ManageEngine
OpManager MSP

5 best practices to manage your clients' network configurations better!

www.manageengine.com/network-monitoring-msp

Table of content

INTRODUCTION

Why is network configuration management a staple rather than a luxury?

Let us spell it out,

- Networks and technology are evolving every day. As a result, the difficulty of managing networks granularly and keeping them away from hazards is making the lives of network admins and business owners harder.
- Monitoring and managing requires a lot of effort, but managing multiple client networks from a central location is more difficult.
- New devices are added to networks often, and configuration changes are made countless times each day. A minor configuration error can easily make the device non-compliant to the latest industry policies. This could lead to security intrusion, customer attrition, and negatively impact your organization's reputation.

Taking into account these points, it is wise for managed service providers (MSPs) to consider network configuration management imperative for their organization and their clients.

The hassle in manual configuration management

Manual, multiclient network configuration management is often challenging because the client networks vary in sizes, and the client requirements are unique. Evolving technologies and the advent of digital transformation add fuel to the fire. The hassle doesn't just stop there. As security loopholes are increasing daily, organizations need to adapt to new internal polices which involve approvals and reviews from higher authorities. This is difficult to accomplish with just manual management tactics.
Let's discuss these crucial aspects in detail.

- Human error
- Losing track of configuration changes
- Delay in troubleshooting issues
- Non-compliance
- Security breach
- Lack of unified visibility

Human error: Researchers at Avaya have found that 81% of the network downtime is due to human errors while making configuration changes to the network devices. Network maintenance slips and lapses are common among all groups of people, regardless of experience and skill. Thus, it's important to consider managing your clients' network configuration changes and compliance holistically. A systematic approach helps eliminate human errors and, even if there are any, it will be easier for the MSPs to spot and rectify them before they snowballs into network downtime.

Losing track of configuration changes: At the end of the day, the service provider's job is to fence up clients' networks from pitfalls. To achieve that goal, it is critical to keep an eye on configuration changes. Unauthorized or unapproved configuration changes can cause misconfigurations, leading to network disruption or causing security breaches that bring massive damage to the organization. The challenge with configuration change management is that it can get out of a network admins' hands easily and especially if it is managed manually because a lot of configuration changes are made to devices daily.

Delay in troubleshooting errors: We all know if an error occurs due to a faulty configuration change, it is essential to fix it as soon as possible to keep the service or site up and running. If not, a minor error can grow into a bigger issue and interrupt your business operations. In short, the longer it takes to fix an error, the longer the list of consequences you are going to face. It is vital to take holistic, longer routes to fix an error rather than considering quick fixes out of a desperate need to keep the multiclient networks error-free.

Non-compliance:

Did you know?

Research conducted by Ponemon Institute notes that the aftereffects of non-compliance can exceed the costs spent to achieve compliance. An impacted organization usually spends $3.5 million on an average to attain compliance, but non-compliance problems cost it around **$9.44 million in the United States and $4.35 million globally, on average.** This can include overall mitigation expenses, lost revenue, and negative impacts on the organization's reputation.

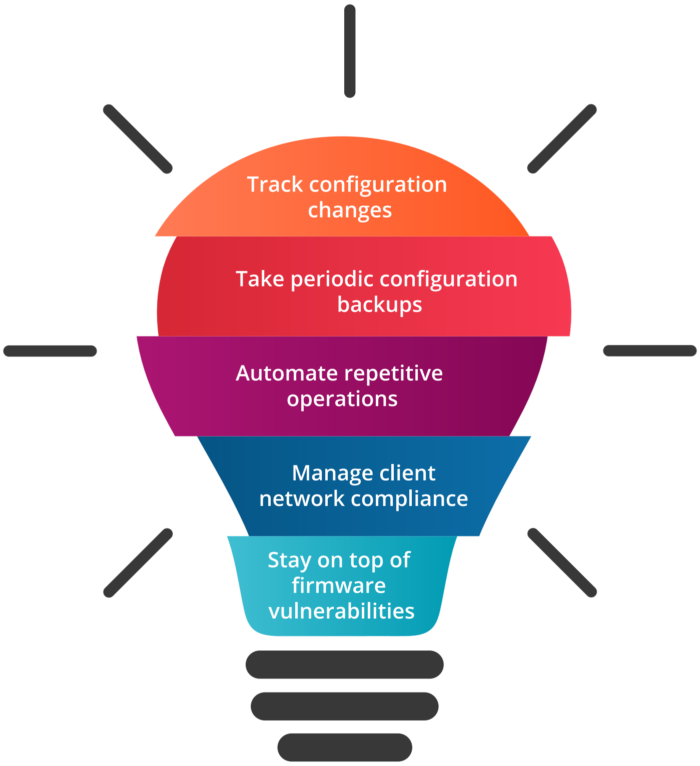
The cost of non-compliance is higher and it doesn't just stop there. Non-compliance could lead to security breaches, customer churn, and more. Your clients' network can seem to be compliant today but the evolution of existing policies, the advent of new standards, new or several operators working on the same device and overwriting each other's changes, can result in your client's network becoming non-compliant in no time. To take non-compliance out of the equation, you should run a compliance check periodically and evaluate the details by generating granular reports.

Security breach: Eclypsium reported a 43% increase in the discovery of firmware vulnerabilities in 2019, and a surge of 750% since 2016. It is important to closely watch for firmware vulnerabilities in your clients' networks round the clock. Vulnerabilities can catch network admins off guard, and put your client's network in danger if they are managed manually and inadequately.

Lack of unified visibility: Unified control over multiclient networks plays a pivotal role in the MSP's game plan of seamless management. Network admins can easily lose track or forget to fix a critical issue when juggling multiple client networks. With unified visibility, network admins can easily avoid network pitfalls and prevent any potential downtime.

5 ways to accomplish error-free configuration management

Managed service providers often face roadblocks that can mislead them from attaining efficient network configuration and compliance management. Here's a to-do list that every MSP should follow.


Track configuration changes
Take periodic configuration backups
Automate repetitive operations
Manage client network compliance
Stay on top of firmware vulnerabilities

- Track client network configuration changes granularly
- Take periodic configuration backups to fortify client networks
- Automate repetitive operations
- Manage your clients' network compliance methodically
- Stay on top of firmware vulnerabilities

1.Track client network configuration changes granularly

Scenario:
A new network admin made a few configuration changes to a client's network devices weeks ago and forgot to sync them to the startup configuration. Later, another admin from the team rebooted the device after updating the hardware. This resulted in a significant loss of data and network downtime until the IT team figured out and resolved the issue.

💡 How can you avoid this problem?

First, it is critical to oversee the who, what, and when of configuration changes in real time. This enables faulty configuration changes to be reverted easily and promptly. Further, network admins can also effortlessly filter unauthorized configuration changes. Second, MSPs should provide access only to essential resources, and not to all the data of all client networks. This improves the security of the multiclient networks.

2. Take periodic configuration backups to fortify client networks

Scenario:
In a 10,000-device network, one device went down due to an issue with a new configuration change, and it caused neighboring devices to fail too. Network admins couldn't fix the issue because they couldn't get to the device's faulty configuration change.

💡 How can you avoid this problem?

MSPs should consider taking backups whenever any configuration change is made to client network devices. This helps compare and spot the origin of an issue and enables admins to easily revert to the baseline configuration set up, and prevent the whole network from going down. Admins can also schedule configuration backups so the process doesn't interfere with standard business operations.

3. Automate repetitive operations

Scenario:
A client wanted to make configuration changes across 500 devices. The organization wasn't equipped to automate the process, so the configuration changes were required to be implemented manually and individually. This consumed a lot of time and resources, and introduced a greater possibility of human error.

💡 How can you avoid this problem?

It's important to eliminate manual tasks when possible. Automation accelerates the process of rectifying network configuration changes while it reduces errors. It enables network admins to implement repetitive configuration changes to numerous devices at once. Updating credentials automatically helps maintain the security of the network.

4. Manage your clients' network compliance comprehensively

Scenario:
An MSP and his admin team failed to notice that a device from one of their clients' network is non-compliant. Regrettably, a hefty fine was imposed on the organization for non-compliance during an audit.

💡 How can you avoid this problem?

Service providers should ensure that the network devices adhere to the latest industry standards, including HIPAA, SOX, CISCO IOS, and PCI. They should be able to create their own custom policies if needed based on clients' requirements, and ensure they abide by those rules as well. Network admins should continually analyze and remediate any violation without delay, and take measures to prevent violations in the future.

5. Stay on top of firmware vulnerabilities

Scenario:

A service provider was under increasing stress as he tried to fix one firmware vulnerability after another, but they kept piling up in one of his client networks. Applying the appropriate patch was time-consuming and each day the unfixed patches placed the network in a vulnerable state.

💡 How can you avoid this problem?

Network admins should stay vigilant and be well-equipped to swiftly deploy the relevant patch for a firmware vulnerability.

What can you gain from OpManager MSP's NCM add-on?

- OpManager MSP's NCM add-on at the service helps managed service providers handle their multiclient networks efficiently. Utilizing its comprehensive client network monitoring capabilities, network admins can track every configuration change made in client networks.

- With OpManager MSP's new NCM add-on, network admins can take backups periodically as well as configure the tool to take a backup every time a change is made to a device. This helps admins avoid disaster whenever there is a network mishap or a downfall due to a faulty configuration change.

- To enhance productivity and efficiency in your organization, network admins can take advantage of this new add-on and automate rudimentary network configuration tasks, like making configuration changes in bulk. This helps MSPs reduce the workload of the organization's internal IT technicians.

- Service providers can holistically fortify their client networks from failures due to incorrect configuration changes. They can monitor firmware vulnerabilities and remediate them with the provided details on patches. MSPs can also easily keep up with the latest compliance rules.

- OpManager MSP's NCM add-on provides centralized and granular visibility across all the client networks. This helps network admins oversee and track configuration changes without needing to switch between networks.

Added benefits of using OpManager MSP

- **Meticulous monitoring:** Monitor the multiclient network devices granularly 24/7, to determine the root cause of all the network issues instantly with OpManager MSP's seamless monitoring feature, and fix issues proactively.

- **Adaptive thresholds:** This reliability feature help MSPs save time and effort, and achieve optimal performance. It eliminates the need for the admins to understand a device's performance trends. It continuously adjusts the thresholds based on its dynamic performance.

- **Automation with workflows:** Automate basic L1 and L2 troubleshooting operations, and mundane maintenance tasks. Workflows help your technicians avoid spending time on less important tasks, and let them focus on those requiring human attention.

- **Powerful ITSM integration:** OpManager MSP integrates with ServiceDesk Plus MSP to enable service providers to resolve a minor issue or a sudden network disruption faster and comprehensively.
- **Extensive reports:** Halt network issues by proactively detecting them using OpManager MSP's reports. This feature-rich resource also enables technicians to customize reports based on the client's requirements.

Give OpManager MSP a try today!

Get Price Quote

Request Demo

Download Free Trial