



Network Outage Prevention, Compliance Automation & Change Management

Restorepoint provides protection, compliance and remote management for multi-vendor network infrastructures. Deployed as a physical or virtual appliance, Restorepoint centralises configuration backup, provides rapid 1-click recovery, automates compliance management, asset and remote management for devices from over 100 network, security and storage vendors.

Overview

Network Disaster Recovery

With increasing dependency on network and cloud services, even small network outages leave organisations vulnerable to loss of service, revenue, productivity and reputation.

Unlike server infrastructure, where many solutions exist for disaster recovery, network devices are often overlooked due to the complexity of managing a backup process for the many different network vendor devices in use.

The ability to recover quickly from a network outage caused by a hardware failure or misconfiguration depends on the skills of network administrators and whether they have a copy of the most recent configuration of the affected network device. However, current backups are often not available due to the complexity and time it takes to perform the backup process.

Restorepoint automates configuration backup, saving the average customer 4-8 hours per week. With out-of-the-box support for more than 100 network, security and storage vendors, it can be deployed and protecting your network in minutes. With an automated 1-Click recovery process, customers can reduce outage costs and restore network availability in seconds not hours.

Compliance

Many organisations are required to meet either internal, best practice or external standards such as PCI, GDPR, ITIL, ISO27001, FCAPS, NIST, SOX, or HIPPA. For those organisations, Network Configuration Change Management (NCCM), Configuration Auditing, and Asset Management processes are requirements, but consume valuable administration time.

Restorepoint's compliance engine provides continual visibility of compliance status by automatically detecting changes in configuration, tracking against configuration policies and baselines.

Policies are easily created and applied to multiple network devices, with compliance analysis performed automatically each time a network device is backed-up. Email, SNMP and Syslog Alerts can be sent, and automated remediation can also be set to identify or resolve violations.

With a built-in Asset Management database, customers can also ensure they have a current asset list with complete inventory information rather than maintaining separate spreadsheets.

Remote Management

Managing even single vendor networks can be time-consuming and overly complicated, even to make the most simple changes. Restorepoint reduces network management costs by simplifying the steps and time required to implement bulk changes or to roll-out new devices.

You can save time by sending commands, scripts, or by push configuration templates to multiple devices rather than making the change manually on each device. Changes can also be scheduled in Restorepoint to be run at a later date or on a repeating schedule.

Repetitive changes including password changes or updates to routing tables can now be performed in seconds instead of hours, and in the knowledge that using Restorepoint you can quickly roll-back to a previous configuration if the change does not go to plan.

Using the Click-to-Terminal feature, administrators can connect to devices over SSH, SCP or Telnet using just a web browser. This simplifies access and increases security as sessions are also recorded.

Key Benefits

- Increase security and protect your organisation from costly network outages. Centrally automate configuration backup for network, security & storage devices from over 100 vendors
- Recover from network device failure or configuration errors in seconds using just a click of a mouse
- Protects the valuable data within network configurations such as IP address info, policies & passwords using AES encryption.
- Analyse configurations for compliance failures each time a backup is taken, helping shorten audit time
- Detect configuration changes and baseline violations
- Simultaneously control multiple devices with ease; push or schedule bulk CLI commands to change passwords, SNMP communities, add routes or users etc.
- Quickly deploy new devices or standardise configurations of existing devices using Configuration Templates
- Connect to devices using a Web-based Terminal, recording all activities

- Integrate with other applications through the JSON based API
- Track and report on live network assets instead of manually updating spreadsheets. Restorepoint collects serial numbers, model numbers, location and firmware information for simplified Asset Management
- Scheduled reports including: backup history, configuration changes, baseline, compliance, device passwords, asset inventory including firmware and serial numbers

Enterprise Features:

- Remote Agents simplify multi-site or MSP deployments. Centrally manage agent tasks and store configurations
- Multi-user and multi-tenant management allows enterprises and service providers to segregate and delegate administration of network assets
- Define granular user permissions to control user access to network configuration data and Restorepoint functionality

Trusted by organisations including:



APPLIANCES	RSP 530	RSP 1020	RSP 2020	RSP-VIRTUAL
Specifications	1U Hardware Appliance	1U Hardware Appliance	1U Hardware Appliance	VMware ESX or Hyper-V
	2 x 500GB HD, RAID-1, Single 250W PSU	2 x 500GB HD, RAID-1, Single 250W PSU	4 x 1TB HD (hot swap), HW RAID-5 controller, Dual 350W PSU	At least 4GB RAM & 256GB storage required
Capacity guidelines	approx. 500 Devices*	approx. 1000 Devices*	approx. 10,000 Devices*	approx. 1000 Devices*
Physical/Environmental				
Average Power Consumption	250W	250W	Dual 350W PSU	
Dimensions (W x H x D)	437 x 43 x 249 mm	426 x 43 x 356 mm	437 x 43 x 503 mm	
Weight	4.5 Kg	6.4 Kg	18.1 Kg	
Rack space	1U	1U	1U	
Access	Front & Rear	Front & Rear	Front & Rear	
Operating Temperature	10 to 35°C	10 to 35°C	10 to 35°C	
Operating Relative Humidity	8% to 90% (non-condensing)	8% to 90% (non-condensing)	8% to 90% (non-condensing)	
Compliance	RoHS, CE, UL, WEEE			
* Capacity guidelines: actual capacity depends on types and number of configurations stored which may vary by customers own retention policy. Virtual Appliance capacity also depends on virtual hardware				