mode

- About
  - Maintenance mode is used to suspend polling and alerts when a device is known to be out of service.
  - Maintenance mode can be activated on demand or devices can be scheduled to be automatically added or removed
- Workflow
  - From the discovered network map, select a device and select “start maintenance mode” from the device navigation menu.
  - To schedule click “monitor setup” on the device card navigate to the polling and maintenance section and select the plus mark to define a maintenance schedule
  - Schedules can be copied to multiple devices from Edit Devices > Set Maintenance Schedule
  - The dynamic device group “devices in maintenance mode” allows you to review suspended devices



Monitor Legend

- ● Up
- ● Down
- ● Maintenance
- ● Unknown



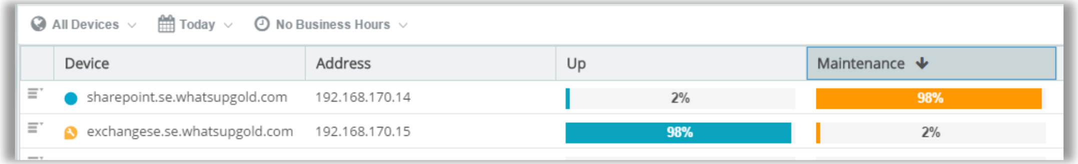
Add Weekly Schedule

Start time: 08 ▾ 00 ▾

End time: 08 ▾ 00 ▾

Duration: 24:00

□ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday



All Devices ⌵ Today ⌵ No Business Hours ⌵

Device	Address	Up	Maintenance
● sharepoint.se.whatsupgold.com	192.168.170.14	2%	98%
● exchangese.se.whatsupgold.com	192.168.170.15	98%	2%

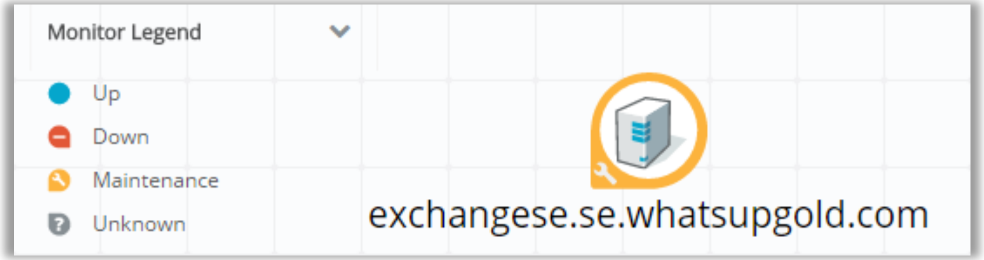
Monitoring: Maintenance Mode

About

- Maintenance mode is used to suspend polling and alerts when a device is known to be out of service.
- Maintenance mode can be activated on demand or devices can be scheduled to be automatically added or removed

Workflow

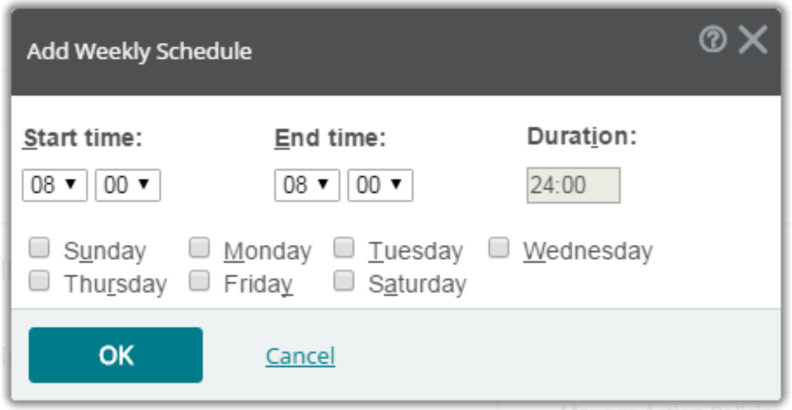
- From the discovered network map, select a device and select “start maintenance mode” from the device navigation menu.
- To schedule click “monitor setup” on the device card navigate to the polling and maintenance section and select the plus mark to define a maintenance schedule
- Schedules can be copied to multiple devices from Edit Devices > Set Maintenance Schedule
- The dynamic device group “devices in maintenance mode” allows you to review suspended devices



Monitor Legend

- ● Up
- ● Down
- ● Maintenance
- ● Unknown

exchangese.se.whatsupgold.com



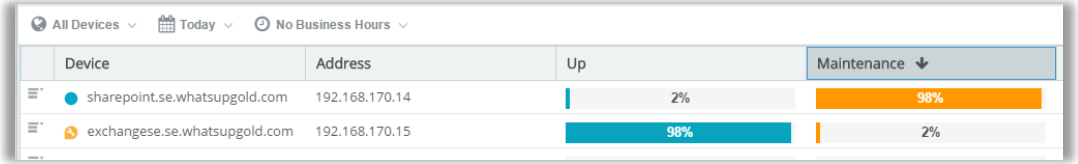
Add Weekly Schedule

Start time: 08 ▾ 00 ▾

End time: 08 ▾ 00 ▾

Duration: 24:00

□ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday



All Devices · Today · No Business Hours

Device	Address	Up	Maintenance
sharepoint.se.whatsupgold.com	192.168.170.14	2%	98%
exchangese.se.whatsupgold.com	192.168.170.15	98%	2%

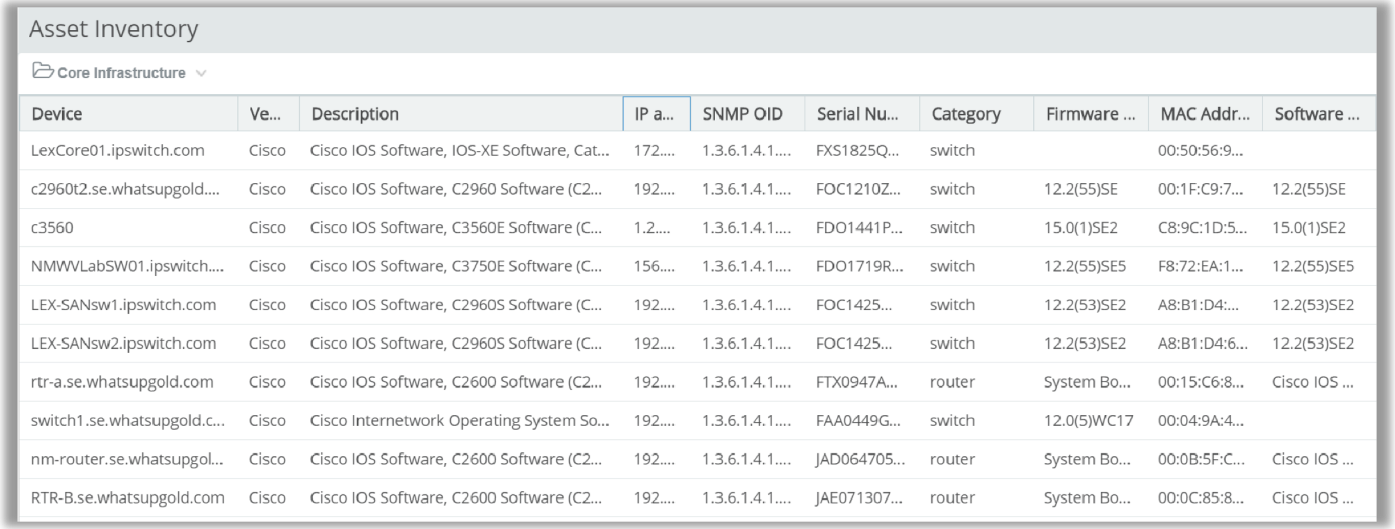
WhatsUp Gold Reporting

Reporting

[Built-in Reports]

[Dashboards]

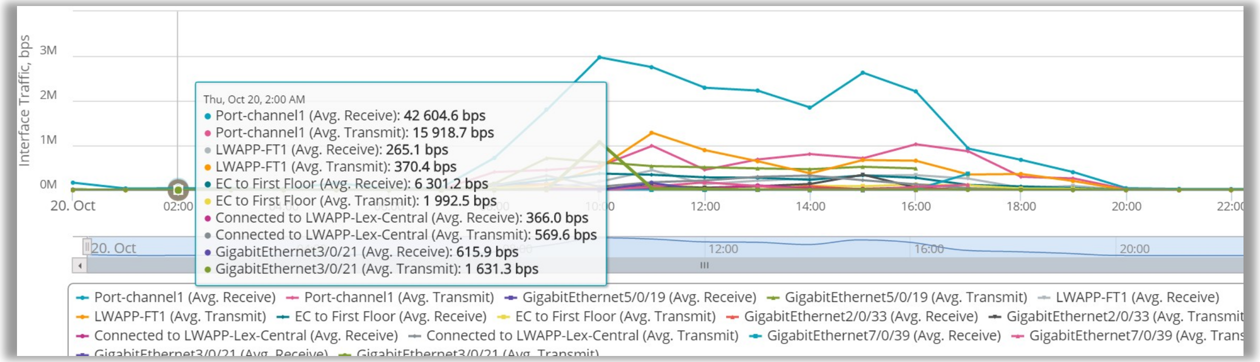
[Application Reporting]



Asset Inventory

Core Infrastructure

Device	Ve...	Description	IP a...	SNMP OID	Serial Nu...	Category	Firmware ...	MAC Addr...	Software ...
LexCore01.ipswitch.com	Cisco	Cisco IOS Software, IOS-XE Software, Cat...	172....	1.3.6.1.4.1....	FXS1825Q...	switch		00:50:56:9...	
c2960t2.se.whatsupgold....	Cisco	Cisco IOS Software, C2960 Software (C2...	192....	1.3.6.1.4.1....	FOC1210Z...	switch	12.2(55)SE	00:1F:C9:7...	12.2(55)SE
c3560	Cisco	Cisco IOS Software, C3560E Software (C...	1.2....	1.3.6.1.4.1....	FDO1441P...	switch	15.0(1)SE2	C8:9C:1D:5...	15.0(1)SE2
NMWVLabSW01.ipswitch....	Cisco	Cisco IOS Software, C3750E Software (C...	156....	1.3.6.1.4.1....	FDO1719R...	switch	12.2(55)SE5	F8:72:EA:1...	12.2(55)SE5
LEX-SANsw1.ipswitch.com	Cisco	Cisco IOS Software, C2960S Software (C...	192....	1.3.6.1.4.1....	FOC1425...	switch	12.2(53)SE2	A8:B1:D4:...	12.2(53)SE2
LEX-SANsw2.ipswitch.com	Cisco	Cisco IOS Software, C2960S Software (C...	192....	1.3.6.1.4.1....	FOC1425...	switch	12.2(53)SE2	A8:B1:D4:6...	12.2(53)SE2
rtr-a.se.whatsupgold.com	Cisco	Cisco IOS Software, C2600 Software (C2...	192....	1.3.6.1.4.1....	FTX0947A...	router	System Bo...	00:15:C6:8...	Cisco IOS ...
switch1.se.whatsupgold.c...	Cisco	Cisco Internetwork Operating System So...	192....	1.3.6.1.4.1....	FAA0449G...	switch	12.0(5)WC17	00:04:9A:4...	
nm-router.se.whatsupgol...	Cisco	Cisco IOS Software, C2600 Software (C2...	192....	1.3.6.1.4.1....	JAD064705...	router	System Bo...	00:0B:5F:C...	Cisco IOS ...
RTR-B.se.whatsupgold.com	Cisco	Cisco IOS Software, C2600 Software (C2...	192....	1.3.6.1.4.1....	JAE071307...	router	System Bo...	00:0C:85:8...	Cisco IOS ...



Reporting: Built-In Reports

About

- WhatsUp Gold comes with a variety of built-in reports covering network performance, inventory information and device availability

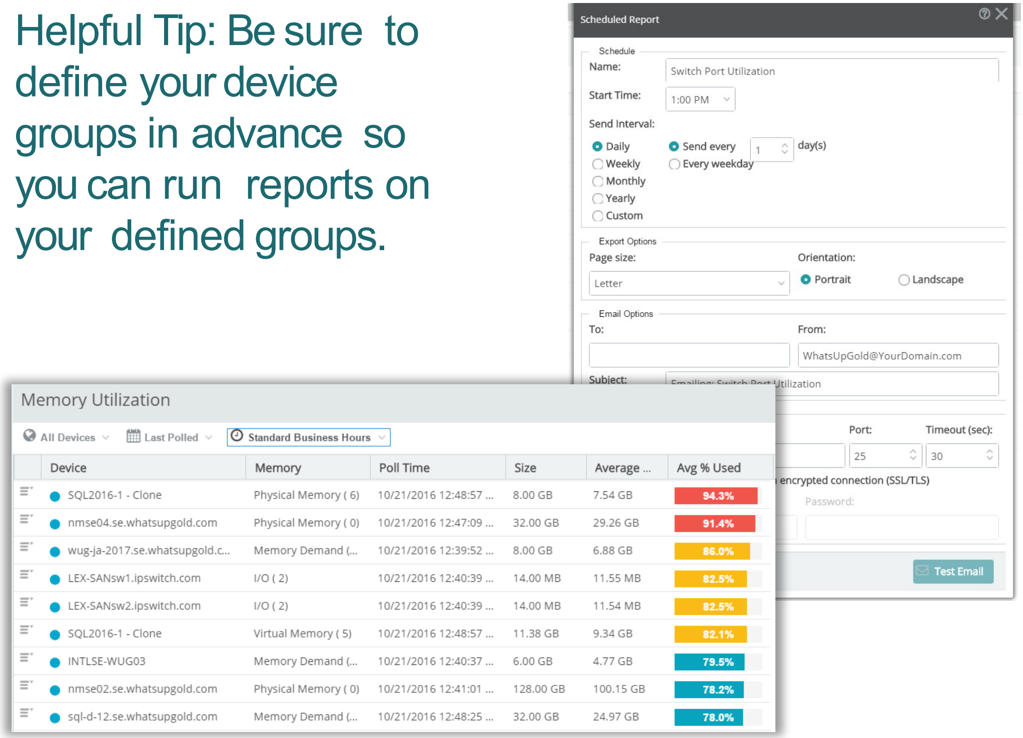
Report Filters

- Once in a report you can sort the data and add or remove report columns. There are filters available to change what the report examines.
- The available filters will vary from report to report. Some may include device groups to examine, timeframes, or business hour filters.

Report Scheduling

- Select Export > Schedule Export
- Select the export button (top right of report) to export the report in a variety of formats
- Reports can also be automatically emailed to users on a regular basis.

Helpful Tip: Be sure to define your device groups in advance so you can run reports on your defined groups.



Scheduled Report

Schedule

Name: Switch Port Utilization

Start Time: 1:00 PM

Send Interval:

● Daily ○ Weekly ○ Monthly ○ Yearly ○ Custom

● Send every 1 day(s)
○ Every weekday

Export Options

Page size: Letter

Orientation: ● Portrait ○ Landscape

Email Options

To:

From: WhatsUpGold@YourDomain.com

Subject: Emailing: Switch Port Utilization

Port: 25

Timeout (sec): 30

encrypted connection (SSL/TLS)

Password:

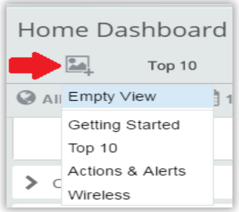
Memory Utilization

Device	Memory	Poll Time	Size	Average ...	Avg % Used
SQL2016-1 - Clone	Physical Memory (6)	10/21/2016 12:48:57 ...	8.00 GB	7.54 GB	94.3%
nmse04.se.whatsupgold.com	Physical Memory (0)	10/21/2016 12:47:09 ...	32.00 GB	29.26 GB	91.4%
wug-ja-2017.se.whatsupgold.c...	Memory Demand (...	10/21/2016 12:39:52 ...	8.00 GB	6.88 GB	86.0%
LEX-SANsw1.ipswitch.com	I/O (2)	10/21/2016 12:40:39 ...	14.00 MB	11.55 MB	82.5%
LEX-SANsw2.ipswitch.com	I/O (2)	10/21/2016 12:40:39 ...	14.00 MB	11.54 MB	82.5%
SQL2016-1 - Clone	Virtual Memory (5)	10/21/2016 12:48:57 ...	11.38 GB	9.34 GB	82.1%
INTLSE-WUG03	Memory Demand (...	10/21/2016 12:40:37 ...	6.00 GB	4.77 GB	79.5%
nmse02.se.whatsupgold.com	Physical Memory (0)	10/21/2016 12:41:01 ...	128.00 GB	100.15 GB	78.2%
sql-d-12.se.whatsupgold.com	Memory Demand (...	10/21/2016 12:48:25 ...	32.00 GB	24.97 GB	78.0%

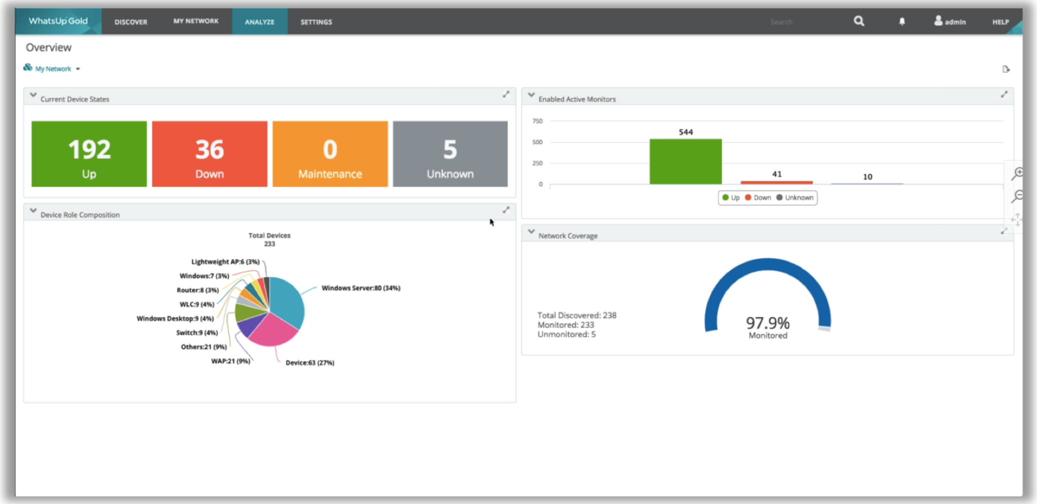
Reporting: Dashboards

- About
  - Create your own custom dashboards at Analyze > Dashboards > Home Dashboards
- Customization
  - From the dashboard screen, select “Add view > Empty view.” Provide a dashboard name and select the amount of columns to be included. Select “Add Reports” to populate dashboard
  - You can ‘filter’ reports’ by selecting the Settings button
  - Use the thumbtack icon to pin the filter – applying it to all reports in a dashboard

Helpful Tip: Users can share dashboard views with other users using the drop down menu on the top left



Dashboards Video

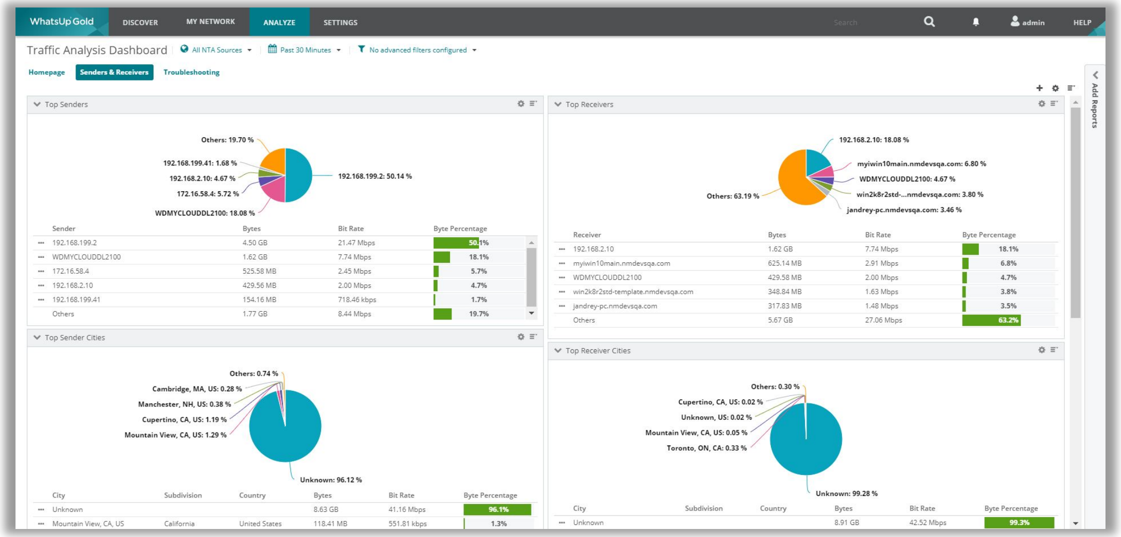


Network Traffic Analysis

About

- Get granular details as to who or what is consuming bandwidth by analyzing Netflow, NSEL, S-Flow, J-Flow and IPFIX records
- Configure devices to send flow data to WhatsUp Gold on port 9999
- From Analyze > Dashboards > Network Traffic Analysis you can apply filters to look at specific interfaces, ports, applications, or protocols
- Alert center thresholds and notifications are available from Settings > Actions & Alerts > Alert Center Libraries

[Network Traffic Analysis]



Traffic Analysis Dashboard | All NTA Sources | Past 30 Minutes | No advanced filters configured

Homepage | Senders & Receivers | Troubleshooting

Top Senders

Sender	Bytes	Bit Rate	Byte Percentage
192.168.199.2	4.50 GB	21.47 Mbps	50.1%
WDMYCLOUDDL2100	1.62 GB	7.74 Mbps	18.1%
172.16.58.4	525.58 MB	2.45 Mbps	5.7%
192.168.2.10	429.56 MB	2.00 Mbps	4.7%
192.168.199.41	154.16 MB	718.46 kbps	1.7%
Others	1.77 GB	8.44 Mbps	19.7%

Top Receivers

192.168.2.10: 18.08 %
myiwin10main.nmdevsqa.com: 6.80 %
WDMYCLOUDDL2100: 4.67 %
win2k8r2std-...nmdevsqa.com: 3.80 %
jandrey-pc.nmdevsqa.com: 3.46 %
Others: 63.19 %

Receiver	Bytes	Bit Rate	Byte Percentage
192.168.2.10	1.62 GB	7.74 Mbps	18.1%
myiwin10main.nmdevsqa.com	625.14 MB	2.91 Mbps	6.8%
WDMYCLOUDDL2100	429.58 MB	2.00 Mbps	4.7%
win2k8r2std-template.nmdevsqa.com	348.84 MB	1.63 Mbps	3.8%
jandrey-pc.nmdevsqa.com	317.83 MB	1.48 Mbps	3.5%
Others	5.67 GB	27.06 Mbps	63.2%

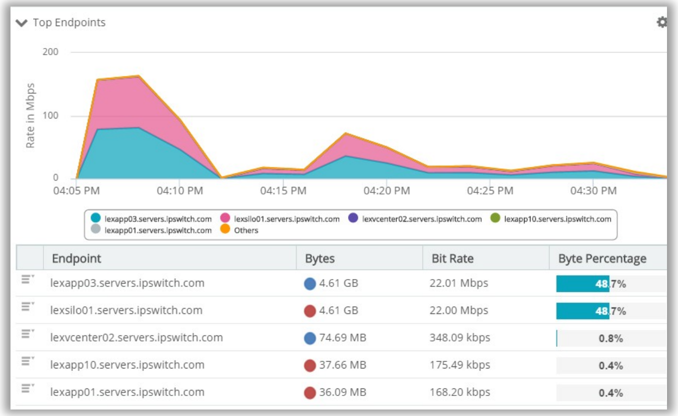
Top Sender Cities

Others: 0.74 %
Cambridge, MA, US: 0.28 %
Manchester, NH, US: 0.38 %
Cupertino, CA, US: 1.19 %
Mountain View, CA, US: 1.29 %
Unknown: 96.12 %

City	Subdivision	Country	Bytes	Bit Rate	Byte Percentage
Unknown			8.63 GB	41.16 Mbps	96.1%
Mountain View, CA, US	California	United States	118.41 MB	551.81 kbps	1.3%

Top Receiver Cities

City	Subdivision	Country	Bytes	Bit Rate	Byte Percentage
Unknown			8.91 GB	42.52 Mbps	99.3%


Top Endpoints

Rate in Mbps
200
100
0
04:05 PM
04:10 PM
04:15 PM
04:20 PM
04:25 PM
04:30 PM
lexapp03.servers.ipswitch.com
lexsilo01.servers.ipswitch.com
lexvcenter02.servers.ipswitch.com
lexapp10.servers.ipswitch.com
lexapp01.servers.ipswitch.com
Others

Endpoint	Bytes	Bit Rate	Byte Percentage
lexapp03.servers.ipswitch.com	4.61 GB	22.01 Mbps	48.7%
lexsilo01.servers.ipswitch.com	4.61 GB	22.00 Mbps	48.7%
lexvcenter02.servers.ipswitch.com	74.69 MB	348.09 kbps	0.8%
lexapp10.servers.ipswitch.com	37.66 MB	175.49 kbps	0.4%
lexapp01.servers.ipswitch.com	36.09 MB	168.20 kbps	0.4%

Configuration Management

About

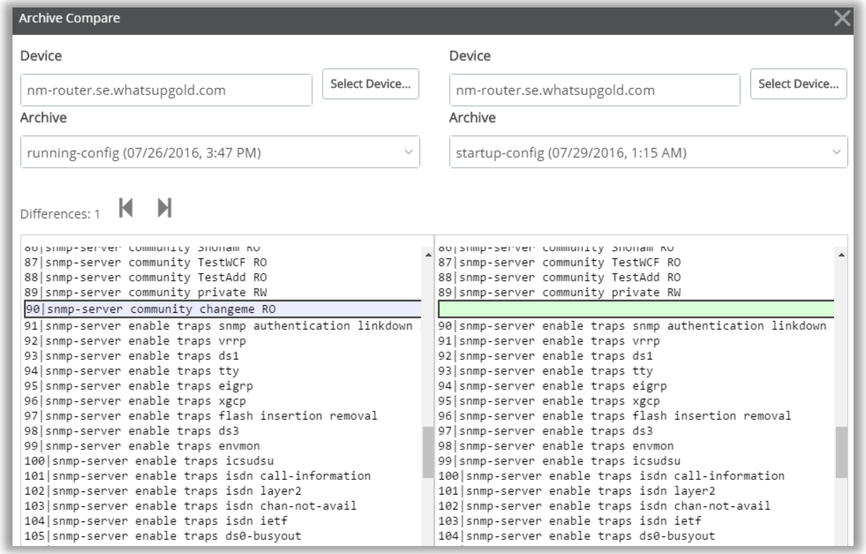
- You can automate network device configuration backups for any device that supports telnet or SSH
- WhatsUp Gold comes with built-in, customizable scripts for common devices to change SNMP strings, add or remove usernames and backup running and starting configurations.

Running and Configuration Task

- From Settings > Configuration Management > Task Library select the script to use, which devices to run against and threshold settings then define a run schedule
- You can also setup email notifications for changes to the configuration or audit the configuration against defined policies
- You can view and compare device configurations inside device properties page

Helpful Tip: Be sure that SNMP and Telnet/SSH credentials are assigned to the device running the configuration task. The credentials should be assigned to the device automatically if it was discovered with proper credentials.

Configuration Manager Video



Archive Compare

Device: nm-router.se.whatsupgold.com
Archive: running-config (07/26/2016, 3:47 PM)

Device: nm-router.se.whatsupgold.com
Archive: startup-config (07/29/2016, 1:15 AM)

Differences: 1

```
snmp-server community TestWCF RO
snmp-server community TestAdd RO
snmp-server community private RW
snmp-server community changeme RO
snmp-server enable traps snmp authentication linkdown
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps xgcp
snmp-server enable traps flash insertion removal
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
```

```
snmp-server community TestWCF RO
snmp-server community TestAdd RO
snmp-server community private RW

snmp-server enable traps snmp authentication linkdown
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps xgcp
snmp-server enable traps flash insertion removal
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
```

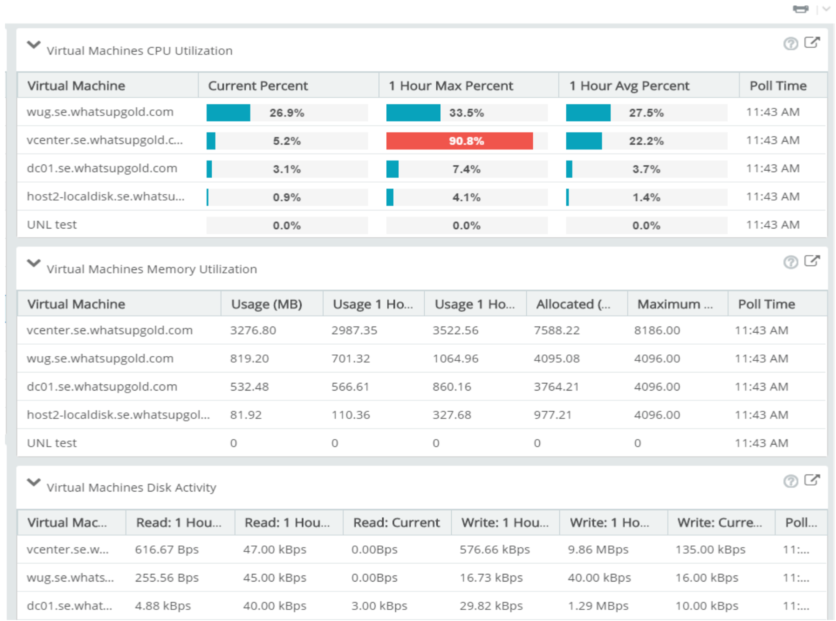
Virtualization Monitoring

About

- Virtual Monitoring gathers performance statistics, maps out the virtual environment and can allows users to be notified based on Hyper-V or VMware event logs
- From Analyze > Dashboards > Virtual Monitoring select a virtual device to view virtual machine statistics
- Navigate to Settings->Actions & Alerts->Alert Center Libraries to setup either VMware or Hyper-V event log notification policies.

Virtualization Monitoring

Helpful Tip: VMware virtual monitoring requires devices to be discovered with VMware credentials. Hyper-V monitoring uses windows credentials.



Virtual Machines CPU Utilization

Virtual Machine	Current Percent	1 Hour Max Percent	1 Hour Avg Percent	Poll Time
wug.se.whatsupgold.com	26.9%	33.5%	27.5%	11:43 AM
vcenter.se.whatsupgold.c...	5.2%	90.8%	22.2%	11:43 AM
dc01.se.whatsupgold.com	3.1%	7.4%	3.7%	11:43 AM
host2-localdisk.se.whatsu...	0.9%	4.1%	1.4%	11:43 AM
UNL test	0.0%	0.0%	0.0%	11:43 AM

Virtual Machines Memory Utilization

Virtual Machine	Usage (MB)	Usage 1 Ho...	Usage 1 Ho...	Allocated (...	Maximum ...	Poll Time
vcenter.se.whatsupgold.com	3276.80	2987.35	3522.56	7588.22	8186.00	11:43 AM
wug.se.whatsupgold.com	819.20	701.32	1064.96	4095.08	4096.00	11:43 AM
dc01.se.whatsupgold.com	532.48	566.61	860.16	3764.21	4096.00	11:43 AM
host2-localdisk.se.whatsupgol...	81.92	110.36	327.68	977.21	4096.00	11:43 AM
UNL test	0	0	0	0	0	11:43 AM

Virtual Machines Disk Activity

Virtual Mac...	Read: 1 Hou...	Read: 1 Hou...	Read: Current	Write: 1 Hou...	Write: 1 Ho...	Write: Curre...	Poll...
vcenter.se.w...	616.67 Bps	47.00 kBps	0.00Bps	576.66 kBps	9.86 MBps	135.00 kBps	11:...
wug.se.whats...	255.56 Bps	45.00 kBps	0.00Bps	16.73 kBps	40.00 kBps	16.00 kBps	11:...
dc01.se.what...	4.88 kBps	40.00 kBps	3.00 kBps	29.82 kBps	1.29 MBps	10.00 kBps	11:...

Application Monitoring

About

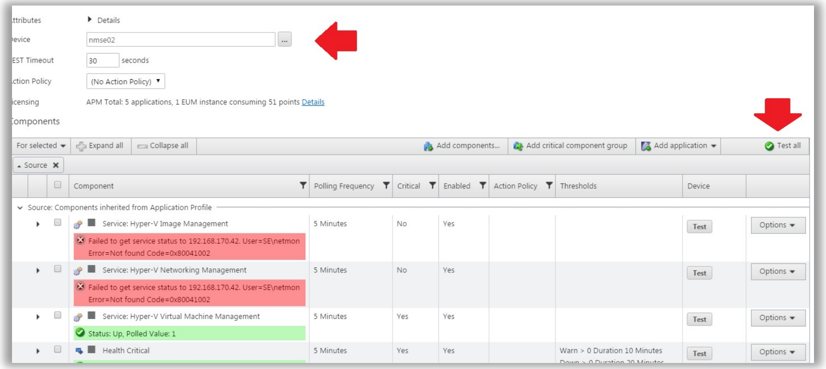
- WhatsUp Gold provides built-in profiles to monitor commonly used applications like Microsoft Exchange, SQL, SharePoint, and Active Directory.
- After applying the application profile to devices running the application, application monitoring dashboards show the health of monitored application components
- Create your own application profile by editing an existing profile or create a new profile by adding components to be monitored

Setup

- From Settings > Application Monitoring > Application and Profile Setup. Select a profile from the menu, and click "add application instance."
- Fill out information about the application, and assign the device running the application to the profile. Test all the components in the profile by selecting the "test all" button. Save and close the profile when complete.

Helpful Tip: To use action policies to be notified of application state changes navigate to Settings > Application Monitoring > Application Monitoring > Actions and Policies

Application Monitoring Video



ttributes ▸ Details

evice: nmse02 ...

EST Timeout: 30 seconds

ction Policy: (No Action Policy) ▾

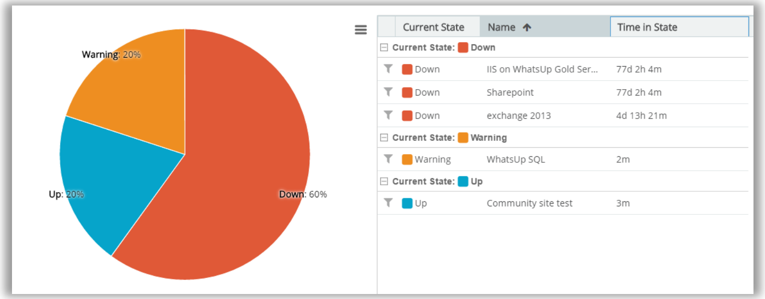
icensing: APM Total: 5 applications, 1 EUM instance consuming 51 points Details

omponents

For selected ▾ | Expand all | Collapse all | Add components... | Add critical component group | Add application ▾ | Test all

Source ✕

□	Component	Polling Frequency	Critical	Enabled	Action Policy	Thresholds	Device	
	Source: Components inherited from Application Profile							
□	Service: Hyper-V Image Management Failed to get service status to 192.168.170.42. User=SE\netmon Error=Not found Code=0x80041002	5 Minutes	No	Yes			Test	Options ▾
□	Service: Hyper-V Networking Management Failed to get service status to 192.168.170.42. User=SE\netmon Error=Not found Code=0x80041002	5 Minutes	No	Yes			Test	Options ▾
□	Service: Hyper-V Virtual Machine Management Status: Up, Polled Value: 1	5 Minutes	Yes	Yes			Test	Options ▾
□	Health Critical	5 Minutes	Yes	Yes		Warn > 0 Duration 10 Minutes Down > 0 Duration 20 Minutes	Test	Options ▾



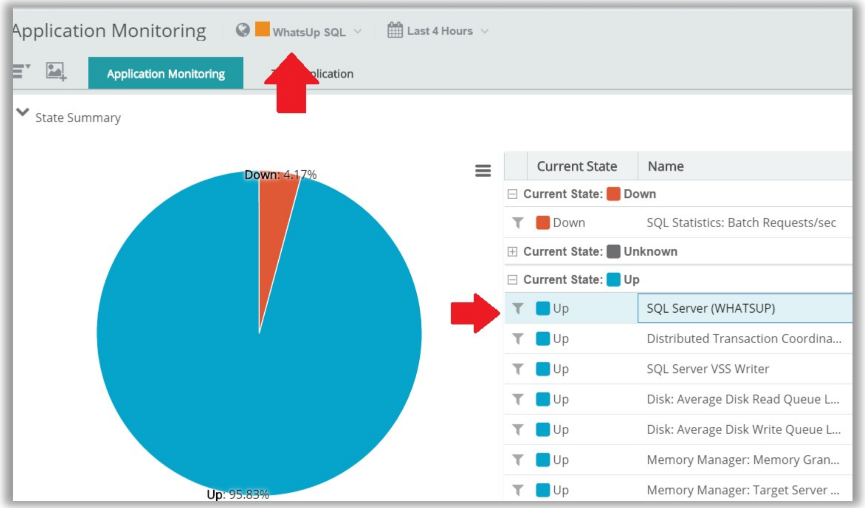
Current State	Name ↑	Time in State
Current State: 🟥 Down		
🟥 Down	IIS on WhatsUp Gold Ser...	77d 2h 4m
🟥 Down	Sharepoint	77d 2h 4m
🟥 Down	exchange 2013	4d 13h 21m
Current State: 🟧 Warning		
🟧 Warning	WhatsUp SQL	2m
Current State: 🟦 Up		
🟦 Up	Community site test	3m

Application Reporting

About

- Application dashboards allow user to drill down into an application profile the component level.
- After Application profiles have been configured, navigate to Analyze > Dashboards > Application Monitoring
- The default state summary re[prt sjpws the health of all monitored applications.
- You can apply a filter from the top of the report to look at the health of each monitored component of an individual application instance
- You can apply a filter on the component level to see the how it performed over time

Helpful Tip: Reports included in the Application Monitoring dashboard can be included in custom dashboards

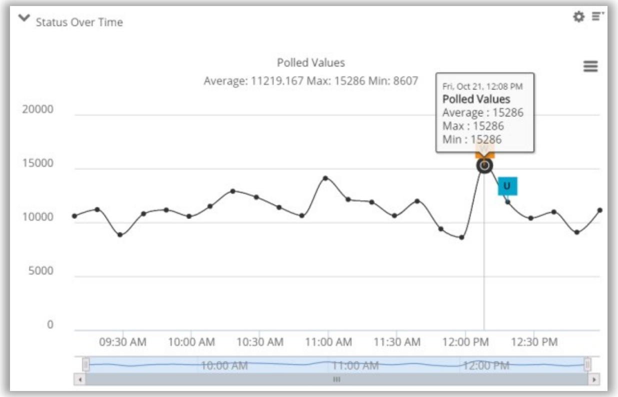


Application Monitoring · WhatsUp SQL · Last 4 Hours

Application Monitoring · plication

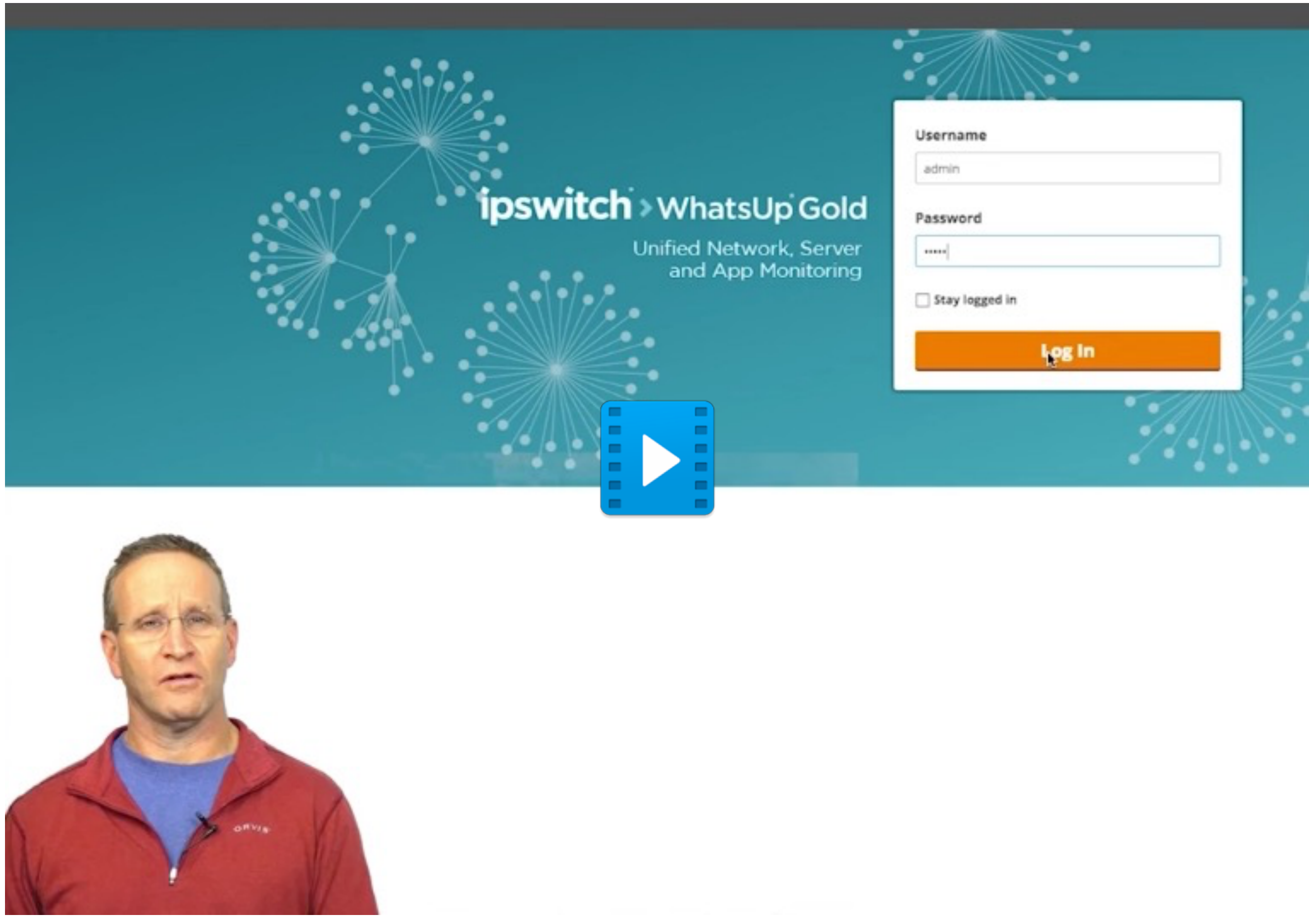
State Summary

Current State	Name
⊟ Current State: 🟥 Down	
🟥 Down	SQL Statistics: Batch Requests/sec
⊞ Current State: ■ Unknown	
⊟ Current State: 🟦 Up	
🟦 Up	SQL Server (WHATSUP)
🟦 Up	Distributed Transaction Coordina...
🟦 Up	SQL Server VSS Writer
🟦 Up	Disk: Average Disk Read Queue L...
🟦 Up	Disk: Average Disk Write Queue L...
🟦 Up	Memory Manager: Memory Gran...
🟦 Up	Memory Manager: Target Server ...



More Features to Check Out

- See WhatsUp Gold 2018
  - Cloud Monitoring
  - Overview Dashboard
  - Meraki monitoring
  - Storage Monitoring
  - Interface Utilization Overlay



Username admin

Password •••••

□ Stay logged in

Contact sales or your Local reseller

to learn more or get pricing information