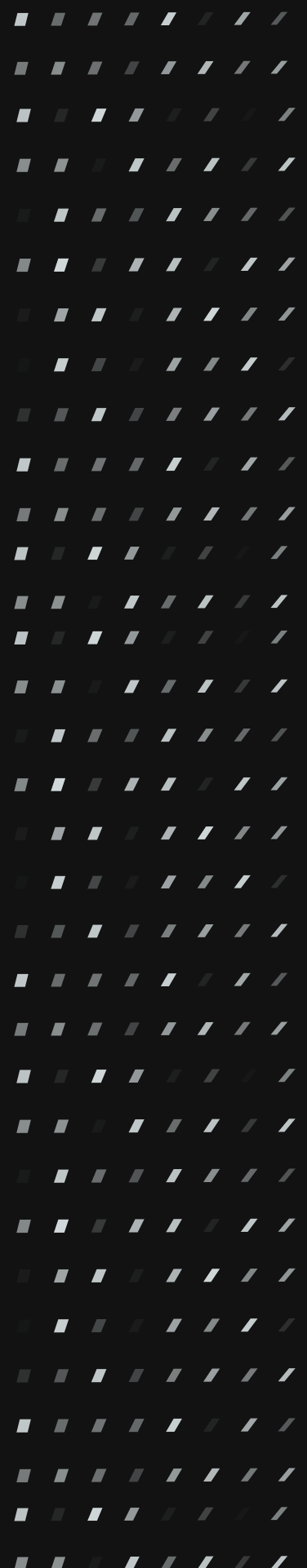


# Compliance Assurance and Remediation With IntelliChecks

---



IntelliChecks enables you to monitor the health of every device in your system by automatically running sets of tests on the device, at regular intervals. You can also run compliance checks to test whether certain devices conform to your specifications. These checks are stored as signatures, which are listed in the Signatures section.

IntelliChecks uses a database of hundreds of signatures that test various conditions across a wide variety of devices for Operational, Health, and Security Compliance. You can clone and edit these signatures or create completely new signatures and signature groups.

There are pre-defined Groups of IntelliCheck Signatures that you can run right out of the box as Jobs against your devices. Jobs can be created within BackBox to run a variety of things such as Notifications, Backups, Tasks, and Intellichecks. These Groups of Signatures can be cloned and edited to allow you to run any subset of signatures you wish to run against your devices.

By using Device Groups, you can simplify the management of similar devices. By putting all the devices of a specific type in a group, you can run a single job, and have it applied to every member of the group, rather than having to specify each device separately.

**IntelliChecks contains the following five options:**

- Signatures shows you all the existing signatures available.
- Groups enable you to set several signatures as a schedulable collection.
- Jobs allow for scheduling individual signatures or groups to run on specified devices.
- Queue shows currently running jobs.
- History lists the executed jobs and their respective statuses.

## Setting Up a Working IntelliChecks Job

**Below we will demonstrate how to create a new IntelliCheck Group that will allow you to create a new IntelliCheck Job to run against a Device. Here are the steps to properly set up a working Intellichecks job:**

**1**

Go to “IntelliChecks Signatures.” In this page you can view all the Signatures currently available, decide the signatures you wish to run against your Devices.

Name	Description	Signature Type	Tags	Site	Predefined
Check Point - VSI - Cluster State, High Availabil...	Backbox will monitor the HA module, sync status...	Operations			<input type="checkbox"/>
Cisco Certificate Check		Operations			<input type="checkbox"/>
Check Point - Identify Awareness Service Status		Performance			<input type="checkbox"/>
Check - Palo Alto - User-ID Agent is reinstalled	Ensure the security policies restricts Palo Alto Us...	Security	PCI-DSS, CIS, ITSC, ISO/IEC-27001, STG		<input type="checkbox"/>
Check Point - Fail Diagnostic		Performance			<input type="checkbox"/>
Check Point - Destination Cache Limit Monitoring	Backbox will monitor the destination cache for r...	Performance			<input type="checkbox"/>
Check Point - Check ipassignment.conf file	Backbox will run a check on ipassignment.conf fi...	Operations			<input type="checkbox"/>
Linux -> Interfaces Throughput Above Threshold		Performance			<input type="checkbox"/>
Check Point - Check specific VPN tunnel is active		Performance			<input type="checkbox"/>
Check Point - Check Log Servers Connection		Performance			<input type="checkbox"/>
Check Point - Kernel tables usage above thresh...	Backbox will monitor the kernel tables and alert...	Performance			<input type="checkbox"/>
Check Point - Failed login attempts	Backbox will monitor and alert if too many failed...	Security			<input type="checkbox"/>
Check Point - Identify Awareness DC connections		Operations			<input type="checkbox"/>
Check Point - Cloud Services Connectivity Check	Backbox Will alert if the firewall has no connect...	Operations			<input type="checkbox"/>
PaloAlto - Show Throughput		Performance			<input type="checkbox"/>
Check Point - ARP Cache Table Size		Operations			<input type="checkbox"/>
Checkpoint - Portal HTTP redirect	Backbox will test if Portal HTTP redirect is enable...	Security			<input type="checkbox"/>
Check Point - Bond Interfaces Status	Backbox will check if bonds are configured and...	Operations			<input type="checkbox"/>
Checkpoint - Accelerator State	Backbox will monitor SecureXL status and alert...	Operations			<input type="checkbox"/>
Blue Coat - CAS - 2.x.x.x -> Active licenses check		Operations			<input type="checkbox"/>
Palo Alto -> Unused security rules on vsys	Backbox will alert and list unused rules if found...	Operations			<input type="checkbox"/>

- 2 After you have decided what to add to a specific Group, go to “Intelligence Groups.” In this screen you will set up a group consisting of all the Signatures you wish to run on the Device(s).
- 3 Give the Group a name of your choosing (ie: Cisco Password Complexity, etc.).
- 4 Assign a Site if you are using sites to logically group your devices.
- 5 Select the appropriate signatures by checking the box at the left of the Signature line. You can use the filter icon to only see Signatures for a specific vendor, product, version, and Connection Option. When you have them all checked, click the Save icon at the top right corner of the window to Save your grouping.

### New IntelliChecks Signatures Group Configuration

Name: \*  Site:

Description:

Available signatures
  Selected signatures

Filter by Vendor: 
 Filter by Product: 
 Filter by Version: 
 Filter by Option:

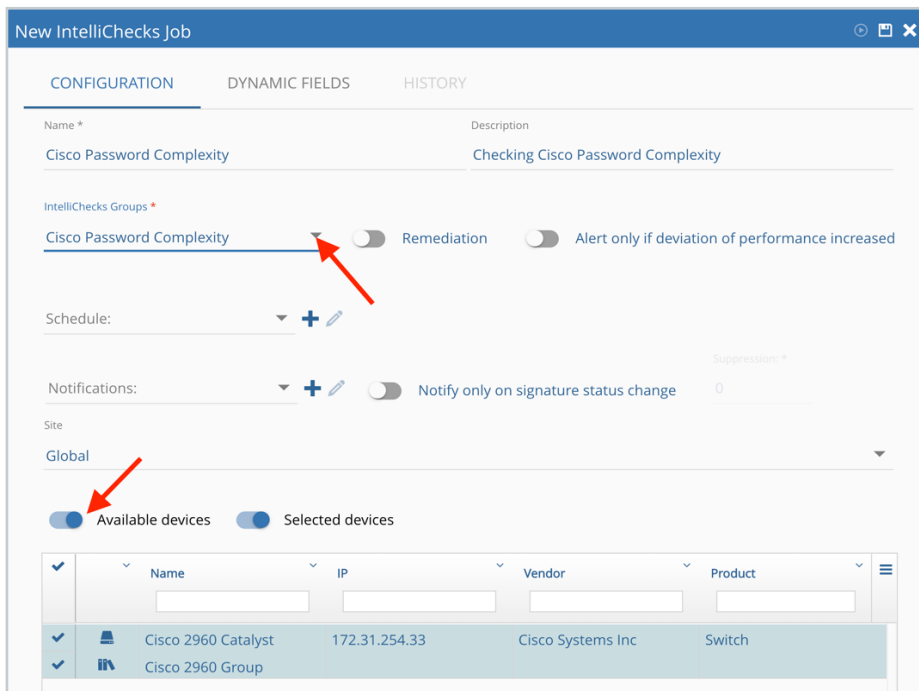
✓	Name	Type	Tags
<input checked="" type="checkbox"/>	Cisco Certificate Check	Operations	
<input checked="" type="checkbox"/>	Cisco -> CPU Usage	Performance	[...]
<input checked="" type="checkbox"/>	Cisco - Switch -> CPU MIC register...	Operations	[...]
<input checked="" type="checkbox"/>	Cisco - Router/Switch -> PortASIC ...	Operations	[...]
<input checked="" type="checkbox"/>	Cisco - Router/Switch -> Proxy ARP	Operations	[...]
<input checked="" type="checkbox"/>	Cisco - Switch/Router -> MAC Add...	Performance	[...]

Available Items:69, Selected Items:0

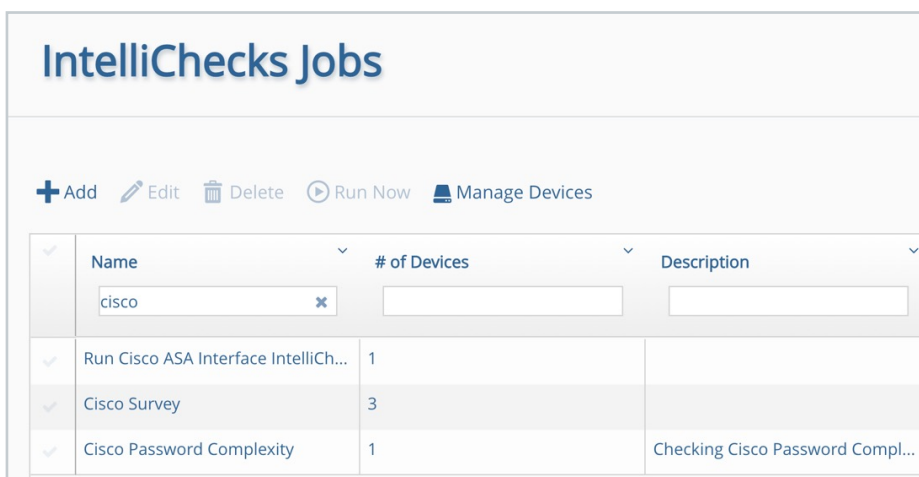
6

Now we will create a Job to run the Groups we select. Go to "Intelligence Jobs." Here we create Job schedules that can be assigned one or several Groups to run at a given time.

- a. Give the Job a name of your choosing (ie: Cisco Password Complexity, etc.).
- b. Select the group(s) you want associated with the job. Multiple groups can be selected.
- c. Choose your Schedule, Notification method, toggle whether you want to run Remediation (if your selected Signatures have that option available), and then choose the devices to run your Intelligence Jobs against. Be sure to have the Available Devices toggle selected, so you can see all your devices.



- d. If you do not see your Devices with the toggle activated, you may need to add them to the available pool by using the Manage Devices applet.



- e. Take Note – Signatures can be version and connection type specific, so if you do not see a given Device in the "Available Devices" listing, it may be due to the Device's options not supporting the Signature parameters.

# How to View the History of IntelliCheck Job

You can view a list of all IntelliChecks jobs and signatures that were run on devices by displaying the IntelliChecks History screen:

Job Name	Signature Name	Device Name	IP	Date	Result/Status Reason	Status	Site	Log
Run Cisco ASA Interface IntelliCheck	Lyntel Cisco -> ASA -> Interfaces	Cisco ASA	172.31.254.2	07-15-2022 00:13		Success	Global	Log
Run Cisco ASA Interface IntelliCheck	Cisco -> ASA -> Last w...	Cisco ASA	172.31.254.2	07-15-2022 00:12	Number of days since last successful scan	Failure	Global	Log
Run Cisco ASA Interface IntelliCheck	Cisco -> ASA -> Certificate Check	Cisco ASA	172.31.254.2	07-15-2022 00:12	An expired certificate was found	Failure	Global	Log
Run Cisco ASA Interface IntelliCheck	Cisco -> ASA -> Memory Utilization	Cisco ASA	172.31.254.2	07-15-2022 00:12		Success	Global	Log
Test Cisco	Cisco -> IDS -> Set AAA accounting en...	Cisco 2960 Catalyst	172.31.254.33	07-14-2022 12:18	The device did not respond to our request in order to start the test	Failure	Global	Log
Test Cisco	Cisco -> IDS -> Require Timeout for S...	Cisco 2960 Catalyst	172.31.254.33	07-14-2022 12:17	The device did not respond in order to start the test	Failure	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Hsp disabled	gw0040-4	172.31.5.4	07-14-2022 12:16		Success	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Hsp disabled	gw0040-4	172.31.5.4	07-14-2022 12:16	Unauthorized messages in history were received	Failure	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Hsp disabled	gw0040-4	172.31.5.4	07-14-2022 12:16	Unauthorized messages in history were received	Failure	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Hsp disabled	gw0040-4	172.31.5.4	07-14-2022 12:16	No zombie processes returned	Success	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Hsp disabled	gw0040-4	172.31.5.4	07-14-2022 12:16	Unauthorized messages in history were received	Failure	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Threat Emu...	gw0040-4	172.31.5.4	07-14-2022 12:16	Current file engine version too outdated	Failure	Global	Log
Check Point Performance	Check Point -> Gsa05 -> Zombie pro...	gw0040-4	172.31.5.4	07-14-2022 12:16	No zombie processes returned	Success	Global	Log

You can see the Signature Name, Device Name, IP, and Date. In the Status column, the screen also shows whether the device successfully ran the job or failed. If the device failed to run the job, the reason for failure is stated. You can also click on a job's Log button to display and download a detailed log of the jobs and their status. The final column will show the Site the device is associated with.

## Contact Us

+1-833-BACKBOX  
(+1-833-222-5269)



**North America**  
14135 Midway Road  
Greenhill Towers, Suite G250  
Addison, TX 75001 USA  
info@backbox.com

**EMEA**  
13 Ha'amal St., Park Afef,  
Rosh-Haain, 4809249 Israel  
info@backbox.com

**APAC**  
apacinfo@backbox.com