Best Practices: IT Management for Educational Institutions

You're a network engineer at an educational institution, primary or secondary school, community college or university, challenged to support the day-to-day operation across distributed campuses for hundreds or thousands of students, faculty and staff. Are you constantly asked to do more with less? Are you looking for cost-effective ways to manage and secure your infrastructure?

Challenges for Educational Institutions

Now, more than ever, students, faculty and staff rely on a functional, secure IT infrastructure to help them with learning, instruction, collaboration and research. Each year, a reliable, optimized and well-run infrastructure becomes even more critical to the success of educational institutions worldwide. Have you encountered any of these challenges before?

- The network is slow and you can't reproduce it
- Virtual proliferation, tracking VM to physical association at all times
- Slow streaming media, end-user complaints
- Inability to measure bandwidth utilization
- Too many monitoring tools and too many consoles
- Trouble identifying under-utilized resources to be re-purposed on a private cloud
- Preparing to meet key compliance regulations (like FERPA and PCI in the USA)

If any of these sounds familiar, read on. This paper will discuss Best Practices to manage and secure your network using WhatsUp Gold.

"With WhatsUp Gold we have full visibility and proactive control of network structure, device configuration, network and device performance, resource utilization and traffic details—all through a single console. And our researchers have the ability to get their work done anytime and anywhere on campus."

-Valerio Raggi, Network engineer and administrator, European University Institute, Italy

Best Practice #1: Know Your Infrastructure

Here at Ipswitch, we think of networks as "living entities," since planned and unplanned changes happen all the time. Additions of students or faculty, reallocations to a new facility or campus, disruptive technology like virtualization, new streaming media applications, purchasing of new hardware and mobile devices, datacenter consolidation projects—they all introduce the need for a complete rediscovery of your infrastructure, hardware assets and port-to-port connectivity. After all, if you don't know what you have running in your infrastructure, how devices in your network are connected, their interdependencies, and their locations, how simple can it be to secure your network, or locate problems and resolve them before the impact of a failure is realized? A layer 2/3 discovery is actually an eye-opener for many organizations since they discover pieces of hardware unaccounted for, or interdevice connections that they didn't even know they were there. Once you have a hardware inventory in place, you can use it to document your network to simplify troubleshooting tasks, for auditing purposes, or simply to try to reduce costs by re-purposing unused resources.

"Out of the box the functionality is amazing. What you see is what you get. When you start to look at the cost/benefits you quickly find that there's literally no comparison to WhatsUp Gold—it's a fraction of the cost of other products."

-Frederick Brenz, Network-WAN/Telecom Manager, Cypress Fairbanks Independent School District, Texas, USA

*How: Use **WhatsUp Gold WhatsConnected** to automatically discover, map, inventory and document your network (devices, servers, virtual resources, hardware, and software assets) and port-to-port connectivity in minutes! Using its powerful auto-discovery and dynamic mapping, and a simple one-click integration with Visio™, your team will always have topology information at their fingertips.*

WhatsUp Gold's IT Management solution offers the best value for educational institutions.

Proven for Education—Worldwide institutions of all sizes utilize WhatsUp Gold for complete IT management.

Quick Implementation, Easy Configuration and Low Operating Cost—You can be up and running in less than an hour!

Simple Licensing Model—Simple and straight-forward pricing—just count the number of devices.

Comprehensive Feature Set—Discover, map and manage your entire IT infrastructure from a single interface with one Alert Center & one integrated discovery. Select the custom solution that's right for you.

Work Across Networks, Buildings, Campuses—WhatsUp Gold Distributed Edition provides you with scalable and secure management and monitoring of any number of remote sites from a centralized location.

Air-Tight Security—WhatsUp Gold is FIPS 140-2-certified, meeting one of the highest security requirement standards available.

Best Practice #2: Monitor Your Infrastructure

Once you have discovered what you have and how everything is connected, you should start monitoring health, availability and performance across all your infrastructure components, including network devices, servers, applications and virtual resources. Using multiple management consoles to monitor performance means that you have to manually examine multiple reports and interfaces to correlate information from different sources. This can be time-consuming and confusing, especially when you are dealing with several virtual machines and hundreds of physical servers. Plus, it will make troubleshooting very difficult (and slower) and can increase MTTR (mean time to resolution).

Here are some key focus areas that you should monitor on an ongoing basis.

Area	What to Monitor
Networking Devices	Key metrics such as interface utilization, and other metrics stored in their MIBs, such as interface errors and discards, CPU and Memory utilization.
Systems, Servers & Workstations	Processor utilization, memory, processes, storage and file system, as well as disk I/O, to help identify both under and over utilized systems. This should be done for Windows, Unix, Linux, Solaris or MAC Operating Systems.
Hardware Performance Indicators	By monitoring areas such as temperate, power supply and fans, you will be able quickly detect if there are instances of overheating or component failures.
Virtual Resources	Similarly to what you'd normally monitor for your physical servers, you should oversee metrics such as CPU, interface, memory, and disk utilization on the VM and host level. By monitoring disk utilization on the host level, you can effectively protect yourself against growing to the limit of your volume. In addition, you should configure real-time alerts on specific VMware problems such as migration errors, clusters being overcommitted, insufficient failover resources, a general VM error, or when host warnings/errors are triggered.

*How: Use **WhatsUp Gold** and **WhatsUp Gold WhatsVirtual** to monitor, alert, manage and report across devices, systems and physical and virtual resources from a single interface. WhatsUp Gold's powerful monitoring, alerting and notification capabilities, combined with custom dashboard views and over 200 reports, will give you the actionable intelligence to make smarter decisions faster, and keep your network infrastructure running smoothly.*

Best Practice #3: Monitor Network Traffic

While performance management has been getting all the buzz in the industry, understanding and managing network traffic and bandwidth usage—regardless of the protocol used—will help you on three key fronts:

1. Understand which users, applications and protocols are consuming your bandwidth. In fact, streaming media applications and non-work related activities could be putting a strain on your valuable network resources, causing network slowdowns and intermittent problems for all your users.

2. Properly measure bandwidth usage, so you can verify ISP providers billing or properly plan for spikes in bandwidth usage and avoid dropped packages or delays.

3. Protect your network and quickly detect DOS attacks and other rogue activity directed at your network. For example, did you know that many attackers are hiding in plain sight and moving data out of organizations using tried-and-true means, such as FTP, HTTP and SMTP, as reported by Black Hat? Firewalls won't flag HTTP traffic as an anomaly.

Educational organizations of all sizes should go deep into their flow data and look for a flow management solution that will let them analyze, alert and report on the different types of traffic traversing the network. This is how it works: each flow enabled router or switch (source) collects and aggregates information about traffic passing through it, and when configured to do so, transmits the information to a flow-enabled network management and monitoring system such as WhatsUp Gold Flow Monitor.

"Our network was more or less a mess. Most of the switches were not manageable and I had no tool at all to help me keep everything up and running," says Don Markese, Technology Director for Freehold Regional High School District. After WhatsUp Gold and WhatsUp Gold Flow Monitor were installed, Markese noticed that there was a large spike in unauthorized bandwidth traffic coming from one of the school buildings. With WhatsUp Gold Flow Monitor, he was able to monitor this abnormality over the next couple of days and noticed that this spike was a daily occurence. As the spike had a detrimental effect on the performance of the entire network, Markese used WhatsUp Gold Flow Monitor to determine the source of this unauthorized traffic. He was then able to notify the principal of the school where this was occurring, and they were able to put a stop to the illegal use ofthe network's bandwidth before it caused any further problems.

Freehold Regional High School District

*How: Use **WhatsUp Gold** and* **WhatsUp Gold Flow Monitor**. *In customer Don Markese's words, "If it weren't for WhatsUp Gold and WhatsUp Gold Flow Monitor, that unauthorized usage of the network bandwidth likely would have gone unnoticed and continued to have a negative effect on the overall performance of the network... So the benefits of having WhatsUp Gold and the plug-ins at the head of our network management strategy have already been noticeable. The comprehensiveness of the product has really given me complete control of the network and has greatly enhanced its overall performance."*

Best Practice #4: Automate Configuration Changes

Configuration management is an often overlooked area, but did you know that 60% of network outages and performance degradations are due to misconfiguration errors? As a network management professional, you spend a significant amount of time establishing and fine-tuning network devices' configurations to ensure stable network performance, protect data and secure networks from unauthorized users. With sometimes hundreds of individual devices to manage and maintain, configuration changes are made almost continuously, and they are hard to track on an ongoing basis. Recreating a device configuration from scratch, or identifying what's changed on a network, when, where, and by whom can be very difficult without a configuration management solution in place. The ability to rapidly react to a device failure or misconfiguration is vital in a sound network management strategy. The capability to download a backup to a

new device or replace an existing file can mean the difference between a network outage and a healthy infrastructure. Here are some quick best practice pointers to help you jump-start your configuration management efforts:

BP 1	Create standard configurations for each device classification (e.g. router, LAN switch, WAN switch, or ATM switch)
BP 2	Maintain the current running configurations for all devices and a set number of previously running versions—at least three to five previous working versions. It will really help with troubleshooting tasks.
BP 3	Keep track of when configuration changes were made for auditing purposes. You might even think about setting up real-time alerts and notifications in this area.
BP 4	Automate the execution of the scheduled tasks relating to current network configuration backups, startup configuration file backups and password change management for an individual device or across groups of devices to reduce errors and save time.
BP 5	Document your network and configuration changes periodically.

*How: Use **WhatsUp Gold WhatsConfigured** to automate network device configuration and change management processes, simplify your life, and eliminate human errors. With WhatsConfigured in place you don't have to perform repetitive and tedious manual configuration tasks, or troubleshoot misconfiguration issues in the dark. Plus, you can rest easy and save time with features such as nightly config backups, bulk config changes, complete audit trails, and real-time alerts triggered by configuration changes.*

Best Practice #5: Consolidate All Alerts in a Central Location

As you know, a network is comprised of any number of different single components, all designed and configured to work interdependently. It is this interdependency that is difficult to decode. As you build your infrastructure management strategy, you should look for ways to obtain a consolidated view of all alerts and problems occurring anywhere in your infrastructure, including performance issues, network traffic bottlenecks, bandwidth usage violations, hardware issues, configuration changes, and so on. That way, you'll increase IT efficiency by ensuring better coordination in response procedures and knowing exactly what's happening in your network. Plus, it's easier to troubleshoot hard-to-resolve issues, such as a slow network or intermittent problems, when you have a unified view of all alerts and problems.

*How: **WhatsUp Gold** includes a central Alert Center—a single integrated workspace that consolidates all alerts, notifications and alert acknowledgements across WhatsUp Gold and its plug-ins for easy configuration and management. That way, you can coordinate an alert response via acknowledgements and multiple levels of escalations, no matter the network location—a hardware problem, a performance bottleneck, a bandwidth usage violation or a misconfigured device.*

> *"The reason we're always using WhatsUp Gold is the front page console—it's more intuitive. It's becoming our help desk dashboard, and that says a lot."*
> -Albert Stadler, Director of Infrastructure and Security, Missouri Southern State University, Missouri, USA

Best Practices #6: Look for Custom Monitoring Tools That Fit Your Schedule

You should look for management capabilities that simplify your life, reduce your workload and fit your schedule—not the other way around. Here is a quick list of some capabilities that you should require, and how they'll make your life easier.

Feature	Why
Business Hours Reporting	Align your reporting to match your business schedule.
Scheduled PDF Reporting	Easy to schedule and share workspaces and full reports with your peers or management.
SMS Alerts	Receive key information on your phone on the go, when you need it, wherever you are.
Blackout Alert Suppression	Define blackout periods and suppress alerts and notifications when you're enjoying your personal life—at night, on the weekends, or when you are away on vacation.
Blackout Alert Summary	Stay on top of everything while enjoying your time off—receive a summary of problems and alerts suppressed during blackout periods when you're back, so you know what happened while you were away.
Mobile Access	Manage your network from your mobile device on the go—get alerts, reports and monitor your network remotely.

*How: **WhatsUp Gold** offers all the capabilities that you need to better balance your career and personal life. Its advanced capabilities, like business hours reporting, scheduled report distribution, blackout alerts suppression and summaries, as well as Mobile Access, give you the ability to react to events immediately anytime, from anywhere.*

Best Practices #7: Secure and Protect Key Information

To protect and secure key information such as student records and employee data, you need to know who is accessing which systems and data, and what users are doing at all times. Records of all events taking place in your environment are being logged right now into event logs and Syslog files across your servers, workstations and networking devices. Think about it—log files contain complete audit trails of access, additions, deletions or manipulation of key information. Therefore, Windows Event, W3C/IIS and Syslog files need to be collected, stored, analyzed and reported on to have near real-time security event detection and response as well as maintained for operational forensics and compliance reporting.

Did you know that under the Family Educational Rights and Privacy Act (FERPA), federally funded, US-based educational institutions must protect student records to keep their funding?

The PCI-DSS standard applies to any organization that is handling credit card transactions. Whether you are collecting card data for the school lunch program, tuition payments or the purchase of books, your institution is also responsible for assuring that cardholder data is protected.

*How: Use **WhatsUp Log Management** to:*

Step 1	Automatically collect and store your log files for as long as you need (e.g. FERPA mandates up to 7 years in some states) with WhatsUp Log Management. Don't forget to: ✓ Leverage its cryptographic hashing capabilities to prevent tampering with archived log files ✓ Collect Syslog, W3C/IIS and Windows Event logs
Step 2	Configure WhatsUp Log Management to generate real-time alerts for key events (e.g. access and permission changes to files, folders, and objects containing education records or personally identifiable information).
Step 3	Generate and automatically distribute the reports that you need to prove compliance with WhatsUp Log Management—see the detailed tables on the following page.

If you're looking for more information on FERPA and PCI-DSS, please read below.

FERPA	
Legal Requirements	**Suggested WhatsUp Log Management Alerts & Reports**
20 U.S.C. § 1232g; Title 34, Part 99—Family Educational Rights and Privacy (4) (A) For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which— • (i) contain information directly related to a student; and • (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution. Part b.1: No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of educational records, or personally identifiable information contained therein other than directory information... • Data and records of electronic transactions, including computer logs can be considered "student records" under FERPA. • According to the America Association of Collegiate Registrars and Admissions Officers (AACRAO), "Education record means those records, files, documents and other materials which contain information directly related to a student and are maintained by an educational agency or institution or by a person acting for such agency or institution," and "record is understood to mean any information or data recorded in any medium (e.g., handwriting, print, tapes, film, microfilm, microfiche, any form of electronic data storage."	• Any changes to File or Folder ACLs • Registry Access - adds, changes, and deletions • User account changes that provide administrator equivalent permissions • Active Directory access and changes • Changes to Groups - adds, changes or deletions • Windows and SSH login failures and successes • System events - process start and shutdown • Application failure, start or shutdown • IDS and anti-virus logs • Interfaces for high TCP and UDP traffic • Server offline or online and reboots • Access to network infrastructure • Changes to ACLs on switches, routers or firewalls • DNS changes • Web server access and permission changes • HTTP "404" errors • FTP server access and file transfers • Server and workstation logs for intrusion incidents and policy changes • Access and permission changes to Files, Folders, and Objects containing student records data **Key Windows Event Logging Categories to Enable** • Logon Events - Success/Failure • Account Logons - Success/Failure • Object Access - Success/Failure • Process Tracking - Success • Policy Change - Success/Failure • Account Management - Success • Directory Service Access - Success/Failure • System Events - Success/Failure

*In addition, **WhatsUp Gold** and **WhatsUp Gold Flow Monitor** can also help you secure your network and detect traffic abnormalities that may indicate viruses, malware and other rogue activities.*

PCI-DSS	
Legal Requirements	**Suggested WhatsUp Log Management Alerts & Reports**
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. 10.2 Implement automated audit trails for all system components to reconstruct the following events: • 10.2.1 All individual user accesses to cardholder data • 10.2.2 All actions taken by any individual with root or administrative privileges • 10.2.3 Access to all audit trails • 10.2.4 Invalid logical access attempts • 10.2.6 Initialization of the audit logs • 10.2.7 Creation and deletion of system-level objects 10.3 Record at least the following audit trail entries for all system components for each event: • 10.3.1 User identification • 10.3.2 Type of event • 10.3.3 Date and time • 10.3.4 Success or failure indication • 10.3.5 Origination of event • 10.3.6 Identity or name of affected data, system component, or resource	• Directory Service Access Attempts • Directory Service Access - Success/Failure • Logon Failures – Active Directory • Logon Failures – Local Logons • Object Access Attempts – Success/Failure • Object Deletions • Password Reset Attempts by Administrators or Account Operators • Process (Program) Usage • User Activity in Auditing Categories • Successful Network Logons – Workstations and Servers • Policy Change - Success/Failure • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure

Summary

WhatsUp Gold is a complete IT Management Solution, simple to install and easy to use, that lets you discover and manage your network, servers, applications, virtual resources, network traffic, configuration, layer 2 port-to-port connectivity and events in a matter of minutes, all from a SINGLE console. WhatsUp Gold has been in the market for 20 years and has been tried, tested, and proven on networks just like yours—over 100,000 of them. See some examples below of how WhatsUp Gold can help support your IT goals:

Your Goal	Recommended WhatsUp Gold Solution
Datacenter consolidation **Moving to a private cloud** **Virtualization**	Pre-virtualization phase **Step 1:** *Use **WhatsUp Gold WhatsConnected** to discover, map, inventory and document everything connected to your network* **Step 2:** *Import your information into **WhatsUp Gold**, and start monitoring performance right away. Identify under-utilized resources that can be virtualized* Post-virtualization phase **Step 3:** *Use **WhatsUp Gold** to ensure optimal performance on an on-going basis* **Step 4:** *Use **WhatsUp Gold WhatsVirtual** to manage and control physical and virtual resources from the same console* **Step 5:** *Use **WhatsUp Gold Flow Monitor** to go deeper into network traffic and understand bandwidth usage—who and how* **Step 6:** *Use **WhatsUp Gold** to secure your network with real-time alerts on key vCenter security events*

Your Goal	Recommended WhatsUp Gold Solution
Solving intermittent slow network problems **Managing streaming media**	Use **WhatsUp Gold** and **WhatsUp Gold Flow Monitor** to go deep into your network traffic and understand not only the overall utilization of the LAN, WAN, specific device, or interface, but also which users, applications and protocols are consuming the bandwidth. In addition, you can use WhatsUp Gold Flow Monitor to baseline your network traffic in normal conditions, and quickly identify abnormal traffic which could indicate viruses, malware and other rogue activities directed at your network.
Meeting key compliance regulations such as FERPA, PCI-DSS, HIPAA, etc.	**Step 1:** *Automatically collect and store your log files for as long as you need to (e.g. some legislation mandates log data retention for 6 years) with* ***WhatsUp Log Management*** **Step 2:** *Configure* ***WhatsUp Log Management*** *to generate real-time alerts for key events (such as Access and permission changes to Files, Folders, and Objects containing financial, customer, patient information…)* **Step 3:** *Generate and automatically distribute the reports that you need to prove compliance with* ***WhatsUp Log Management*** In addition, **WhatsUp Gold** and **WhatsUp Gold Flow Monitor** can also help you secure your network and detect traffic abnormalities that may indicate viruses, malware and other rogue activities.
Simplifying troubleshooting efforts **Consolidating multiple monitoring tools**	**WhatsUp Gold** lets you discover map and manage network devices, servers and applications from the same interface. It's built on an integrated, extensible architecture, and functionality is controlled by licensing—easily activate the additional WhatsUp Gold plug-ins you need without reinstalling or installing anything new. **WhatsConnected**—for layer 2/3 discovery, mapping, inventory and asset reporting **WhatsVirtual**—manage and control your virtual resources from the same interface **Flow Monitor**—get deep visibility into your network traffic to locate bottlenecks, understand bandwidth usage—who, how and for what purpose—and identify bandwidth hogs **WhatsConfigured**—automate network device configuration tasks And with **WhatsUp Gold Alert Center** (included in WhatsUp Gold), you can track all problems happening anywhere in your infrastructure—hardware issues, network traffic, configuration problems, performance bottlenecks, etc.—from a single unified interface.
Managing a distributed network spanning across multiple buildings and locations	Use **WhatsUp Gold Distributed Edition** to monitor any number of remote sites from a centralized location with centralized reports, rotating views and drill-down capabilities to remote sites and problematic devices.
Automating device configuration tasks	Use **WhatsUp Gold** and **WhatsUp Gold WhatsConfigured** to automate network device configuration and change management processes, simplify your life, and eliminate human errors. With WhatsConfigured in place, you don't have to perform repetitive and tedious manual configuration tasks or troubleshoot misconfiguration issues in the dark. Plus, you can rest easy and save time with features such as nightly config backups, bulk config changes, complete audit trails, and real-time alerts triggered by configuration changes.

Download your 30-day free trial of WhatsUp Gold today at:
http://www.whatsupgold.com/products/download/network-software-download.aspx

Download your 30-day free trial of WhatsUp Log Management today at:
http://www.whatsupgold.com/log-management/

Ipswitch, Inc.
83 Hartwell Avenue
Lexington, MA 02421
Phone: (781) 676-5700
www.whatsupgold.com