

DeviceAuthority™ Suite

Solution Overview: Effective Change Management

Summary

With over 60% of network downtime caused by device configuration errors, it is imperative for IT organizations to effectively manage the changes occurring to network devices.

DeviceAuthority Suite, the leading Network Change and Configuration Management (NCCM) solution, is specifically designed to ensure configuration errors do not occur in the first place. DeviceAuthority Suite provides the ability to keep network device changes in-line with company, security and regulatory policies, preventing configuration errors and providing real-time change and configuration reporting. If configuration issues do occur, DeviceAuthority Suite detects them in real-time, allowing immediate remediation of the issue and preventing an impact to business service.

Managing Change with DeviceAuthority Suite:

- Understand what, when and why change occurred
- Safely initiate change to one or thousands of network devices
- Real-time reporting and auditing of network change and configuration issues
- Leverage embedded intelligence to eliminate the risk of human error
- Validate device configurations are up-to-date and in line with compliance and policy
- Allow remediation of errant changes to be fixed immediately, reducing or preventing impact to the business
- Implement, control and measure network infrastructure change in-line with ITIL best practices

Effective Change Management

Every company must define and implement a change management approach that is appropriate for its unique business needs, technical environment and culture. Regardless of the make up of that environment, DeviceAuthority Suite provides the fundamental capabilities to effectively simplify, automate and control the change management process. Every network change management program has one thing in common—a heavy reliance upon data related to device configuration. Generating and managing the flow of this data is a considerable challenge. However, with DeviceAuthority Suite, this is easily achievable.

DeviceAuthority Suite ensures that when changes are made, they are accomplished quickly and safely, with security maintained, compliance adhered to and configuration issues immediately dealt with. Through automation and applied intelligence, DeviceAuthority Suite eliminates the risk of human error from the change management process. If an unexpected outage due to network device configuration occurs, DeviceAuthority Suite gets the business back on-line rapidly by either rolling back an erroneous change to the last steady state or by quickly and securely implementing a fix to the issue. Unlike passive network monitoring products, when DeviceAuthority Suite detects an issue, it fixes it—permanently. This change management capability can be leveraged across a single device or thousands.

Change Management Improving overall Service Availability:

Is your IT support organization aware of the changes being made to the network infrastructure?

When a network fault occurs, the first question most administrators ask is “What changed?” Using DeviceAuthority Suite, changes to network device configurations can be immediately identified and, in one click, the administrator can:

- View the changes between the current and previous version of the configuration
- Initiate an immediate fix or roll back to a previous known-good configuration or initiate a fix to address the difference

Rolling back a change to the last steady state allows troubleshooting to occur later, minimizing network downtime and increasing service availability.

Managing change across thousands of devices can prove to be a challenge and pose significant risks to IT organizations. To reduce the risk associated with rolling out mass changes, organizations traditionally follow these steps: 1.) A small amount of network devices are identified. 2.) The change is made. 3.) After a suitable waiting period (to see if the change created issues), the next subset of devices are identified and the change is made to them. This cycle continues until the change is made to all known network devices needing the change. This method of change management is a long, high-risk, resource-intensive, high-cost endeavor, which also assumes that the IT support team understands the configuration state of all network devices and if they are ready or safe to change.

DeviceAuthority Suite removes this risk associated with implementing mass change to network devices. This includes changes spanning different types of network devices or different revisions of operating system. DeviceAuthority Suite provides a complete end-to-end change implementation process which includes: real-time identification of configuration status of network devices through automated reports (change readiness), confirmation of change syntax, automatic validation of network devices for change readiness, verification that a change was implemented successfully, and comprehensive audit reporting on the changes.

DeviceAuthority Suite is the only NCCM solution that provides support for all network devices. Partial device support will only provide partial change control. DeviceAuthority Suite provides out-of-the-box support for over 25 hardware vendors, 1000 models and 10 technologies—routers, LAN switches, firewalls, WAN switches, remote access gateways, VOIP gateways, WAPs, VPN appliances, load balancers, and uninterrupted power supplies.

DeviceAuthority Suite is also the only NCCM solution that provides end-to-end change management capabilities that fully adheres to ITIL (IT Infrastructure Library) best practices. IT managers are able to plan, implement, verify, validate, remediate and audit changes efficiently, allowing organizations to streamline day-to-day operations and optimize overall service.

IP Address	Hostname	Class	Model	OS	Config Type	Changed Date	Config Type	Changed By	Changes
10.10.1.1	101R1	Router	Cisco	2611	2004-08-08	15:47:00.0	Startup Config	rhphip	3 version 02.2 12 use authorization exec default local 13 username htdm privilege 15 password ? 14 username htdm privilege 15 password ? 15 username htdm privilege 15 password ? 16 username htdm privilege 15 password ? 17 no ip dhcp bootstrap 18 no ip dhcp bootstrap 19 no ip dhcp bootstrap 20 no ip dhcp bootstrap 21 no ip dhcp bootstrap 22 transport http none
10.10.1.2	101R2	Router	Cisco	2611	2004-08-08	15:47:00.0	Running Config	rhphip	16 username htdm privilege 15 password ? 17 username htdm privilege 15 password ? 18 username htdm privilege 15 password ? 19 username htdm privilege 15 password ? 20 username htdm privilege 15 password ? 21 no ip dhcp bootstrap 22 transport http none
10.10.2.1	102S1	Switch	Cisco	3602	2004-08-04	17:05:03.0	Running Config	Albin	31 Let configuration change at 05:53:19 UTC Tue Aug 3 2004 by htdm 41000000 config last updated at 05:53:21 UTC Tue Aug 3 2004 by htdm
10.10.2.2	102S2	Switch	Cisco	3602	2004-08-04	17:16:20.0	Running Config	inf	14 access list 100 deny tcp host 1.1.1.1 any 15 access list 100 deny tcp host 1.1.1.2 any 16 access list 100 deny tcp host 1.1.1.3 any 17 access list 100 deny tcp host 1.1.1.4 any 18 access list 100 deny tcp host 1.1.1.5 any 19 access list 100 deny tcp host 1.1.1.6 any 20 access list 100 deny tcp host 1.1.1.7 any 21 access list 100 deny tcp host 1.1.1.8 any
10.10.2.3	102S3	Switch	Cisco	3602	2004-08-04	17:31:03.0	Startup Config	inf	31 Let configuration change at 05:53:19 UTC Tue Aug 3 2004 by htdm 41000000 config last updated at 05:53:21 UTC Tue Aug 3 2004 by htdm
10.10.2.4	102S4	Switch	Cisco	3602	2004-08-04	17:41:03.0	Startup Config	Albin	14 access list 100 deny tcp host 1.1.1.1 any 15 access list 100 deny tcp host 1.1.1.2 any 16 access list 100 deny tcp host 1.1.1.3 any 17 access list 100 deny tcp host 1.1.1.4 any 18 access list 100 deny tcp host 1.1.1.5 any 19 access list 100 deny tcp host 1.1.1.6 any 20 access list 100 deny tcp host 1.1.1.7 any 21 access list 100 deny tcp host 1.1.1.8 any
10.10.2.5	102S5	Switch	Cisco	3602	2004-08-04	17:41:03.0	Running Config	Albin	14 access list 100 deny tcp host 1.1.1.1 any 15 access list 100 deny tcp host 1.1.1.2 any 16 access list 100 deny tcp host 1.1.1.3 any 17 access list 100 deny tcp host 1.1.1.4 any 18 access list 100 deny tcp host 1.1.1.5 any 19 access list 100 deny tcp host 1.1.1.6 any 20 access list 100 deny tcp host 1.1.1.7 any 21 access list 100 deny tcp host 1.1.1.8 any
10.10.2.6	102S6	Switch	Cisco	3602	2004-08-07	19:59:53.0	Startup Config	Albin	14 access list 100 deny tcp host 1.1.1.1 any 15 access list 100 deny tcp host 1.1.1.2 any 16 access list 100 deny tcp host 1.1.1.3 any 17 access list 100 deny tcp host 1.1.1.4 any 18 access list 100 deny tcp host 1.1.1.5 any 19 access list 100 deny tcp host 1.1.1.6 any 20 access list 100 deny tcp host 1.1.1.7 any 21 access list 100 deny tcp host 1.1.1.8 any

Figure 1: A compliance report generated from DeviceAuthority Suite tracks and reports on all configuration changes occurring across the network. This report defines who, what, when and why something changed in a configuration.

Effective Change Management using DeviceAuthority Suite

Plan Change

- Automated discovery and full support for ALL network infrastructure devices
- Real-time audit reporting to identify what you have and its current state

Implement Change Securely and Efficiently

- AutoScripting and decision support ensures change is rapid, safe and secure for both simple and complex changes
- Centralized software library and automated change capabilities for Software Image and Patch Management
- Vendor-neutral change wizard simplifies and automates complex or routine changes (passwords, SNMP community string, etc)
- Best practice change templates ensure that device changes are made in a consistent, precise and efficient manner across multiple devices

Change Verification and Validation

- Detailed, real-time feedback of the success or failure of a change
- Pre-change (validation) or post-change (verification) checkpoints quickly pinpoint any necessary preventive or remedial actions

Configuration Remediation

- Rapid, real-time, detection of unauthorized or errant network device changes
- One-click restoration (roll-back) to an established good configuration or initiate a fix to address the difference

Audit and Reporting

- Comprehensive, customizable, real-time reporting and auditing on backups, restores and changes for the entire network
- Real-time auditing and reporting of network device compliance state for HIPAA, Sarbanes-Oxley, FIPS and other standards and regulations
- Identify what you have and its current state in real time
- Establish all devices are in a working steady/compliant state
- Predefined Change Management reports document all changes occurring within defined parameters
- Diff Reports quickly compare multiple configurations and identify what changed
- Real-time notification of all changes occurring in the network

Adherence to Standards and Best Practices

- DeviceAuthority Suite fully supports ITIL for Configuration and Change Management. DeviceAuthority Suite provides the network management foundation supporting ITIL's best practices and is the natural, proven, choice to manage the growing network complexity currently experienced in today's IT Enterprise.

Establish Network Resilience

- Define, monitor and enforce security, compliance and policy
- Ensure network resilience with secure role-based user access (e.g. by need and responsibility)

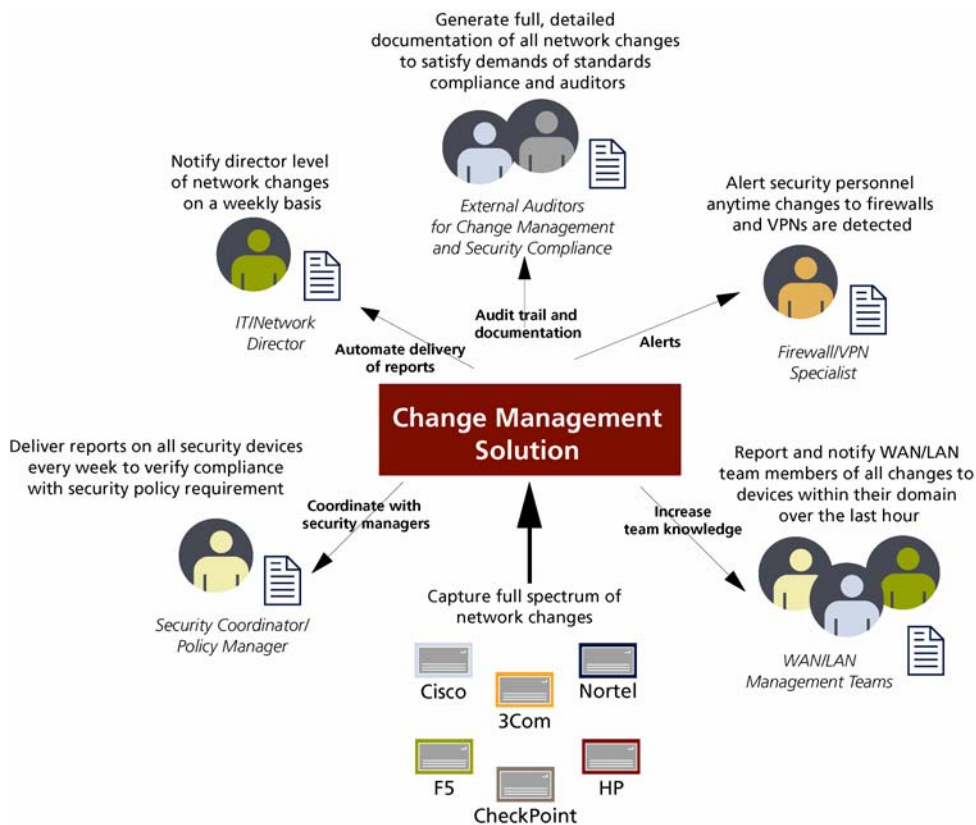


Figure 2: NCCM Benefiting the Organization

For more information, or to request a product evaluation, please contact us at sales@alterpoint.com.