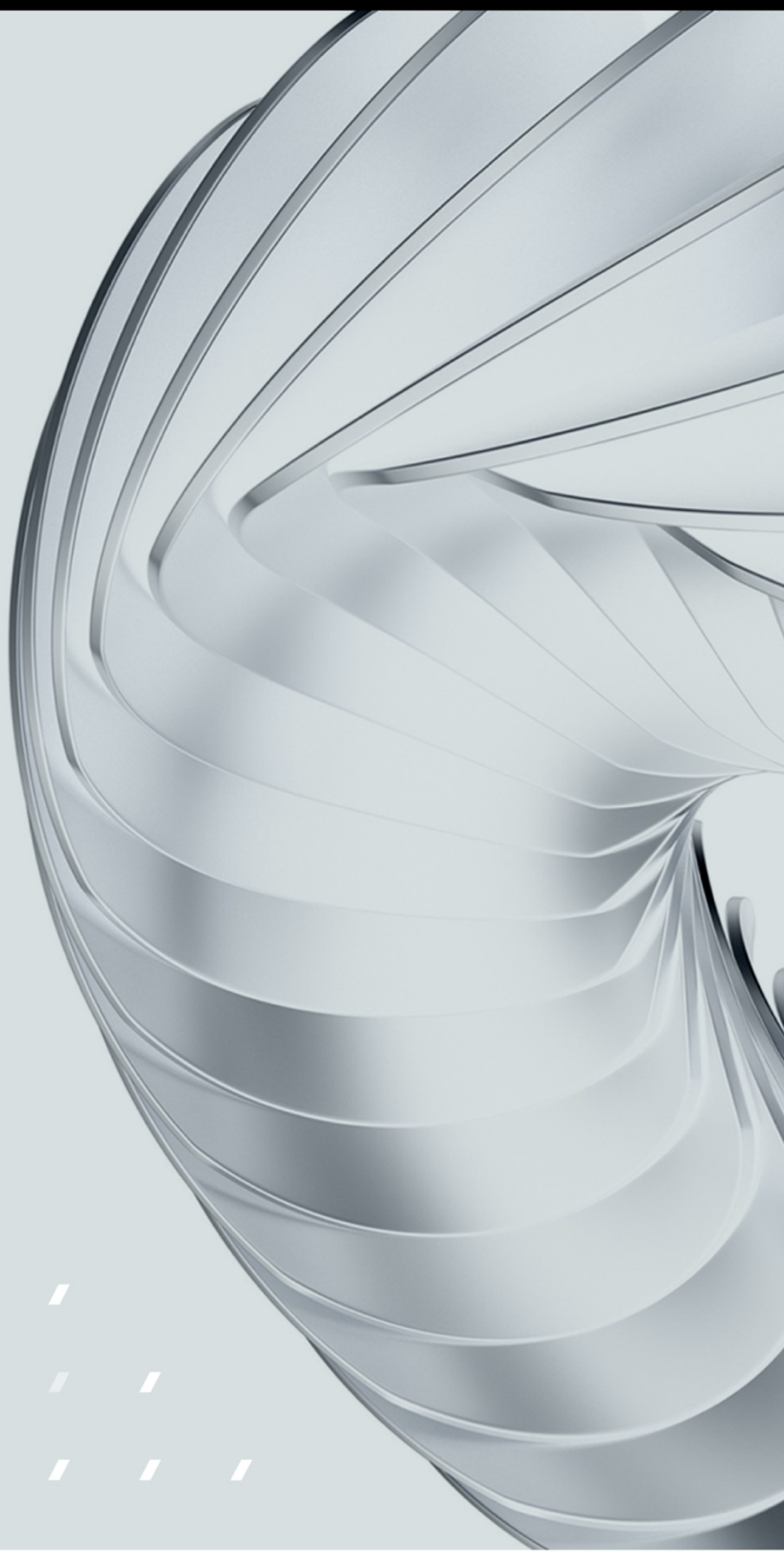
BACKBOX

User Guide
Version 6



info@backbox.com + 972-73-3266400 backbox.com

Copyright © 2021 BackBox Software LTD. All rights reserved.
No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from BackBox Software LTD.
All copyright, confidential information, patents, design rights and all other intellectual property rights of whatsoever nature contained herein are and shall remain the sole and exclusive property of BackBox Software LTD. The information furnished herein is believed to be accurate and reliable.
However, no responsibility is assumed by BackBox Software LTD for its use, or for any infringements of patents or other rights of third parties resulting from its use.
The BackBox name and BackBox logo are trademarks or registered trademarks of BackBox Limited.
All other trademarks are the property of their respective owner

TABLE OF CONTENTS

LIST OF FIGURES 7
LIST OF TABLES 10
CHAPTER 1 INTRODUCTION 11
Features 11
Who should use BackBox 11
CHAPTER 2 INSTALLATION 12
System Requirements 12
Prerequisites 12
Installing BackBox 13
CHAPTER 3 GETTING STARTED 15
Logging In 15
Dashboard System Status Screen 20
The BackBox Interface: Screens and Tables 21
Configuring Table Columns 21
Sorting a Table 21
Grouping Table Rows 22
Filtering Tables 23
Understanding the Dashboard 28
Configuring the Widgets 28
CHAPTER 4 SETTINGS 34
Interfaces 35
Routing 36
Adding or Editing a Route 36
Deleting a Route 36
DNS 37
Date and Time 37
Alerts 38
Administration 38
Settings Tab: 39
Maintenance Tab: 41
Customizations Tab: 41
Cluster Tab: 42
Licenses 42
Access Rules 43
Sites 43
Adding a Site 44
Editing a Site 44
Deleting a Site 45
Agents 45
Adding an Agent 45
Editing an Agent 46
Upgrading an Agent 46

Deleting an Agent 46
Viewing the Audit Logs 47
Viewing the Messages Log 49
Viewing the VSFTPD Log 49
Viewing the Secure Log 50
Viewing the General log 50
CHAPTER 5 AUTHENTICATION 51
Authentication Templates 51
To add an authentication template: 51
Authentication Servers 53
BackBox Users 54
Adding a New User 54
Editing a User 55
User Roles 55
Adding a New Role 55
Editing a Role 56
Deleting a Role 56
Operating System Users 56
Adding a New Operating System User 56
Editing an Operating System User 57
Deleting an Operating System User 57
Connected Users 57
CHAPTER 6 NOTIFICATIONS 58
Configuring Notification Jobs 59
Adding a Notification 59
Editing a Notification 60
Deleting a Notification 60
Testing a Notification 60
CHAPTER 7 SCHEDULES 61
Adding a new Schedule 61
CHAPTER 8 BACKUPS 62
The Backup Jobs Screen 62
Adding a Backup Job 63
Deleting a Backup Job 65
Running a Backup Job 65
The Backup Queue Screen 65
Removing a Job from the Queue 65
Backup History Screen 65
Filtering the Backup History 66
Backup Trail Log 66
CHAPTER 9 DEVICES 67
Devices Screen 67
Devices Table Legend 70

Adding a New Device 70
Using Export/Import to Add Multiple Devices 73
Displaying the Details of an Individual Device 74
Device Details Tab 75
Retention Button 76
Device History Tab 77
IntelliChecks Tab 79
Inventory Tab 80
Network Info Tab 80
Usage Tab 81
Performance Tab 81
Technical Survey Tab 82
Notes Tab 82
Deleting a Device 83
Comparing Backups 83
Devices Groups Screen 86
Adding a New Device Group 87
Editing a Device Group 87
To delete a Device Group: 87
IP Address Management 88
Adding a Segment 88
Editing and Deleting Segments 89
Synchronizing Existing Devices into Segments 89
Network Map 89
Network Database 89
Discovery 90
Jobs Tab 90
Adding a new job 91
Credentials Tab 92
Rules Tab 93
CHAPTER 10 TASKS 94
How It Works 94
The Task Configuration Screen 94
Adding a New Task 95
Creating a Task Script 95
Quick Tasks 97
Assigning Tasks to Devices and Scheduling Task Execution 97
Mode 99
Viewing Task Job History 100
Modifying an Existing Task Job 100
Viewing Task History 101
CHAPTER 11 REPORTS 103
Adding a New Report 103

Editing a Report 104
Deleting a Report 104
Types of Predefined Reports 104
Enable IntelliChecks 105
IntelliChecks Signatures Screen 105
Adding a new Signature 106
IntelliChecks Groups Screen 106
Creating a New IntelliChecks Job 107
IntelliChecks Queue Screen 108
IntelliChecks History Screen 108
Technical Survey 109
CHAPTER 13 ACCESS 110
Connecting to Devices Using the Terminal Screen 110
Running A Toolbox's Command Script 111
Editing Toolboxes and Commands 113
Editing Commands 114
CHAPTER 14 CUSTOMIZE 115
Customizing Vendor, Product, and Version Lists 115
Option Configuration Screen 116
Option Configuration Scripting Tabs 117
Understanding the Compare Exceptions Section 118
Understanding the Connect Section 121
Understanding the Backup Section 121
Understanding the Inventory Section 122
Understanding the Restore Section 122
Appendix A VMWare Installation 123

LIST OF FIGURES

Figure 1: Installation Screen 13
Figure 2: Configure TCP/IP Screen 13
Figure 3: Manual TCP/IP Configuration Screen 14
Figure 4: BackBox Access Screen 14
Figure 5: Login Screen 15
Figure 6: Dashboard System Status Screen 20
Figure 7: Changing the Width of a Column 21
Figure 8: Column Sort Menu 21
Figure 9: Example of Group Option 22
Figure 10: Example of Grouping According to Vendor 22
Figure 11: Example of Expanding a Grouped Row 22
Figure 12: Example of a Filtered Table 23
Figure 13: Sidebar Screen Navigation Buttons 23
Figure 14: System Status Screen 28
Figure 15: Widget Menu 28
Figure 16: Widgets Sub-menus 29
Figure 17: Charts Display Options 30
Figure 18: Interfaces Screen 35
Figure 19: Edit Interface Dialog Box 35
Figure 20: Routing Screen 36
Figure 21: New Route Configuration Dialog Box 36
Figure 22: DNS Screen 37
Figure 23: Date and Time Screen – NTP View 37
Figure 24: Alerts Screen 38
Figure 25: Administration Screen 38
Figure 26: License Screen 42
Figure 27: Access Rules Screen 43
Figure 28: Add Access Rule Dialog Box 43
Figure 29: Sites Screen 44
Figure 30: New Site Configuration Dialog Box 44
Figure 31: Agents Screen 45
Figure 32: New Agent Configuration Dialog Box 45
Figure 33: Auditing Screen 46
Figure 34: Audit Log Screen 47
Figure 35: Auditing Screen 47
Figure 36: Audit Details Log Screen 48
Figure 37: Trail Log Screen 49
Figure 38: Trail Log Screen 50
Figure 39: Trail Log Screen 50
Figure 40: Authentication Templates Screen 51
Figure 41: Authentication Template Dialog Box 51

Figure 42: Authentication Servers Screen 53
Figure 43: Authentication Servers Screen 53
Figure 44: BackBox Users Screen 54
Figure 45: Add a New User Dialog Box 54
Figure 46: User Roles Screen 55
Figure 47: New Role Configuration Dialog Box 55
Figure 48: Operating System Users Screen 56
Figure 49: Add OS User Dialog Box 56
Figure 50: Connected Users Screen 57
Figure 51: Notification Alerts Screen 58
Figure 52: Jobs Notifications Screen 59
Figure 53: New Notification Configuration Dialog Box 59
Figure 54: Schedules Screen 61
Figure 55: New Schedule Configuration Dialog Box 61
Figure 56: Backup Jobs Screen 62
Figure 57: New Backup Job Configuration Dialog Box 63
Figure 58: Backup Queue Screen 65
Figure 59: Backup History Screen 66
Figure 60: Devices Screen 67
Figure 61: Device Table Legend 70
Figure 62: New Device Configuration Dialog Box - Step 1 of 4 70
Figure 63: New Device Configuration Dialog Box - Step 2 of 4 71
Figure 64: New Device Configuration Dialog Box - Step 3 of 4 71
Figure 65: New Device Configuration Dialog Box - Step 4 of 4 72
Figure 66: Export Devices Password Encryption 73
Figure 67: Spreadsheet with new devices added 73
Figure 68: Import Devices File Upload 73
Figure 69: Devices Screen Displaying Newly Added Devices 74
Figure 70: Device Details Screen 74
Figure 71: Upper Right Corner of the Devices Details Tab 75
Figure 72: Retention Policy Dialog Box for a Device 77
Figure 73: Device History Tab 77
Figure 74: Example for Backup Trail Log Screen 78
Figure 75: IntelliChecks Tab 79
Figure 76: Example of Network Info Tab 80
Figure 77: Example of Usage Tab 81
Figure 78: Connected Users 81
Figure 79: Example of Technical Survey Tab 82
Figure 80: Example of Notes Tab 82
Figure 81: Confirm Delete Devices Prompt 83
Figure 82: Deletion Process Message 83
Figure 83: Successful Deletion Message 83
Figure 84: Compare Backups Dialog Box 84

Figure 85: Compare Backups Screen with Files Selected 85
Figure 86: Compare Backups Screen with File Comparison Result 85
Figure 87: Compare Screen Showing Excluded Line in Grey and Export Options 86
Figure 88: Devices Groups Screen 86
Figure 89: Device Group Dialog Box 87
Figure 90: The IP Address Management Screen 88
Figure 91: New Segment Dialog Box 88
Figure 92: The Network Map Screen 89
Figure 93: Network Database 89
Figure 94: The Jobs Tab Screen 90
Figure 95: The Jobs Tab Screen 91
Figure 96: The Credentials Tab Screen 92
Figure 97: The Rules Tab Screen 93
Figure 98: Task Configuration Screen 94
Figure 99: Adding a New Task Screen 95
Figure 100: Edit Task Configuration Dialog Box displaying Add Access 95
Figure 101: Edit Task Configuration Dialog Box Displaying Task Commands 96
Figure 102: Conditions Dialog Box 96
Figure 103: Quick Tasks Screen 97
Figure 104: Task Jobs Screen 97
Figure 105: New Task Job Configuration Screen 98
Figure 106: Add User Configuration Screen 99
Figure 107: Task Job History Tab 100
Figure 108: Task Queue Screen 100
Figure 109: Task History Screen 101
Figure 110: Tasks File Repository Screen 101
Figure 111: New Tasks File Dialog Box 101
Figure 112: Edit Tasks File Box 102
Figure 113: Reports Screen 103
Figure 114: New Report Configuration Dialog Box 103
Figure 115: Report Type List 104
Figure 116: Enable IntelliChecks Dialog 105
Figure 117: IntelliChecks Signature Screen Displaying Signatures, Types, Tags, and Site 105
Figure 118: New IntelliChecks Signature Configuration screen 106
Figure 119: IntelliChecks Groups Screen 106
Figure 120: IntelliChecks Jobs Screen 106
Figure 121: New IntelliChecks Job Configuration Screen 107
Figure 122: Search for IntelliChecks Group 107
Figure 123: IntelliChecks Queue Screen 108
Figure 124: IntelliChecks History Screen 109
Figure 125: IntelliChecks Technical Screen 109
Figure 126: Devices Tab on the Terminal Screen 110
Figure 127: Changing the Port 111

Figure 128: Terminal Screen with Multiple Devices Connected 111
Figure 129: Commands Tab Listing Toolboxes 112
Figure 130: Toolbox Displaying Category and Commands 112
Figure 131: Command Options Menu 112
Figure 132: Add Node Dialog Box 113
Figure 133: Edit Command Dialog Box 114
Figure 134: Customize Screen 115
Figure 135: Customize Editing Interface 116
Figure 136: Customize Configuration Screen 116
Figure 137: Firewall Rule Menu 118
Figure 138: Inventory Section of the Dynamic Fields Tab 120
Figure 139: Connect Tab 121
Figure 140: Inventory Tab 122
Figure 141: Restore Tab 122

LIST OF TABLES

Table 1: Functions of Sidebar Screen Navigation Buttons 24
Table 2: Widgets 30
Table 3: Settings Screens 34
Table 4: Settings Tab 39
Table 5: Maintenance Tab 41
Table 6: Customizations Tab 41
Table 7: Cluster Tab 42
Table 8: Audit Log Filter 47
Table 9: Authentication Template Fields 52
Table 10: Notification Alerts Columns 58
Table 11: New Notification Configuration Fields 60
Table 12: Backups Jobs Screen: Fields and Buttons 62
Table 13: New Backup Job Configuration Fields 64
Table 14: Device Fields 67
Table 15: Devices Toolbar Buttons 69
Table 16: Device Details Fields and Buttons 75
Table 17: Device History Buttons 78
Table 18: Task Job Fields 90
Table 19: Option Configuration Scripting Tabs 117
Table 20: Options Columns of Dynamic Fields 118

CHAPTER 1 INTRODUCTION

BackBox is a market leader in network automation, security and management solutions. We help companies worldwide automate and streamline complex tasks, ensure network health and performance, achieve business continuity and do more with fewer resources.

BackBox provides comprehensive backup/restoration management, the ability to automate any kind of task, signature-based health checks and compliance, and jumpbox functionality.

The intuitive dashboard uses a single pane to display all your devices (network/security/telephony/etc.) so that you can easily see the status of backups and selected IntelliChecks signatures.

BackBox enables security and network administrators to manage complete backup schedules and monitor the health of every device in the system, with configurable status alerts.

BackBox's unique multi-check engine ensures backups have run successfully and verifies that all saved configurations meet the criteria needed for successful restoration.

Features

- Automated Backup & Recovery
- Task Automation
- Inventory Management
- Network Visualization
- IntelliChecks + Trends
- Access Management
- Single application for backup/restore of all security and networking devices
- Intelligent automation for device mgmt. tasks, health checks, and compliance
- Support for over 180 vendors with out-of-the-box connection scripts
- Web-based management for alerts, notifications, and reports
- Multiple authentication options and granular user role options
- Jumpbox functionality with video capture and indexed keyword searches
- Live dashboard with real-time backup and monitor status display

Who should use BackBox

Backbox was designed and intended for a wide audience with varying levels of network and IT knowledge. Installation and operation will require basic IT experience. Specifically, the target audiences are:

- System administrators – to install, configure, and schedule backups
- Backup Operators – to configure and schedule backups
- Networking and Auditing Users – to review backups, compliance, and system statuses
- DevOps – to script and automate backup tasks across homogenous or heterogenous networks

CHAPTER 2 INSTALLATION

This chapter outlines the system requirements and prerequisites necessary to run BackBox.
It also provides instructions for installing the system.
BackBox provides an ISO image that is installed on a physical, cloud, or virtual server that has access to all or portions of a customer network. Once installed, BackBox Administrators can configure the product and utilize the out of the box scripts.

System Requirements

The following are the ***minimum*** hardware requirements:

- Intel 4 CPU
- Disk space: 250GB (estimated for 6 months of backups)
- Memory: 8GB
- At least one network interface card (NIC)
- CD-ROM drive (for physical hardware installations)

Prerequisites

- Static IP address
- DNS server IP address (and DNS suffix)
- IP address of SMTP server (and routing/SMTP access between the BackBox server and the SMTP server)
- Routes through firewalls to target devices on required ports
- Chrome or Firefox browser. IE doesn't follow HTML5 and causes GUI errors

Installing BackBox

After downloading the latest ISO from backbox.com, to install BackBox:

1. Insert the ISO or CD in the drive. The Installation screen appears.

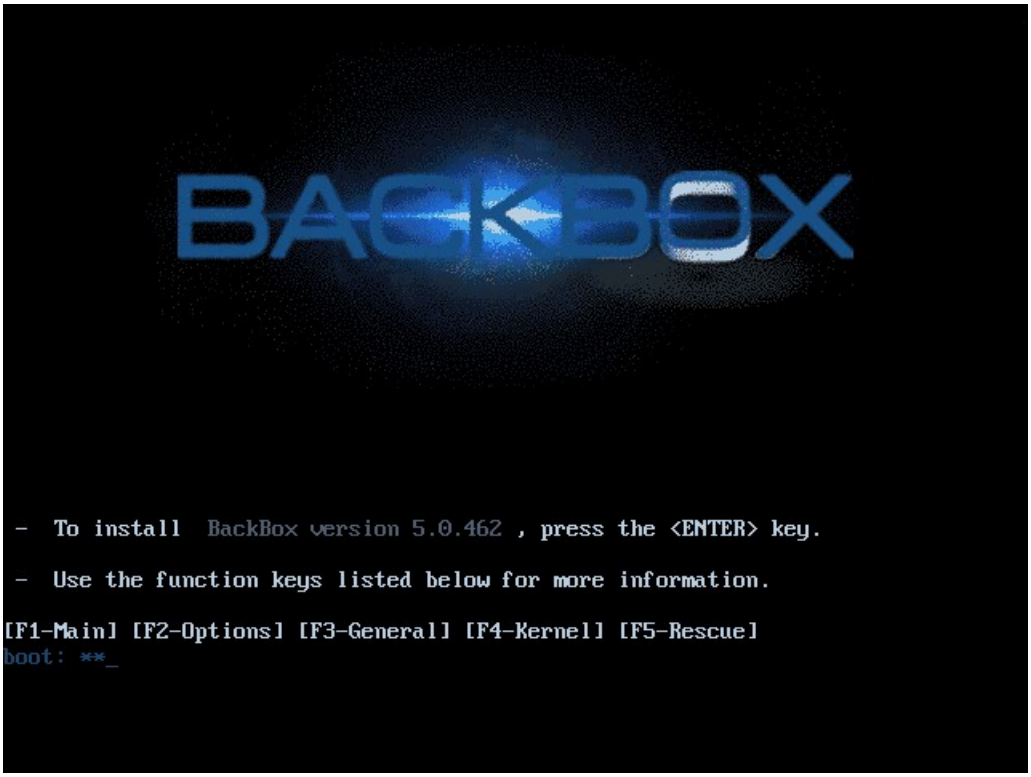


Figure 1: Installation Screen

2. Press Enter. The Configure TCP/IP screen appears.

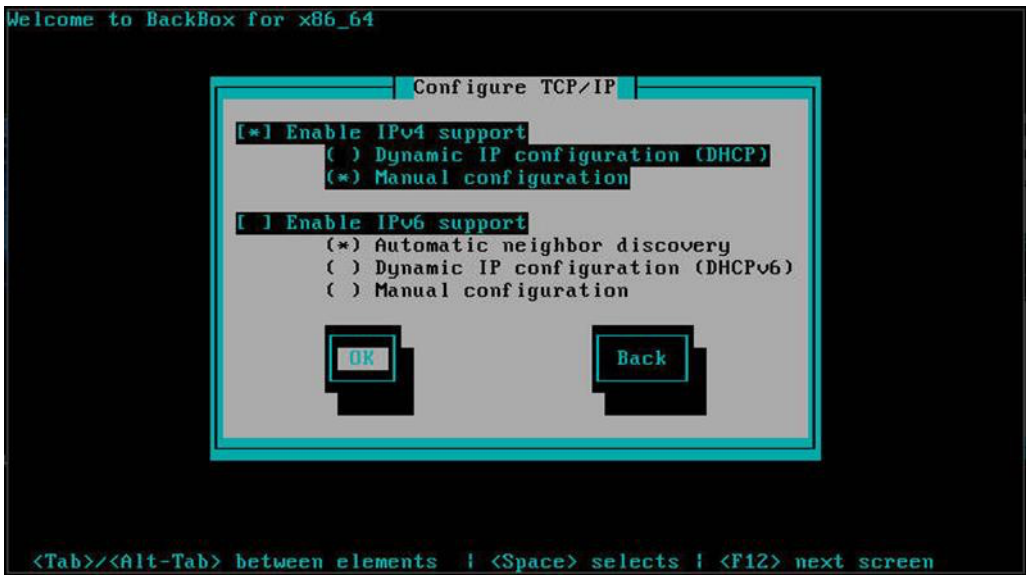


Figure 2: Configure TCP/IP Screen

Specify the TCP/ IP settings for the primary NIC and click OK. If you specify Manual configuration the following screen appears:

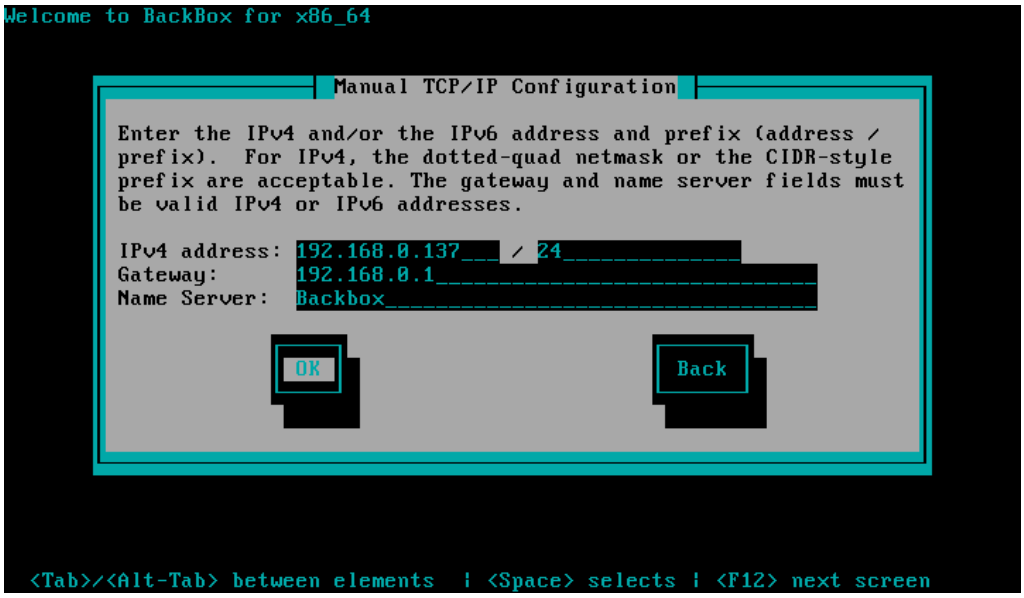


Figure 3: Manual TCP/IP Configuration Screen

Note: If Dynamic configuration is selected then the VM will automatically configure, and the BackBox Access screen appears. See Figure 4.

4. After IP configuration completes, the BackBox Access screen appears:

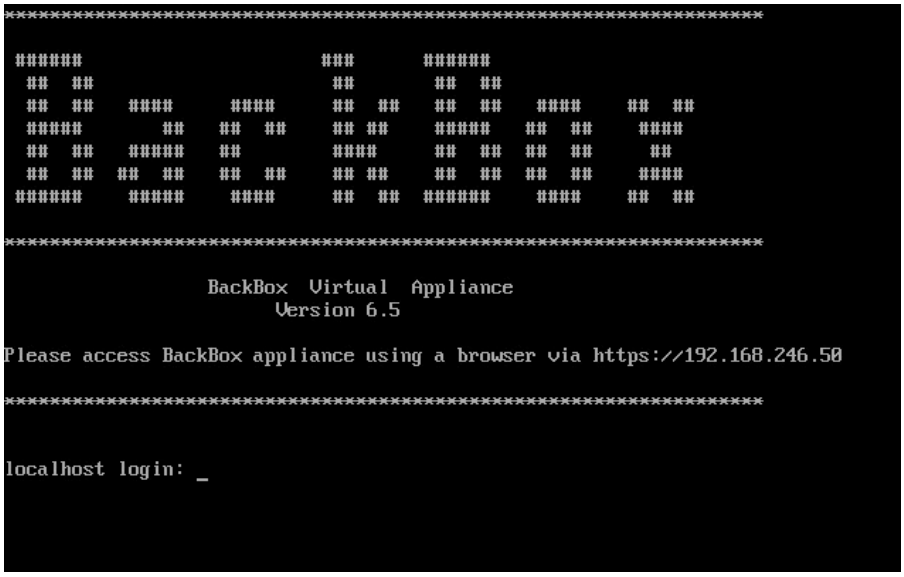


Figure 4: BackBox Access Screen

CHAPTER 3 GETTING STARTED

Logging In

To login to BackBox, in your web browser, enter the IP address or host name:
https://<BackBox_IP_or_Hostname>

The Login screen is displayed:

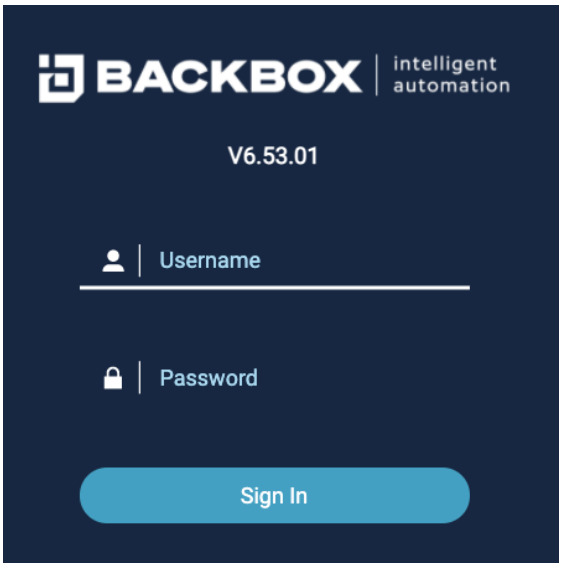


Figure 5: Login Screen

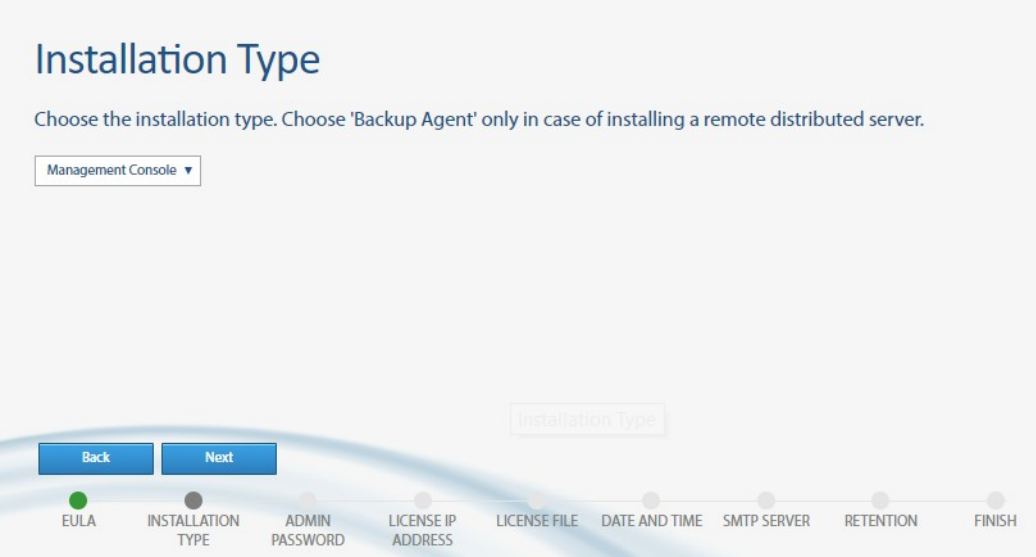
Enter your BackBox Username and Password and press Enter. The following default values appear:

Username: admin
Password: "password" (default supplied with system)

If this is the first time you have logged into the GUI, you will be taken through the First Time Configuration Wizard, to help you get your BackBox instance correctly set up and ready to go.

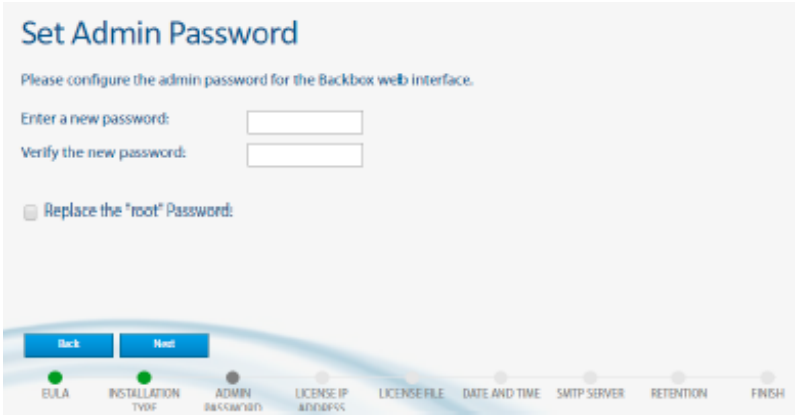
The initial Wizard screen will look like this:

Once you agree to the terms and click Next, you will see this screen:



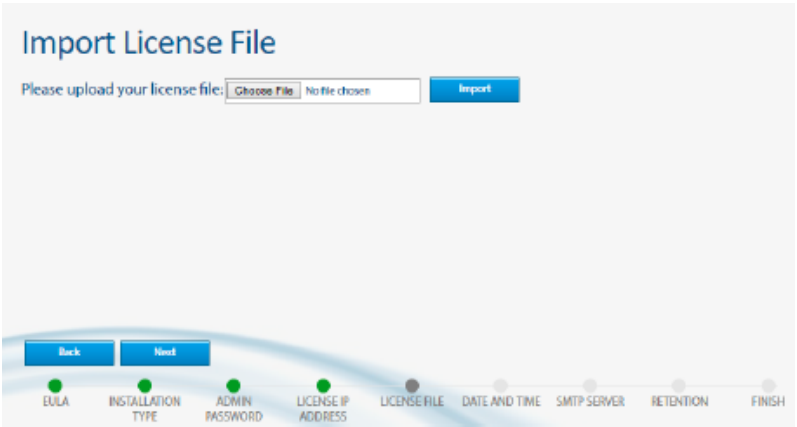
This is where you choose between Management (main unit) or Agent (dependent unit). Agent units are only able to accept commands from a Management unit, so be sure you already have a Management unit before choosing Agent. Click Next when ready.

Best Practice:
BackBox strongly recommends that you change the default passwords for the admin user (admin/password) and the CLI ID root user (root/HayaldaB@gan1).

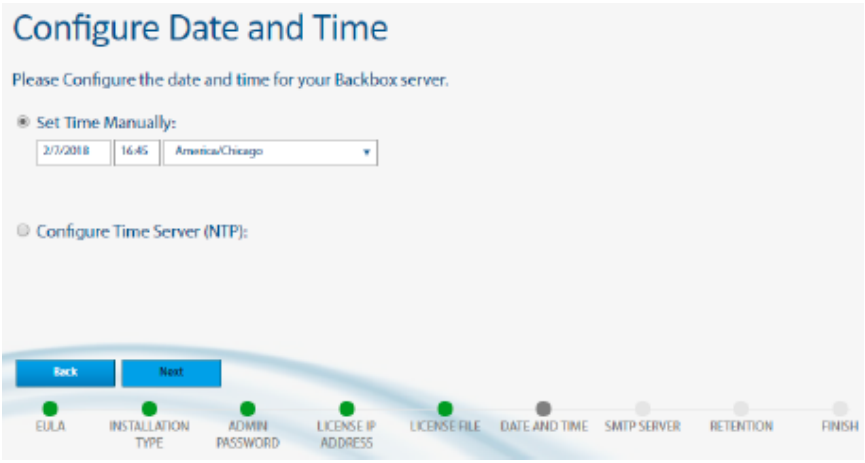


After setting the passwords, click Next.

Ensure the IP address is correct, then click Next.



Browse to your license file and import it. If you don't have it yet, just click Next.

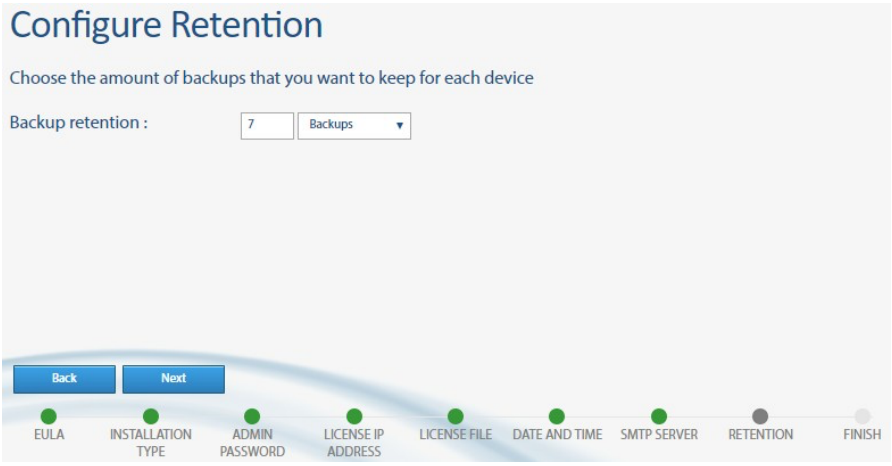


Set the date to the method you prefer, then click Next.

Best Practice: BackBox recommends using an NTP server.

Enter your SMTP information

Best Practice: BackBox recommends setting up an identifying email address such as Backbox@CompanyDomain.com) and click Next.



Configure your global retention option. The default value is 30 meaning there will be 30 backups retained for each device. The number of backups retained will increase storage requirements.

Best Practice:
This should match your company's retention policy for devices. It can be overridden at the device level. More retention requires more storage.

Click Download on the Complete Configuration Wizard screen to download your encryption key.

Best Practice:

Store the encryption key in a safe place. Your key is unique to your installation. Click Finish to implement your choices and then restart Backbox.

After restarting, the Login screen reappears. When you login again, the Dashboard's System Status screen is displayed.

Dashboard System Status Screen

The Dashboard System Status Screen looks like this:

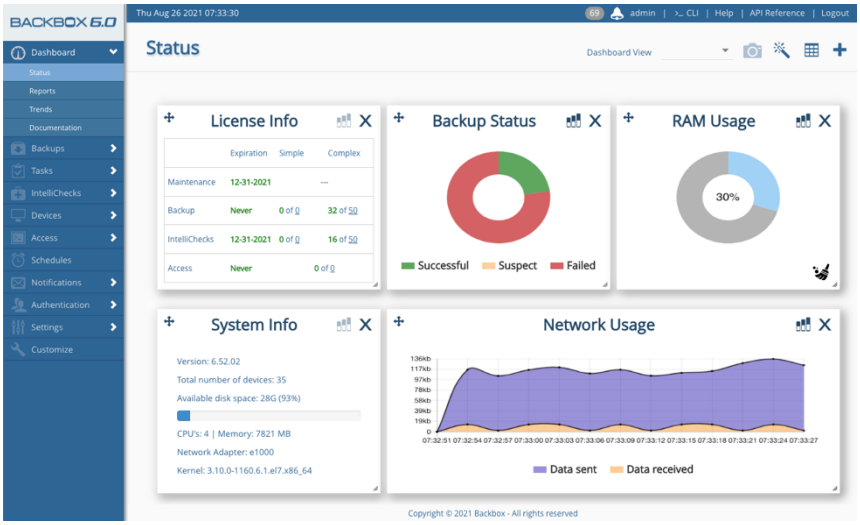


Figure 6: Dashboard System Status Screen

At the top left of the screen are displayed the time and date. On the right side are an Alerts button as well as buttons for Username, Help and Logout. Clicking the Alerts button displays the Notification Alerts screen. (The button is highlighted when there are indeed notification alerts.) Clicking on Help displays BackBox Online Help.
CLI: >_ CLI open a CLI window to BackBox.

The dashboard includes widgets that the user can add or remove.

There are two types of widgets, system widgets, and automation-related widgets. See Understanding the Dashboard covered later in this guide.

Best Practice:

Users can also create separate views and replace them in the dashboard view dropdown.

The BackBox Interface: Screens and Tables

Aside from the Dashboard Status screen, BackBox screens consist of tables that display information on backups, devices, health checks, etc. BackBox tables are dynamic – that is, you can choose the columns to display and, in many cases, you can group rows to make a more readable display.

Configuring Table Columns

At the right of each table is the Columns button ≡ . Clicking the Columns button ≡ displays a list of columns to choose from. Select the columns you want to display in the table and click outside the list to return to the table.

You can change the width of a column by placing your mouse cursor at the right side of thecolumn's head and dragging the column guide right or left to widen or narrow the width; forexample, in the following screen, the Notification column will be altered by dragging:

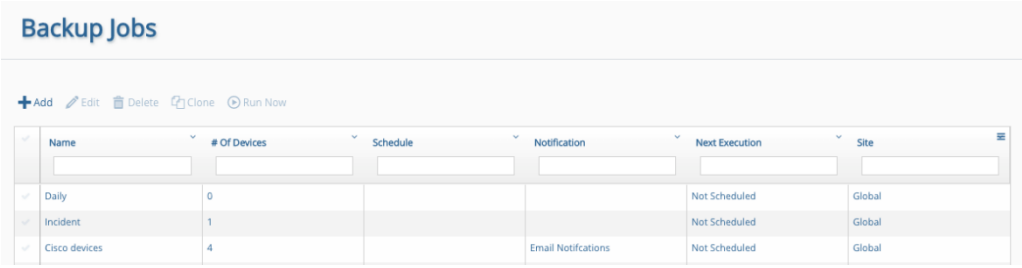


Figure 7: Changing the Width of a Column

You can also reposition columns by pressing on an empty space in a column's head and dragging the entire column right or left.

Sorting a Table

You can sort tables by any column by clicking the Sort button ⌄ located at the right side of the head of the column by which you want to sort; a menu like the following is displayed:

Figure 8: Column Sort Menu

Select an option and click outside the menu. For a quick sort, just click the column's name at the top of the column: clicking the name toggles between Ascending and Descending sort orders.

Grouping Table Rows

For some tables, BackBox enables you to group multiple rows into one row according to selected criteria. To group rows, click the Sort button in the head of the column by whichyou want to group the rows, to display a menu as in the following screen:

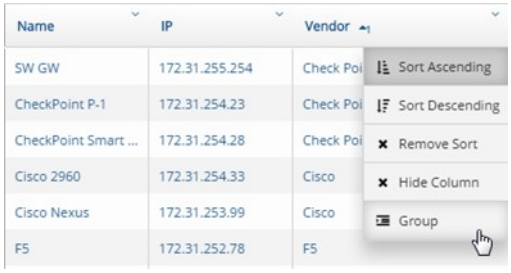


Figure 9: Example of Group Option

By clicking Group in the above example, the table's rows with identical vendors will be collapsed into single rows; each row indicates how many items have been grouped, like this:

Figure 10: Example of Grouping According to Vendor

Clicking the Expand/Collapse buttons / in the left column of a row displays/collapses the rows underneath, like this:

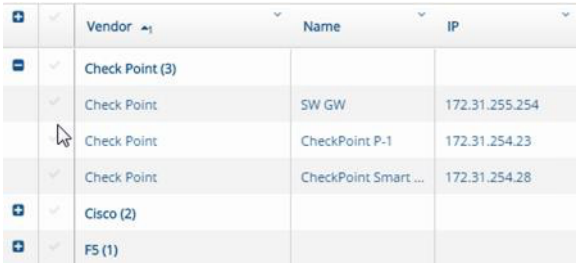


Figure 11: Example of Expanding a Grouped Row

By using the features to display and sort columns and to group rows, you can create easy to read tables that give you the data you need.

Filtering Tables

To filter a table, click the Filter box. You can also filter for more than one value. The following example shows a table with the filter value “Cisco” in the Vendor column and “Successful” in the Status column:

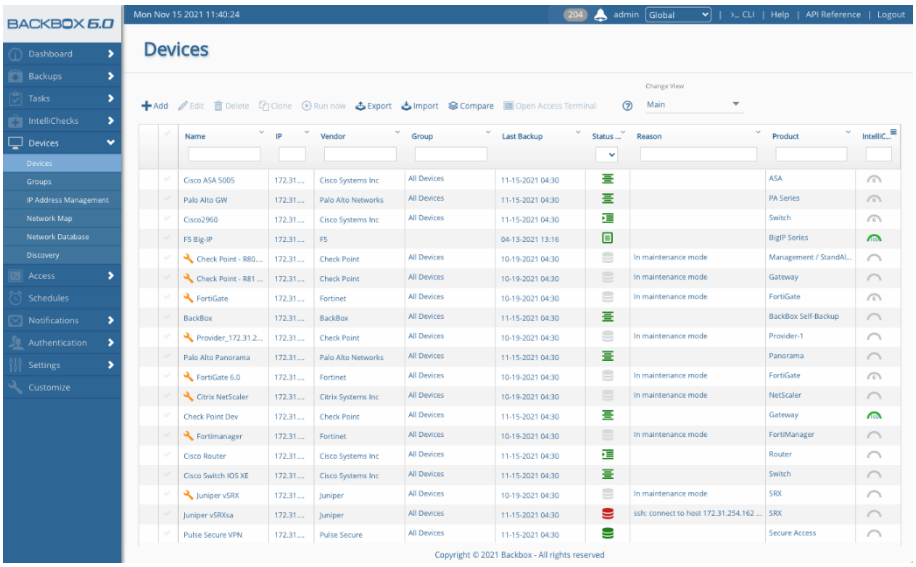


Figure 12: Example of a Filtered Table

Understanding the Sidebar

The Sidebar enables you to quickly navigate BackBox screens:

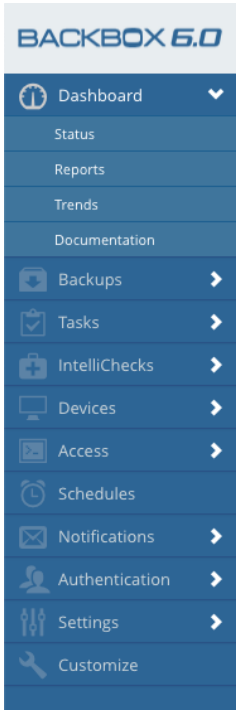
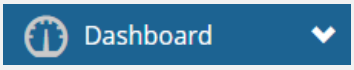
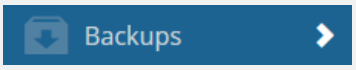
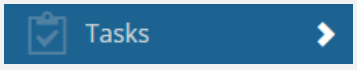
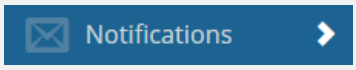
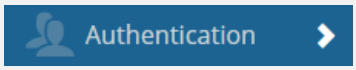
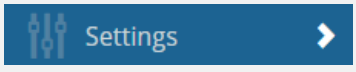


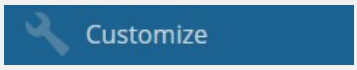
Figure 13: Sidebar Screen Navigation Buttons

Table 1: Functions of Sidebar Screen Navigation Buttons

Button	Description
	The dashboard has four options: • Status displays System Information, License Information, Network and RAM Usage, as well as the status of Device Backup and Health Checks. • Reports displays the list of reports Backbox has been set to generate. Here you can add, edit, and delete reports as needed. • Trends is where you can create your own Trending graphs, based on the tracked data you want displayed. • Documentation is where you can view links to vendor documentation for devices.
	Backups enables you to create, schedule, and run backup jobs. Backups includes the following four options: • Jobs is where you specify which devices run on which schedule. • Queue is where you can see which jobs/devices are currently running. • History will show you all the jobs that have run, the time, and their status. • Exports allows the exporting of backups to AWS or other remote locations.
	Tasks enables you to automate, schedule, and track various activities to be performed on devices in your system. Tasks includes the following options: • Configuration is where you can see the existing tasks that can be cloned and/or run. • Quick tasks tab enables you to run tasks on-demand tasks without the need to schedule them. • Jobs will allow you to schedule tasks to run on specified devices. You can chain existing tasks together into a single job. • Queue will show you any currently running tasks. • History shows all tasks that have been run, the time, and the status. • File Repository contains files that you want to reference in tasks, be it configuration files to copy, or patch files to be used for upgrades.

IntelliChecks	IntelliChecks enables you to decide which health checks you wish to run on a set of devices. This is also where you can run tests for specific devices to ensure that their configuration is following organizational guidelines. IntelliChecks contains the following six options: • Signatures shows you all the existing signatures available. • Groups enables you to set several signatures as a schedulable collection. • Jobs allows 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. • Technical Survey allows the user to add fields that he will be able to save IntelliChecks info into them and show them in the technical survey report.
Devices	Devices is where you can manage backups and restores, and functionality around your infrastructure. Devices has four options: • Devices is where you can add/edit/remove device profiles, and view statuses for a device's tasks backups, and IntelliChecks. • Groups will allow you to set functional or operational hierarchies to simplify management. • IP Address Mgmt. will show you your IP segments and their members. • Network Map will graphically display all devices and show how they connect to each other. With Discovery the user will able to scan the network with SNMP and add devices automatically to BackBox with defined rules.
Access	Access is the Jumpbox functionality module. It enables you to use BackBox to run commands and scripts directly on devices within the system. Scripts can include task, health checks, IntelliChecks, and backup scripts. The chapter on Writing Command Scripts has detailed information on syntax and grammar.
Schedules	Schedules is where you to create, modify, and delete schedules used for backups, tasks, IntelliChecks, and reports.

	Notifications enables you to configure and view notifications for failed actions. Notifications has two options: • Alerts serves as an internal bulletin board that can show failed/suspect actions for any device. Alerts will send output to the internal Notification-Alerts screen. • Jobs is where external notifications can be configured for combinations of Email, Syslog, SNMP, and HTTP.
	Authentication enables you to create groups out of the devices that share authentication details. Authentication Authentication divides to two parts. • The first one is local Authentication which relates to ways to authenticate to BackBox itself. • The second one is device authentication which refers to ways to authenticate to the devices. Options: • Authentication Templates allows for simplifying password mgmt. by entering credentials into a single field that can be used for many devices of a given type. • Authentication Servers is where you choose an authentication method (RADIUS, TACACS, LDAP, SSH, or CyberArk). • Backbox Users is where you create users (individuals or groups) who can access the GUI. • User Roles allows for RBAC. Unchecking the Read attribute will result in that section not being displayed for the given role. • Operating System Users is used to create landing zones for devices that write backups to BackBox, with an associated local credential set. • Connected users show you which users are currently connected to BackBox.
	Settings enables you to set parameters for your BackBox instance. Settings contains twelve options: • Access Rules restricts routes to BackBox. • Administration is where you set global retention policy, encryption, backup retry, proxies, and clustering (HA) This is also where patching, SSL certificates, and GUI customization are handled. • Agents allows for the management of the remote Agent VMs. • Alerts is where you set up SNMP traps and Syslog destinations. • Auditing allows for easy monitoring of BackBox's actions, via Auditing, Messages, and Vsftpd, general and security logd • Date and Time manages time zones and date formats. • DNS allows for DNS server entries. • Interfaces allows you to set IP addresses, speed, and DHCP status. • Licenses allows for license management.

	• Routing displays the routing settings and allows you to add/edit a route. • Sites is where you manage multi-tenancy groupings, their license and retention settings.
	Customize enables you to clone and customize or create new BackBox scripts that perform various activities.

Understanding the Dashboard

The Dashboard provides general information about BackBox and the computer on which it is running. You can configure the Dashboard with many different widgets as explained in this section. A typical Dashboard looks like this:

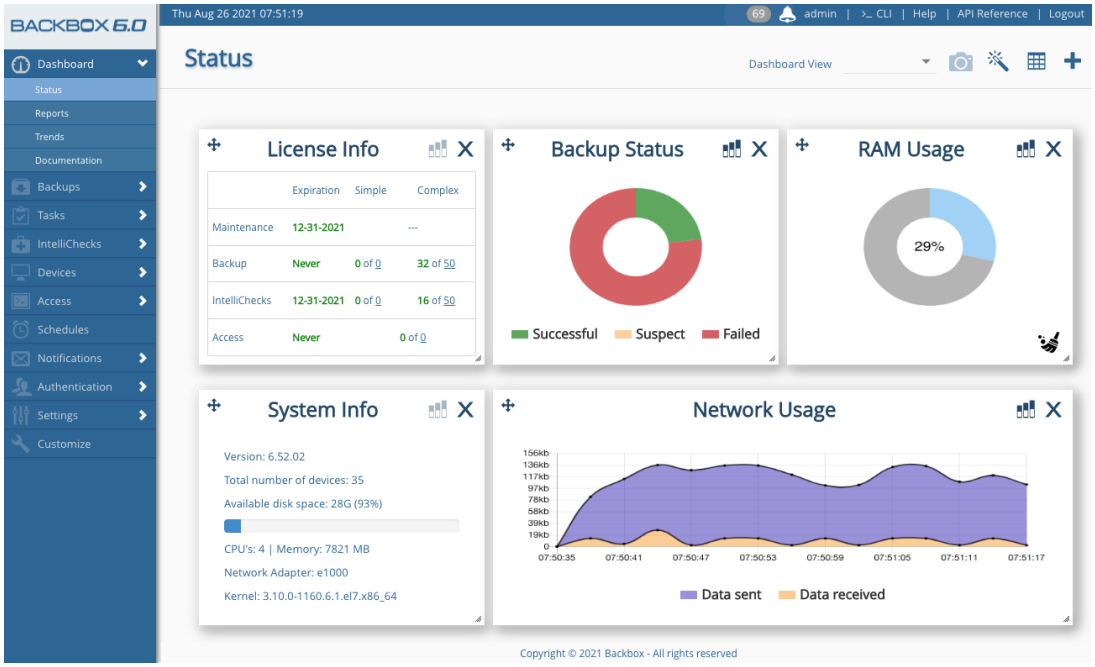


Figure 14: System Status Screen

Configuring the Widgets

You can easily configure the widgets shown on the dashboard by clicking the Add a Widget symbol + in the upper left corner of the screen. After clicking, the following window appears:

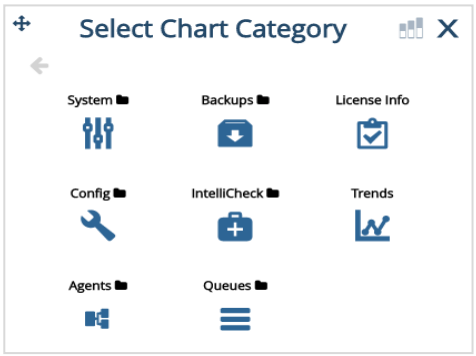
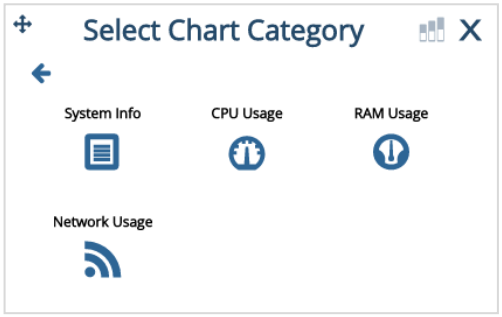


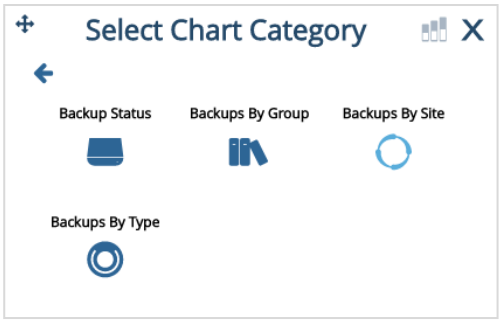
Figure 15: Widget Menu

Click on the widget you want to add. The following sub-menu is displayed (if applicable):

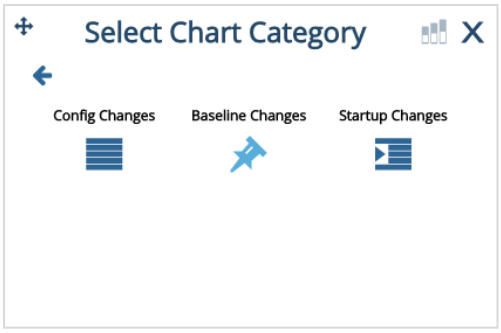
System



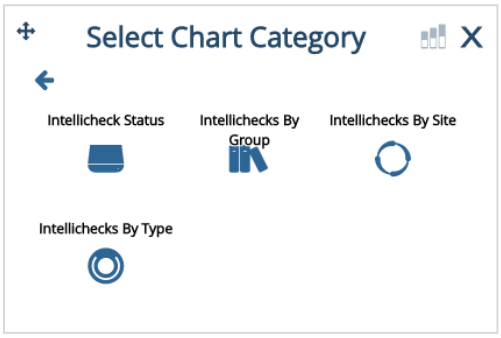
Backups



Configure



IntelliChecks



Trends

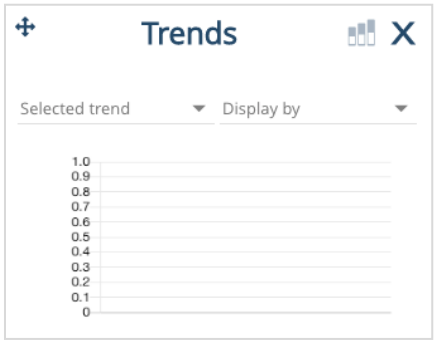


Figure 16: Widgets Sub-menus

Selecting Trends displays a dropdown menu that lets you decide according to which IntelliChecks group or single signature you wish the Trends graph to display data.

For graphs that support multiple display formats you can choose a format by clicking the ChartDisplay icon (three bars), and then making your choice from the dropdown menu.

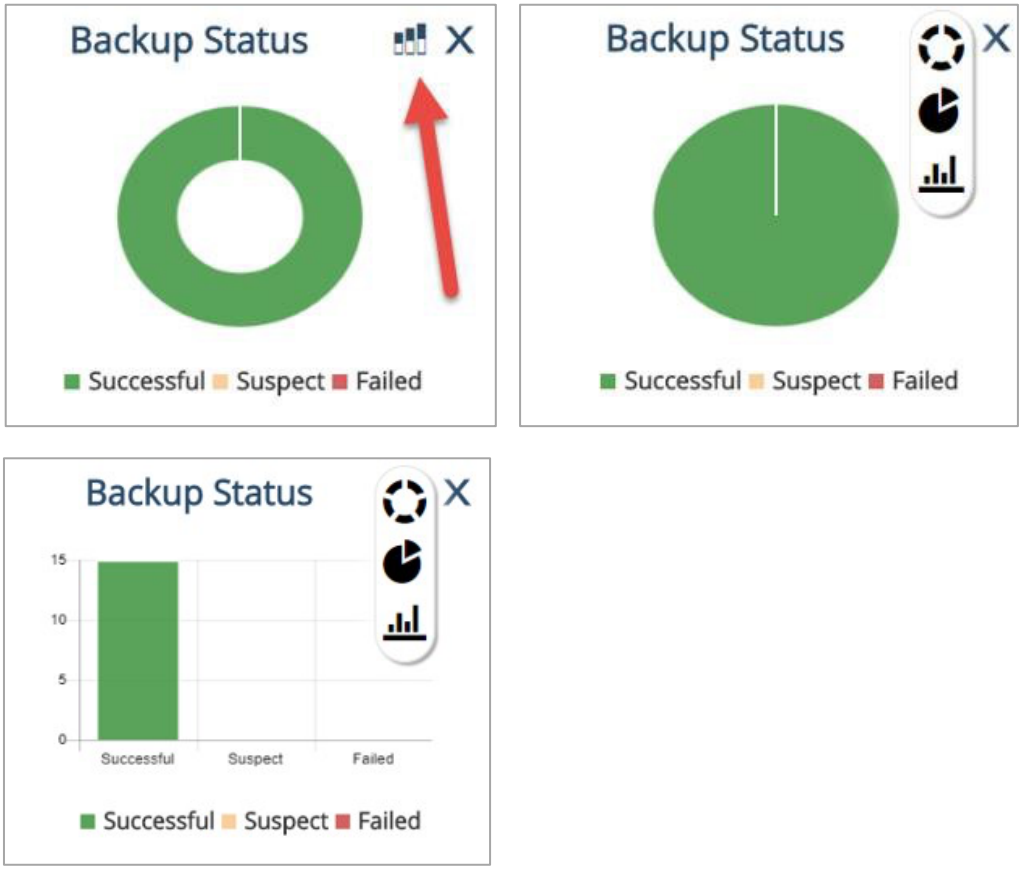
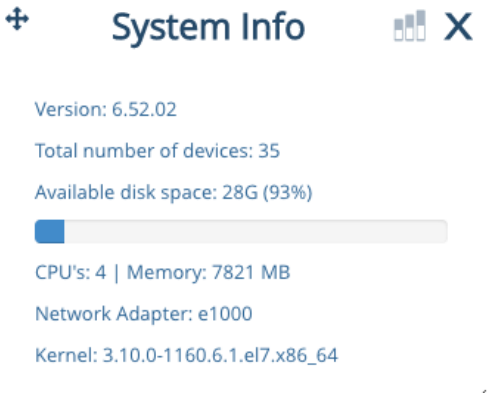
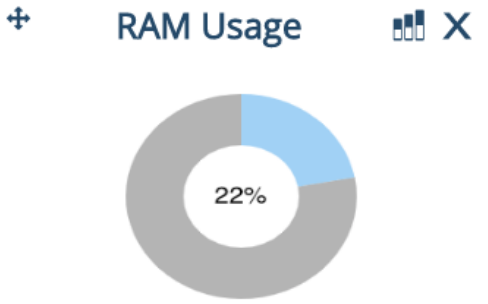
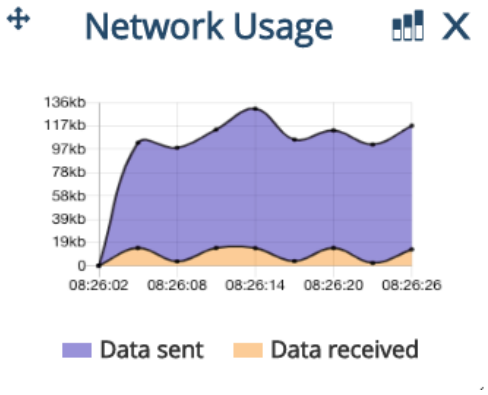


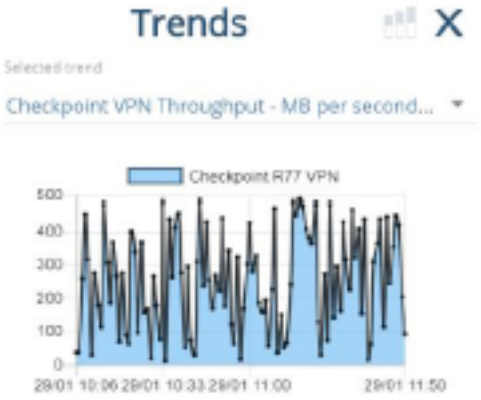
Figure 17: Charts Display Options

Table 2: Widgets

Widget	Description
	Backup Status displays a chart showing the statuses of the device backup operations performed: Successful, Suspect, and Failed. Clicking on a status on the chart displays the Devices screen with only the devices for that status listed. In addition to the All Devices view, you can sort by type, by group, and by site.

Widget	Description
	System Information displays the version you are running, total devices, available disk space in both, the number of Gigabytes and the percentage of disk used, as well as a bar graph. Clicking available disk space displays the Devices Disk Usage screen. The Devices Disk Usage screen shows all devices, their usage, and whether they are using global, local, or no retention settings. CPU and Memory information are also displayed.
	RAM and CPU Usage show data points related to their respective statistics. You can choose Real-Time, Daily Avg, or Monthly History.
	Network Usage displays the amount of network bandwidth being used by BackBox on a real-time basis. You can choose to display the values by Real-Time, Daily Avg, or Monthly History.

Widget	Description
	License Information displays detailed license numbers for every module, with color coding to indicate when the license is within 30 days of expiration (yellow) or expired (red).
	Config Changes displays the percentage of devices whose configuration was changed or remained the same as detected in the backup. There are separate widgets for configuration changes by startup and baseline.
	IntelliChecks displays the status of signatures that have been run for a specified device list. IntelliChecks can be displayed according to Status, Group, Site, and Type.

Widget	Description
	Trends is where you can view graphical displays over time for specified statistics on devices you choose. Last value option will always give you what was the result of the last automation running.

Dashboard view gives the user the option to create several views of widgets and replace between them.

CHAPTER 4 SETTINGS

Settings displays a list of options that enable you to access various functions. Only the administrator has access to Settings.
On the Sidebar, clicking Settings, defaults to the Interfaces screen.

The following table provides an overview of the screens accessible from Settings.

Table 3: Settings Screens

Screen	Description
Access Rules	Displays the settings that control the local Firewall of the BackBox server. This determines which IP address can access the web interfaces and the CLI interfaces.
Administration	Displays general settings for backup retention, execution time, and server IP address.
Agents	Displays a list of agents and their IP addresses. It also shows which operating systems are assigned to the agent.
Alerts	Displays the fields for setting alert protocols. There are three different protocols: SNMP, SMTP, and Syslog.
Auditing	Auditing gives the ability to view the logs of BackBox, including audit logs, messages, VSFTPD etc.
Date and Time	Displays the fields where the date and time are set. The time can be set as Static or NTP.
DNS	Displays the DNS settings that specify the location of the domain name servers.
Interfaces	Displays the interfaces which define the connections to the devices in the system and whether the link is up or down. They are used in routing entry definitions.
Licenses	Enables uploading a license and displays license information.

Screen	Description
Routing	Displays the routing tables of the BackBox servers.
Sites	Displays information about existing sites, such as the number of devices assigned, and the number of users. You can also add, delete, and edit sites.
System Logs	Displays a detailed log of each user's activity while in the system.

Interfaces

Interfaces displays basic network information. When the Status button is green, it indicates the link is up; when it is red, the link is down.

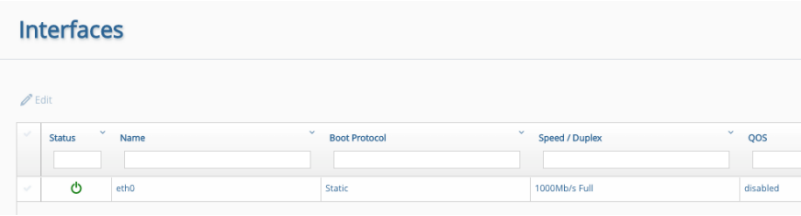


Figure 18: Interfaces Screen

Editing an Interface

You can edit the interface by selecting the interface you want to edit and clicking the Edit button . You can edit the IP address, subnet mask and other settings as shown here:

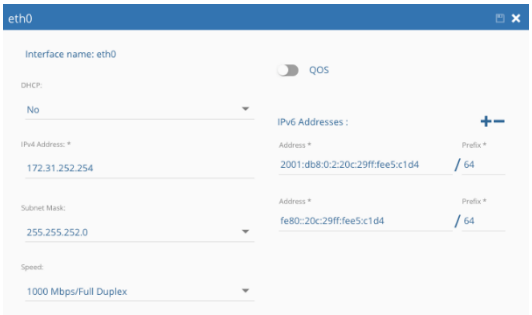


Figure 19: Edit Interface Dialog Box

Edit the fields and click Save.

Routing

To display the Routing settings, click Routing:

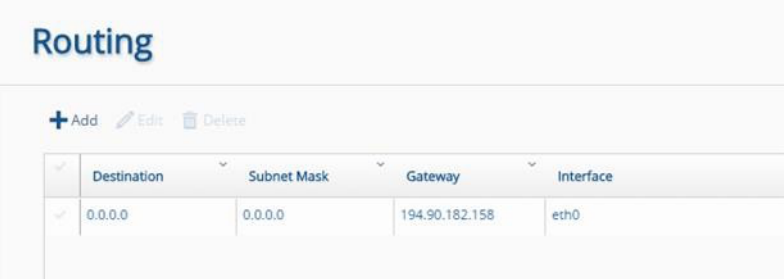


Figure 20: Routing Screen

Adding or Editing a Route

You can add or edit a route.
To add a route, on the Routing screen, click the Add button Add . The New Route Configuration dialog box appears:

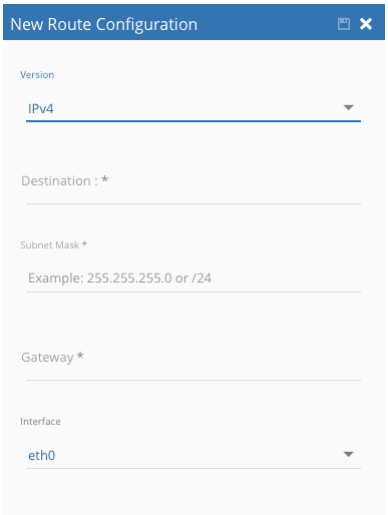


Figure 21: New Route Configuration Dialog Box

Fill in the fields and click Save.
To edit a route, on the Routing screen, select the route you want to edit and click the Edit button .
Edit the fields and click Save.

Deleting a Route

To delete a route:
In the list of routes, select the route you want to delete and click the Delete button Delete
You are prompted to confirm the delete. Click Yes.

DNS

On the DNS screen you can define primary, secondary, and tertiary settings as well as a domain name.

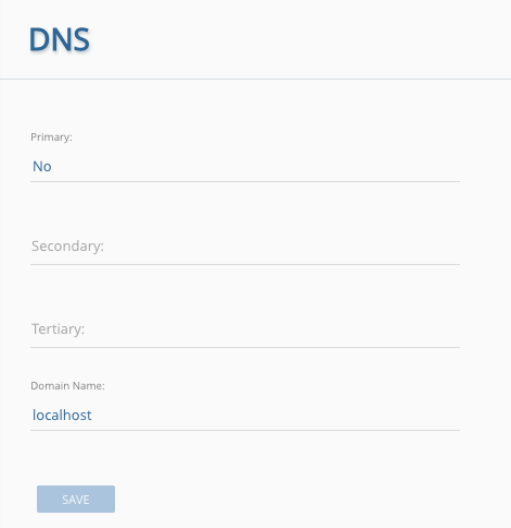


Figure 22: DNS Screen

Date and Time

The Date and Time screen, enables you to configure the date and time:

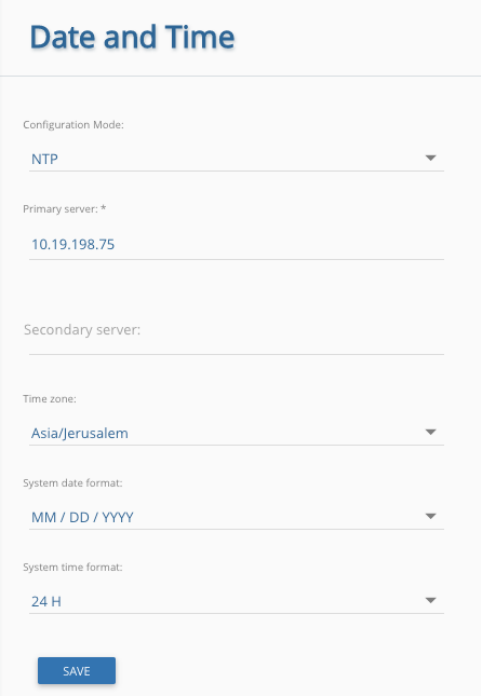


Figure 23: Date and Time Screen – NTP View

Note: The tab defaults to the NTP (Network Time Protocol) view. Click the Static button to view the current date, place, and time.

Alerts

The Alerts screen enables the administrator to create the following alert protocols: SMTP, SNMP monitoring, SNMP traps, Syslog, and HTTP.

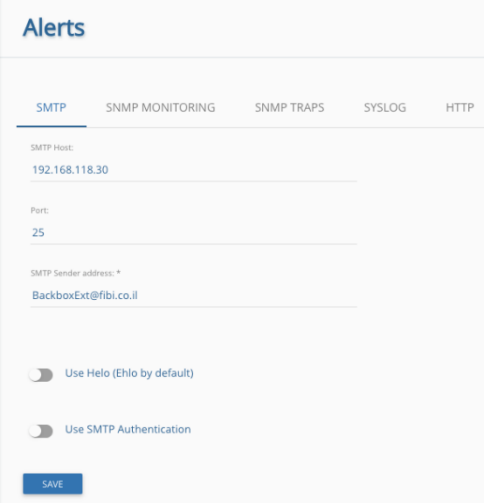


Figure 24: Alerts Screen

Note: The SNMP monitoring and SNMP traps have three versions to choose from: v1, v2c, or v3. Each version has different fields to be completed. Complete the appropriate fields in the desired protocol and click Save.

Administration

The Administration screen is used to add and edit general settings, perform maintenance tasks, implement customizations such as uploading a logo, and create clusters of devices:

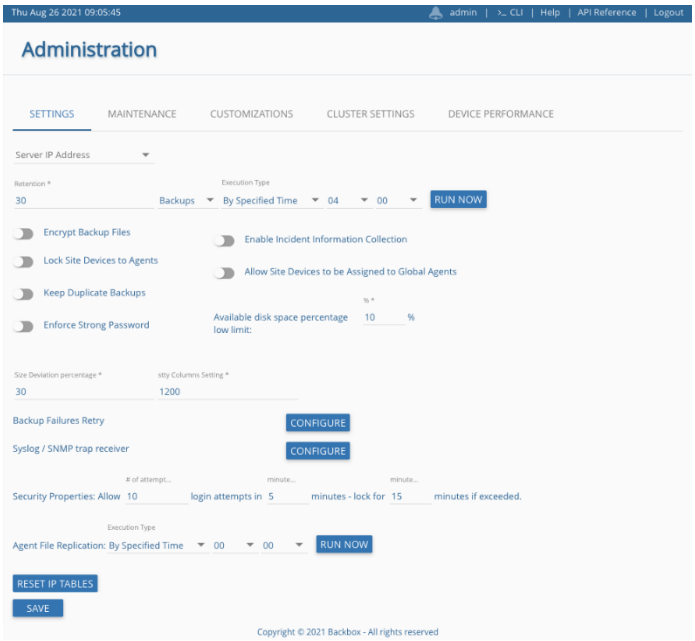


Figure 25: Administration Screen

Settings Tab:

Table 4: Settings Tab

Field	Description
Backup Retention	Can be set for either the number of backups to keepor a retention policy before deletion occurs.
Execution Time	Specified time to run the retention checks.
Encrypt Backup Files	Files may be encrypted while at rest using AES-256
Lock Site Devices to Site Agents	Enables/disables locking site devices to site agents.
Keep Duplicate Backups	Enables/disables option to keep only unique backups.
Stty Columns Setting	Linux default setting for STTY.
Backup Failures Retry	Instructs BackBox to use retry parameters should a backup fail to complete.
Syslog/SNMP Trap Receiver	Allows for Trap Receiver configuration.
Server IP address	Select the server address to be matched against the license
Enforce strong passwords	BackBox will start to enforce strong passwords you enter into the GUI
Enable incident information collection	Helps integrate with 3rd party software ticketing systems
Allow site devices to be assigned to global agents	Devices in sites will be allowed to be assigned to global agents

Available disk space percentage low limit	Control when BackBox will alert on low disk space
Size deviation	Control the default size deviation alert
Security properties	Control login attempts and time outs
Agent file replication	Control when will agent replication occurs
Reset IP tables	Rebuild the IP tables from scratch
Device performance	control parameters for performance feature

Maintenance Tab:

Table 5: Maintenance Tab

Field	Description
Upgrade to New Version	Uses hotfix zip files to upgrade/patch.
Restore Configuration	Restore BackBox configuration from backup file.
Rollback to version X	Allows for rollback to previous working version.
Backup (Config only)	Backs up the configuration of the BackBox instance. Can also select if to include files in task repository and also external backup and OS users directories
Download Tech Support Info	Downloads and zips the common log files.
Clear SSH Keys	Wipes out existing keys and forces reloading for all SSH keys.
System	Allows for Reboot or Shutdown of VM from the GUI.
Proxy	Enter the Name, Port, and creds for the Proxy

Customizations Tab:

Table 6: Customizations Tab

Field	Description
Upload Custom Logo	Replace the default BB logo with another logo.
Restore Default Logo	Restore the default BB logo.

Field	Description
Configure SSL Ciphers	Allows specifications of which ciphers are allowed or disallowed.

Cluster Tab:

Table 7: Cluster Tab

Field	Description
Enable Cluster	Enables HA clustering.
Cluster Role Selection	Choose primary or secondary role for the instance.
Cluster IP Entry	Enter the IP of the target cluster member.
Shared key	Unique key to authenticate the cluster members.
Sync Schedule	Set the scheduled sync time.

Licenses

The License screen enables uploading a license and displays information about the current license. The fields are populated when the license is uploaded.

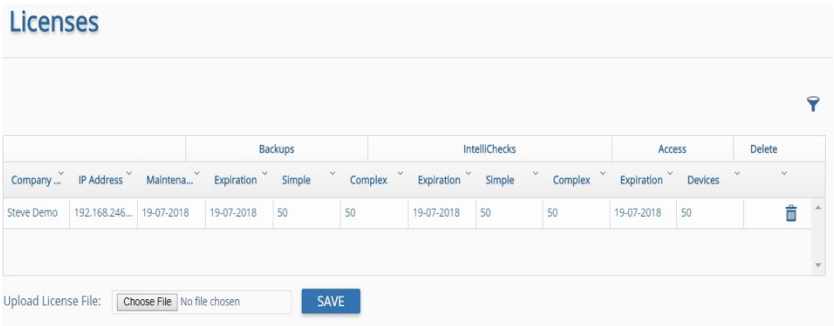


Figure 26: License Screen

Access Rules

The Access Rules screen allows the administrator to control the local Firewall of the BackBox server. This determines which IP address/network can access BackBox via SSH, the web interfaces, or the CLI interfaces.

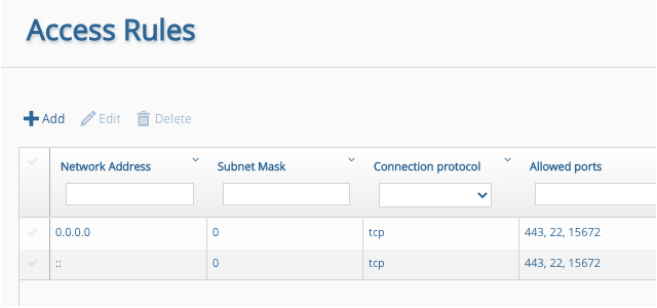


Figure 27: Access Rules Screen

To add an Access Rule, click Add to display the following dialog box:

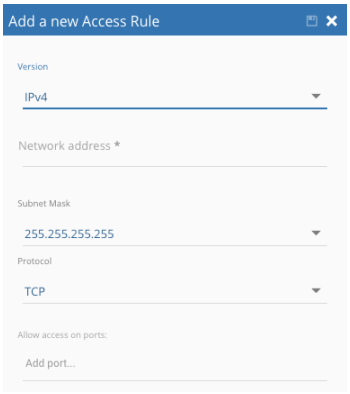


Figure 28: Add Access Rule Dialog Box

Specify the desired settings and click Save.

Sites

A site is a logical partition which contains devices, device groups, templates, or backup instructions. It is a mechanism used by the Global administrator to delegate administration of all aspects of the BackBox application to local servers. These local servers are managed by site administrators who control the configuration, notifications, and backup jobs. Creating sites is an efficient and effective way to help organize and manage the devices and backups in larger and more complex installations.

Sites help users know what devices they are authorized to access. Sites can be assigned based on the combination of geographic location, device type, and whatever other criteria the Global BackBox Administrator may determine is useful for their BackBox installation.

On the Sidebar, under Settings, click Sites:

Figure 29: Sites Screen

For each site, the Sites screen displays site information, including site name, and number of devices, users, retention (how long backups are retained), and the number of simple and complex licenses for backups and IntelliChecks.

Adding a Site

1. On the Sites screen, click the Add button Add to display the New Site Configuration dialog box:

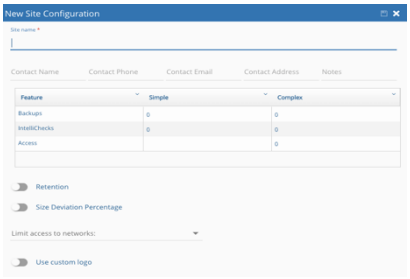


Figure 30: New Site Configuration Dialog Box

2. Type a name for the site, fill in the appropriate fields, and click Save. The new site is displayed in the list.
3. Choose if to override global size deviation verification of backups to site
4. Create access rules to networks
5. Add logo to site

Editing a Site

1. On the Sites screen, in the list of sites, click the site whose settings you want to change and click the Edit button .
2. Make the relevant changes and click Save.

Deleting a Site

1. On the Sites screen, select the sites that you want to delete and click the Delete button Delete
   A prompt appears requesting confirmation.
2. Click Yes to confirm.

Agents

Agents are used to manage backups when there are larger installations with multiple servers in an off-site network. On the Sidebar, under Settings, click Agents. The Agents screen appears:

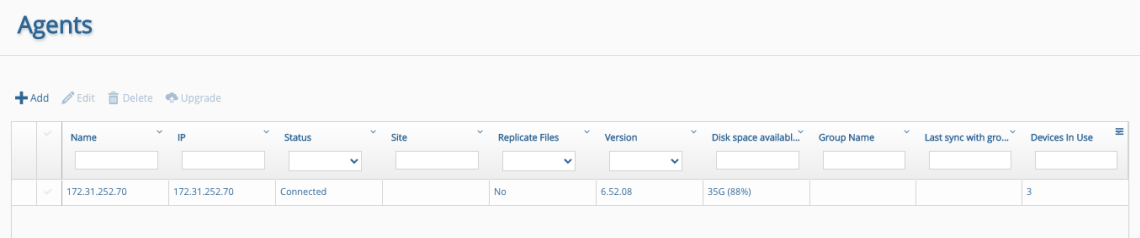


Figure 31: Agents Screen

Adding an Agent

1. On the Agents screen, click the Add Add button. The Configure New Agent dialog box appears.

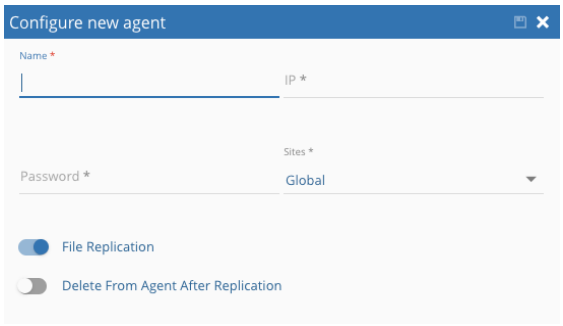


Figure 32: New Agent Configuration Dialog Box

2. Fill in the agent's name, IP address, password (customer created and used to authenticate the mgmt. and agent instances to one another), and site; then click Save.

Note: File Replication will result in backup files from the Agent being copied back to the Mgmt. server, resulting in redundant backups. Replicate and delete option will first copy the file to the management and then erase it from the management.

Editing an Agent

You can edit the details of an agent, as well as the agent's OS users.
To edit the details of an agent:

1. On the Agents screen, in the list of agents, click the agent whose settings you wantto change and click the Edit button .
2. Make the relevant changes and click Save.

Upgrading an Agent

You can upgrade an agent to a new version by clicking the Upgrade button Upgrade .

Deleting an Agent

1. On the Agents screen, select the agent to be deleted.
2. Click the Delete button Delete . A prompt requesting confirmation appears.
3. Click Yes.

Auditing

BackBox allows administrators to audit each user who accesses the system. The program keeps a detailed log of each action performed in the system, as well the object of the action. The log details each time a user logs-in, adds, updates, or deletes. It also records the objects of these actions such as devices, backup jobs, time and date, etc.
For example, if a device group is changed, the log will show which user made the change,what the change was, when it was done and whether the change was successful.
When you click Auditing, the following is displayed:

Figure 33: Auditing Screen

The screen displays five types of logs: Auditing, Messages, Secure. General and Vsftpd. These are explained in the following sections.

Viewing the Audit Logs

To view the audit logs, click the View Log button. in the View column of the Auditing row. The Audit Log screen appears:

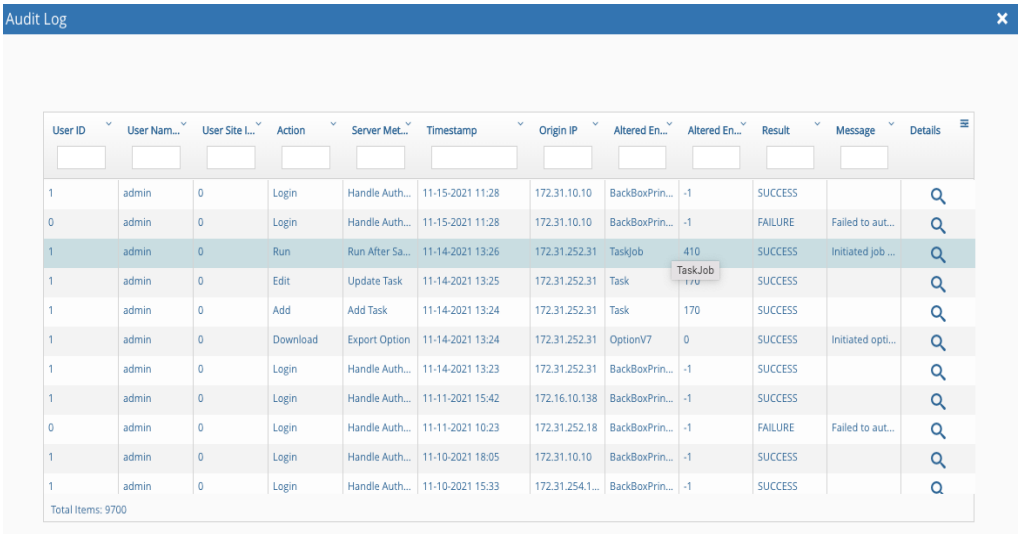


Figure 34: Audit Log Screen

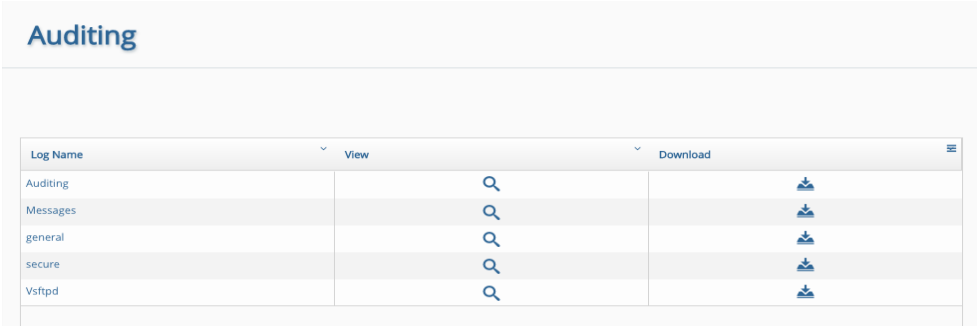


Figure 35: Auditing Screen

Table 8: Audit Log Filter

Criterion	Description
User ID	System ID of the user
User Name	Name of the user
User Site	Site of the user

Timestamp	Date and time
Origin	Origin IP of the user made the changes
Screen	The screen that was accessed
Action	You can filter for the following actions: Login, Add, Update, Delete
Server Method	What call to the server was made
Altered entity	What entity was changed during the action
Altered entity ID	The id of the entity that was affected
Result	What was the result of the action
Message	Display message output of the action

On some of the items displayed, there is more detailed log information available. To view the additional log details, click the View Change button at the end of the row. The Audit Details Log screen appears:

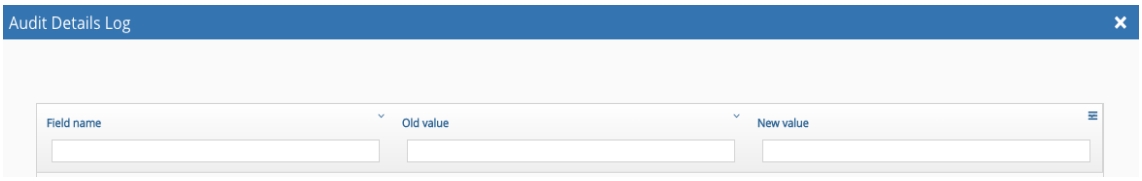


Figure 36: Audit Details Log Screen

Note: Each object will display different details in the log.

Viewing the Messages Log

The Messages log shows a trail log from the BackBox operating system (/var/log/messages). To open the Messages' Trail Log screen, in the System Logs screen, click the View Log button in the View column of the Messages row. The Trail Log screen appears:

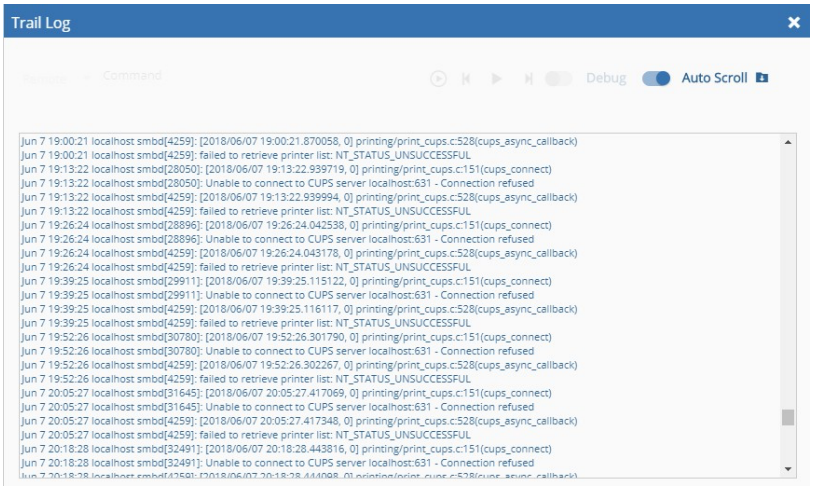


Figure 37: Trail Log Screen

You can download message logs to your computer by clicking the Download Log button at the end of the Messages row.

Viewing the VSFTPD Log

VSFTPD shows the BackBox VSFTPD log (/var/log/vsftpd.log).

To open the VSFTPD's Trail Log, click the View Log button in the View column of the VSFTPD row. The VSFTPD Trail Log appears. You can download the VSFTPD log by clicking the Download Log button at the end of the VSFTPD row.

Viewing the Secure Log

The secure log window will show you security events occurring at OS level like SSH login tries ETC.

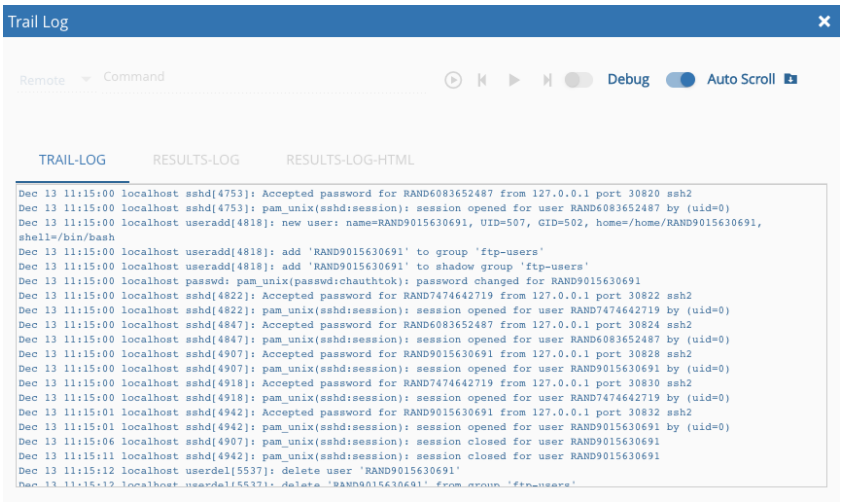


Figure 38: Trail Log Screen

Viewing the General log

Viewing the messages log will show you the general log of the system. The general log contains a handful of things occurring on BackBox and helps debug the system in case of issues.

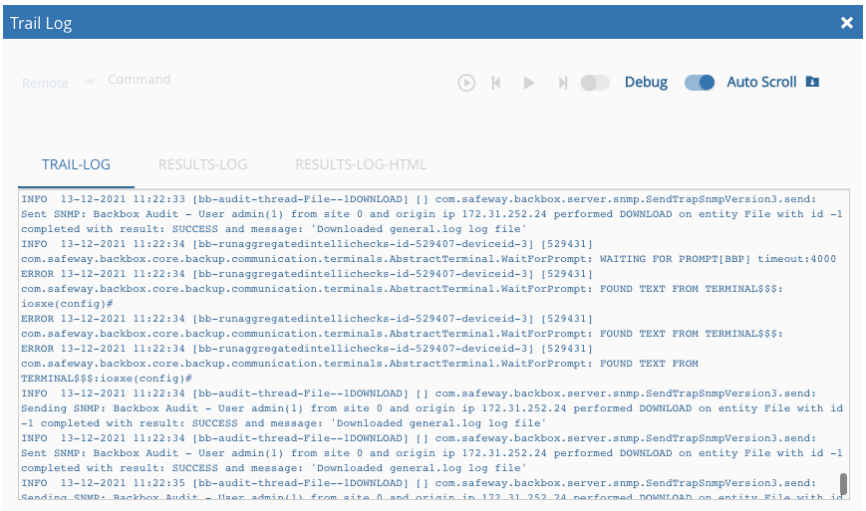


Figure 39: Trail Log Screen

CHAPTER 5 AUTHENTICATION

The administrator controls how users access the system, and the level of permissions they have after authenticating.

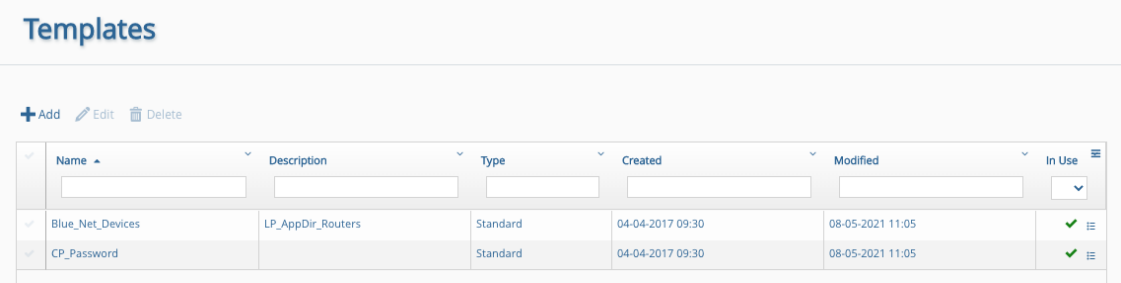


Figure 40: Authentication Templates Screen

Authentication Templates

BackBox allows you to create templates to store common credentials and simplify password management for large groups of devices. When the password for that group changes, you change the password once in the template, causing all the device profiles using the template to use that new password, when running backups, tasks, etc.

To add an authentication template:

1. On the Authentication Template screen click the Add button Add . The Authentication Template dialog box appears:

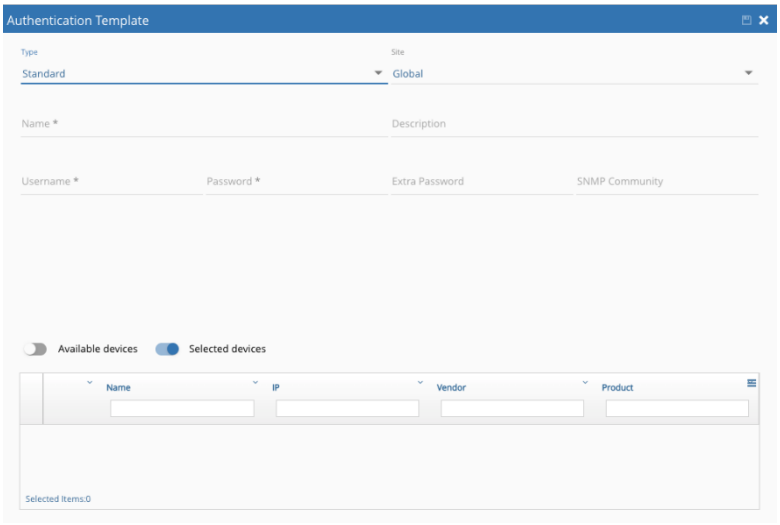


Figure 41: Authentication Template Dialog Box

2. Complete the fields as detailed in the following table and click Save.

Table 9: Authentication Template Fields

Field	Description
Type	Standard creds, CyberArk, Wallix Bastion, Arcon and Thycotic
Site	The site to which the template is assigned (optional).
Name	The name given to the template.
Description	A short description of the template (optional).
Username	Username authorized to access the device.
Password	Password required for authentication.
Extra Password	Field to enter additional passwords, e.g. Expert Mode or othersecondary authentications.
SNMP Community	The SNMP community string (optional).

Deleting an Authentication Template

To delete an Authentication Template:

1. Select the template(s) you wish to delete and click the Delete button

. A prompt appears requesting confirmation.
2. Click Yes.

Authentication Servers

You can specify RADIUS, LDAP, TACACS, or SSH key for authentication methods.

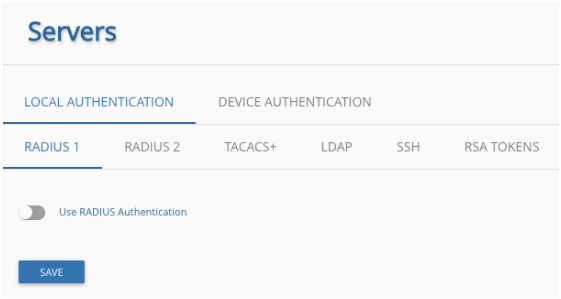


Figure 42: Authentication Servers Screen

Device Authentication

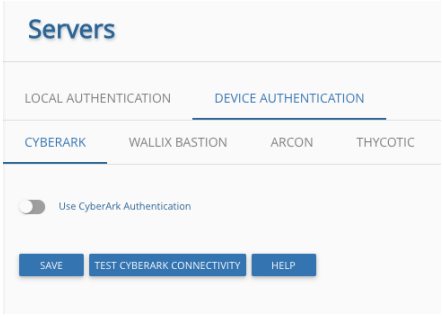


Figure 43: Authentication Servers Screen

Cyberark

To use Cyberark authentication to devices, please select the option.
Help button will give you details about configuring the authentication.
You can test the connectivity to Cyberark with the test button.

Wallix Bastion

To use Wallix authentication to devices, please select the option.
You will need to enter the server IP and the port to use.

Arcon

To use Arcon authentication to devices, please select the option.
You will need to choose the server protocol, server IP, and port.

Thycotic

To use Thycotic authentication to devices, please select the option.
You will need to choose the server protocol, server IP, and port.

BackBox Users

The BackBox Users screen shows existing users and groups, detailing username/group name,email address, site, user role, and account type.

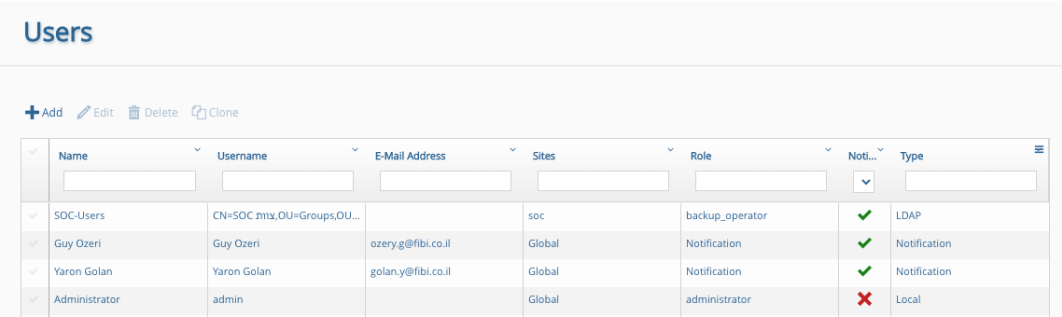


Figure 44: BackBox Users Screen

Adding a New User

To add a new user:

1. In the BackBox Users screen, click the Add button Add to display the Add a New User screen:

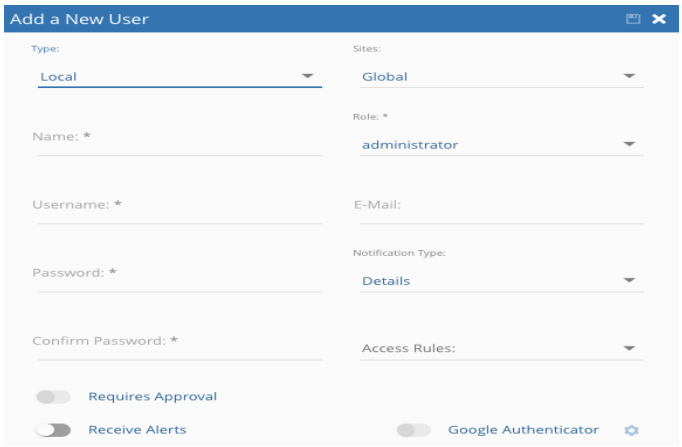


Figure 45: Add a New User Dialog Box

2. Select a type, and specify a name, user name, password, confirm password, and an E-mail address (Notification accounts are used for group email addresses or for distro lists).
3. Specify whether the user is to receive system alerts by clicking the Receive System Alerts button Receive System Alerts : .
4. Select a notification type: Details or Summary.
5. Select a role. For example: Administrator.
6. Optionally, select a site by clicking the the Sites field to display a list of available choices.
7. Requires approval rule let you create users that need permission to run task jobs

8. Select the receive alerts if you want the user to get alerts
9. Select Google Authenticator to allow login with 2FA

Note: Accounts created in the BackBox User section enable access to the web GUI.

Editing a User

To edit a user, in the BackBox Users screen, click the username to display the Edit User dialog box for that user and edit the fields. Click Save .

User Roles

The User Roles screen enables you to create a user role and configure permissions for the role. Permissions can be configured for every part of the BackBox system. For example, you can configure a role so that someone with that role can only initiate a backup, but not stop one or edit device information.

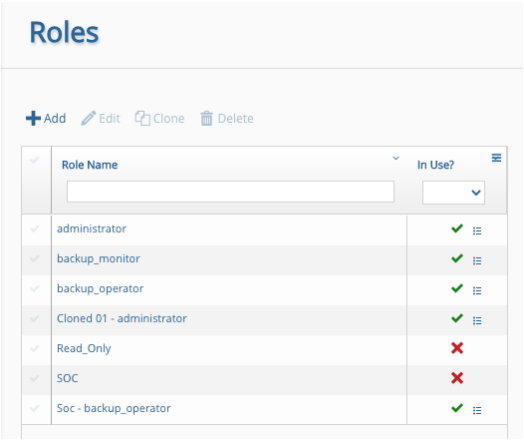


Figure 46: User Roles Screen

Adding a New Role

To add a new role, click the Add button Add. The New Role Configuration dialog box appears:

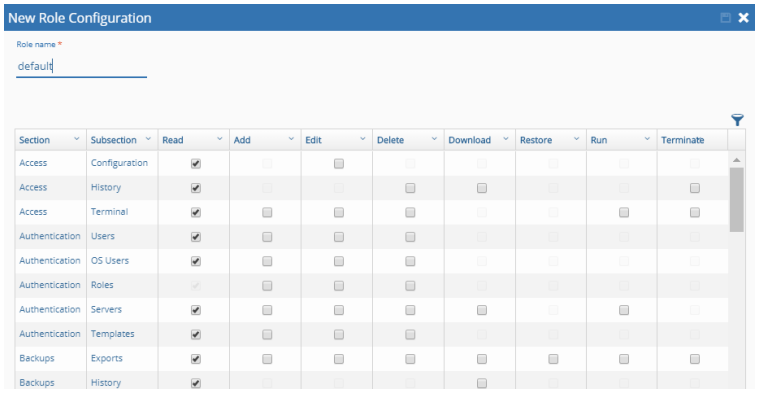


Figure 47: New Role Configuration Dialog Box

In the New Role Configuration dialog box, check the permissions for the role and click Save. If you uncheck the Read options from an entire section that section will not display for users assigned to that role.

Editing a Role

To edit a role, on the User Roles screen, select the role you want to edit and click the Edit button Edit to display the Edit Role dialog box. Edit the relevant fields and click Save.

Deleting a Role

To delete a role, on the User Roles screen, select the role and click the Delete button Delete

Operating System Users

The Operating System Users screen enables you to create accounts that connect to BackBox via SSH to the CLI. This can also be user to create Landing Zones for devices that simply write their backups out to a network location. After creating the OS User (which automatically creates the assiated LZ) remember to create a Device Probile to schedule the collection, encryption, and transfer of the file from the LZ.

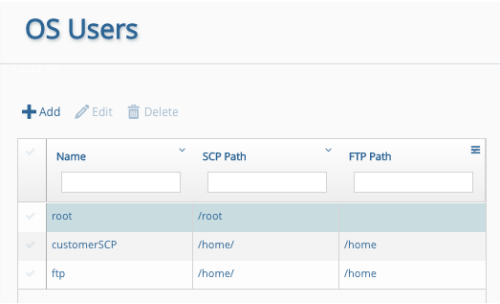


Figure 48: Operating System Users Screen

Adding a New Operating System User

To add a new operating system user, in the Operating System Users screen, click the Add button Add. The Add OS (Operating System) User dialog box appears:

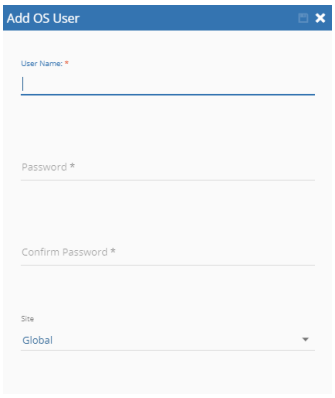


Figure 49: Add OS User Dialog Box

Fill out the fields and click Save.

Editing an Operating System User

To edit an operating system user, in the Operating System Users screen, select the operating system user you want to edit and click the Edit button Edit . Edit the fields and click Save.

Deleting an Operating System User

To delete an Operating System User, in the Operating System Users screen, select the user you want to delete and click the Delete button Delete .
A prompt will appear requesting confirmation. Click Yes to delete.

Connected Users

The connected user's screen allows the user to see who is connected to BackBox GUI.

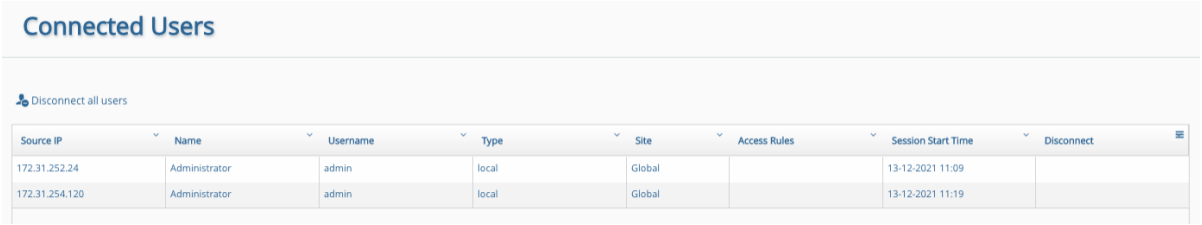


Figure 50: Connected Users Screen

Field	Description
Source IP	The IP from which the user is connected
Name	Name of the user
Username	Username of the user
Type	What is the type of the user: Local, RADIUS, TACACS+ etc.
Site	The site this user is belong to
Access Rules	Does this user have access rules configured
Session Start Time	Timestamp when the user first connected
Disconnect	Disconnect a connected user from BackBox GUI

CHAPTER 6 NOTIFICATIONS

BackBox is designed to send notifications to specified vectors with information concerning the backups, tasks, or IntelliChecks. The Notifications screen enables you to review and configure notifications and alerts.

To open the Notifications screen, on the Sidebar, click Notifications. The Notification Alerts screen is displayed:

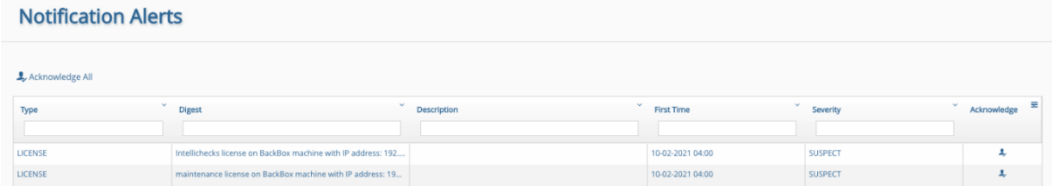


Figure 51: Notification Alerts Screen

The screen will display a list of unacknowledged alerts, and includes the following:

Table 10: Notification Alerts Columns

Field	Description
Type	Type of alert
Digest	A short digest of what the alert is about
Description	A more detailed description of the alert
Fire Time	When the alert was generated
Severity	The Severity of the alert (Critical, Warning, etc.)
Acknowledge	By clicking the Acknowledge button Acknowledge, you indicate that you are aware of the alert. You can also click the Acknowledge All button Acknowledge All at the top of the screen to indicate that you have seen all the alerts listed. This will clear the acknowledged alerts from the screen.

Configuring Notification Jobs

You can use the Notification Jobs screen to set up notification vectors. The screen displays the name of the notification and the chosen notification method, namely E-mail, Syslog, SNMP, HTTP, or Alerts. Further, it displays the site to which the notification can be received, when it was created, when it was last modified, and whether it is in use. You can add a new notification as well as edit or delete an existing one.

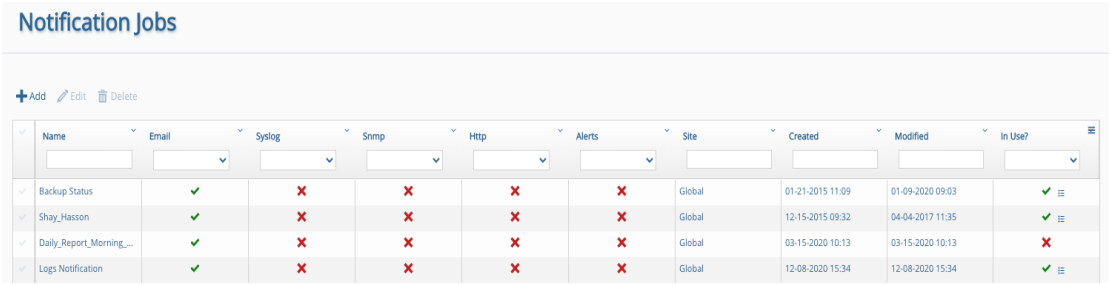


Figure 52: Jobs Notifications Screen

Adding a Notification

To add a notification:

1. On the Jobs Notifications screen, click the Add button

. The New Notification Configuration dialog box appears:

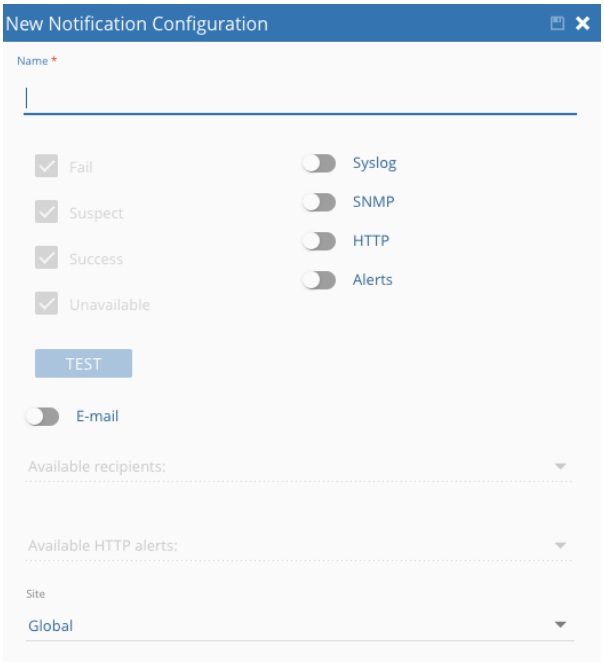
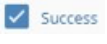


Figure 53: New Notification Configuration Dialog Box

2. Complete the fields and click Save. Deselecting the Success button 

will result in the Notification only being sent for failed/suspect states.

Table 11: New Notification Configuration Fields

Field	Description
Name	Name of the notification
Email/Syslog/SNMP/Http/Alerts	Select the way you want the notification to be received. Checking Alerts will send the results of a given task to the Notifications-Alerts screen. Create a Notification User as a placeholder for group email boxes/distro lists.
Site	The site to which the notification will be available.
Email - Available Recipients	The people available to receive notifications (of the backup). Choose the recipients by selecting their names
Available HTTP alerts	Select from the list of available http alerts configured in settings-> Alerts

Editing a Notification

To edit a notification method in the list, select the method and click the Edit button Edit to display the dialog box. Edit the settings and click Save.

Deleting a Notification

To delete a notification method, select the notification you want to delete and click the Delete Button Delete .

Testing a Notification

Clicking the Test button TEST in a notification's dialog box enables you to send a test notification to the specified recipients.

CHAPTER 7 SCHEDULES

BackBox allows you to schedule any action. Actions can be set to run hourly, daily, weekly, or monthly. The Schedules screen lists all the schedules defined in the system. You can add more schedules to the list as well as delete any of them.

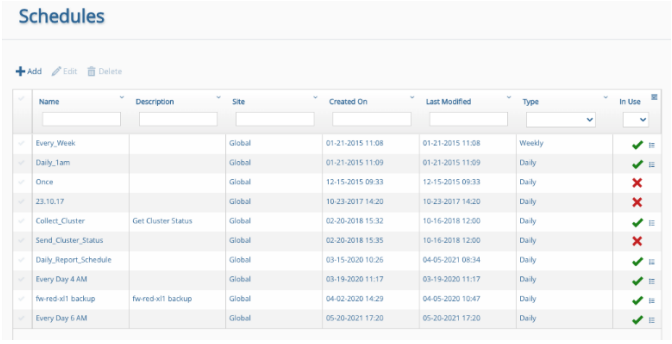


Figure 54: Schedules Screen

The Schedules screen displays the name given to the schedule, the description, the assigned site, the date the schedule was created, when it was last modified, the type, and whether it is in use ✔ or not ✘ .

Adding a new Schedule

You can add new schedules to the list of schedules. To add a new schedule:

1. On the Schedules screen, click the Add button Add. The New Schedule Configuration dialog box appears:

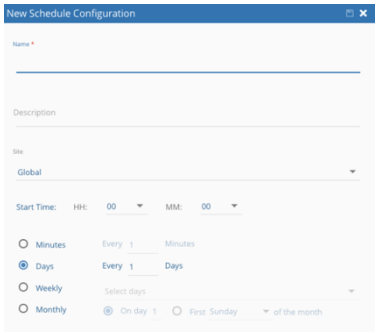


Figure 55: New Schedule Configuration Dialog Box

2. Fill in the fields and specify the interval and time for the new schedule and click Save.

Deleting a Schedule

To delete one or more schedules:

1. Select the schedule(s) you wish to delete
2. Click the Delete Button Delete
3. A prompt appears requesting confirmation.
4. Click Yes

CHAPTER 8 BACKUPS

Clicking Backups on the Sidebar displays the Backup Jobs screen. The screen lists all the backup operations that have been defined in the system, as well as when they are scheduled to run, the current status of the backup, and other relevant information. Clicking on Queue displays the current jobs in the backup queue. Clicking on History displays the backup history of each device in the system.

The Backup Jobs Screen

The Backup Jobs screen displays a list of backup jobs along with their schedule, notification, next execution, site, and status:

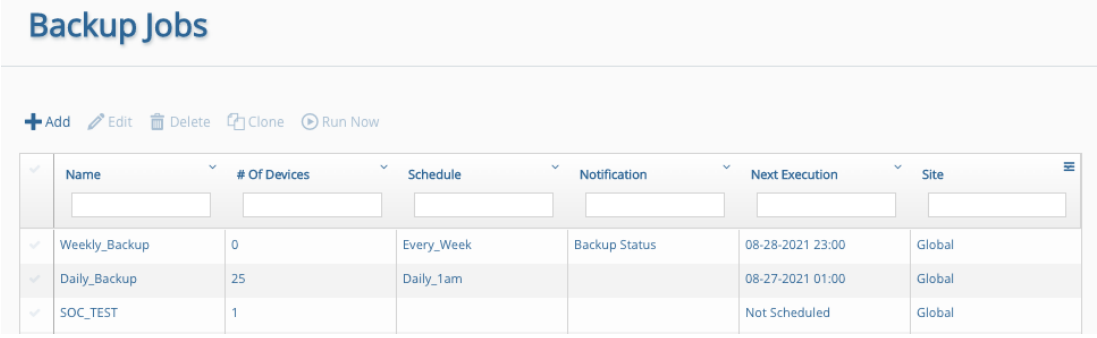


Figure 56: Backup Jobs Screen

Table 12: Backups Jobs Screen: Fields and Buttons

Field	Function
Name	Displays the name assigned to the backup
# Of Devices	Number of devices selected in this job
Schedule	Displays the schedule that has been configured for the backup. To create a Schedule, see the chapter on Schedules.
Notification	Displays the people to be notified in case of failure or after the completion of the backup. To add a notification, see the chapter on Notifications.
Next Execution	Displays the date and time of the next scheduled backup, providing the job is enabled.
Site	Displays the site on which the backup will be run.

Field	Function
Edit	Enables you to edit the configuration for a backup.
Delete	Enables you to delete a backup job listed in the Backup Jobs screen. To delete a backup job, select the job you want to delete and click the Delete button Delete.
Run Now	Manually runs the backup now, regardless of the scheduled time. Check the box next to the desired job and click the Run Now button Run Now.
Add	Add new backup job
Clone	Clone an existing backup job

Adding a Backup Job

BackBox allows you to add additional backups to meet your needs. To add another backup job:

1. On the Backup Jobs screen, click the Add button Add. The New Backup Job Configuration dialog box appears:

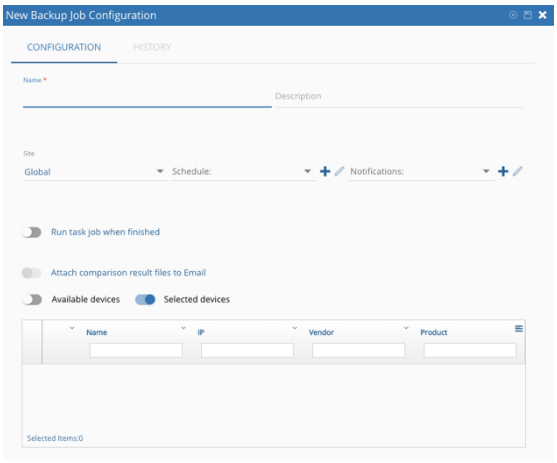


Figure 57: New Backup Job Configuration Dialog Box

Table 13: New Backup Job Configuration Fields

Field	Description
Name	Type a name that identifies the new backup.
Description	Type a brief description of the backup – this field is optional but recommended.
Site	Select the name of the site to which the device is assigned. If the site is locked to an agent, you cannot run a backup from Global. Sites can be locked to an agent in the Agent screen, which is located under Settings in the Sidebar.
Schedule	Select a schedule for the backup. You can create a new schedule by clicking the Add Schedule button Add next to the Schedule list or select a schedule from the list. For further details, see the
Notifications	Select the notification configuration to be implemented regarding the completion/failure of the backup. If the notification configuration includes E-mail, below notifications, an additional button is displayed on the screen enabling you to attach comparison result files to the E- mail. In addition, you can click the Add Notification button Add next to the Notifications list to configure a new notification. For further details, see the chapter on Notifications.
Run task job when finished	In case you want to run a task job in the end of a backup job, you can turn on the switch and select which task job you want to run
Attached comparison results file to email	In the notification of a backup job select this to get PDF reports of changes in the text-based configuration

2. Complete the fields with the desired parameters.
3. Click the Add Devices button Add (under Site:) to display a list of available devices. Available columns display item type (with an icon), device name, IP, vendor, site, and group to which the device belongs.
4. Click one or more devices which you want to add to the backup job and click the Add button Add .
5. To remove a device from this list, click the Remove Device button Delete .

Deleting a Backup Job

To delete a backup job:

1. On the Backup Jobs screen, select the Backup Job to be deleted.
2. Click the Delete button Delete The Delete Backup Job dialog box appears requesting confirmation.
3. Click Yes.

Running a Backup Job

Backup jobs will run according to the schedule that you assigned them. Their next execution is displayed on the Backup Jobs screen. However, you can run a backup immediately by selecting a backup job and clicking the Run Now button Run now .

The Backup Queue Screen

The Backup Queue screen contains all the backup jobs currently running or waiting to run. Each entry listed contains the device name (one line for each device in the queue), IP address, date started, duration (the time taken to run until now, if currently running) and the run status, i.e. running or pending. The View and Terminate columns display buttons for viewing the backup job or terminating it.

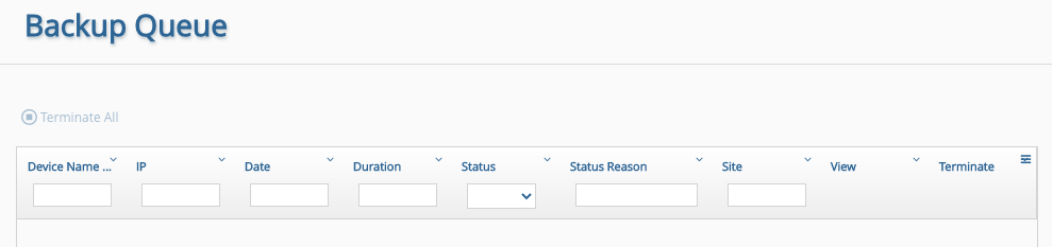


Figure 58: Backup Queue Screen

Removing a Job from the Queue

A job can be removed from the queue, or stopped if currently running, by clicking the Terminate button displayed in the job's Terminate column. To terminate all the jobs in the queue, double-click the Terminate All button Terminate All .

Note: Due to the significance of terminating a backup job, you must double-click the Terminate All button Terminate All as opposed to a single click for most other functions.

Backup History Screen

The Backup History screen is a log of all the backups. Each entry listed displays the device name, its IP address, the date and time it was run, and the status of the run (Success, Success - Configuration Changed, Failure, or Suspected Failure). For those with a Failure status, the adjoining column also records the failure reason as shown in the following:

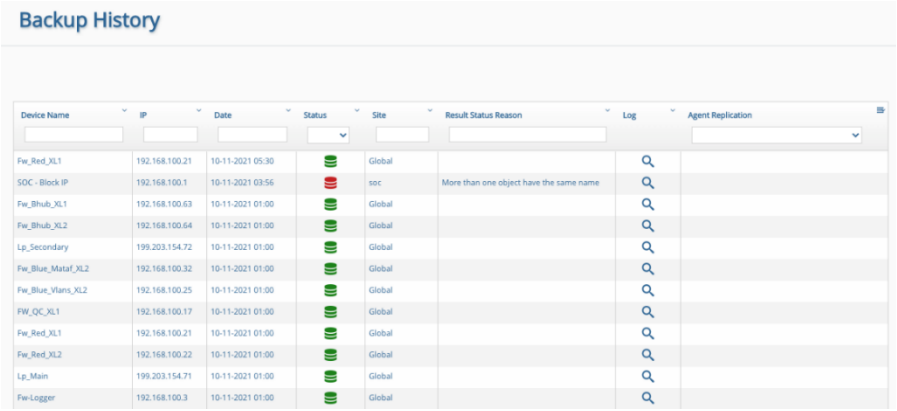


Figure 59: Backup History Screen

Also, you can view the status of the backup replication if this device is configured on the agent and replicate the files to the agent.

Filtering the Backup History

You can filter backup jobs listed on the Backup History screen. To filter a table, click the Filter box. You can also filter for more than one value: Device Name, IP, Date, and Status columns. To filter the backup jobs listed on the Backup History screen, type a value into the filter box by which you want to filter the table. To remove the filter, click the filter boxe's Cancel button ✖ .

Backup Trail Log

For any backup, clicking on the View Log button 🔍 in the Log column displays a backup trail log that you can download

CHAPTER 9 DEVICES

The Devices screen displays all the devices you are authorized to view. You can display these by any field (Vendor, Group, etc.) to make it easier to navigate.

Devices Screen

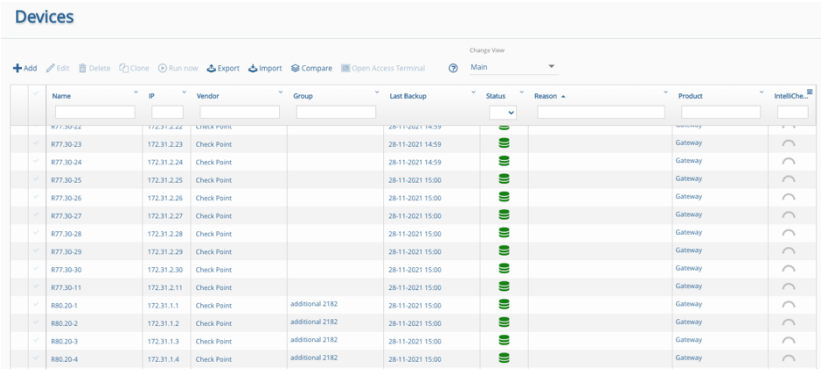


Figure 60: Devices Screen

The Devices screen displays the following columns:

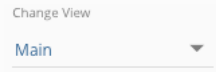
Table 14: Device Fields

Fields	Description
Name	The name given to the device profile.
IP Address	The IP address assigned to the device. IPv6 addresses are supported.
Vendor	Vendor of the device.
Group	The group to which the device is assigned.
Last Backup	Date of last backup.

Fields	Description
Status	Displays information about the backup status: Successful/ Suspected/ Failed/Maintenance and more. Click the icon or see Devices Table Legend for other statuses.
Reason	Reason a backup failed or was considered suspect.
IntelliChecks	Gauge showing the percentage of successful signatures.
Description	Additional details about the device.
Device ID	The is of the device in BackBox
Type	Type of the device for example : Firewall/Router/Switch
Agent	Name of agent this device is connected through
Site	Name of site this device connected to
External ID/Tag	If the user customizes an external ID or tag it will appear in this column.

The Devices screen also displays buttons that enable you to perform the following tasks:

Table 15: Devices Toolbar Buttons

Buttons	Description
	Add a device for backup.
	Edit a device's details.
	Delete a device.
	Clone an existing device so that the clone has the same backup parameters.
	Click to run the backup immediately.
	Export a device list to a CSV file.
	Import a device list from a CSV file.
	Compare Backup files by comparing their ASCII.
	Select a device and open an access terminal with the default configuration to it.
	Change between main view and device view. Device view will give you also the history of the device automation
	Legend: displays the icons and their meaning.

Devices Table Legend

The Devices Table Legend provides a key to understanding the status icons in the Status column on the Devices screen:

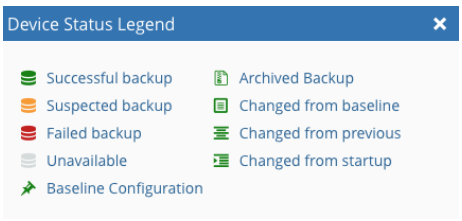


Figure 61: Device Table Legend

Adding a New Device

To add a new device:

1. On the Devices screen, click the Add button Add. The New Device Configuration dialog box (Step 1 of 4) appears:

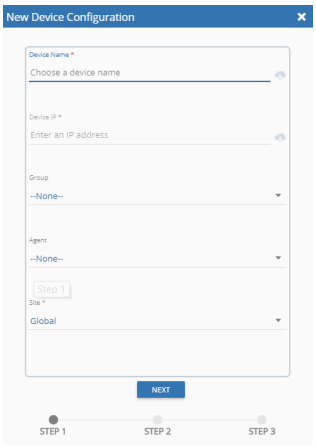


Figure 62: New Device Configuration Dialog Box - Step 1 of 4

2. Add the device name, the device IP address (*and if you have created them, add the Group, Agent, and/or Site you wish to assign to the device*), then click Next NEXT

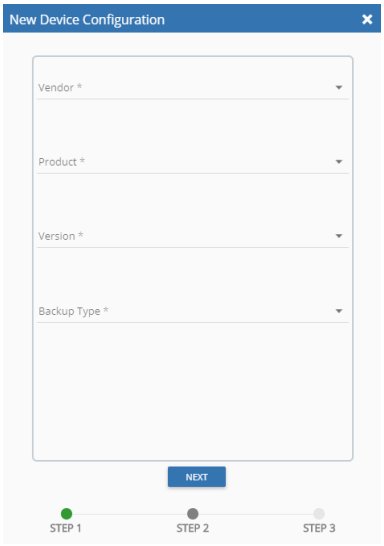


Figure 63: New Device Configuration Dialog Box - Step 2 of 4

3. Complete the Vendor, Product, Version, and Backup Type fields, and click Next . NEXT The third dialog box appears:

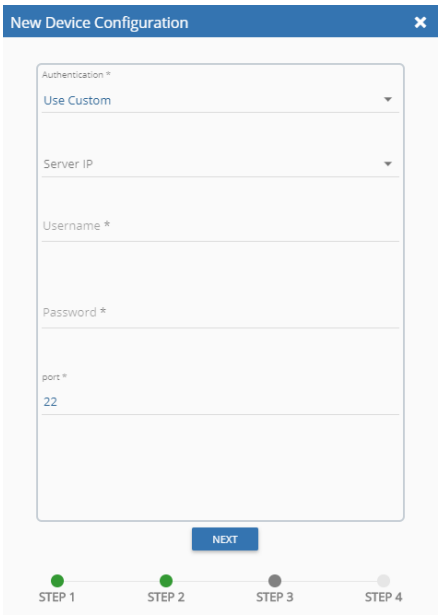


Figure 64: New Device Configuration Dialog Box - Step 3 of 4

4. Complete the Authentication (Custom=profile specific, Template=group creds) Username, Password, (Expert Password if applicable) and Port fields, and click Next NEXT . The fourth dialog box appears:

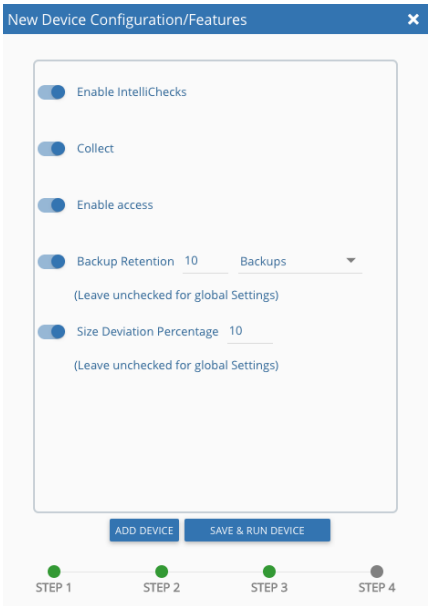


Figure 65: New Device Configuration Dialog Box - Step 4 of 4

5. Optionally, check Enable IntelliChecks and/or Enable Access to turn on that functionality for the device.
6. If you want to create local retention settings for the device, click the Backup Retention field.
   Note: Leave unchecked to apply Global retention settings.
   If you turn on Backup Retention, two additional fields are displayed: one for the number of days that backups are retained, and one for choosing backups or setting retention policy. Indicate the number of backups to be retained or select Retention Policy and click the Edit button to set a new retention policy.
7. Click Add Device ADD DEVICE or Save & Run Device SAVE & RUN DEVICE
8. Size deviation – override global settings for size deviation verification

Using Export/Import to Add Multiple Devices

The Devices screen Export Button Export enables the export of the selected list of devices to a password protected spreadsheet.

To export a list of devices:

1. Click the Export button and in the Export Devices dialog box, type a password to be used when reimporting the exported devices:

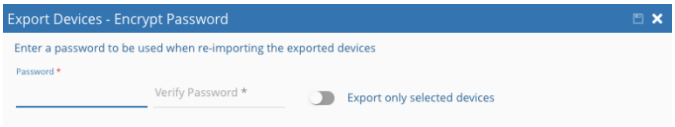


Figure 66: Export Devices Password Encryption

2. Add new devices to the spreadsheet.
   You can speed up your work by copying a device row and then overriding the Device Name and IP fields with the information of additional devices you want to add. For example, in the following spreadsheet, we have copied the F5 BiG-IP2 device row, and then pasted it in twice, thereby adding two additional F5 devices: F5 BiG-IP2-1, and F5 BiG-IP2-2.

	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Site ID	Device Host	Vendor ID	Product ID	Version ID	Backup Ty	Group ID	Retention	Port	Debug Mc
2	TrendMicro IWSVA 5.5	0	172.31.254.107	-58	-135	-199	-404	0	0	22	FALSE
3	Radware AppDirector	0	172.31.254.111	-52	-119	-176	-342	0	0	443	FALSE
4	R71.10 Module Splat	0	172.31.255.188	-3	-3	-234	-424	0	3	22	FALSE
5	Cisco ASA	0	172.31.254.2	-5	-46	-242	-709	1	0	22	FALSE
6	F5 BiG-IP2	0	172.31.252.40	-30	-71	-113	-880	0	0	22	FALSE
7	F5 BiG-IP2-1	0	172.31.252.41	-30	-71	-113	-880	0	0	22	FALSE
8	F5 BiG-IP2-2	0	172.31.252.42	-30	-71	-113	-880	0	0	22	FALSE
9	Gaia R77 VSX	0	172.31.255.175	-3	-187	-291	-809	0	4	22	FALSE
10	ESXi 110	0	172.31.255.110	-60	-138	-203	-401	0	0	22	FALSE
11	BackBox Self Backup	0	172.31.252.171	-17	-25	-30	-711	0	0	22	FALSE

Figure 67: Spreadsheet with new devices added

3. Click the Import button Import to import the spreadsheet back into BackBox. Ignore any errors about devices that already exist. We are only concerned about the new devices being imported.

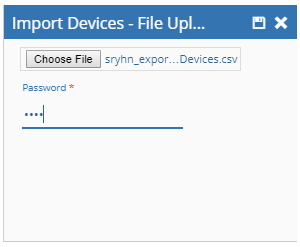


Figure 68: Import Devices File Upload

The Devices screen displays all the new devices with the same Backup Jobs, Notifications, Group, and Site settings as the original device.

Vendor	Name	IP	Group	Last Backup	Sta...	Reason
BackBox (1)						
Check Point ...						
Cisco (2)						
F5 (3)						
F5	F5 BiG-IP2	172.31.252.40		29-12-2017 ...		
F5	F5 BiG-IP2-1	172.31.252.41		Never		Never been executed
F5	F5 BiG-IP2-2	172.31.252.42		Never		Never been executed
Linux (2)						
PaloAlto (4)						

Figure 69: Devices Screen Displaying Newly Added Devices

Displaying the Details of an Individual Device

To display the details of an individual device listed on the Devices screen, click a device name in the list. The Device Details screen appears with the device name, displaying the following tabs: Details, History, IntelliChecks, Inventory, and Network Info. The default view upon opening is the Device Details tab.

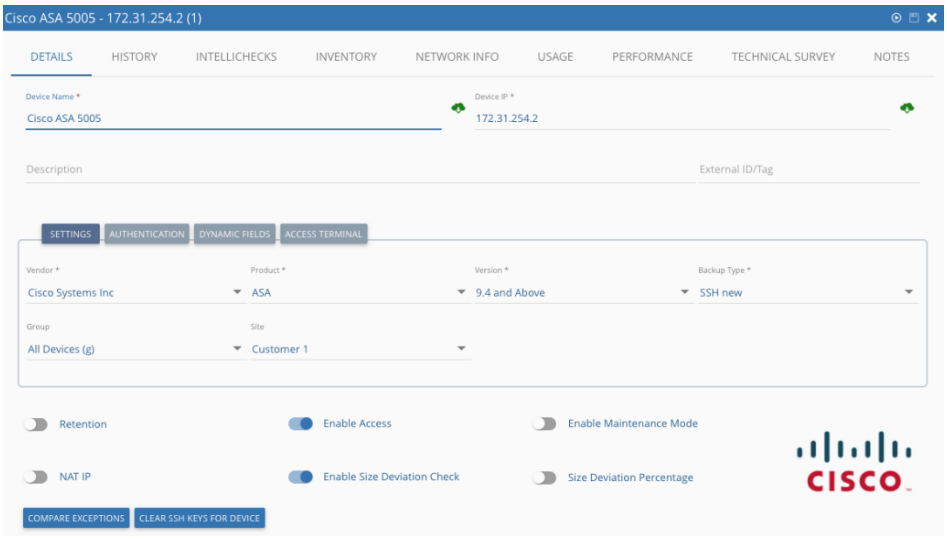


Figure 70: Device Details Screen

Device Details Tab

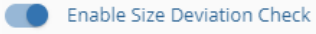
The Device Details tab displays information about the device. You can edit the details, then click Save to save the details, or click Run to immediately apply the device details/backup information and run a backup. These actions can be run using the row of icons in the upper right corner:

Figure 71: Upper Right Corner of the Devices Details Tab

Depending on the device, some, or all the fields in the following table appear:

Table 16: Device Details Fields and Buttons

Field/Button	Description
Device Name	Name of the device
Device IP	IP address of the device
Clear SSH	This button clears the SSH key for authorization.
Vendor	Vendor's name
Product	Product name
Version	Product version
Backup Type	Backup type
Group	The group to which the device is assigned for backup.
Agent	The agent to which the device belongs.
Site	The site to which the device belongs.

Field/Button	Description
	Specify how many days backups and other files are retained. See below for details.
	Click NAT IP to specify a NAT address for the device.
	Enables the device to interact with the Access module.
	Allow size check of current backup against previous backup. Suspect status assigned if the backups have a +/- 30% size difference
	Enables you to specify a Compare Exception for a device so that you can exclude specific lines from the configuration when running the comparison feature.
	Clears out SSH keys, forcing new collection.

Retention Button

Click the Retention button to specify how many days backups and other files are retained. Clicking Retention displays two options:

- Backups
- Retention Policy

Backups enables you to type the number of backups you want to retain.

Retention Policy enables you to edit the retention policy for backups and other files. Select the Retention Policy option and click the Edit button next to it. The **Retention Policy** dialog box for the device appears:

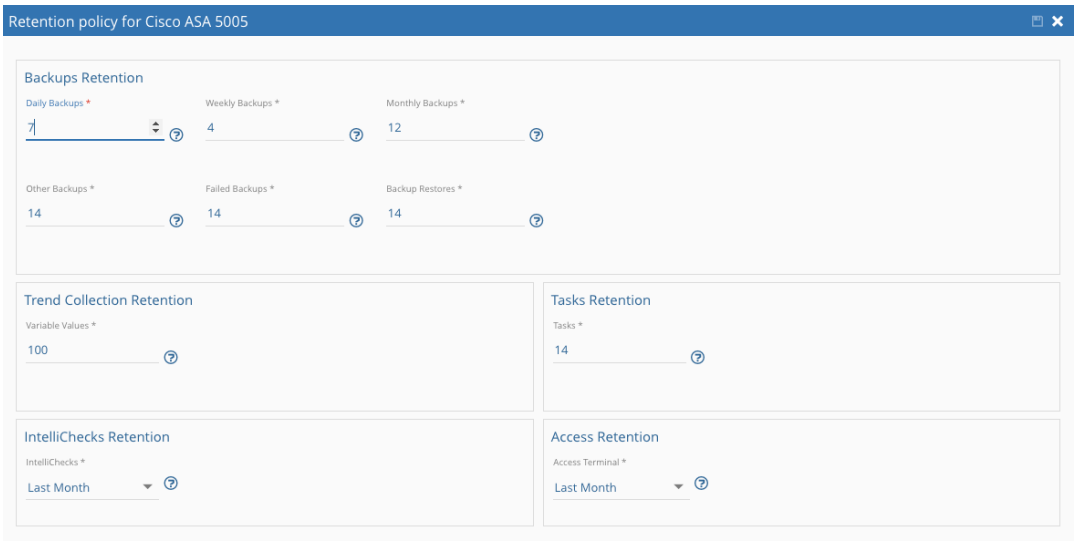


Figure 72: Retention Policy Dialog Box for a Device

Edit the number of backups for a given field and click Save. The default values allow 23 backups to provide coverage for roughly 12 months.

Device History Tab

The Device History tab lists all the backups and Access sessions for the device. The details displayed include the type of backup (scheduled/manual), date performed, file size, status (success, failure, suspect), failure reason (if the backup failed), log (and stream/download for Access sessions), comment (which can be edited by you to type a short comment), Site (if applicable), and Remote Status.

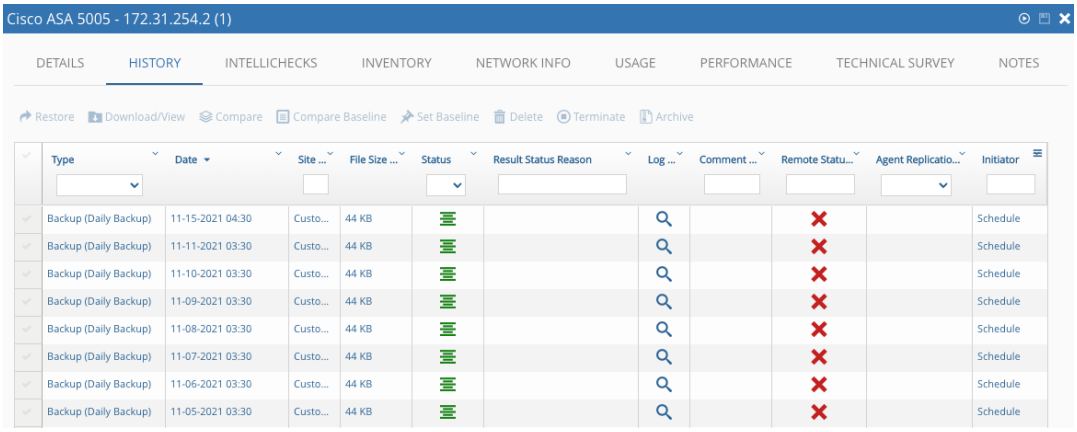


Figure 73: Device History Tab

You can view a detailed log of each backup by clicking the View Log button in the Log column. The **Backup Trail Log** screen appears:

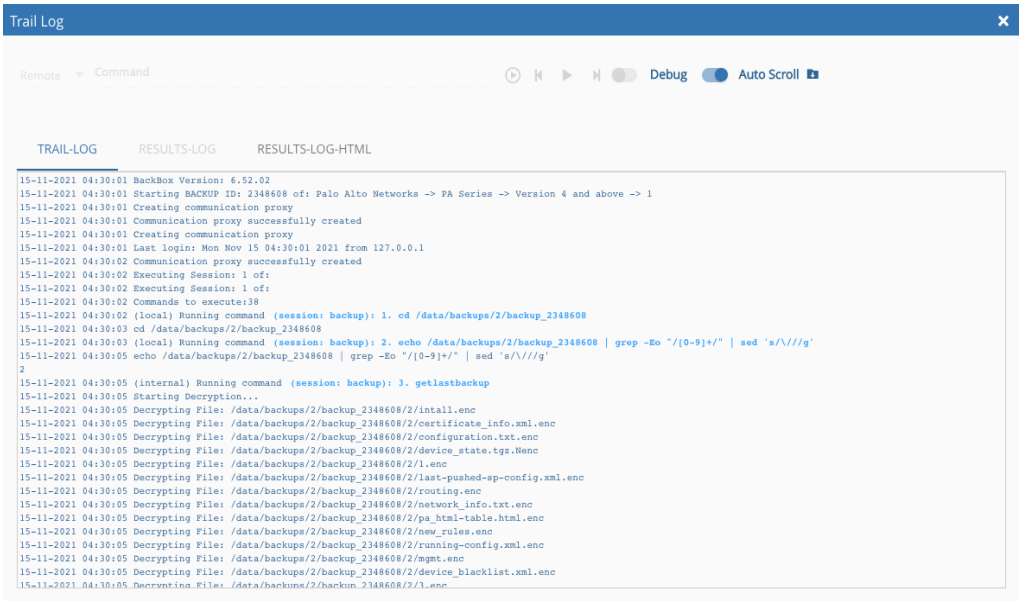


Figure 74: Example for Backup Trail Log Screen

To download the log, click the Download button at the upper right corner
The Device History screen is also where you initiate a Restore, or perform other actions as detailed in the following table:

Table 17: Device History Buttons

Button	What it Does
Restore	Restores the selected device configuration. If a Restore script was written for a device on the Restore tab of Customize, clicking this button will start the script.
Download	Downloads the selected configuration
Compare	Compares backup files, either same files from different backup or files in the same backup
Compare Baseline	Compares the selected configuration to a Baseline configuration

Set Baseline	Enables you to set a configuration as a Baseline
Delete	Deletes a backup from the list
Terminate	Terminates selected running backup job in the list
Archive	Archives selected backup files

IntelliChecks Tab

The IntelliChecks tab displays the health checks and compliance tests for the device:

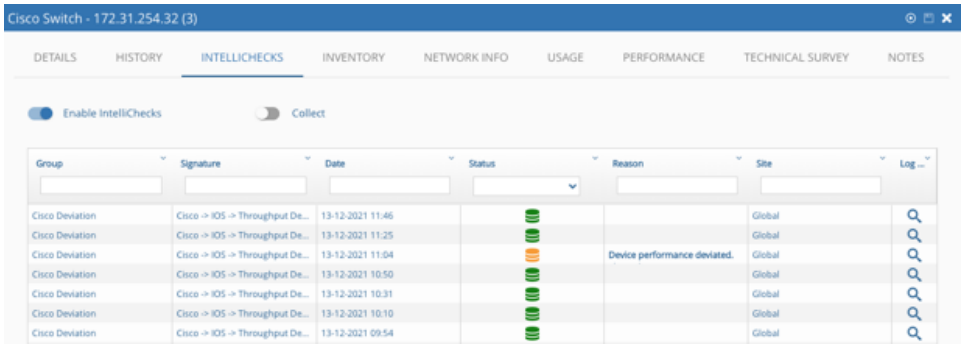


Figure 75: IntelliChecks Tab

If a device has multiple IntelliChecks groups that run against it, the output is separated with headers, providing summary information for the group. Whether the device can have IntelliChecks run against it is controlled by the Enable IntelliChecks button at the stop of the screen. The Collect button determines whether the information can be used by the Trends widget on the dashboard.

Inventory Tab

The Inventory Tab displays additional information about the device such as Serial Numbers, OS Versions, License Info, and other defining data points about the device.

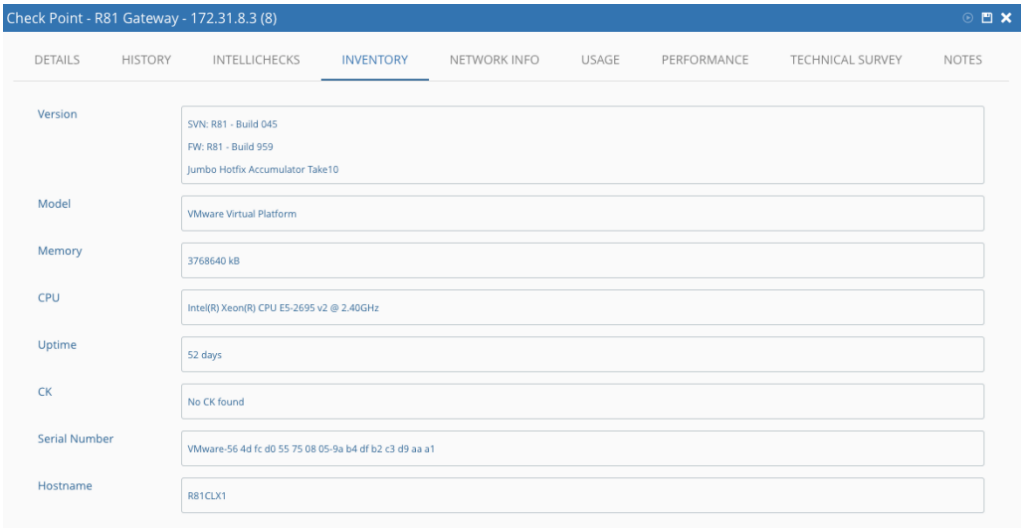


Figure 75: Example of Inventory Tab

Network Info Tab

The Network Info tab displays details around the interface used by the device (Type, Name, IP, etc.), and any Routing rules that have been applied to the device.

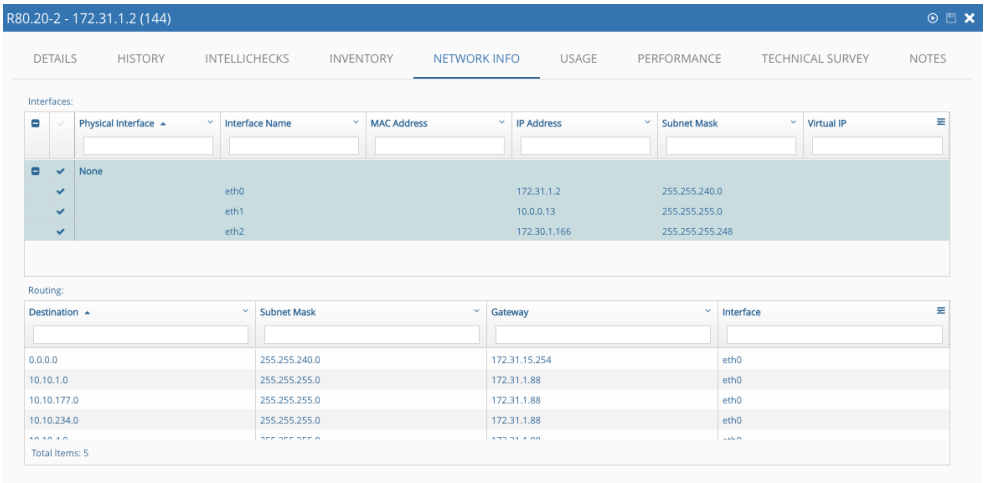


Figure 76: Example of Network Info Tab

Usage Tab

Usage tab will list all the jobs (Backup/Tasks/IntelliChecks) this device is scheduled with. It will help the user to know in one place where this device is used.

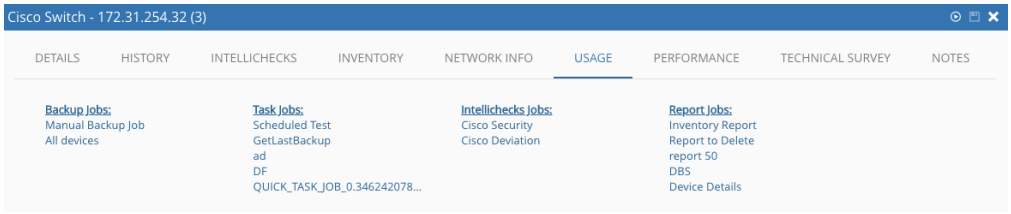


Figure 77: Example of Usage Tab

Performance Tab

The performance tab will show all collected information that BackBox is gathering from running Health IntelliChecks on the device. There are two types of data, the deviation table that's shows the current measurement, the average, and the deviation. The table is divided into days of the week and hours of the day. The second data is a graph showing the measurements over time (24 hours/7 days/30 days/365 days)

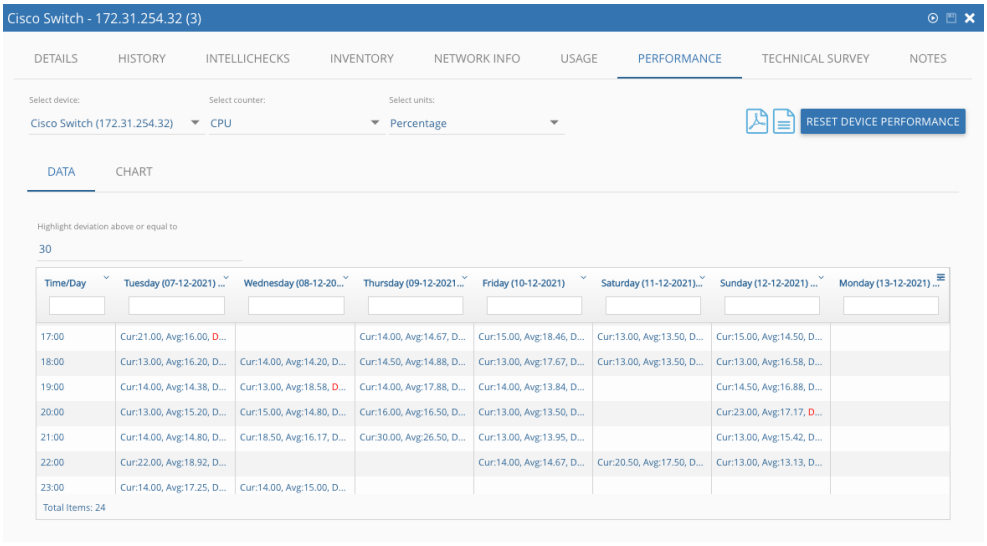


Figure 78: Connected Users

Technical Survey Tab

The technical survey tab shows all information gathered by technical survey IntelliChecks running on the devices. Each field related to IntelliChecks gathering information on the device config hardware or software information will be displayed in this tab.

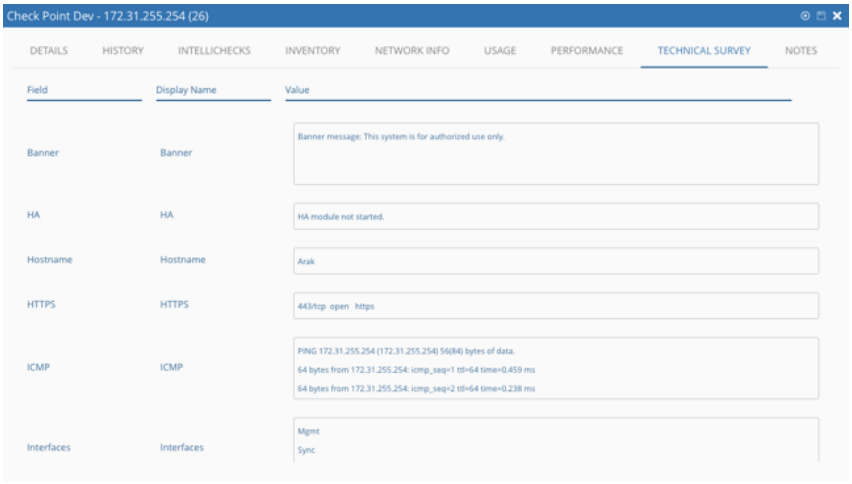


Figure 79: Example of Technical Survey Tab

Notes Tab

The notes tab allows the user to add his own notes to the device.

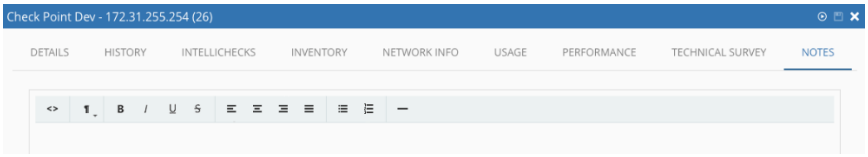


Figure 80: Example of Notes Tab

Deleting a Device

To delete a Device:

1. On the Devices screen, select the Device to be deleted.
2. Click the Delete button Delete . The Delete Device dialog box appears requesting confirmation.

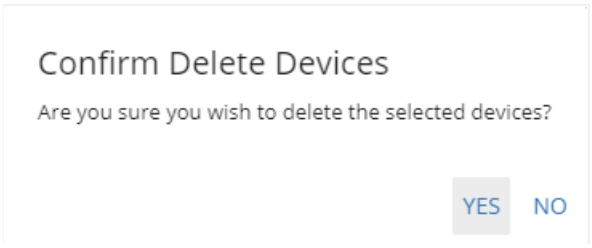


Figure 81: Confirm Delete Devices Prompt

3. Click Yes.
4. You will see a deletion process message, and then a message informing you of successful deletion:

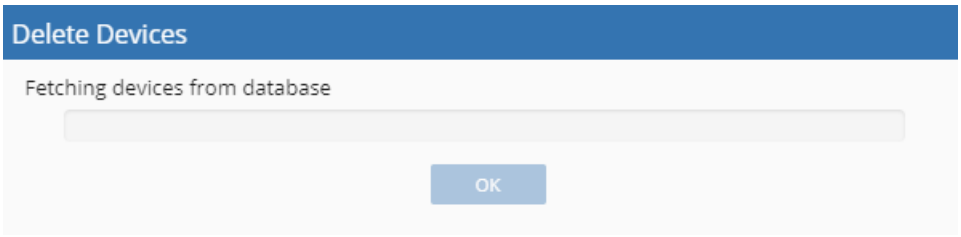


Figure 82: Deletion Process Message

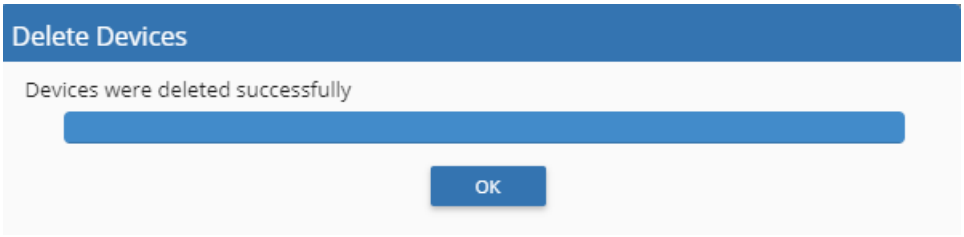


Figure 83: Successful Deletion Message

Comparing Backups

BackBox enables you to compare backup files, line by line. This enables you to identify where backups have added or deleted lines, etc.

To compare backups:

1. In the Devices screen, click the Compare button Compare at the top of the screen.The Compare Backups dialog box appears:

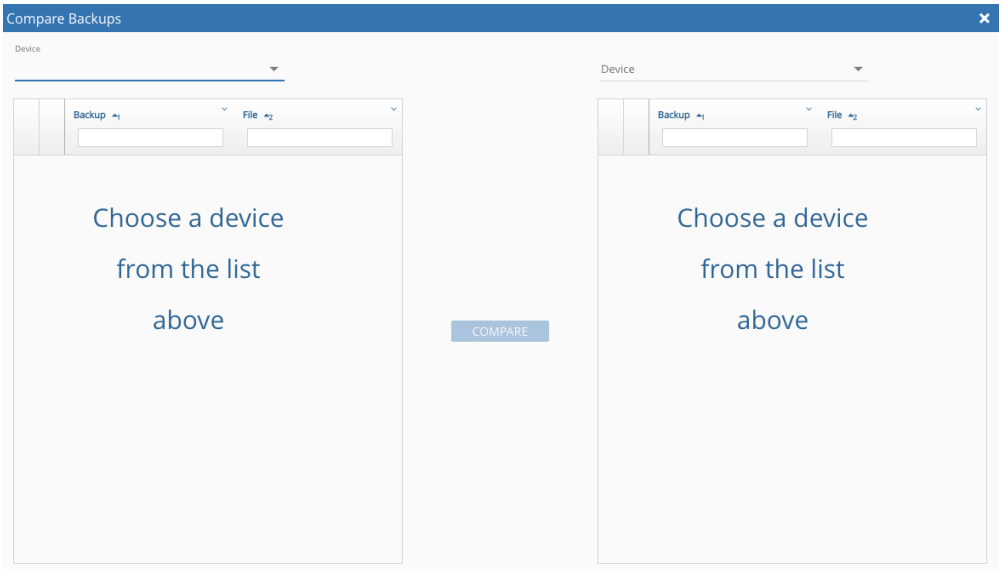


Figure 84: Compare Backups Dialog Box

All the devices with backup files in the BackBox system appear in both the left and right columns.

2. In the left column, click a device and its subfolder. In the subfolder, click the backup file that you want to compare. The selected backup file will be highlighted in blue and a message above the Compare button Compare appears, indicating that the file will be compared.
3. Follow the same procedure for the right column. The selected backup file will be highlighted in blue, and a message below the Compare button Compare appears, indicating that the file will be compared.
   For example, in the left column you may want to select a txt file that was generated at a certain date and time. In the right column, you might select the same file that was generated for the same device at a later date and time.

The **Compare Backups** dialog box records your selections like this:

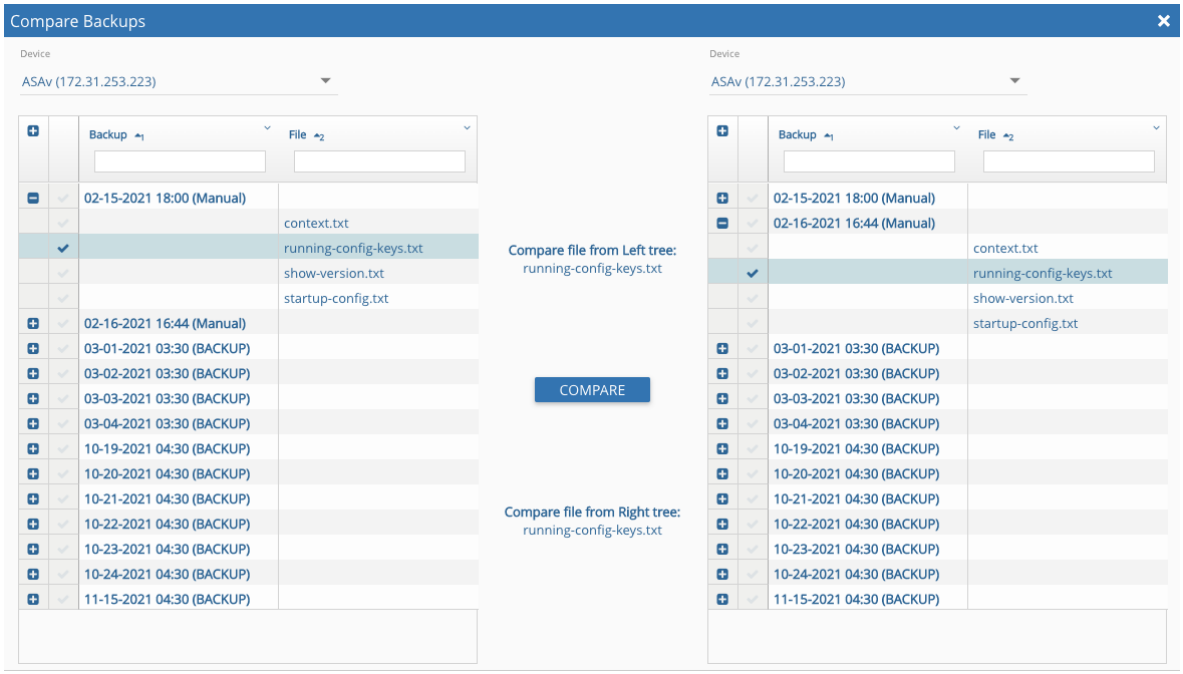


Figure 85: Compare Backups Screen with Files Selected

4. Click the Compare button compare. The Compare screen appears, listing each line of both backups, like this:

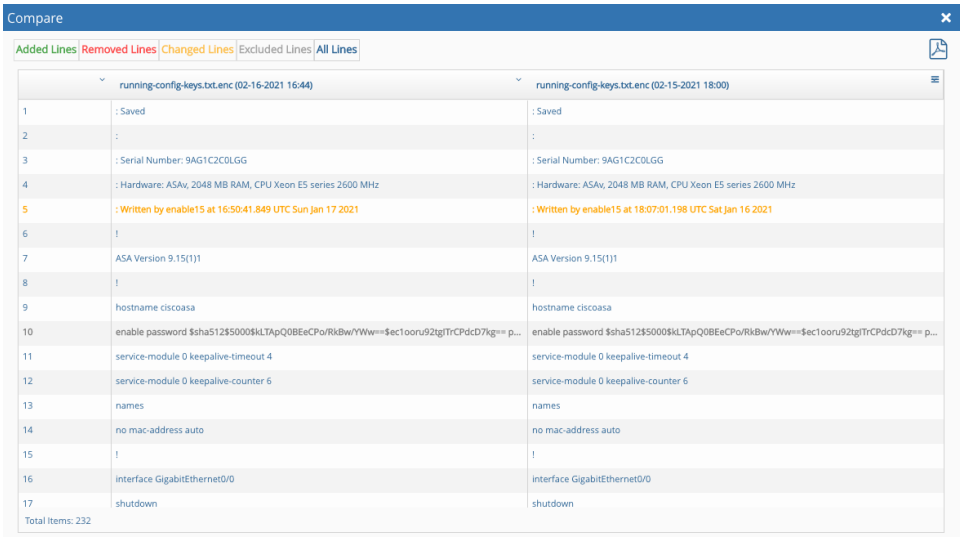


Figure 86: Compare Backups Screen with File Comparison Result

If the backup files are identical, an additional message is displayed informing you of this.
If the backup files are not identical, you can scroll through the lines of the backup files and note the differences. Additions, deletions, and changes are highlighted by color as indicated by the colored buttons at the top of the screen.

Additionally, you can click the buttons above to view the changed lines. Moreover, you can export the comparison as a CSV or PDF, by clicking the Columns button ≡.

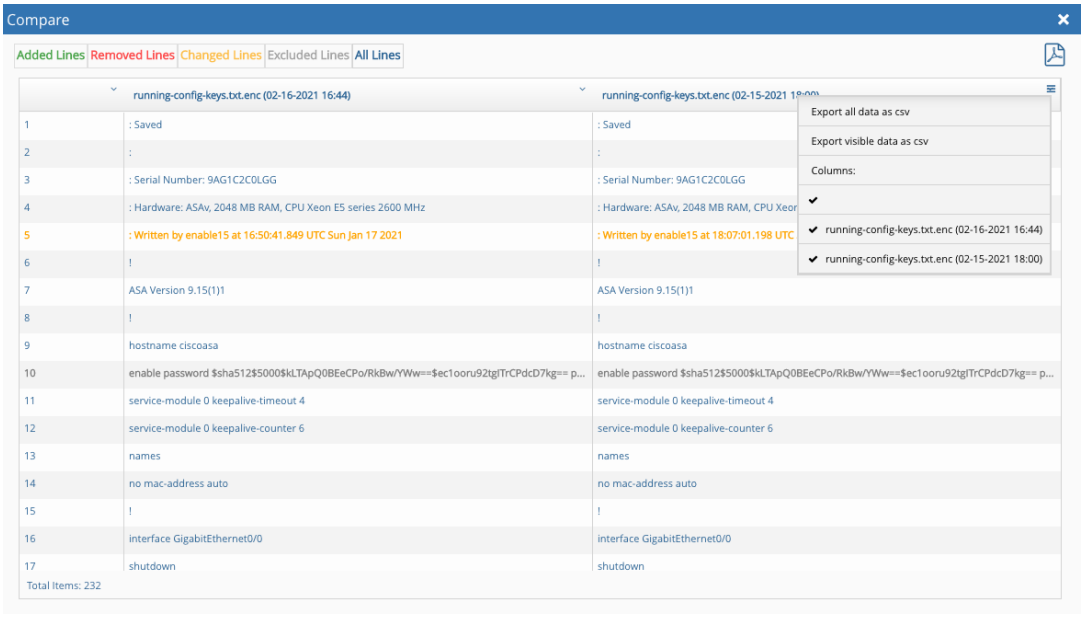


Figure 87: Compare Screen Showing Excluded Line in Grey and Export Options

Devices Groups Screen

Backups can be done on a single device or on a group of devices at the same time. BackBox enables the grouping of devices to make backups more manageable and efficient. The Devices Groups screen displays the list of devices grouped together for backup. Groups can be created based on vendor or by the device function such as Firewall, Load Balancer, Switch etc.

The Device Groups screen displays the device group name, together with information on how many devices are included in the group, when the group was created and when it was last modified:

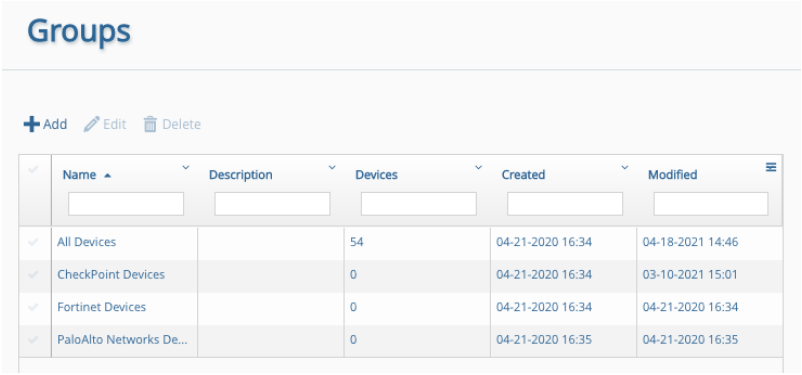


Figure 88: Devices Groups Screen

Adding a New Device Group

To add a new Device Group:

1. On the Device Groups tab click the Add button Add . The Device Group dialog box appears.

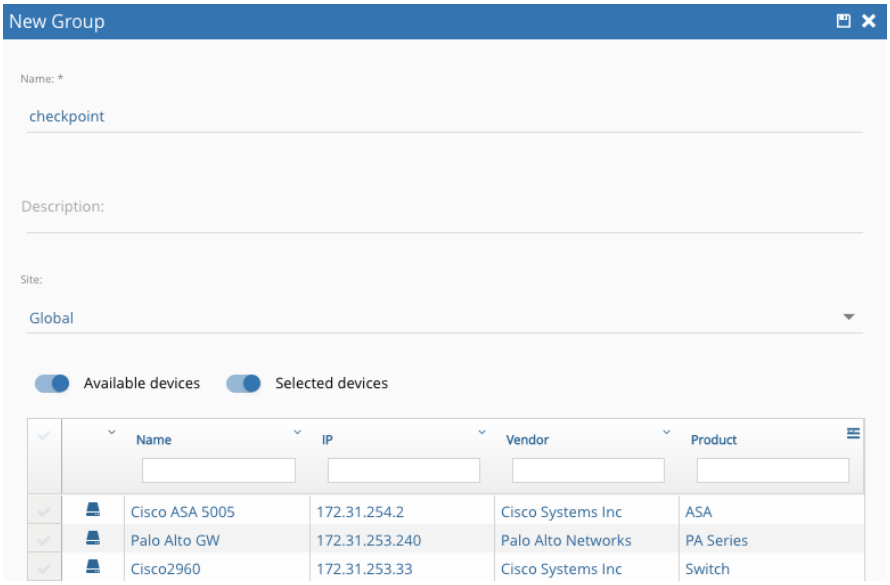


Figure 89: Device Group Dialog Box

2. Specify a name for the new group, and, optionally, a short description. In the Site field, select the site to which you want to assign the group.
3. In the list, select the devices according to name, IP address, or vendor that you want to add to the group and click Save .
   The group is created with the specified devices.

Editing a Device Group

To edit a Device Group, on the Device Groups screen, click a device group in the list to display the Device Group dialog box. Edit the group details you want to change and click Save .

To delete a Device Group:

1. Select the device group you wish to delete and click the Delete button Delete . The Delete Groups dialog box appears, requesting confirmation.
2. Click Yes.

IP Address Management

The IP Address Management screen displays a list of segments that contain IP Addresses. You can create segments or edit/delete a segment. You can also synchronize existing devices into segments.

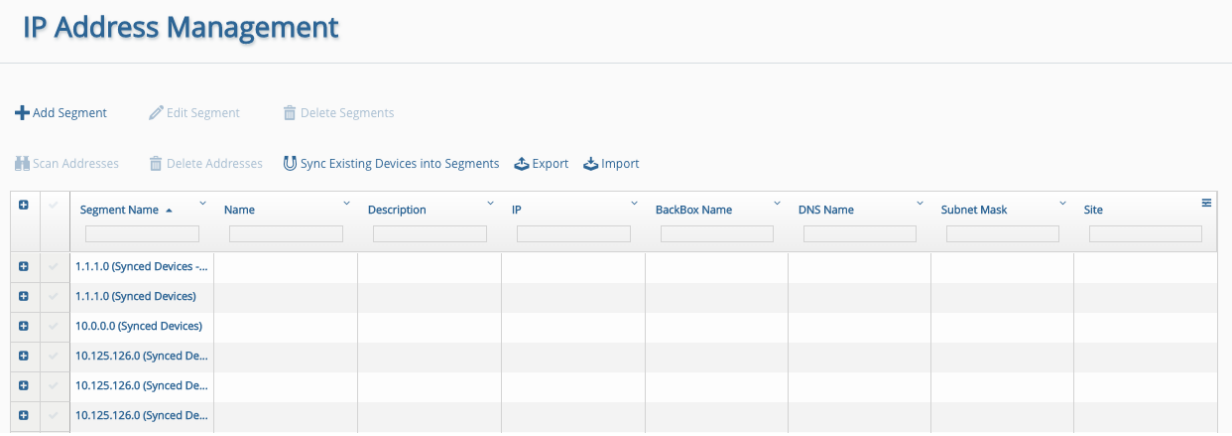


Figure 90: The IP Address Management Screen

Adding a Segment

To add a segment to the BackBox system, in the IP Address Management screen, click the Add Segment button

. The New Segment dialog box appears:

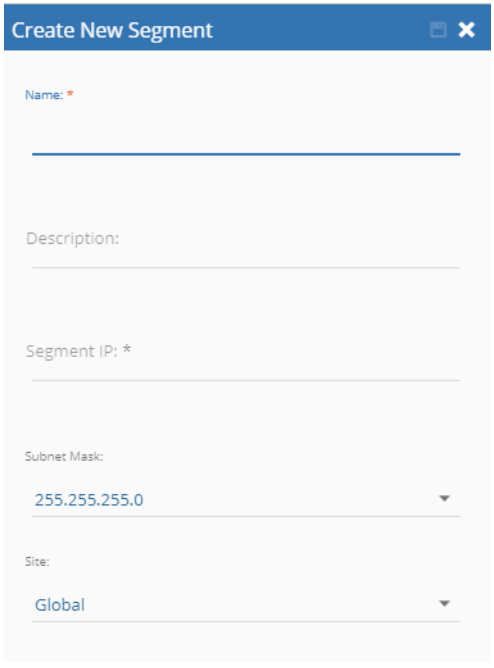


Figure 91: New Segment Dialog Box

Specify a name, description, IP address, subnet mask, and site for the segment and click Save.
Note: IPv6 is supported.

Editing and Deleting Segments

To edit or delete a segment, select the segment and clidk the Edit button Edit or the Delete button Delete.

Synchronizing Existing Devices into Segments

After creating the segments, you can synchronize existing devices into the segments by clicking the Sync Existing Devices into Segments button Sync Existing Devices into Segments

Network Map

The Network Map screen displays the devices as a network topographical map, complete with routing paths and function-based icons.

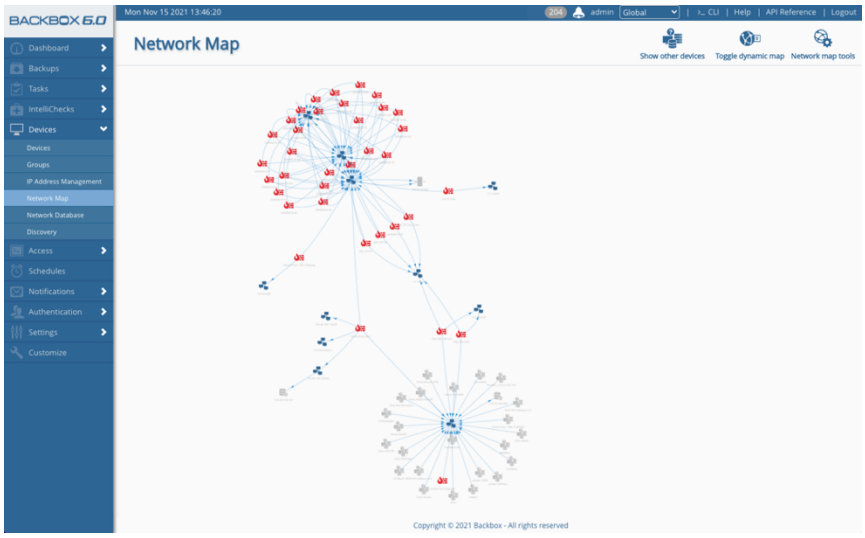


Figure 92: The Network Map Screen

Network Database

The network database tab shows collected information from network database tasks phase 1, 2,3 and 4 running on devices.

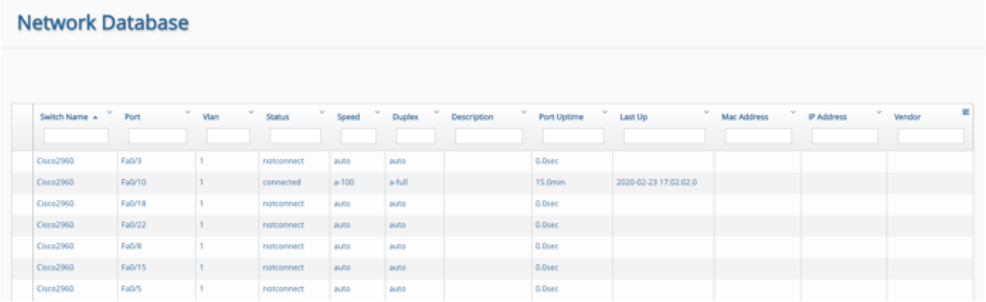


Figure 93: Network Database

Discovery

The Discovery tab lets you configure SNMP scan to the network with the ability to create rules that will tell the system how to add those devices.

Jobs Tab

The job tab will let you add new jobs of discovery. Each job can be scheduled differently, applied to different rules, have different IP ranges, and work on different subnets.

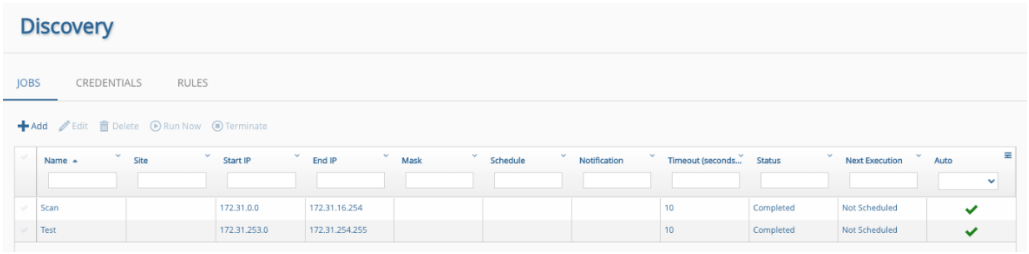


Figure 94: The Jobs Tab Screen

Table 18: Task Job Fields

Button	What it Does
Add	Add button will let you add new discovery jobs
Edit	When selecting an existing job, the help button will let you edit it.
Delete	Deletes a job
Run now	Run a job on-demand
Terminate	Terminate a running job

Adding a new job

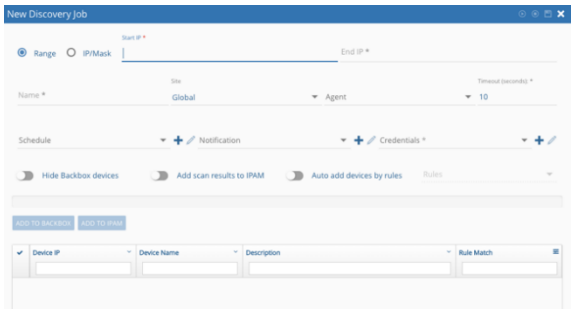


Figure 95: The Jobs Tab Screen

Button	What it Does
Range/IP MASK	The user can configure the IP range for the scan
Name	Name of the discovery job
Site	The discovery job can be attached to a specific site
Agent	Run the discovery job through an agent
Timeout	How much time to wait for SNMP answer from the scanned IP range
Schedule	Attach the discovery job to a schedule
Notification	Attach the discovery job to a notification
Credentials	Select a set of SNMP credentials configured in the credentials tab
Hide BackBox devices	Hide in the result table devices already configured in BackBox
Add scan results to IPAM	Any device discovered in the scan will be added automatically to the IPAM list in BackBox
Auto add devices by rule	Select rules that the user defined to match criteria and add them automatically to BackBox
Add to BackBox and Add to IPAM	Buttons that let you add the results manually to the matching lists

Credentials Tab

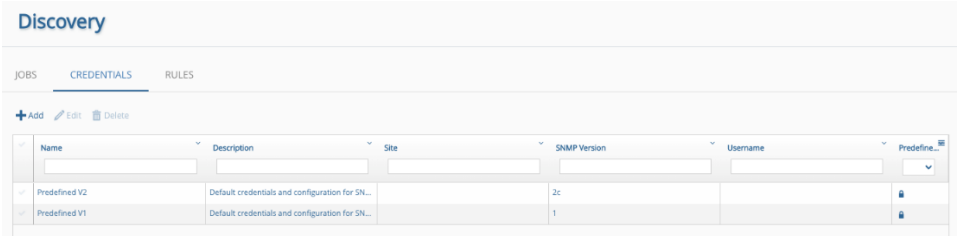


Figure 96: The Credentials Tab Screen

The credentials tab lets the user add a new set of credentials to the SNMP scan.

Pressing on Add will open a new window:

Button	What it Does
Name	The name the user gives to the credentials set
Site	Allows the user to attach the credentials to a specific site
Description	Enter the description for this set of credentials
SNMP version	Select the version of SNMP to be used
Port	Port used for the SNMP scan
Community/Username/Security level	Relating to the SNMP version selected, the user should add SNMP credentials to the scan

Rules Tab

This screen lets the user add new rules that will match criteria and add devices to BackBox automatically.

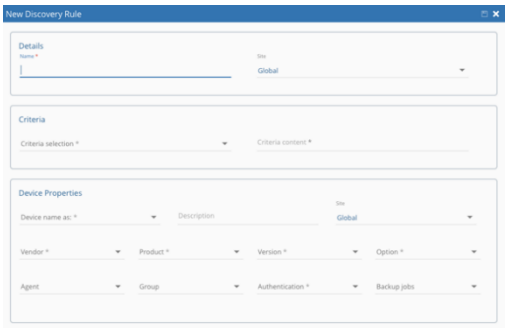


Figure 97: The Rules Tab Screen

Button	What it Does
Name	The name the user gives to the rule
Site	Allows the user to attach the rules to a specific site
Criteria	The criteria to match the scan result: IP Range/Hostname/Description
Criteria content	Select the criteria content matching the selected criteria
Device name as	Add the device to BackBox with the device name set as the scan result hostname or a given prefix and the result IP
Description	Set a description to the added device
Site	Add the device to a site
Vendor/Product/Version/Option	Add the device with the following parameters
Agent	Add the device to an agent
Group	Add the device to a group
Authentication	Apply an authentication template to the added device
Backup jobs	Add the device to a backup job

CHAPTER 10 TASKS

Tasks enables you to automate routine tasks to be performed on various devices within your system. You can create and schedule tasks such as changing passwords and permissions, maintenance tasks such as deleting, copying, or moving data, powering devices on or off, and many others. You can also specify conditions that restrict or trigger the tasks to be performed.

How It Works

The Task Configuration screen displays a list of previously configured tasks and enables you to configure new tasks. A task can include any sequence of commands (a script) that the device normally responds to when using the command line. By writing a script, you are actually writing a series of commands that will be executed as if you were at the command line. The Task Configuration screen helps you to write the script by enabling you to select commands from a simple dialog box as explained below.

After saving the task, you can then use the Task Jobs screen to assign the task to various devices and determine when the task is executed (see Understanding the Dynamic Fields Sections).

Assigning Tasks to Devices and Scheduling Task Execution).

The Task Configuration Screen

To display the Task Configuration screen, click Tasks on the Sidebar:

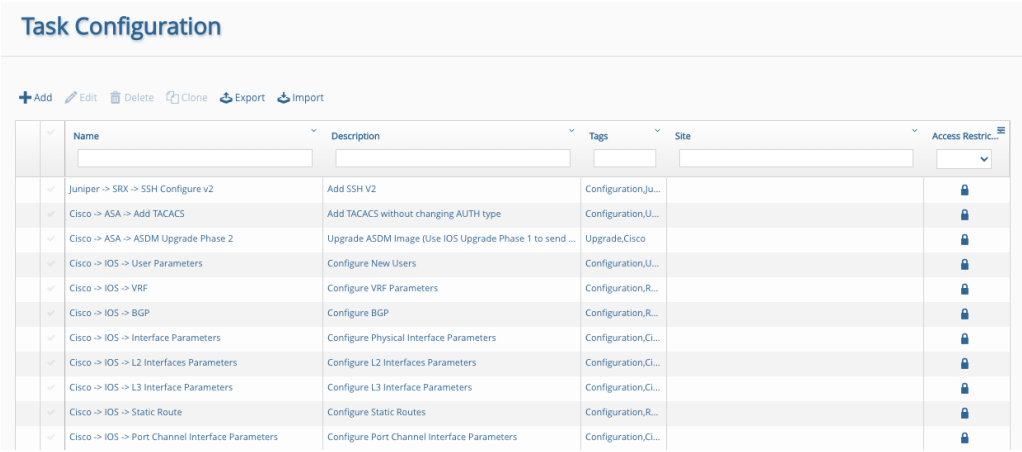


Figure 98: Task Configuration Screen

Adding a New Task

You can add a new task and write a task script using the Task Configuration screen.

To configure a new task:

1. On the **Tasks** screen, click the Add button Add to display the **New Task Configuration** dialog box:

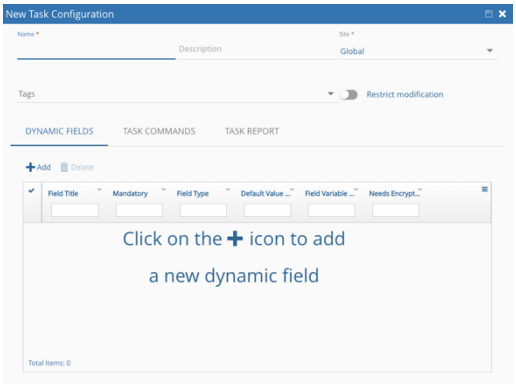


Figure 99: Adding a New Task Screen

2. Type a Name for the Task and click Save. The task now appears in the list of tasks in the Task Configuration screen, where you can edit it and write a script as shown in the next section,
3. Select a tag from the pre defined tags or create a new one
4. Creating a Task Script.

Creating a Task Script

You can create a task script for any task listed in the Task Configuration screen. Creating a task script enables you to insert conditions, variables, and other elements that provide greater control of the automated task.

To create a script for a task:

1. In the Task Configuration screen, select a task and click the Edit button Edit. Alternatively, click on a task name displayed in the list. A dialog box appears with the name of the selected task, which by default displays the Dynamic Fields Tab, for example

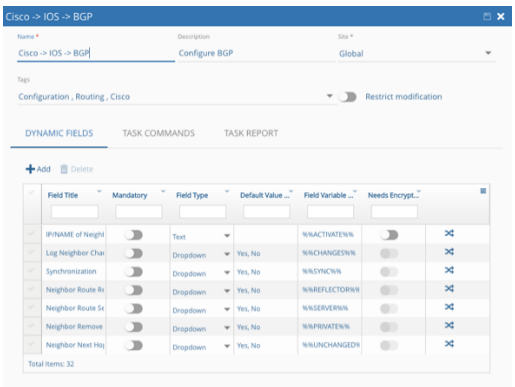


Figure 100: Edit Task Configuration Dialog Box displaying Add Access

2. Edit the Name, Description, and Site fields as desired.
3. To add fields and variables, click the Add button Add.
4. To add a command to the script, or to edit commands in the script, click the Task Commands tab. If the task already has a script, a list of commands to be executed is displayed, for example:

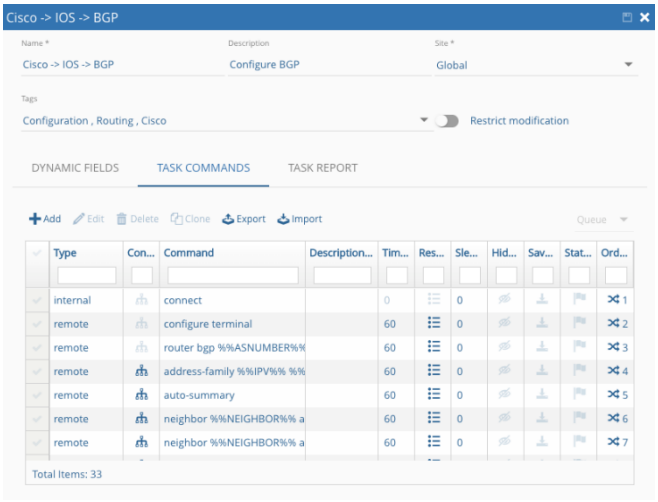


Figure 101: Edit Task Configuration Dialog Box Displaying Task Commands

The dialog box enables you to change the order of command execution by dragging the command's Reorder button up or down. You can also specify indicators for the command's execution by clicking the Results Options button in the command's Results field or the Status button in the Status field. For an explanation of Timeout and other fields, see the chapter Understanding the Dynamic Fields Sections.

5. To add a new command to the script, click the Add button Add . The Conditions dialog box appears:

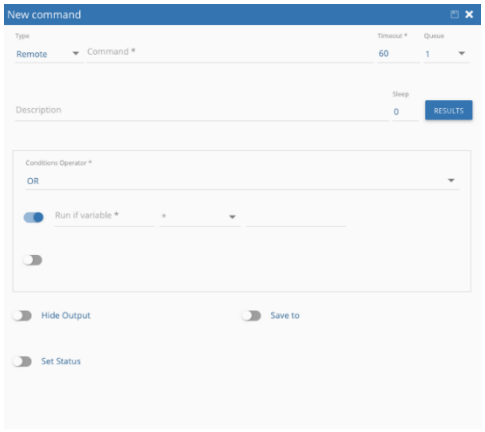


Figure 102: Conditions Dialog Box

6. Select the type of command (Internal, Local, Remote, or Verification), type the exact command in the Command field and use the remaining fields as desired. For details on these fields, as well as examples on writing command scripts, see the section Understanding the Dynamic Fields Sections.

Quick Tasks

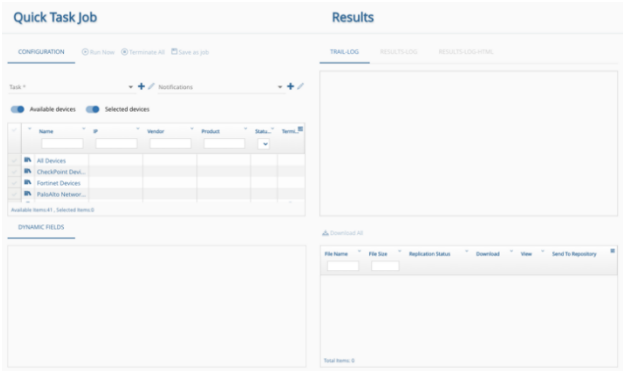


Figure 103: Quick Tasks Screen

The quick tasks screen lets you run on-demand tasks without scheduling a job

1. Select a task to run
2. Select a notification if needed
3. Choose the devices to run the task on
4. Enter dynamic field if existing in the task
5. Press on run now to run the task

Assigning Tasks to Devices and Scheduling Task Execution

The Task Jobs screen enables you to assign tasks to specific devices and to specify when the task is executed:

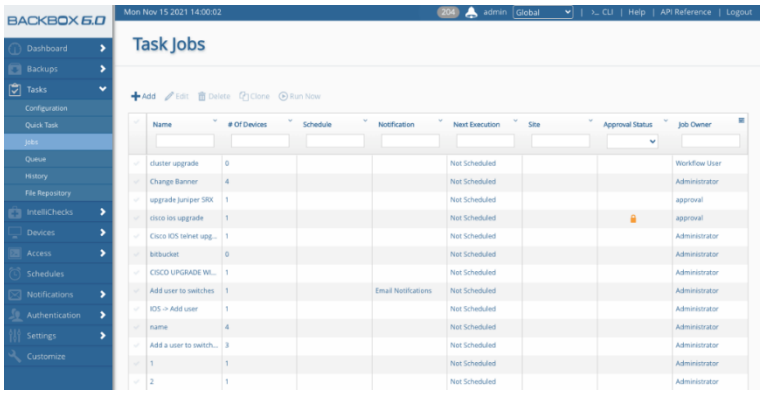


Figure 104: Task Jobs Screen

The **Task Jobs** screen displays a list of tasks, the number of devices to which the task has been assigned and other information. The following fields and buttons are displayed:

Table 18: Task Job Fields

Field/Button	Description
Name	Name which identifies the task job.
# of Devices	Number of devices to which the task has been assigned.
Schedule	The schedule assigned to the task that determines when it is executed. See below, To assign a task to a device and schedule its execution, for instructions on assigning a schedule.
Notification	The notification configuration to be implemented regarding the completion/failure of the task. To add a notification, see the section on Adding a Notification.
Next Execution	The date and time of the next execution of the task.
Site	The site to which the task is assigned.
Status	Enabled/Disabled
Add	Displays the New Task Job Configuration screen.
Edit	Displays the Task Job Configuration screen for selected task jobs.
Delete	Deletes selected task jobs.
Clone	Clones selected task jobs.
Run Now	Runs selected task jobs immediately.

To assign a task to a device and schedule its execution:

1. On the Task Jobs screen, click the Add button Add the New Task Job Configuration screen appears:

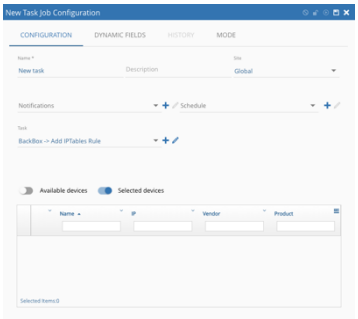
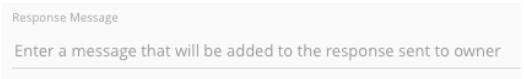


Figure 105: New Task Job Configuration Screen

2. Specify a name and description for the task job.
3. In the Notifications list select the desired notification configuration. Use the Add Notification button + or Edit Notification button to create or edit a notification configuration.
4. In the Site list, select a site for the task.
5. In the Schedule list, select a schedule that specifies when the task is to run. Use the Add Schedule button + or Edit Schedule button to create or edit a schedule. Alternatively, select Run once on, and specify a date and time for the task to run.
6. In the Task list, select the task that you want to execute. To create a new task on the fly, click the Add Task to System button + next to the Task field. Alternatively, you can select a task and edit it by clicking the Edit Task button .
7. If this task is created by a user that requires approval, a response message field will appear to enter the response to the user who created this task.



8. As an administrator, you can approve or deny the request to run the job .
9. If you are a user creating a task that needs approval from the administrator, you can select the admin recipient to receive the request.
10. You can add additional tasks or remove tasks by clicking the Add Task to Job button + or Remove Task from Job button − that are displayed underneath the Task list. For each task, a Dependency list appears that enables you to specify the task that will trigger the next.
11. To add devices to the task, click the Add Devices button + underneath Tasks. The Add Devices dialog box appears. Select the Devices you want to add and click Add Add.
12. To remove a device from the Device list, select the device you want to remove and click the Remove button −.
13. You can also use the Filter button to display the filter boxes by which to filter the Device list.
14. Click Save and run .

Mode

In the mode tab, you can select how to run multiple tasks related to each other.

Figure 106: Add User Configuration Screen

1. Select the run mode of tasks: Parallel or Sequential
2. If you choose sequential, there is an option for devices on task or tasks on devices and the ability to abort the job in case of failure
3. Enable task chaining: chain tasks to be run one after another with the option to create dependency on the result of the last task

Viewing Task Job History

You can view the history of a task job by clicking the Task Job History tab in the Task Job Configuratoin screen for the selected task job. The Task Job History tab displays the following parameters: Start Time, End Time, Status, Comments, and Task Name.

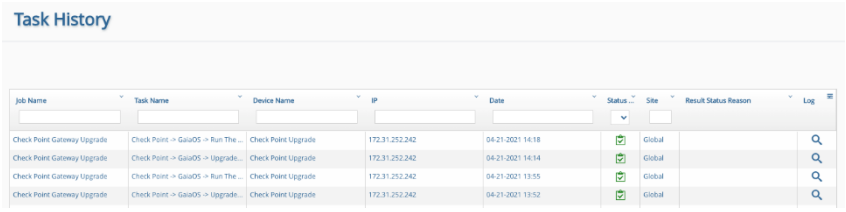


Figure 107: Task Job History Tab

Modifying an Existing Task Job

You can edit a task job listed in the Task Jobs screen by selecting a task job displayed in the list and clicking the Edit button Edit . The Task Job Configuration screen for the selected task job appears with the same fields as those in the New Task Job Configuration screen. Edit the fields as desired and click Save or Run .

Viewing a Task Job in the Queue

You can view the progress of a task job in the Task Queue screen:

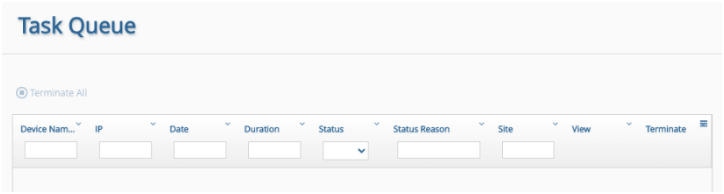


Figure 108: Task Queue Screen

For each device to which the task is assigned, the screen displays the device name, device IP, date, duration (how long the device has been running the task), and status of the job (for example, Running). To terminate a task job for a specific device, click the button in the Terminate column for that device. To terminate all task jobs in the queue, double-click the Terminate All button Terminate All .

Viewing Task History

The Task History screen displays a list of devices that have run task jobs, along with the job name, the task name, device name, device IP, the date when the task job was run, its status (success, failure) and, if the status is failure, the reason for the failure.

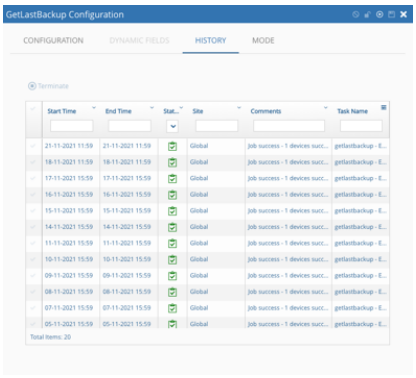


Figure 109: Task History Screen

You can download a log of the history by clicking the View Log button in the Log column for the device.

Task File Repository

You can upload a task file in the Tasks File Repository screen.

1. You can choose to download existing files to your PC

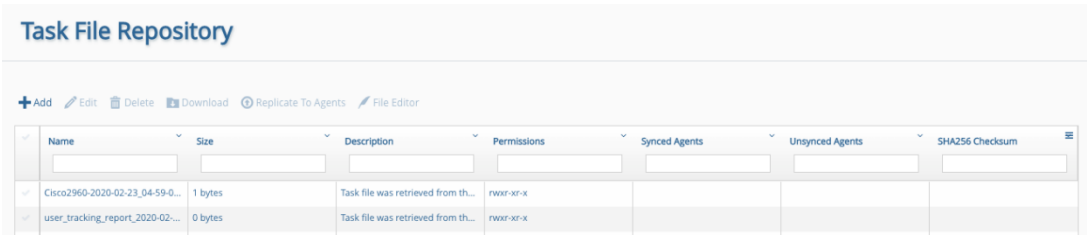


Figure 110: Tasks File Repository Screen

2. You can choose to replicate the files to unsynced agents Replicate To Unsynced Agents
3. You can edit text-based files in the file editor File Editor
4. Download

To upload a new tasks file:

1. In the Tasks File Repository screen, click the Add button Add. The New Tasks File dialog box appears.

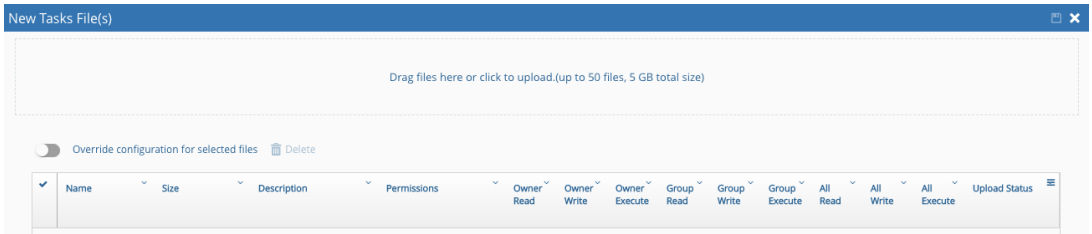


Figure 111: New Tasks File Dialog Box

2. Drag a file from your computer to the Upload File Box in the center, or alternately, click on the Upload File Box and select a file to upload.
3. Add a description, select an agent, and click Save .

To edit a tasks file:

1. Select a file and click the Edit button Edit The Edit Tasks File dialog box appears with the name of the tasks file in the Title Bar, for example:

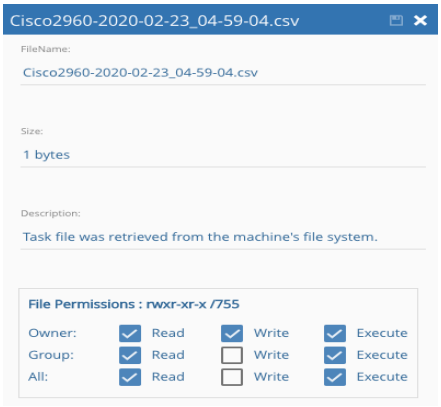


Figure 112: Edit Tasks File Box

2. File permission options let you control the file permissions on the saved file in the file repository
3. Edit the Description and Agents fields as desired and click Save .

To delete a tasks file:

1. Select the file you want to delete and click the Delete button Delete. A prompt appears, asking you to confirm deletion.
2. Click Yes.

CHAPTER 11 REPORTS

BackBox enables you to generate reports that provide information about your devices and the statuses of the backups, using all the data available in the BackBox system. You can either use BackBox's wide range of predefined report types, or you can create your own customized reports. For either kind of report you can specify scheduling and notification.
To display reports that have already been generated, on the Sidebar, click dashboard, then click Reports; the Reports screen appears:

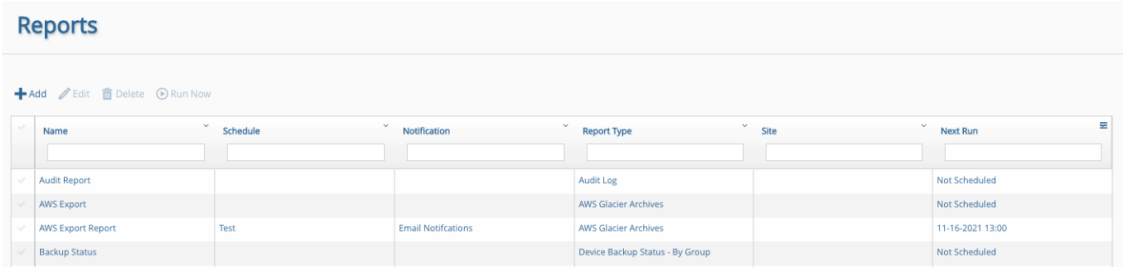


Figure 113: Reports Screen

Adding a New Report

Use the Reports screen to create and schedule new reports. You can create reports by either selecting predefined reports or by selecting a customized report. For information on how to create a customized report, see Creating Customized Reports.
To add a new report:

1. On the Reports screen click the Add button Add. The New Report Configuration dialog box appears.

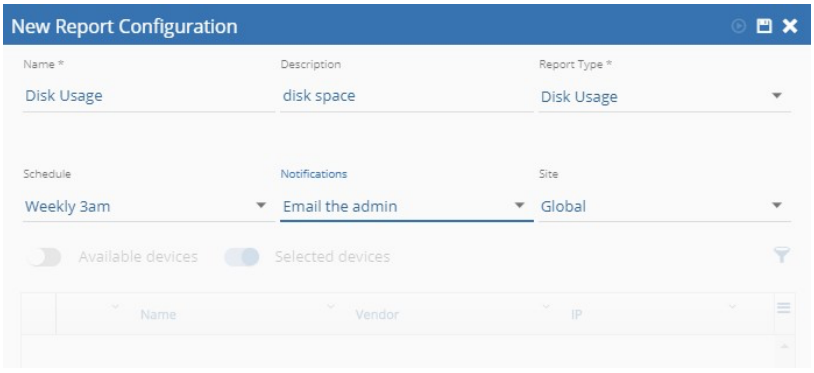


Figure 114: New Report Configuration Dialog Box

2. Type a name and a short description for the report.
3. In the Report Type list, select a Predefined or Customized Report type for your report. For a description of predefined report types, see Types of Predefined Reports below. Customized report types also appear in the Report Type list. For an explanation of how to create a customized report type, see Creating Customized Reports.
4. Select a schedule and method of notification.
5. Select the site where you want the report to be implemented.
6. Click Save.

Editing a Report

You can change report parameters using the Edit button Edit .
To edit a report:

1. In the list of reports, select a report and click the Edit button Edit. The New Report Configuration dialog box appears with the details for the selected report.
2. Edit the appropriate fields.
3. Click Save.

Deleting a Report

To delete a report:

1. In the Report Types list, select the report to delete and click the Delete button Delete
   A prompt appears requesting confirmation.
2. Click Yes.

Types of Predefined Reports

You can create reports from a list of 17 predefined report types. This section provides examples of each predefined report type.

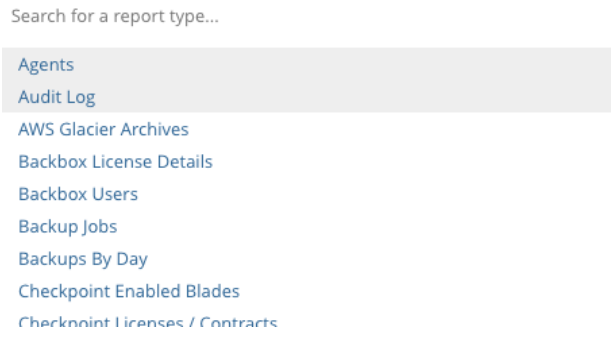


Figure 115: Report Type List

CHAPTER 12 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.

Enable IntelliChecks

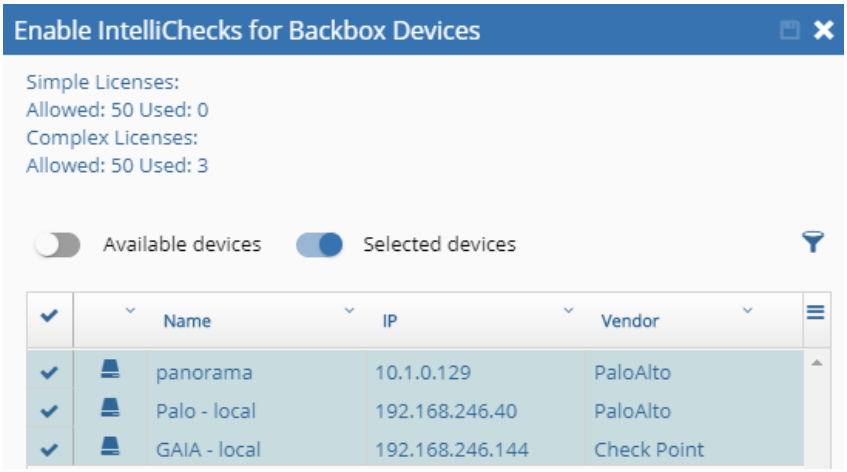


Figure 116: Enable IntelliChecks Dialog

IntelliChecks Signatures Screen

IntelliChecks uses a database of hundreds of signatures that test various conditions across a wide variety of devices. This page displays the list of existing signatures and enables you to clone/edit them or create completely new signatures.

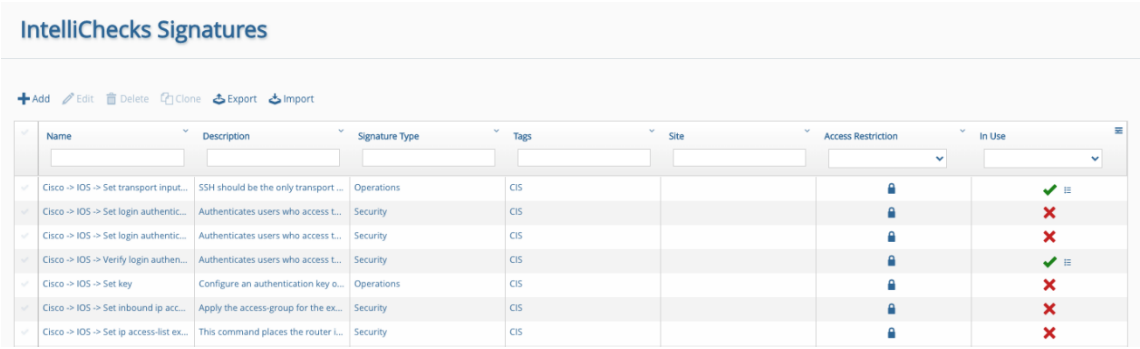


Figure 117: IntelliChecks Signature Screen Displaying Signatures, Types, Tags, and Site

Adding a new Signature

To add a new IntelliChecks signature:

1. In the IntelliChecks Signature screen, click the Add button Add. The New IntelliChecks Signature dialog box appears

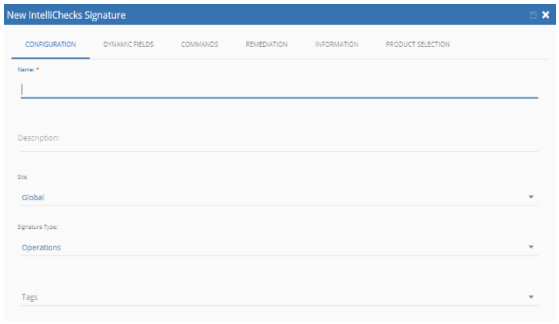


Figure 118: New IntelliChecks Signature Configuration screen

2. In the dialog box, you can add values for new signatures or edit values for cloned existing signatures.

IntelliChecks Groups Screen

By using Groups, you can simplify management of similar devices. By putting all of the devices of 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.

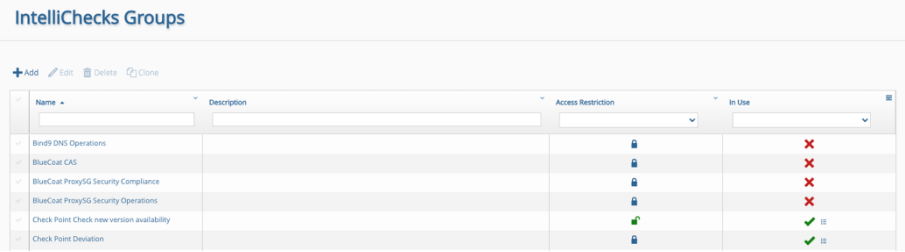


Figure 119: IntelliChecks Groups Screen

IntelliChecks Jobs Screen

This screen shows the name and description of the job along with the specified schedule and notification and whether or not the job will attempt remediation.

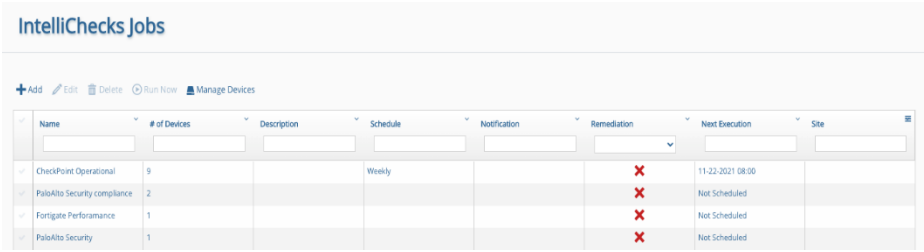


Figure 120: IntelliChecks Jobs Screen

The screen also displays when the next execution will occur.
In addition, you can select a job in the list and use the buttons at the top of the screen: Edit, Delete, or, Run Now.

Creating a New IntelliChecks Job

1. Click the Add button Add. The New IntelliChecks Job Configuration dialog box appears:

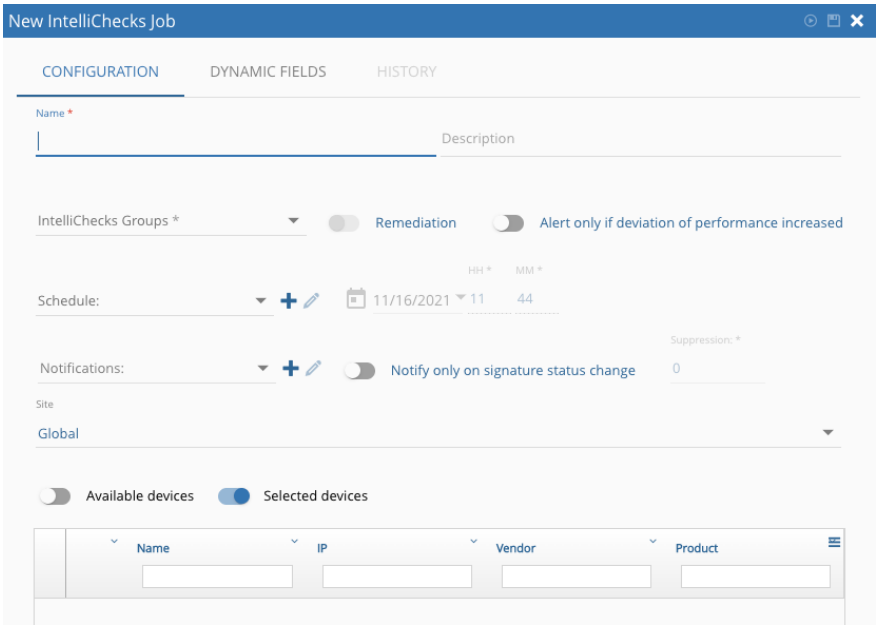


Figure 121: New IntelliChecks Job Configuration Screen

2. Type a name and description for the job in the appropriate fields. Select the group on which you want to run the job, using the dropdown menu.
3. The switch Alert only if deviation of performance increased let you control getting notification only on positive deviation
4. The switch Notify only on signature status change let you control getting notification only if status has changed from the last time the IntelliChecks was running
5. Suppression let you control after how many times the signatures were running at the same status to stop getting notifications

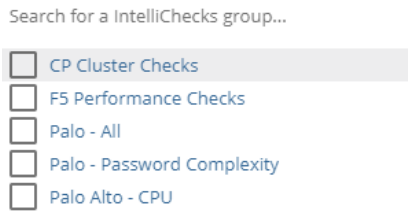


Figure 122: Search for IntelliChecks Group

6. If you want the job to run the remediation commands for the signature, click the toggle for it: Remediation

7. Choose a Schedule and Notification for the job, and then select the devices on which you want to run the job. Selecting both the Available devices Selected devices buttons display all devices with a checkmark next to the selected devices.
8. Dynamic fields tab let you enter info into dynamic files when the IntelliChecks signature requires it.
9. The history tab lists the IntelliChecks job history and the signatures running as part of it.
10. To run the IntelliChecks job ad hoc, select the Run Now option Run Now.
11. Manage Devices lets you view and assign IntelliChecks licenses.

IntelliChecks Queue Screen

You can view a list of devices for which you have scheduled IntelliChecks jobs in the IntelliChecks Queue screen:

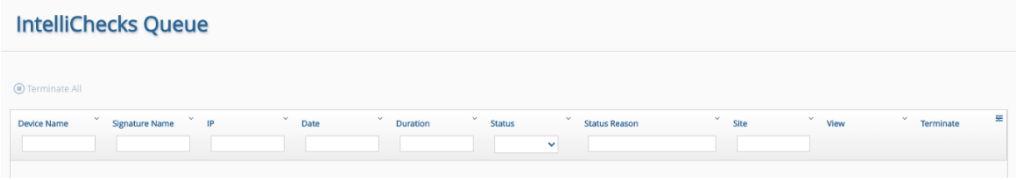


Figure 123: IntelliChecks Queue Screen

The **IntelliChecks Queue** screen displays the device name, signature name, IP, date and duration of the IntelliChecks job, and its current status (running, pending, or enqueued). It also enables you to view the job's log in real time. In addition, you can terminate selected IntelliChecks jobs, or terminate all IntelliChecks jobs:

- To terminate a single job, click the Terminate button at the right side of row for that job.
- To terminate all the IntelliChecks jobs for all devices in the queue, click the Terminate All button Terminate All at the top of the screen.

IntelliChecks History Screen

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

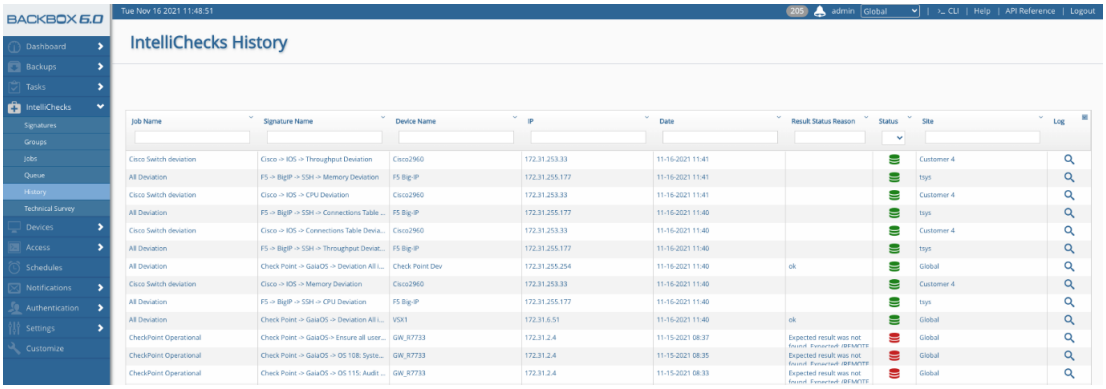


Figure 124: IntelliChecks History Screen

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.

Technical Survey

The technical survey tab allows the user to view predefined fields for the technical survey IntelliChecks. The user can also add new fields and create new IntelliChecks to save information to the relevant variables.

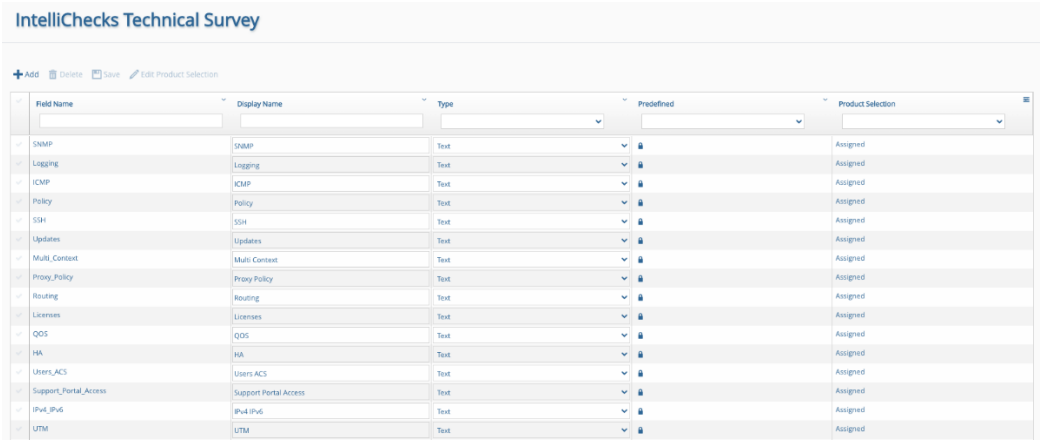


Figure 125: IntelliChecks Technical Screen

This information will be presented in the device technical survey tab and the technical survey report.

1. Add button will let you add new fields Add .
2. With the delete button, you can remove existing fields Delete .
3. Edit product selection will allow you to choose which products are relevant to which technical survey field Edit Product Selection .

CHAPTER 13 ACCESS

Access enables you to use BackBox as a jump box and funnel all connections to your devices through a single point. This simplifies firewall rule management (as you no longer need rules for every person to every device), helps thwart man-in-the-middle attacks, and even allows for greater accountability for employees.

Once connected to a device, you can run commands ad hoc, or you can use toolboxes of preconfigured commands. BackBox has several toolboxes already configured, but users can easily create their own as well.

Connecting to Devices Using the Terminal Screen

The Terminal screen enables you to connect to one or more devices. For each device, a terminal is opened on which you can run commands.
To connect to devices:
On the Sidebar, click Access; the Terminal screen is displayed by default.
Click the Devices tab; a list of devices is displayed:

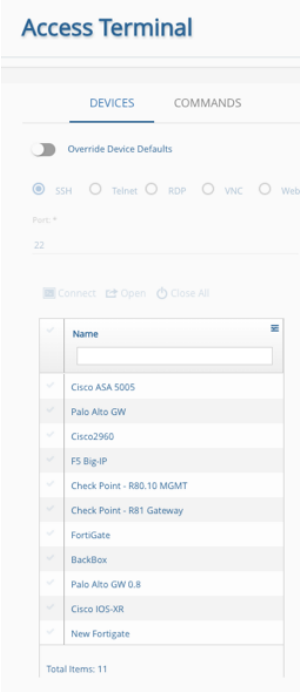


Figure 126: Devices Tab on the Terminal Screen

1. Select devices to which you want to connect by clicking in the column to the left of the device.
2. Select the method of connection: SSH, Telnet, RDP, or Web.
3. Edit the Port if desired by clicking the port number and using the Increment/Decrement button that appears to specify another port and click the Submit button.

Figure 127: Changing the Port

4. Click the Connect butto Connect ; a name is displayed at the top of the screen for each device that you selected. Clicking the device name displays the terminal for that device. You can run scripts on more than one device by clicking from device to device:

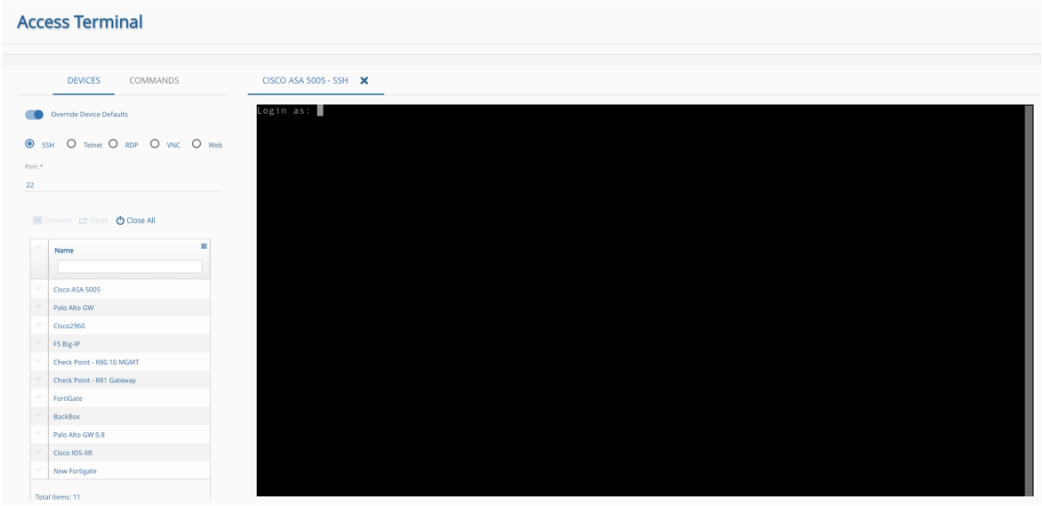


Figure 128: Terminal Screen with Multiple Devices Connected

Running A Toolbox's Command Script

Once you connect to one or more devices, the Access's Terminal screen enables you to run toolbox scripts on the terminal display for each device.

To run commands on a device:

1. Once you have your connection running, click the Commands tab; a list of toolboxes appears:

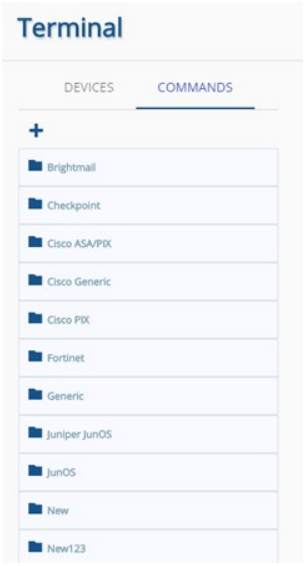


Figure 129: Commands Tab Listing Toolboxes

2. Click a toolbox to display its commands. Some toolboxes have Categories; click the Category to display its commands:

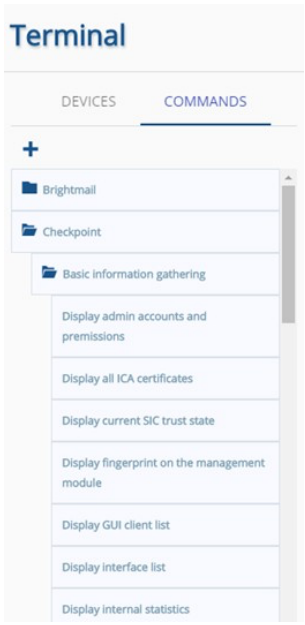


Figure 130: Toolbox Displaying Category and Commands

3. To run a command, on the device's terminal, click the command and right-click to display the following menu:

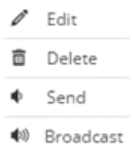


Figure 131: Command Options Menu

4. Click one of the following options:
    - Edit to make changes to the command.
    - Delete to remove the command from the toolbox.
    - Send to execute the command.
    - Broadcast to send the command to all open windows.

Editing Toolboxes and Commands

You can edit toolboxes and their commands directly on the Commands tab on the Terminal screen.
You can edit the name of the toolbox, as well as add commands or sections to it. Categories help organize commands.

Adding Categories or Commands to a Toolbox

To add a category or command to a toolbox:

1. Right-click the toolbox to which you want to add the category or command. The Add Node dialog box appears:

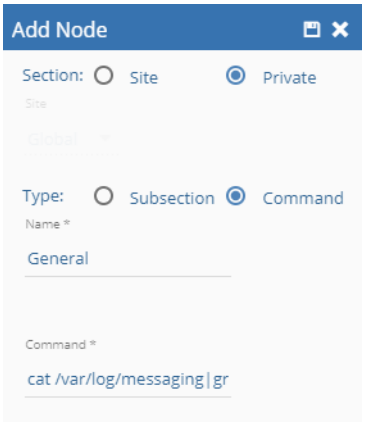


Figure 132: Add Node Dialog Box

2. If you select Subsection for the Type, you will enter the name for the subsection. If you select Command as the Type, then you enter a name for the command as well as the code of the command in the field at the bottom.
3. Click Save.

Editing the Name of a Toolbox

To edit the name of a toolbox:

1. Right-click the toolbox you want to edit and click Edit. A dialog box with the name of the toolbox appears.
2. Edit the name and click Save.

Cloning a Toolbox

To clone a toolbox:

1. Right click the toolbox and click Clone. The Clone Toolbox dialog box appears.
2. Edit the name of the clone as desired and click Save. The cloned toolbox appears in the list of toolboxes on the Terminal screen.

Deleting a Toolbox

To delete a toolbox:

1. Right-click the toolbox you want to delete and click Delete. A Delete prompt appears.
2. Click Yes.

Editing Commands

You cannot edit BackBox created commands, but you can Clone them and then edit the clones. You can always edit commands that you have created, without the need to clone. To edit a command:

1. Right-click the command you want to edit and click Edit.

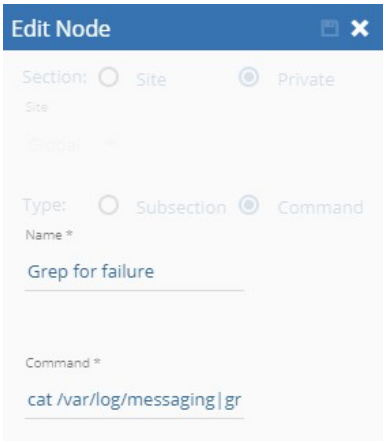


Figure 133: Edit Command Dialog Box

2. Edit the command's name, or the command's code and click Save.

Deleting a Command

To delete a command:

1. Right-click the command you want to delete and click Delete. A Delete prompt appears.
2. Click Yes.

CHAPTER 14 CUSTOMIZE

The Customize screen enables you to customize backup scripts, restore scripts, inventory information, toolbox commands, automated tasks, and health checks. BackBox supports a robust scripting environment that makes it easy to write and edit scripts with easy-to-use tabs and drop-down lists. The scripting environment is available in various modules in BackBox including Tasks, Health Checks, IntelliChecks, Devices, and Customize.

Besides enabling you to write scripts, the Customize screen also allows you to customize lists that appear in other BackBox screens.

On the Sidebar, click Customize. The Customize screen appears:

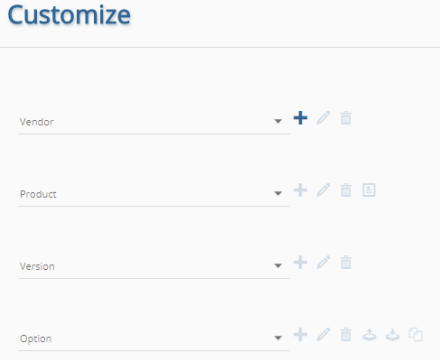


Figure 134: Customize Screen

Customizing Vendor, Product, and Version Lists

The Customize screen enables you to customize Vendor, Product, and Version lists that appear in other screens in BackBox such as in the Devices screen. Use the Add, Edit, and Delete buttons + ✎ 🗑 next to each list to add, edit or delete items. Some of the items listed are dependent on others. For example, if you selected a vendor in the Vendor list, the products that appear in the Product list are from that vendor only.

BackBox issued interface scripts cannot be edited; however, they can be cloned and the clones can be edited.

After selecting Vendor, Product, Version, and Option, click the Edit icon ✎. The Customize editing interface appears:

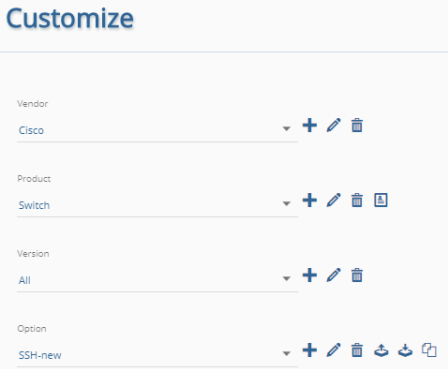


Figure 135: Customize Editing Interface

Option Configuration Screen

The Option Configuration screen enables you to customize backups for any device in your system. It enables you to write command scripts for device backup, inventory, restore, and cleanup as well as define additional options and fields for the Devices screen. You can customize additional fields and their defaults for the Device Details tab and the Inventory tab for a device.

To display the Option Configuration screen, on the Sidebar, click Customize. The Customize screen appears. Select the vendor, product, and version, and in the Option box, select the option you want to edit or click the Add Option button + to create a new option. In either case, the Option Configuration screen appears:

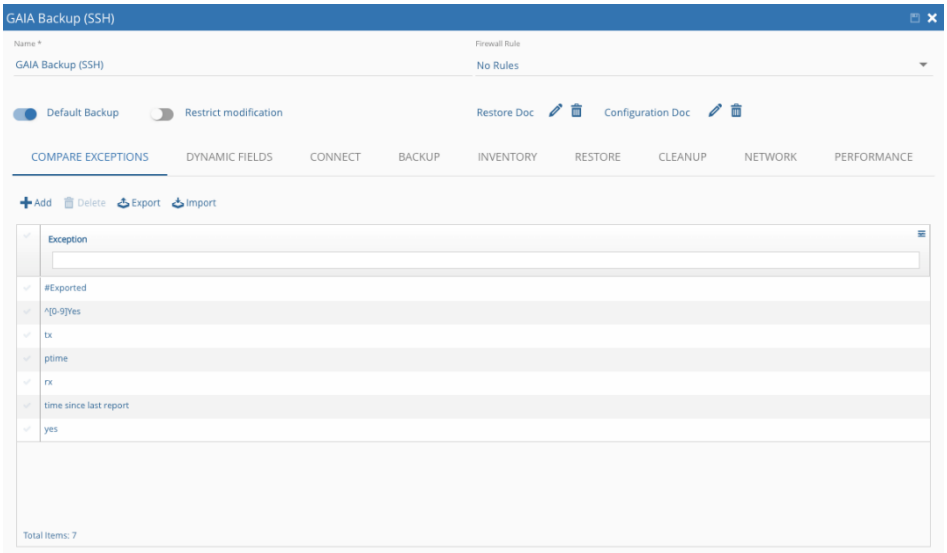


Figure 136: Customize Configuration Screen

Option Configuration Scripting Tabs

The Option Configuration screen's scripting tabs include: Compare Exceptions, Dynamic Fields, Connect, Backup, Inventory, Restore, Cleanup, and Network.
The scripting tabs enable you to write and edit scripts for a variety of actions. You can add a sequence of commands that will be executed, line by line.
Note: Commands on the Connect tab and the Inventory tab can only be initiated if called by a command on the Backup tab as explained in the relevant sections below.
The scripting tabs and their uses are as follows:

Table 19: Option Configuration Scripting Tabs

Tab	Used for
Compare Exceptions	Listing fields that can be selected for comparisons.
Dynamic Fields	Creating dynamic variables.
Connect	Connecting to a remote device.
Backup	Creating a backup for the device.
Inventory	Providing information about the device.
Restore	Restoring the device.
Cleanup	Cleaning up remains of the backup process.
Network	Providing network information

The relationship between the six scripting tabs is as follows:

- The command sequence on the Connect tab can be called by a Connect command from the Backup, Restore, IntelliChecks, and Cleanup tabs.
- The command sequence on the Inventory tab can be called by an Inventory command from the Backup, Restore, IntelliChecks, and Cleanup tabs.

1. In the Name box, type or edit the name of the option as desired. It is recommended to indicate the protocol in use in the name. For example, common names are SSH, TELNET, FTP.
2. If you want to select Firewall rules, the dropdown menu has several choices:

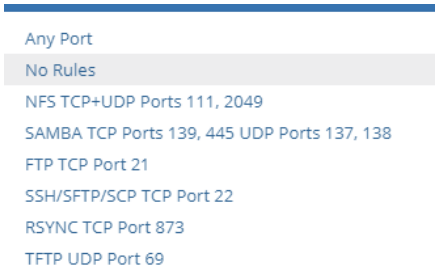


Figure 137: Firewall Rule Menu

Understanding the Compare Exceptions Section

Compare Exceptions will allow you to select fields that you want to have compared from one backup to another.

Understanding the Dynamic Fields Sections

Dynamic Fields enables you to define fields that appear on the Device Details tab for a device listed in the Devices screen. The tab contains two sections:

- Dynamic Fields section in the upper part of the tab. Here you determine whether a field is Mandatory, Encrypted, or Hidden.
- Inventory section in the lower part of the tab (you may need to scroll the tab to display this part). Here you assign the fields to be shown in the Inventory report for the device.

Table 20: Options Columns of Dynamic Fields

Selecting this:	Causes this:
Mandatory	The field becomes required. You cannot save the settings on the Device Details tab without supplying a value for this field.
Encrypt	Encrypts the field's contents so that it appears as dots. This is the default for fields such as Password.

Selecting this:	Causes this:
Hide Command	The field will not appear in the Backup log.
Free Text	Displays the text that will appear as the name of the field on thescreen.
Default Value	A default value will appear in the field when the screen is displayed. This is optional.

Authentication

Determines whether this device will be enabled to use with authentication templates. The default action is that they will, and that the authentication will be mandatory. If an authentication template is chosen, the Username / Password / etc. fields that are irrelevant will be hidden.

Authentication Templates

When Use Templates is selected in the Authentication list, it displays a list of authentication templates to select from.

Server IP

Displays a list of IP addresses of the BackBox server. These IP addresses will be used by BackBox to determine the IP address to which to send the file.
Variable: %%SERVER_IP%%

Username

Displays a field for the Username login to the remote device.
Variable: %%USER%%

Password

Displays a field for the Password login to the remote device.
Variable: %%PASSWORD%%

Extra Password

Displays a field for the Extra Password (expert mode, enable mode, priv mode, su, etc.) to the remote device.
Variable: %%SU_PASSWORD%%

Username 2

Sometimes a device will need a dual login. This field is for the second username to log-in to the remote device.
Variable: %%COMMAND_USER%%

Password 2

Sometime a device will need a dual login. This will display a field for the second user password to the remote device.
Variable: %%COMMAND_PASSWORD%%

SNMP Version

Displays a field for the SNMP version login to the remote device.
Variable: %%SNMP_VERSION%%

SNMP Community string

Displays a field for the SNMP community to the remote device.
Variable: %%SNMP_COMMUNITY%%

Port

Displays a field for the communication port to the remote device.
Variable: %%PORT%%

Note: In this field, the free text value will be configured as the default value, and the label is hard-coded to the port.

Backup Custom Field

Displays a custom field to use with the remote device.
Variable: %%CUSTOM_1%%

Cluster Node IP

Some devices may be part of a cluster. This field displays a field for the cluster node IP.

The Inventory section of the Dynamic Fields tab is in the lower part of the tab (scroll down) and looks like this

Figure 138: Inventory Section of the Dynamic Fields Tab

This section enables you to create fields for the device's Inventory tab in the Devices screen. To create a field for the device's Inventory tab, click the Add button Add. The new Inventory field is added to the list of field labels. In the Free Text column, type a name for the field and click the Submit button . After clicking Save, the fields will be displayed on the Inventory tab for the device in the Devices screen.

Variables: To access the contents of any of the Inventory fields in backup command scripts, use the variables %%Custom_Field1%%, %%Custom_Field2%%, etc., and not the name given in Free Text.

Clicking the Add button Add on a scripting tab's toolbar or clicking on the large Add icon + in the middle of the tab's screen, displays the Conditions dialog box, in which you can configure the command and its parameters. Clicking Save returns you to the Option Configuration screen, which now displays information on your configuration, including such items as the type of command, description, timeout, the message that the command generates upon execution or failure (Result Option), etc.

Understanding the Connect Section

The Connect section contains the commands used to log into the target device.
This command set can be invoked by other sections by using the Internal command "Connect".

Understanding the Backup Section

The Backup section is where the backup commands for a given device are located. You use these commands to backup additional files

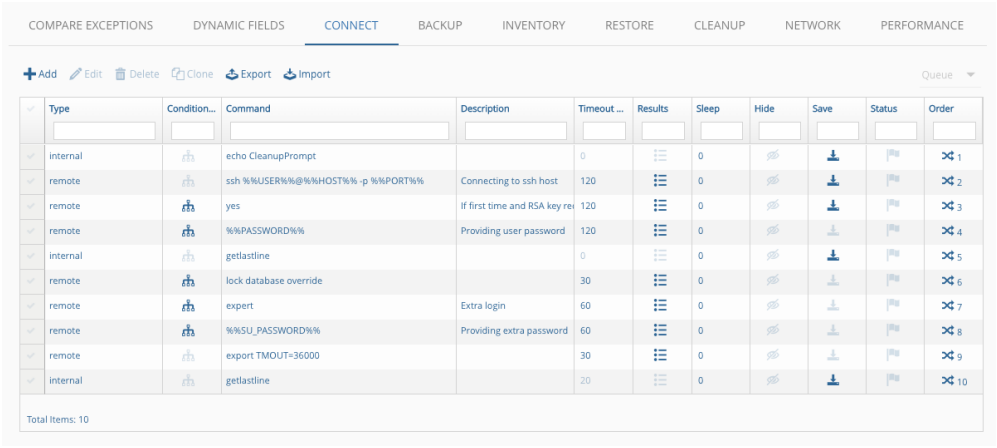


Figure 139: Connect Tab

Understanding the Inventory Section

This is where the commands are given to collect specified inventory data items.

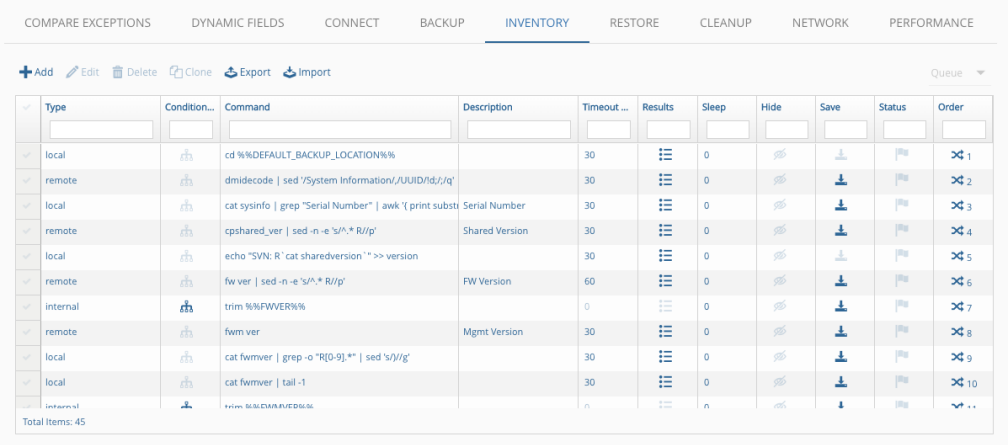


Figure 140: Inventory Tab

Understanding the Restore Section

These commands are used when a Restore is selected.

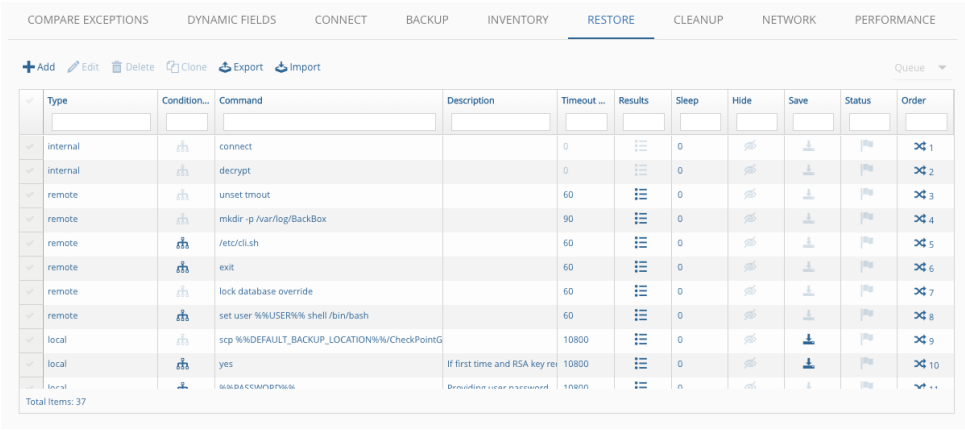
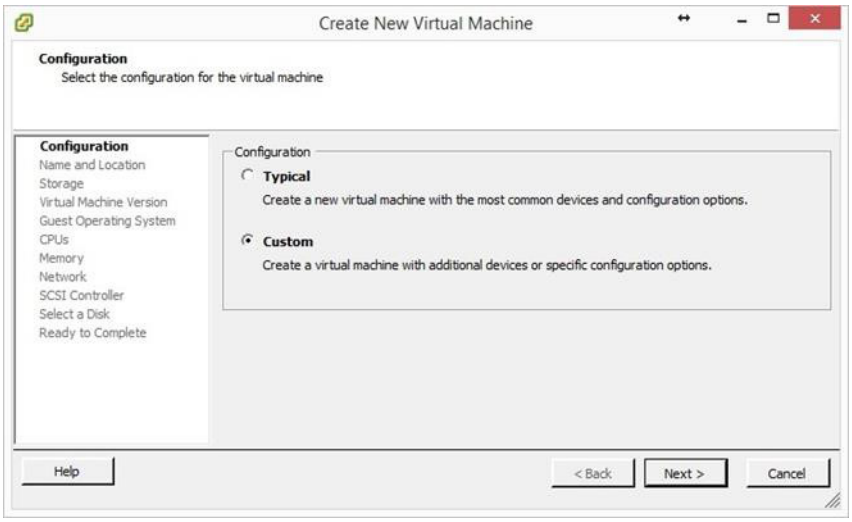


Figure 141: Restore Tab

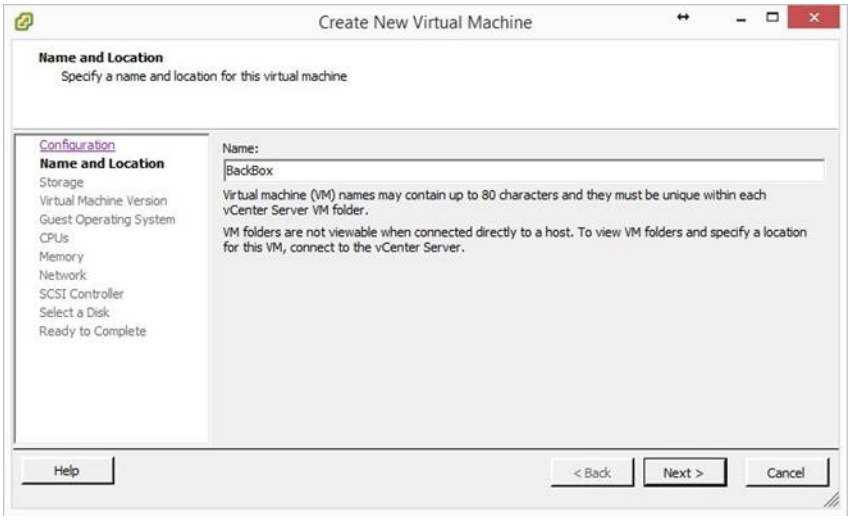
Appendix A VMWare Installation

This chapter provides instructions on how to install BackBox on a system running VMWare.

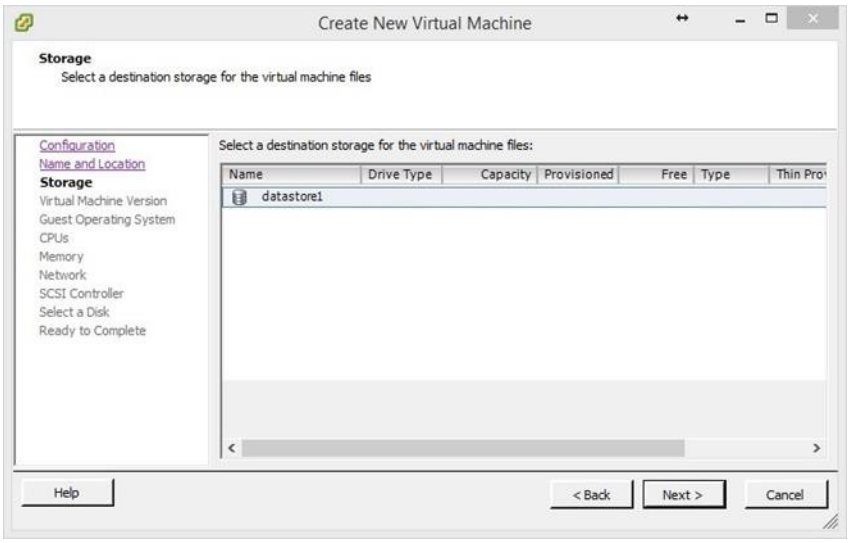
1. Open the vSphere client.
2. From the upper pane, click on File.
3. Select New -> Virtual Machine.
4. On the Configuration pane, select Custom and click Next.



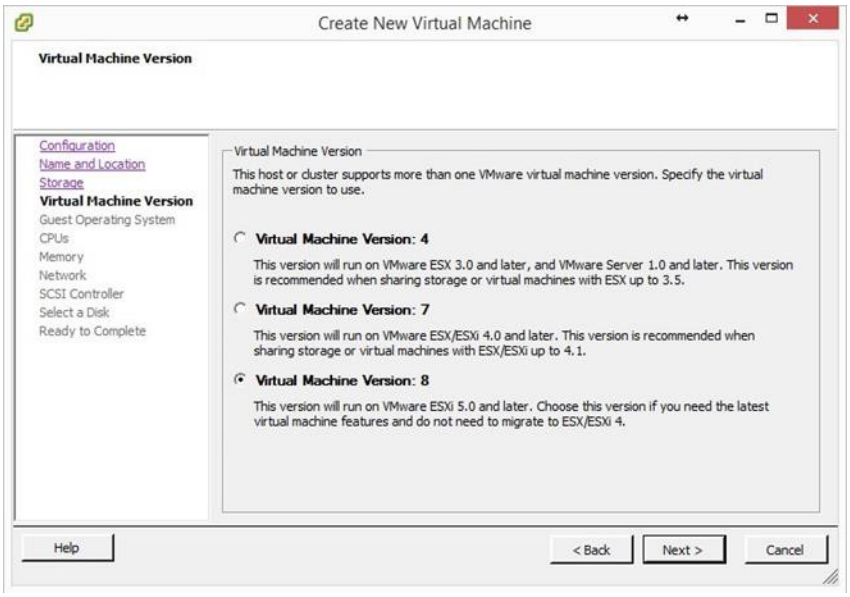
5. On the Name and Location pane, in the Name field, specify "BackBox" or any other name, and click Next.



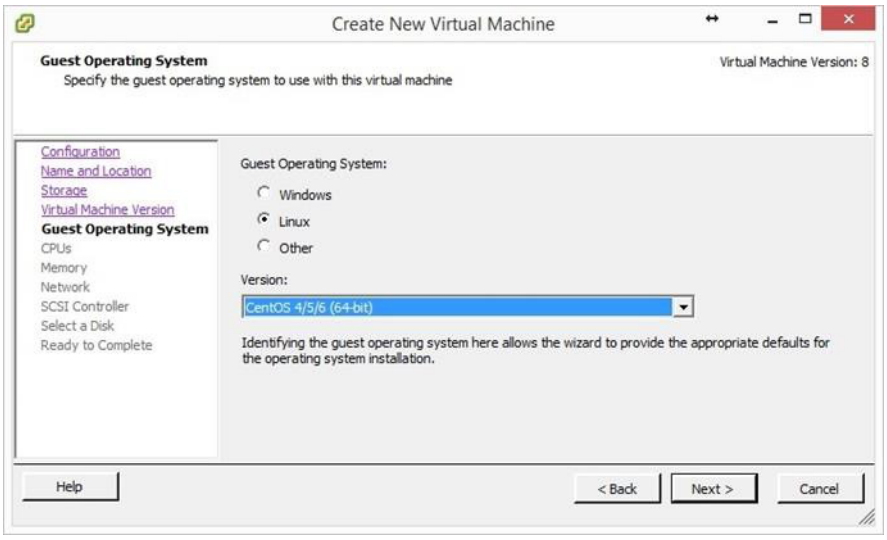
6. On the Storage pane, select the data store that you want BackBox to reside on and click Next.



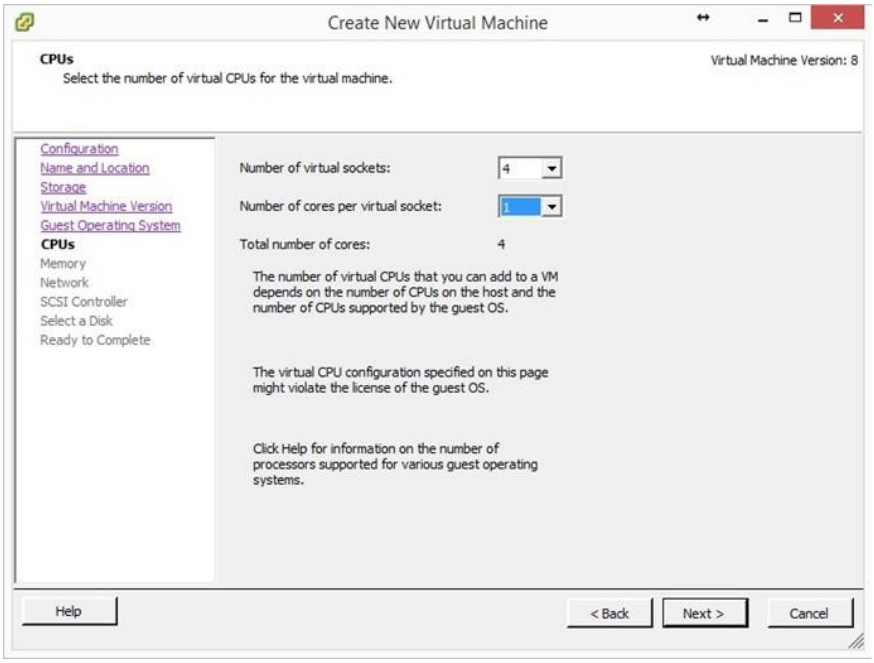
7. In the Virtual Machine Version pane, select Virtual Machine Version 8, and click Next.



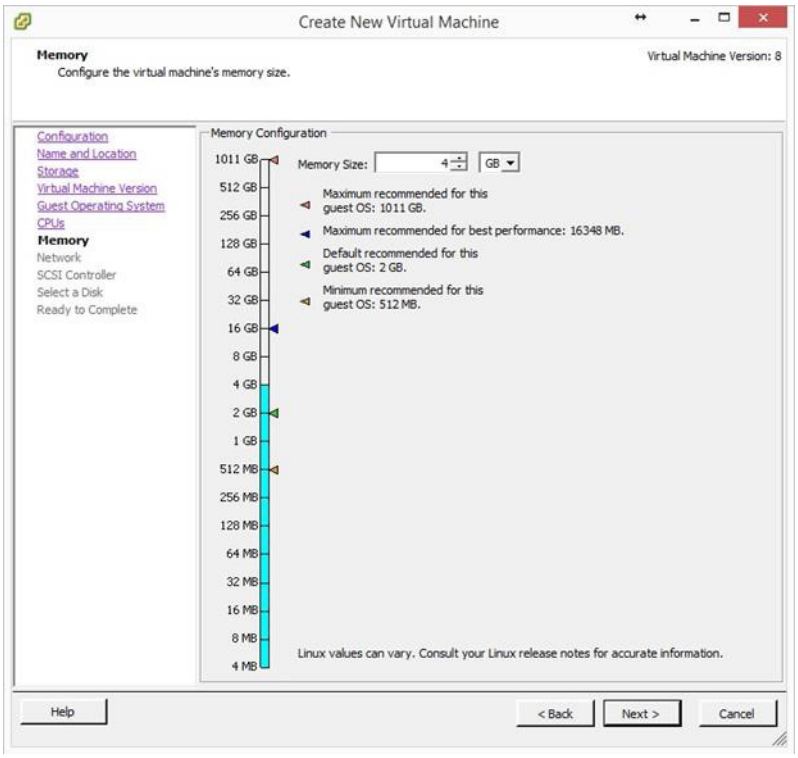
8. On the Guest Operating System pane, select Linux and in the Version box, select CentOS 4/5/6 (64-bit) and click Next.



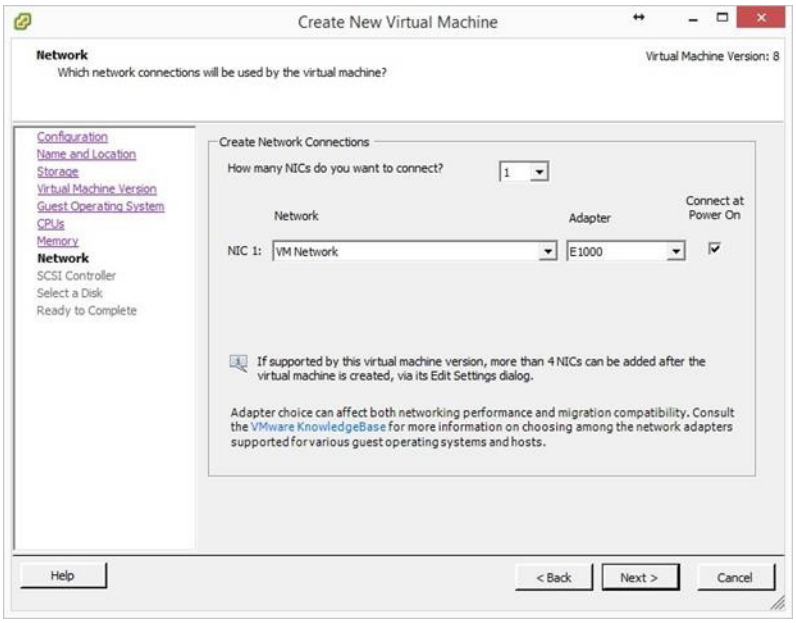
9. On the CPU pane, make sure that the Total number of cores is at least 4, and click Next. For more specific details, consult the Sizing document.



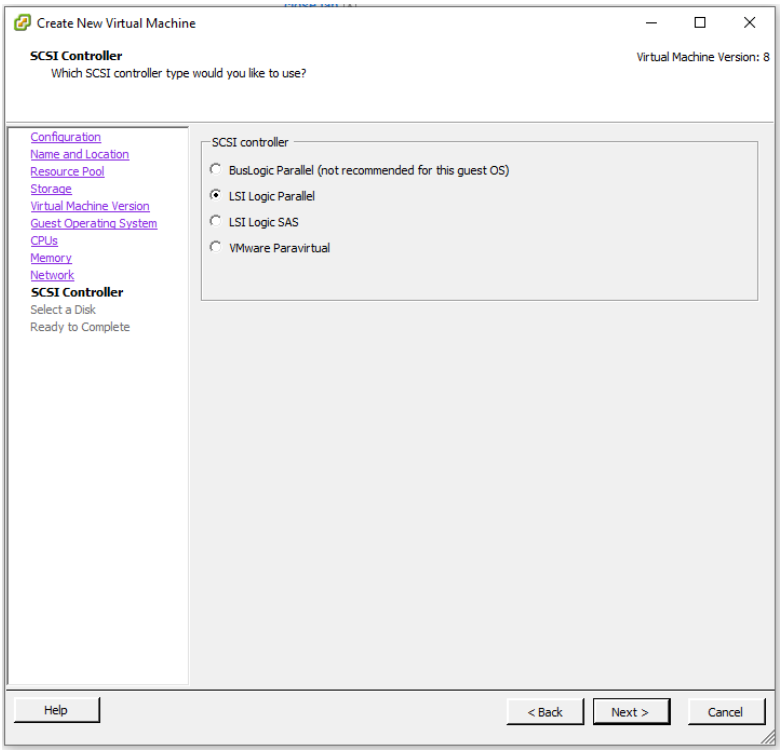
10. On the Memory pane, for Memory Size, specify a minimum of 4096MB. For more specific details, please consult the Sizing document.



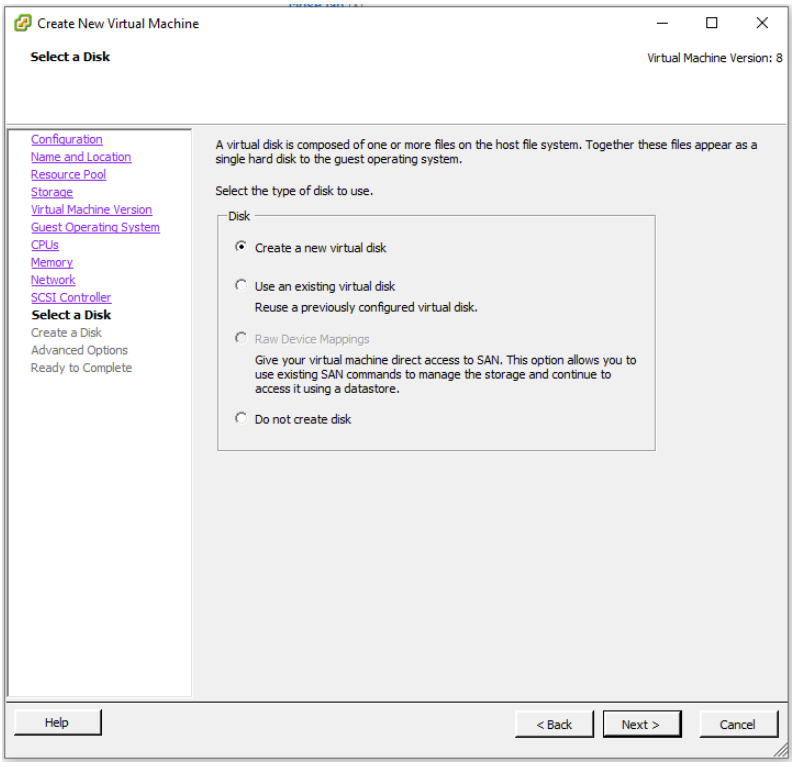
11. On the Network pane, select the E1000 network adapter and click Next.



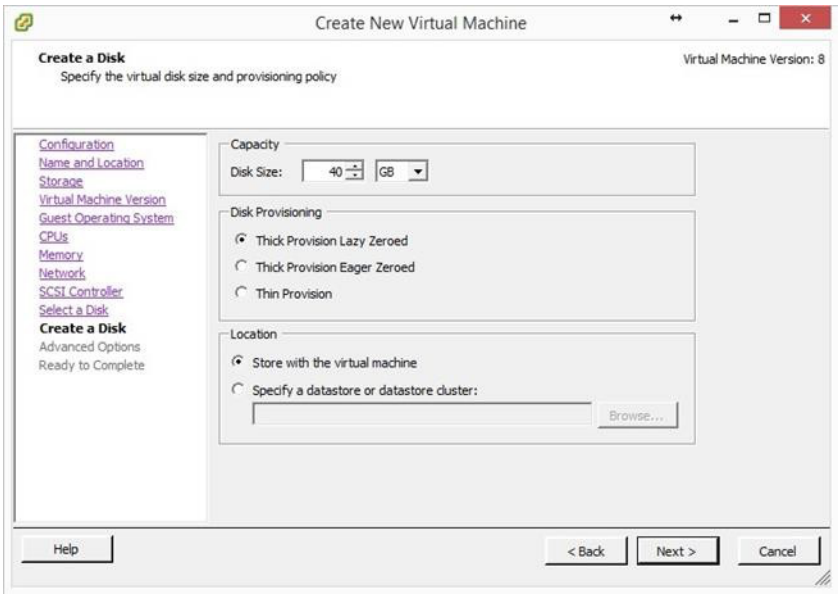
12. On the SCSI Controller pane, select LSI Logic Parallel and click Next.



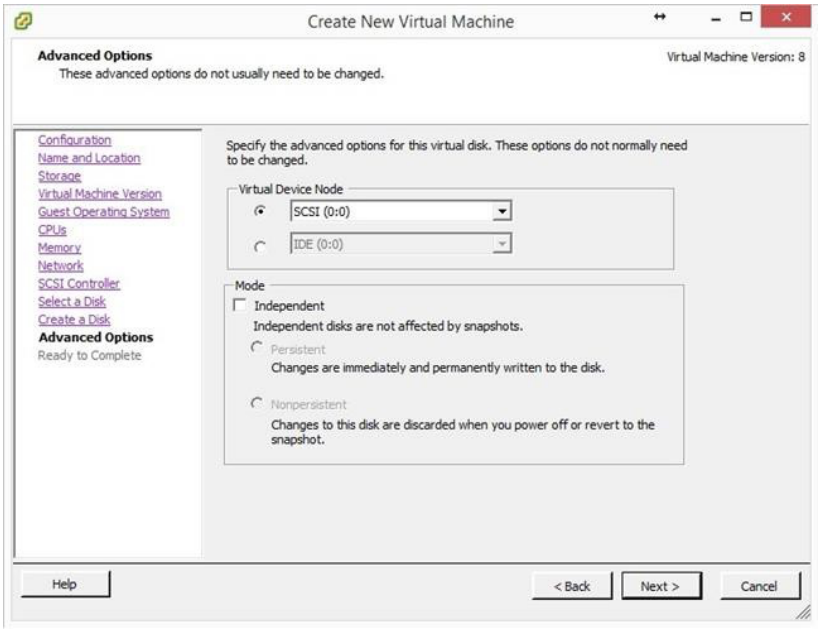
13. On the Select a Disk pane, select Create a new virtual disk and click Next.



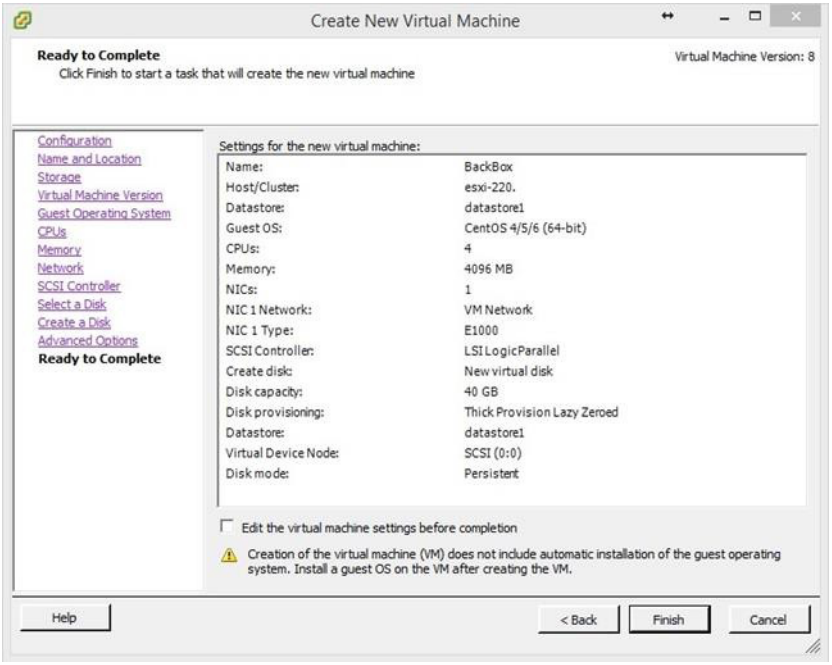
14. On the Create a Disk pane, select a Disk provisioning option and location. Note that the Minimum disk size for BackBox is 40 GB.



15. On the Advanced Options pane, in the Virtual Device Node list choose SCSI (0:0) and click Next.



16. On the Ready to Complete pane, select Edit the virtual machine settings before completion and click Continue.



17. From the left pane, select CD/DVD.
18. From the right pane, select Data store ISO file and click on Browse to locate the BackBox ISO file.
19. Click Finish.