

Automate Compliance with BackBox

Automatic configuration audit and drift remediation keep your devices aligned with your compliance regime.

Overview

Compliance is a big topic that means different things to different people. For some, it means being compliant with regulatory regimes or industry standards – like CIS Benchmarks, PCI-DSS, NIST, HIPAA, or DISA STIGs. For others, it means simply staying compliant with a golden config that represents your organization’s best practices.

The challenges of compliance projects are three-fold:

- 1. How to start?** It can be overwhelming for network administrators with a population of hundreds of network and security devices, across vendors, to comb through configurations just to check and see if they meet your standards.
- 2. How to keep compliant over time?** When configuration changes are made in complex networks, sometimes the result is falling out of compliance. Many companies do a bi-annual audit to check for configuration drift because it’s simply too time consuming to manually check compliance on a regular basis across the device population. However, six months is a long time to be out of compliance.
- 3. How to groom configurations into compliance when non-compliance is discovered?** Eventually, when you do discover non-compliance, grooming the configuration back into compliance requires multiple manual steps, an engineer’s expertise, and hours of time.

Compliance is an ongoing process, which makes it a suitable start for an automation project. Manual tracking of compliance adds too much overhead to teams already unable to keep up with demands and exposes organizations to risk.

92%

of network teams say more network updates are needed than they can keep up with

THE AUTOMATION ADVANTAGE

- Teams can accelerate compliance by creating automation templates that define their compliance requirements. For compliance standards like HIPAA, STIGs, PCI-DSS, CIS Benchmarks, and others, BackBox has many automations prebuilt in the Automation Library ready to be used.
- Teams can maintain compliance and avoid configuration drift with automated checks against the compliance requirements. Non-compliant devices can be automatically remediated, or trouble-tickets can be opened in an ITSM like ServiceNow for manual investigation and remediation.
- Compliance audits are performed regularly, often nightly without burdening your teams, and compliance reporting can be shared as needed with other parts of the organization.

Automate the Complete Compliance Lifecycle with BackBox

Configuration compliance is not something that can be managed with most device vendor software. So, organizations often rely on a manual process for device onboarding combined with infrequent audits of the configurations to ensure that compliance is maintained over time.

Unfortunately, we know that this doesn't work. Configuration drift is a given; in any complex network configurations are likely to drift due to changes to software that are made ad hoc and are not recorded or tracked in a comprehensive and systematic fashion.

Manual tracking of configuration changes is error-prone. And, irregular compliance checks are inefficient. As such, the way compliance is done today is fundamentally broken and outdated, considering the opportunity provided by automation.

Let's take a look at how the end-to-end compliance process can be improved with automation.

Get Started

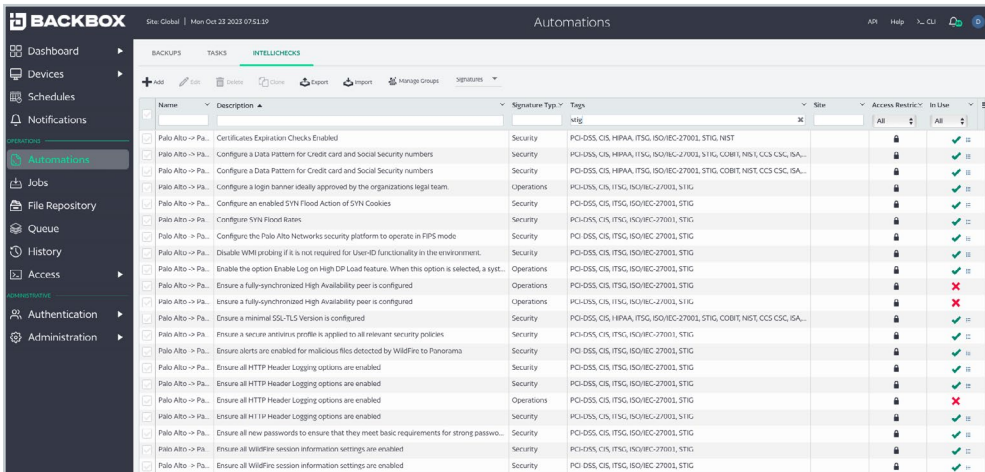
There are two questions that kick-off every compliance project:

1. What rules do we want each device to comply with?
2. What is the current state of devices and their configurations?

INTELLICHECKS

Deciding the compliance rules is an organization's responsibility. Once these rules are decided, in BackBox parlance, IntelliCheck automations are then created that check and enforce these rules.

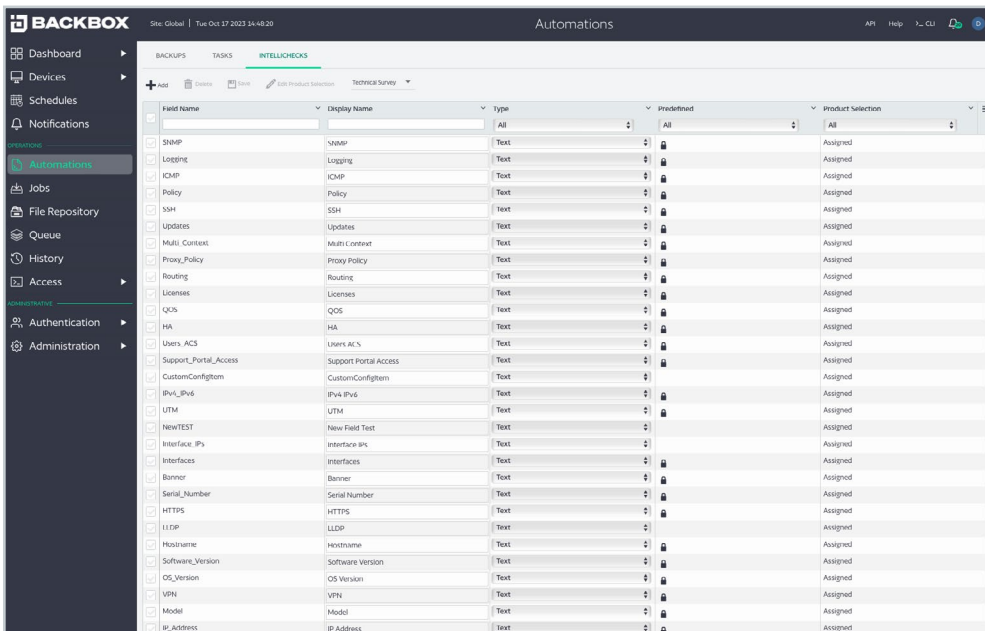
BackBox contains prebuilt IntelliChecks that express the rules defined by CIS Benchmarks, PCI, HIPAA, NIST, STIGs, and others. These rules are often a good starting point for organizations to build out custom rules based on their own internal standards.



Name	Description	Signature Type	Tags	Site	Access Restrict	In Use
Palo Alto -> Pa...	Certificates Expiration Checks Enabled	Security	PCI-DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, NIST		All	✓
Palo Alto -> Pa...	Configure a Data Pattern for Credit card and social security numbers	Security	PCI-DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, COBIT, NIST, CCS, CSC, ISA...		All	✓
Palo Alto -> Pa...	Configure a Data Pattern for Credit card and Social Security numbers	Security	PCI-DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, COBIT, NIST, CCS, CSC, ISA...		All	✓
Palo Alto -> Pa...	Configure a login banner ideally approved by the organizations legal team	Operations	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Configure an enabled SYN Flood Action of SYN Cookies	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Configure SYN Flood Rates	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Configure the Palo Alto Networks security platform to operate in FPS mode	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Disable WHM probing if it is not required for User-ID functionality in the environment.	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Enable the option Enable Log on High DP Load feature. When this option is selected, a syst...	Operations	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure a fully-synchronized High Availability peer is configured	Operations	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✗
Palo Alto -> Pa...	Ensure a fully-synchronized high Availability peer is configured	Operations	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✗
Palo Alto -> Pa...	Ensure a minimal SSL-TLS Version is configured	Security	PCI-DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, COBIT, NIST, CCS, CSC, ISA...		All	✓
Palo Alto -> Pa...	Ensure a secure antispoof profile is applied to all relevant security policies	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure alerts are enabled for malicious files detected by WildFire to Panorama	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure all HTTP Header Logging options are enabled	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure all HTTP Header Logging options are enabled	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure all HTTP Header Logging options are enabled	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✗
Palo Alto -> Pa...	Ensure all HTTP Header Logging options are enabled	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure all new passwords to ensure that they meet basic requirements for strong passwo...	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure all WildFire session information settings are enabled	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓
Palo Alto -> Pa...	Ensure all WildFire session information settings are enabled	Security	PCI-DSS, CIS, ITSG, ISO/IEC-27001, STIG		All	✓

TECHNICAL SURVEY

During the process of building out compliant standards, it's useful to be able to "ask the network questions". For example, to easily find out what machines are not running SNMP or which machines have password requirements shorter than 10 characters.



Field Name	Display Name	Type	Predefined	Product Selection
SNMP	SNMP	Text	✓	Assigned
Logname	Logging	Text	✓	Assigned
ICMP	ICMP	Text	✓	Assigned
Policy	Policy	Text	✓	Assigned
NM	SSH	Text	✓	Assigned
Updates	Updates	Text	✓	Assigned
Multi_Context	Multi Context	Text	✓	Assigned
Proxy_Policy	Proxy Policy	Text	✓	Assigned
Routing	Routing	Text	✓	Assigned
Licenses	Licenses	Text	✓	Assigned
QOS	QOS	Text	✓	Assigned
HA	HA	Text	✓	Assigned
Users_ACS	Users ACS	Text	✓	Assigned
Support_Portal_Access	Support Portal Access	Text	✓	Assigned
CustomConfigItem	CustomConfigItem	Text	✓	Assigned
IPv4_IPv6	IPv4 IPv6	Text	✓	Assigned
UTM	UTM	Text	✓	Assigned
NewTEST	New Field Test	Text	✓	Assigned
Interface_IPs	Interface IPs	Text	✓	Assigned
Interfaces	Interfaces	Text	✓	Assigned
Banner	Banner	Text	✓	Assigned
Serial_Number	Serial Number	Text	✓	Assigned
HTTPS	HTTPS	Text	✓	Assigned
LLDP	LLDP	Text	✓	Assigned
Hostname	Hostname	Text	✓	Assigned
Software_Version	Software Version	Text	✓	Assigned
OS_Version	OS Version	Text	✓	Assigned
VPN	VPN	Text	✓	Assigned
Model	Model	Text	✓	Assigned
IP_Address	IP Address	Text	✓	Assigned

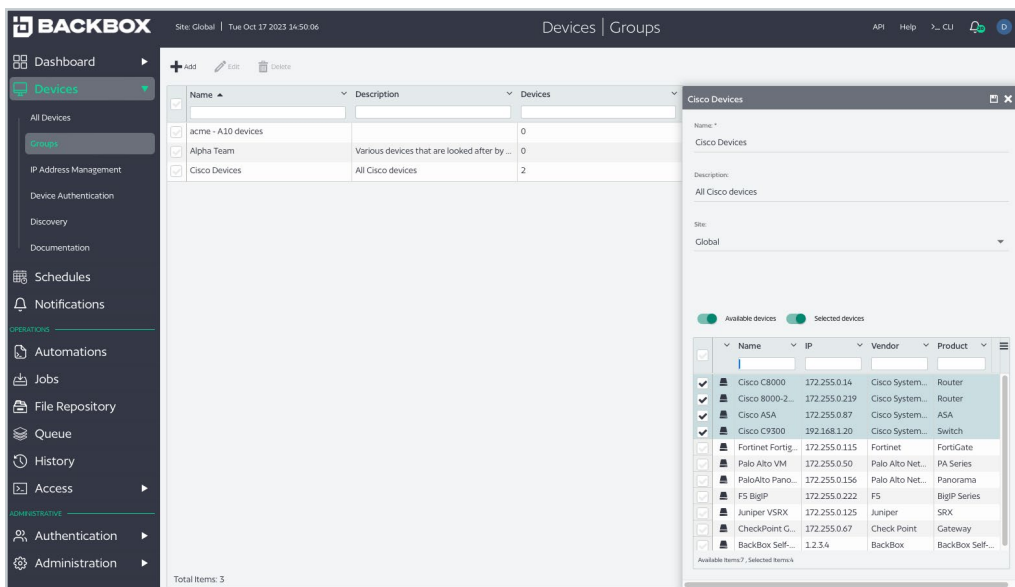
Investigating network configuration parameters provides a baseline for building out the compliance standards.

BackBox offers a Technical Survey capability which is easily accessible and lets network administrators quickly determine the current state of device configurations across vendors.

Find Non-Compliance

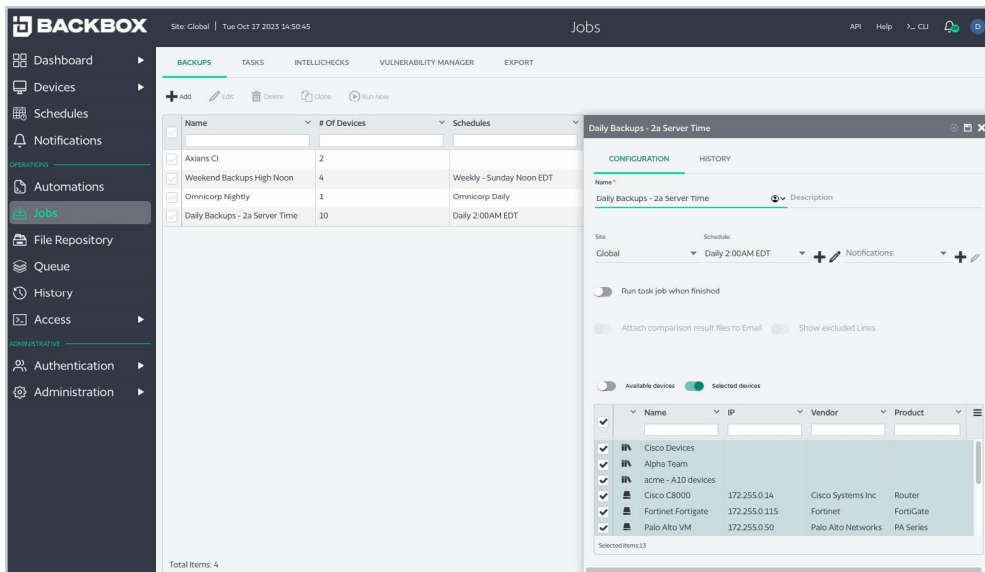
GROUPS

Once all the compliance automations are created, they're put into a Group so they can be run collectively on whatever set of devices and combination of vendors you wish.



JOBS

With the Group setup, a Job is created and applied to the devices you wish to be compliant. The Job can be run manually or automatically, and typically serves as a starting point report. The Job should also be run on a daily schedule so that every day BackBox is searching for and reporting non-compliant devices.



Stay Compliant

Remediation is an important part of compliance. BackBox IntelliChecks can include remediation capabilities so that when non-compliant devices are found they can be groomed back into compliance. Automatic remediation is, of course, optional.

With remediation optional, there are two other ways that organizations use BackBox to respond to compliance violations.

- 1. Reports.** Reporting is an integrated part of compliance because reports are often shared with other teams to assure them that the network is configured the way it's supposed to be. Reporting can be done by the Job, showing the complete state of compliance, or can be done by IntelliChecks, showing the status of any individual compliance rule across all devices. Reports include a column showing whether any remediation has been taken, and if so, the status.

- 2. Automate trouble tickets.** It's understandable if automatic remediation makes teams uncomfortable. It's often better to have a human hand at the configuration keyboard. That's where external integrations come in play. BackBox can setup notifications to call out to external systems to notify of compliance violations. For example, BackBox can connect to an ITSM like ServiceNow to open a trouble ticket to resolve a compliance violation. And, because we know the remediation steps, we can put information about the remediation steps into the trouble ticket to help speed up resolution. engineer's expertise, and hours of time.

Another important part of staying compliant is ensuring that new devices are compliant when they're added to the network. Customers often create a Job with all the compliance configuration tasks, so that it becomes easier to onboard new devices in a compliant configuration than manually installing a golden configuration.

CUSTOMER EXAMPLE

A customer was implementing DISA STIGs for their Juniper switches. This entailed a 92-step manual configuration check every week or two, with the output being an XML-formatted report of the configurations.

With BackBox, they were able to automate all 92 steps, saving the equivalent of almost a full-time engineer's worth of time.

Conclusion

Non-compliant devices are a risk to the organization. Yet, device compliance is hard. It usually involves infrequent audits and contentious interactions between the network team and the compliance organization. The infrequent nature of compliance audits means that devices that fall out of compliance often stay that way for some time. Tracking device configurations manually and frequently is often too much overhead for teams already saddled with more work than they can keep up with.

Automation is simply the only way to have a timely compliance regime that's enforced. It ensures that configuration drift is groomed back into compliance – either manually or automatically – and that there's clear daily reporting on compliance status, with reports that can be shared among teams to help build trust.

With the ability to complete a Technical Survey and understand how devices are configured, BackBox serves as an ideal on-ramp to automation at your next compliance audit, creating reports that serve as project plans for grooming the current state of the network into compliance.



About BackBox

Backbox is a Network and Security Device Automation Platform that supports over 180 vendors, with thousands of pre-built automations and a scripting-free way to build new ones. Enterprises and service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance, BackBox gives you confidence that your automations will deliver the expected outcome every time.

Find out more at www.backbox.com

