# TOP TIPS FOR TIME STRETCHED ADMINS

ControlNow$^{TM}$ Whitepaper

CONTROLnow™

# Table of Contents

# Introduction

## This guide provides time-saving tips that IT admins at small and mid-sized companies can use to stay on top of their workloads, keep systems running and protected, and maintain a healthy work/life balance.

Administering IT in small and mid-sized companies can be a difficult task, as there is often a very small team responsible for ensuring the productivity of hundreds of workers.

In addition to solving urgent day-to-day issues, the IT team must balance delivery of work on strategic long-term projects, and provide advice to keep the business competitive. This juxtaposition often makes workload planning and scheduling difficult.

Changes in the IT landscape - including rising trends of BYOD (bring your own device), '-as-a-service' solutions, and hybrid environments - mean that 'the IT department' must be familiar with many more systems, devices, and environments than ever before, and know how to keep all of them running and secure.

It is perhaps not surprising then that more and more IT managers are reporting stress at work, an increase in overtime, and a decrease in work/life balance happiness; with rising numbers of IT admins considering leaving the profession[1].

This guide looks at some key areas where time can be saved and stress reduced.

[1] Survey Shows Rise in IT Administrators Wanting Career Change Due to Stress
http://www.gfi.com/Company/GFI-news-detail.aspx?id=136073

# Event-driven actions vs scheduled days

As an IT admin, you will be familiar with the following scenario. While working on a particularly complex problem, there is a knock at the door: "Hi! Do you have five minutes to...?" Nerf gun at the ready, you wait to hear if this end user has read the manual, the guide, the wiki, the Q&A site, Google, or any of the other resource available to them before coming to you.

This is a classic scenario, but there are other distractions that are less obvious, including:

- Getting caught up in day-to-day firefighting, when other colleagues are capable of handling the situation

- Becoming the 'friendly expert resource', with employees contacting you first before attempting basic resolutions or contacting the helpdesk

**Improving daily flow**

Maximizing scheduled work and minimizing interruptions is key. Disruptions are a time-waster.

- If you provide frontline support as part of a team, block chunks of time away from the helpdesk to allow you to concentrate on detailed work. For example, split the role before and after lunch, taking the first line position when you know you are less productive.

- Adopt the magic hat/earphones/flag-on-the-cubicle signal. Educate your colleagues and employees that a hat or earphones on your head, or a flag on display is a request not to be disturbed, allowing you to focus your undivided attention on a task. Just don't wear the hat all the time, because then it stops working!

- If you have a dual monitor setup, put all your comms and notifications on your second (smaller) screen, then blank it or turn it off. Your email monkey is not going to warn you of a fire, but it will distract you. (If you don't have dual monitors, investigate multiple desktops or virtual window managers for your OS.)

# Patching machines – The lose-lose task?

With so many new patches appearing weekly, and more operating systems and applications to support, keeping machines up to date has become a full time role, but if resources are strapped there is a risk that patches may not be applied quickly, leaving your organization open to known exploits.

Fortunately more and more operating systems and software vendors are adopting the best practice of auto-updating, downloading and applying patches in the background, and prompting a restart only if required.

For those patches that remain there are a couple of things you can do to reduce your patching workflow (until such times as the powers that be sign-off to employ a full time 'patcher').

**Automate and centralize:**

Patching is repetitive, and therefore automation provides an obvious win. Your organization may already have a library of standard procedures and shell, Perl or Python scripts that optimize most of this process.

However, while detecting and assessing the need for patches are relatively easy tasks to automate (frequent simple tasks), acquiring patches from different providers, prioritizing the patches and deploying them can be more tricky (frequent difficult tasks). Additionally, maintaining an auditable trail showing that patches are up to date requires more than simple scripting.

If you have a number of machines to patch, need to manage machines across locations, or are forced to deploy patches outside of working hours, a patch management tool will significantly reduce the time spent patching. ROI on automated patching is particularly high when extensive weekend working or overtime hours would normally be required.

Automated patch management tools greatly simplify patching by:

- Automatically deploying patches, hands-off and out of hours
- Sourcing and applying patches from multiple vendors, especially non-OS patches
- Providing one central point of control (e.g., through a single web-based dashboard) showing status and exceptions
- Testing patches in your QA environment first, and then allowing you to push them into production
- Automatically deploying pre-approved patches (as managed by group policies) as soon as vendors release them, thereby minimizing the vulnerability window
- Handling edge cases and patches from small vendors better, because of the economies of scale obtained from operating across many organizations

# Antivirus protection

Today, with APTs (advance persistent threats) affecting even small organizations, it is essential to ensure that virus scanning is well implemented and maintained. Several well-published incidents (e.g. Conficker, Daprosy) have highlighted the cost of removing a large infection, and reinforced the value of a strong preventative strategy.

Today's best practice requires that:

- Virus scanning occurs on all machines (including servers)
- Scanners automatically update, silently, without user confirmation or intervention
- IT have total visibility that scanning has not been disabled and that definitions are being kept up to date

**Optimizing AV to minimize time spent**

Selecting and implementing a strong virus scanning strategy will pay off in the long run by significantly reducing IT time spent dealing with and recovering from infections.

- Identify a virus scanner that operates and updates silently, and runs in a lightweight manner on users' machines. Virus scanners that are noticed by users may be disabled ("only temporarily"), reducing protection.
- Use one vendor's product consistently across your estate. If employees bring their own devices, encourage them to use your chosen AV provider. Using a single vendor avoids conflicts between tools, and ensures that there are no gaps in coverage. When selecting a vendor, it is worth checking that they provide migration tools to safely remove existing products, as this can be a significant hidden cost.
- Use business-grade AV coordination tools that include centralized reporting on coverage. A centralized monitoring dashboard should provide quick identification of problem machines, and provide real-time alerting and reporting of threats. However, when we're talking specifically about email security or web protection, it is also highly recommended that you choose a product that features multiple AV engines. These are designed in such a way that they work together and complement each other within the same product. Multiple AV engines for email security and web protection reduce the risk of infection considerably and boosts your email /web protection capabilities.
- Chose a solution that provides best protection against zero-day exploits. Some vendors may only provide weekly definition updates, or supply clients with default settings that infrequently check for updates. Where possible use a solution that pushes updates to clients in real-time as they are released.
- Select a solution with minimal additional infrastructure. Virus definitions should be provided from a cloud service or CDN, minimizing internal overhead, and protecting mobile machines without requiring a VPN connection as a prerequisite to receiving updates.

# Fixing problems and machine upgrades

Over time, components age, hard drives fill up, and cooling becomes less efficient, but manually identifying machines that require attention is a time sink, and user-submitted reports or upgrade requests can have a poor signal-to-noise ratio.

With manual monitoring, machines can arrive at IT unexpectedly, requiring immediate fixes. In these instances, not only is user time lost, but IT staff must respond urgently, disrupting planned work. These situations are almost always complicated by the poor logging of some mainstream OSs and the additional heartache of an unexpected failure meeting 'typical user backup discipline'.

An automated monitoring and logging tool that reports on machine health and provides up-to-date system specs, will often allow faults to be diagnosed preemptively, and has the additional advantage of allowing targeted upgrades, maximizing the effectiveness of capex budgets.

**Get ahead of the game**

An online asset register, combined with centralized machine health reporting, can provide powerful intelligence on the state and health of an IT estate, reducing unnecessary work.

Use one central register, capable of logging both physical and software assets. Some registers will raise alerts when assets are due for attention, allowing efficient scheduling of upgrade work.
Implement automated monitoring of machine health, with remote reporting. This can be used to flag possible upcoming failures, allowing for a proactive resolution, reducing break/fix time for the users and reducing the burden on helpdesk staff.

# Mobile workforce

With more and more people working from home and on the road, protecting remote machines has never been so important.

The machines of mobile workers are often more susceptible to infection and attack because they are used in multiple, shared environments; and mobile workers' roles often requires them to transfer files onto USB drives.

Should a mobile machine become infected, it is important to be able to diagnose and, ideally, resolve the problem remotely (without connecting to your main network). This eliminates the need for the machine (and its user) to return to base, and decreases the risk of infecting the rest of your estate.

**Better than remote desktop**

Using a remote desktop session is a partial solution to managing mobile machines, but this still requires support time, offsets working hours for the user and is best done on a good Internet connection, which may not always be available.

Consider adopting an automated solution that can:

- Report on the health and status of remote machines, filing the report when an Internet connection is available, and automatically filtering reports to discern important action items
- Report that patches, upgrades and malware definitions are up-to-date
- Provide these services without requiring full access to your network. This ensures that mobile machines are protected, yet they are kept at arms' length from other assets

# Onboarding new employees

Onboarding is Sysadmin 101. As the majority of actions are identical for all new users, a checklist-driven procedure ensures that they are all completed.

You may already have scripted a solution that sets up services for new users (VoIP, email, domain accounts) and have an image-based wipe-and-fresh-install procedure for setting up machines.

However, this process can be optimized to minimize time spent customizing the installation, and to reduce follow-up support requests.

# Policies and nudges

Extend your machine configuration to use group-based policies, automatically configuring the machine for each use case (e.g. working from home or forming part of the marketing team), including installing software and setting up security tools.

Create a unique 'Welcome!' page for each user which includes key information, and nudges them into correct use of your support process. Add this to machines as part of setup (bookmark, and if possible set as the first run homepage) and create a printed copy to hand to them on their first day.

It is good practice to include:

- The employee's username, phone number and office address
- An overview list of useful services and servers they will use
- Instructions on how to keep their password safe and use encryption software
- Information on how to access the support ticketing system

# Avoiding suspected data breaches

A data breach can be a huge headache for everyone in an organization, and because loss of customer data results in loss of customer trust, even a suspected breach will require significant internal investigation.

With 63% of small businesses being attacked by an unauthorized outsider in the last year, with a two-fold difference between best and worst small company breaches,[2] robust protection will reduce the impact of a breach on your organization.

**Preparation saves time**

Preparation is the best defense against data breaches:

- Draft a data breach response plan before you need it. This activity should include all the people required to handle a data breach.
- Address security vulnerabilities using a multi-layered approach. For example, good virus scanning is insufficient if your network is insecure; similarly, removing a virus is ineffective if the website which was the original source of infection is still accessible.
- Adopt a single solution that can target several areas of vulnerability at once. This will often prove more effective than a suite of tools, as users only require to be familiar with a single tool, and better coverage can be achieved.
- Businesses with remote workers or with offices in multiple locations, should ensure that security problems are fixed simultaneously across their entire IT estate to avoid weak points and reinfection vectors. Cloud-hosted security tools, which can monitor multiple sites and remote assets from a single interface are advantageous for ensuring consistent management.

[2] UK Department for Business, Innovation and Skills – 2013 Information Security Breaches Summary: http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf

# Work, life and learning

While IT admins may love solving problems and helping users, the role has its ups and downs. Most ex-IT admins stated in a survey that their reasons for leaving were: not challenging enough work, dissatisfaction with repetitive tasks and extra hours, keeping them away from home[3].

This guide has identified areas where automation and best practice can get you out of the office earlier, giving you more time to unwind at home, and more opportunities for learning and personal projects.

[3] http://www.slideshare.net/SolarWinds/netadmin-and-sysadmin-survey-results-aus

USA, Canada, Central and South America
4309 Emperor Blvd, Suite 400, Durham, NC 27703. USA

Europe and United Kingdom
Vision Building, Greenmarket, Dundee, DD1 4QB, UK

Australia and New Zealand
2/148 Greenhill Road, Parkside, SA 5063

www.controlnow.com/contact

Disclaimer

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. LogicNow is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, LogicNow makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. LogicNow makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

CONTROLnow™