



Restorepoint 5.4 User Guide

Release 2022, Wednesday, August 10, 2022

Table of Contents

Overview of Restorepoint version 5.4	6
Installing Restorepoint	7
Before You Begin	8
Firewall Requirements	8
Traffic from Clients to Restorepoint	8
Traffic from Restorepoint to Network Devices	8
Other Traffic Originating from Restorepoint	9
Browser requirements	9
Restorepoint Virtual Appliance	9
IP Address Setup	10
Alternative Method for Setting the IP Address	11
Connecting to Restorepoint for the First Time	11
Connecting to Restorepoint After a Reboot	12
Basic Operation	13
My Account	15
Activity Display	16
Editing Views	16
Encryption	17
System Status Page	17
Scheduled Tasks	19
Adding Devices to Restorepoint	20
Manually Adding a New Device	21
Importing Multiple Devices Using a CSV File	24
Device Discovery	24
Discovery Setup	25
Discovered Devices	26
Ignored Devices	26
Device Types	27
Automatic Import	27
Running a Manual Backup	27
Automatic Backup Scheduling	28
Exporting the Device List	28
Editing an Existing Device	28
Editing Multiple Devices	28
Deleting an Existing Device	28
Device Monitoring	29
Enabling Monitoring	29
Displaying Monitoring Information	29
Configuration Templates	30
Creating and Editing Templates	30
Pushing Templates	30
Software Management	32
Uploading and Editing Firmware Images	33
Pushing Firmware	33
Credential Sets	35
Using Credential Sets	36
Asset Fields	37
Global Search	38
Viewing the List of Configurations for a Device	38
Backup File Operations	41

Backup Failures	42
Restoring to an Existing Device	42
Restoring to a New Device	43
Cloning	43
Compliance	44
Device Policies	45
Creating a Policy	45
Alert Criteria	46
Rules	46
Remediation	48
Devices	48
Regular Expressions	49
Lua Functions	50
Variable Definitions	51
Password Policies	53
Configuration Baselines	53
Reports	54
Creating a Report	56
Report Formats	56
Report Types	57
Periods	57
Sort By	57
Filters	57
Scheduling a Report	57
Managing Users	59
Listing Logged-in Users	60
Adding a New User	60
Editing an Existing User	63
Broadcasting to Users	64
Deleting a User	65
Password Reset	65
Password Recovery Configuration	65
Recovery Procedure	65
Custom User Roles	66
Authentication Servers	71
RADIUS Authentication	71
LDAP Authentication	71
Device Control	73
Controlling a Device	74
Using Parameters	76
Scheduled Actions	76
Lua Applets	79
Restorepoint Built-in Functions	80
Examples	80
Show Version (Cisco)	80
Show Interface (Cisco)	81
IP Spoofing (ScreenOS)	81
IP Spoofing (Palo Alto)	82
File Storage	83
File Servers	84
Auto Export	84
Data Export	85

Data Usage	85
Agents	86
Agent Firewall Requirements	87
Agent Installation	87
Initial Setup	87
Adding an Agent to Restorepoint	89
Changing the Master IP Address	91
Remote Operations Using Agents	92
Managing Agents	93
Administration Domains	94
Managing Domains	95
Administrator Roles	97
Adding a New Domain User	98
Editing Devices	101
Logs	102
Event Log	103
Syslog	104
Appliance Administration	105
System Settings	106
Network Settings	106
Network Interfaces	106
Primary / Secondary Interface	106
IP Configuration	106
Network Access	107
Network Address Translation (NAT)	107
Additional Static Routes	107
Bandwidth Management	108
Appliance Operations	108
Platform	108
Branding	109
Software Updates	109
Date and Time	109
System Archive	110
Taking an Archive	110
Restoring from an Archive	110
Workstation DB Archives	111
Log Settings and Alerts	111
SNMP	112
Security	113
Protocol Versions	113
Services	113
HTTPS Certificate	113
Timeouts	114
Admin Allowed Networks	115
High Availability	115
HA Requirements	115
Creating a Cluster	115
Labels	117
SAML	119
System Updates	121
Disabling Automatic Updates	121
Manual Updates	122

Getting Help	123
Error Messages	124
Errors During Backup Operations	124
Other Messages	125
Using the System Shell	126
Factory Reset	127
Frequently Asked Questions	128
Contacting Technical Support	129
Support Portal	129
Copyright and Contact Information	130
Copyright Notice	130
Trademarks	130
Contact Details	130

Chapter

1

Overview of Restorepoint version 5.4

Overview

Restorepoint is a Disaster Recovery and Secure Configuration Management appliance for network devices such as, routers, switches, proxies, and firewalls. Restorepoint can automatically retrieve your network device configurations, detect changes and compliance violations, and report these automatically to network administrators.

To add new devices to Restorepoint, you can set the backup frequency for each device individually or as a group. Once you have stored your device configurations on Restorepoint, you can restore network devices when needed.

All backups, device configurations, and passwords are encrypted, and cannot be read by an unauthorized user.

You can configure, monitor, and control Restorepoint through an easy-to-use web interface, which gives you access to all your devices, stored backups, user configurations, and activity logs.

Devices currently supported by Restorepoint are listed in the plugin guide. Check the [Restorepoint website](#) for the latest updates to this list.

Chapter

2

Installing Restorepoint

Overview

Restorepoint is available as a hardware appliance or a VMware virtual appliance. This section describes how to perform the initial configuration of your Restorepoint appliance and configure it to communicate with other devices on your network.

This section covers the following topics:

<i>Before You Begin</i>	8
<i>Firewall Requirements</i>	8
<i>Browser requirements</i>	9
<i>Restorepoint Virtual Appliance</i>	9
<i>IP Address Setup</i>	10
<i>Connecting to Restorepoint for the First Time</i>	11

Before You Begin

Before you install your Restorepoint appliance, ensure you meet the following requirements:

- For hardware installations, 1U of rack space available to install the appliance, with a standard 240V power socket
- For hardware installations, allocate a port on your Ethernet switch for the appliance
- The appliance has an allocated static IP address
- You have configured your firewall to allow traffic between the appliance, and the network devices and servers that Restorepoint will control
- For virtual deployments, verify that you are running VMware ESX vSphere 4 or above and
- For virtual deployments, verify your ESX host has 4 GB RAM available and the datastore where the virtual machine will be deployed has 256 GB available
- Configure your firewall to allow outbound traffic from Restorepoint to the Internet. If you have a firewall between any of your devices and Restorepoint, you may need to open additional ports. For more information, see device-specific details in the Plugin Guide ([Help > Plugin Guide](#)).
- Configure your mail server to allow Restorepoint to relay email

Firewall Requirements

This section lists the ports used to by clients connecting to Restorepoint and the ports used by Restorepoint to connect to network devices and other servers.

NOTE: Your firewall policy might need to be modified for Restorepoint to function correctly.

Traffic from Clients to Restorepoint

The following table lists traffic from Restorepoint to network devices:

Port	Purpose
443/tcp	Restorepoint user interface
22/tcp	Restorepoint shell access
161/udp	(optional) SNMP monitoring

Traffic from Restorepoint to Network Devices

Restorepoint connects to network devices in a variety of ways, depending on the vendor. Sometimes, devices use back-connections to transfer their configuration to Restorepoint. See the device-specific details in the Plugin Guide ([Help > Plugin Guide](#)).

Other Traffic Originating from Restorepoint

The following table lists outbound firewall requirements:

Port	Purpose
443/tcp	Download updates from Restorepoint update servers, and HA database sync
53/udp	Lookup to DNS servers
25/tcp	Send notification emails using SMTP
123/udp	Time synchronization with NTP servers (optional)
22/tcp	Initiate remote support requests, or communicate with an Agent's master (optional)

Browser requirements

Restorepoint requires a modern browser with JavaScript enabled. Restorepoint has been tested with the following:

- Chrome (v35)
- Firefox (v25)
- Internet Explorer 10
- Safari (v6)
- Opera (v12.10)

Restorepoint Virtual Appliance

The Restorepoint Virtual Appliance can be downloaded as a ZIP archive from the Restorepoint website. The following steps refer to VMware vSphere 4.0.

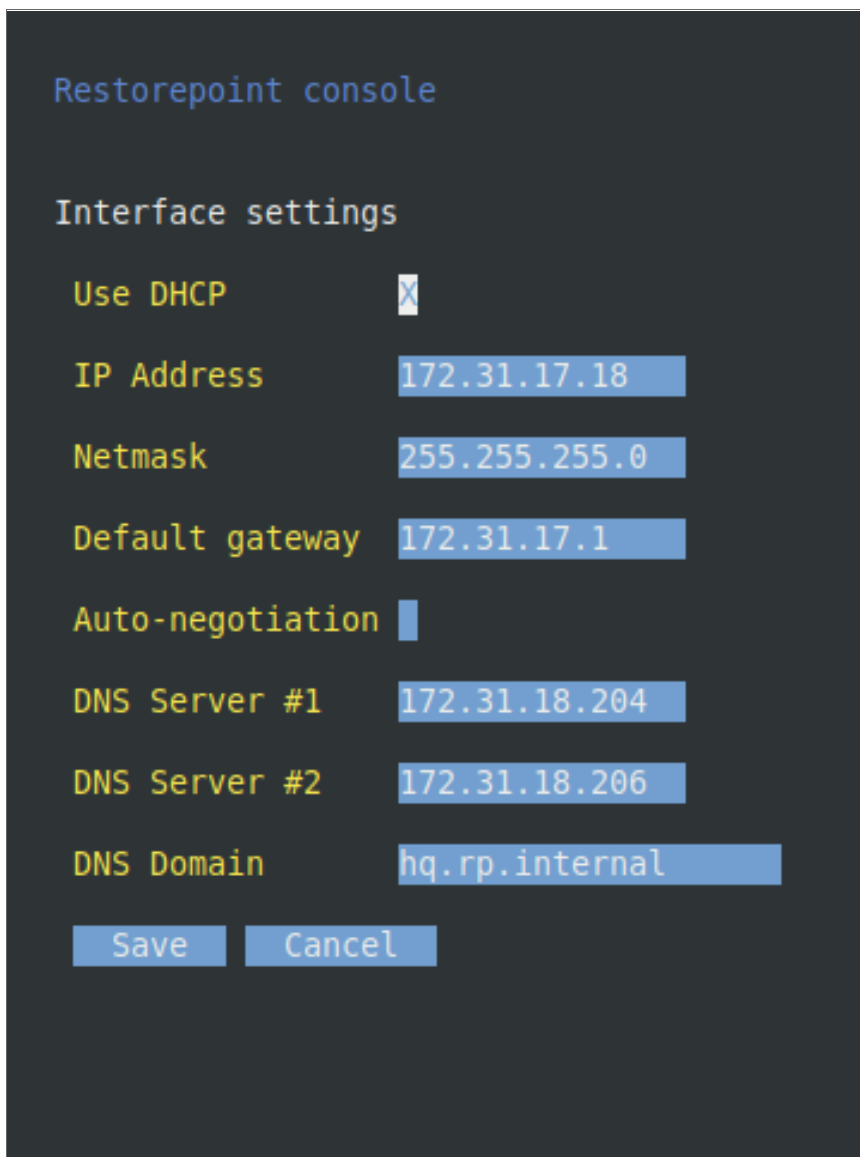
1. Expand the Restorepoint ZIP file in a suitable location on your PC.
2. Launch the vSphere Client.
3. Right-click on the desired destination in the left-hand column and choose Deploy OVF Template, select Deploy from file and browse to the OVF file inside the extracted folder.
4. Select all the files in the folder. There should be a mf file, an ovf file, and 2 vmdk files.
5. Click **Next**.
6. Click **Next**.
7. Use the default name or enter a name for the virtual machine and the inventory location, then click **Next**.
8. Choose the host or cluster, then click **Next**.
9. Select which datastore should be used, then click **Next**.
10. Choose **Network Mapping**, then click **Next**.

11. Check the summary information, then click **Finish**.
12. The virtual machine will now deploy. After completion, click **Close** in the completion dialog box.

IP Address Setup

To set up Restorepoint, you must configure the network parameters, which include the static IP address you have allocated to the appliance, and the DNS and gateway settings for your network. Follow these steps:

1. Connect a monitor and keyboard to suitable ports on the rear panel of the appliance, or open the virtual machine console in the Virtual Infrastructure client.
2. At the login prompt, typed the default user name (*admin*) and password (*admin*) for the device and then choose option 1 on the console menu:



The screenshot shows a terminal window titled "Restorepoint console". Under the heading "Interface settings", there are several configuration options:

- Use DHCP**: A checkbox that is currently checked (indicated by an 'X' in a box).
- IP Address**: A text input field containing "172.31.17.18".
- Netmask**: A text input field containing "255.255.255.0".
- Default gateway**: A text input field containing "172.31.17.1".
- Auto-negotiation**: A checkbox that is currently unchecked.
- DNS Server #1**: A text input field containing "172.31.18.204".
- DNS Server #2**: A text input field containing "172.31.18.206".
- DNS Domain**: A text input field containing "hq.rp.internal".

At the bottom of the form, there are two buttons: "Save" and "Cancel".

3. Type the IP address, Netmask, default gateway, and primary DNS server as prompted. The DNS server must be able to resolve public names (for example, support.restorepoint.com), otherwise the appliance cannot retrieve software updates.
4. Enter *y* to confirm the settings. If the settings are applied successfully, the console menu will be redisplayed. You can **exit** now.

You can disconnect your monitor and keyboard. To continue the initial setup, open a browser window on a network connected PC and enter the IP address you set for the appliance in the URL bar.

Alternative Method for Setting the IP Address

You can also connect to the Restorepoint appliance for initial setup over a network using the factory-configured default IP address/netmask (192.168.1.1/255.255.255.0), if these settings do not conflict with any devices already on your network. Use a browser to connect to `https://192.168.1.1` and set the IP address as shown above.

If these settings *are* in use on your network, you may connect the device directly to a PC using an Ethernet cross-over cable. Configure your PC to use an address in the 192.168.1.2 - 254 range, then use a browser to connect to `https://192.168.1.1`.

Connecting to Restorepoint for the First Time

After you set the IP address for Restorepoint, use a browser on a network-connected PC to connect to the IP address and complete the initial configuration.

NOTE: Restorepoint initially uses a self-signed certificate. Because of this, your web browser will warn you of an invalid (untrusted) certificate. This is normal behavior because the appliance certificate is not signed by a Trusted Certificate Authority. The session will still be encrypted. Refer to your browser instructions on how to proceed and accept the unsigned certificate. A valid (signed) certificate can be uploaded to Restorepoint after the initial configuration is completed.

To connect to Restorepoint for the first time:

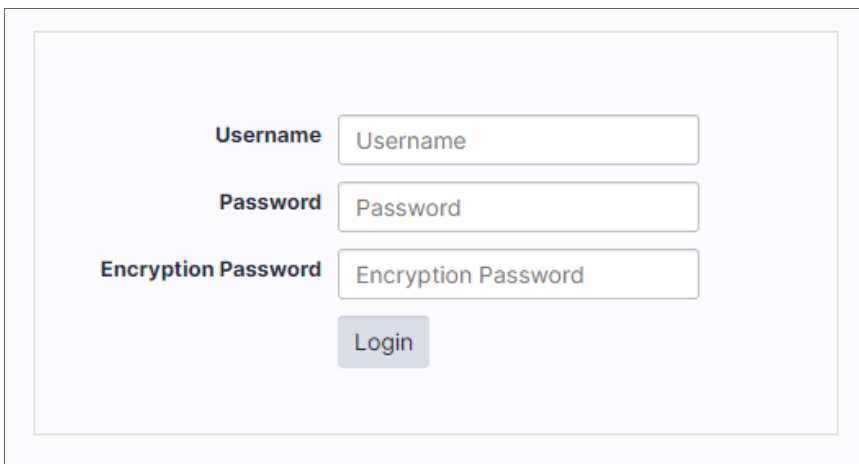
1. Log in with the default username (*admin*) and default password (*admin*). Restorepoint displays the End-User License Agreement.
2. Read the terms of the Agreement, then click **Accept** to signify that you accept the Agreement. You will not be able to use Restorepoint if you do not accept the Agreement.
3. Enter your company details, then click **Next**.
4. Confirm the network configuration and the SMTP details. If Restorepoint is not connected to the Internet, select the relevant box. Click **Next**.
5. If Restorepoint needs a proxy to connect to the Internet, or needs additional static routes to connect to your network devices, enter the details on page 4. Click **Next**.

6. Enter the details for the first administrator. You must change the default administrator password and encryption password; these cannot be identical, and must be at least 8 characters long. You will also need to enter your email address and a password recovery question and answer, which can be used to reset your password. It is important to choose a question that only you know the answer. Restorepoint will send you a password recovery token by email. See the [Recovery Procedure](#) for more information. Click **Next**.
7. Click **Install**. Restorepoint will contact the update servers to verify the license and download the device plugins. To allow this, ensure that your firewall allows the required traffic (for more information, see [Firewall Requirements](#)).

Connecting to Restorepoint After a Reboot

When Restorepoint is rebooted, it will start in a locked state. It is not able to perform any operations until the encryption password is entered, and only admin-level operators can log in to the appliance.

To enter the encryption password, use a browser to connect to the appliance and provide your administrator credentials and the encryption password:



The image shows a login form with the following elements:

- Username**: A text input field containing the placeholder text "Username".
- Password**: A text input field containing the placeholder text "Password".
- Encryption Password**: A text input field containing the placeholder text "Encryption Password".
- Login**: A button located below the Encryption Password field.

The appliance will then transition to the normal operation mode, and subsequent administrator logins will not require an encryption password.

Chapter

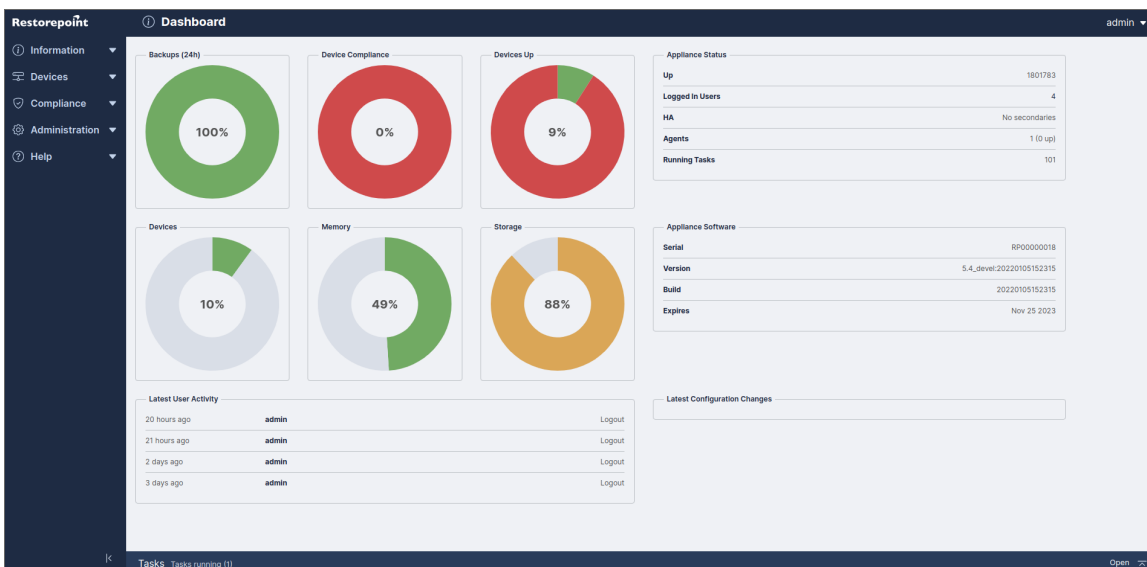
3

Basic Operation

Overview

The Restorepoint user interface pages share some common features. These features include:

- A menu bar at the top of the page, for navigating between the different functions
- The username of the logged in user at the top right-hand side of the screen
- A footer that displays the current software version, serial number, license expiry, and time



Tables display a grey header. For example, in the **Device List** page shown below, you can change column widths by double-clicking on the header, or by clicking and dragging the heading separators. You can change the sorting criterion by clicking on a column heading. You can also perform a full text search by typing in the **Search** field.

<input type="checkbox"/>	Name ↑	Plugin	Domain	Agent	Address	Disabled	Backup Interval	Last Backup	Last Attempt	Next Backup	Protocol
<input type="checkbox"/>	smartcenter77...	Check Point Gaia	Global		172.16.21.72	No	Manual				scp
<input type="checkbox"/>	gaiaR7720	Check Point Gaia	Global		172.16.21.14	No	Manual				ssh
<input type="checkbox"/>	Gaia	Check Point Edge	Global		172.16.21.197	No	Manual				ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		55.62.147.104	No	Every hour, on the h...		2021-11-10 13:25	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		6.11.50.67	No	Every hour, on the h...		2021-11-10 13:23	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		86.71.157.63	No	Every hour, on the h...		2021-11-10 10:41	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		185.1.216.111	No	Every hour, on the h...		2021-11-10 13:03	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		71.44.158.45	No	Every hour, on the h...		2021-11-10 12:53	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		94.103.200.2	No	Every hour, on the h...		2021-11-10 12:18	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		18.243.244.130	No	Every hour, on the h...		2021-11-10 12:47	2 months ago	ssh
<input type="checkbox"/>	Checkpoint Sg8...	Check Point Embedd...	Global		103.36.142.122	No	Every hour, on the h...		2021-11-10 13:17	2 months ago	ssh

This section covers the following topics:

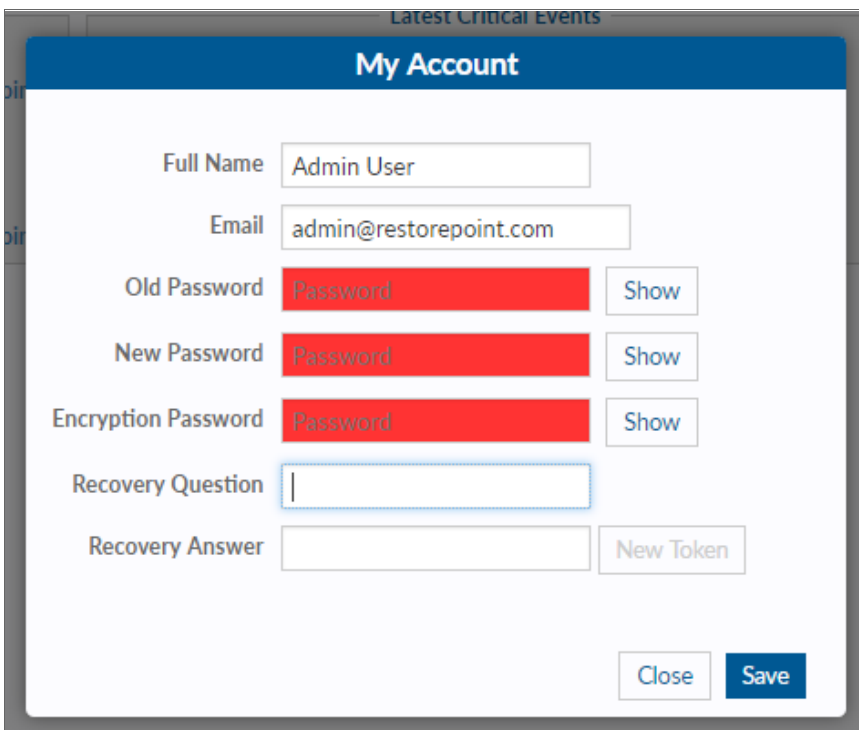
My Account	15
Activity Display	16
Editing Views	16
Encryption	17
System Status Page	17
Scheduled Tasks	19
Adding Devices to Restorpoint	20
Device Discovery	24
Running a Manual Backup	27
Exporting the Device List	28
Editing an Existing Device	28
Device Monitoring	29
Configuration Templates	30
Software Management	32
Asset Fields	37
Global Search	38
Viewing the List of Configurations for a Device	38
Backup File Operations	41
Cloning	43

My Account

You can hover over the username on the top of the user interface for two options. The **Logout** option includes a clock that shows how many minutes until a user is automatically logged out, and the **My Account** option that allows you to change the following user settings:

- Full Name
- Email
- Password
- Encryption Password
- Recovery Question
- Recovery Answer

NOTE: To change a password, you need to specify the **Old Password**.



The screenshot shows a 'My Account' settings window. At the top, it says 'Latest Critical Events' and 'My Account'. The form contains the following fields and buttons:

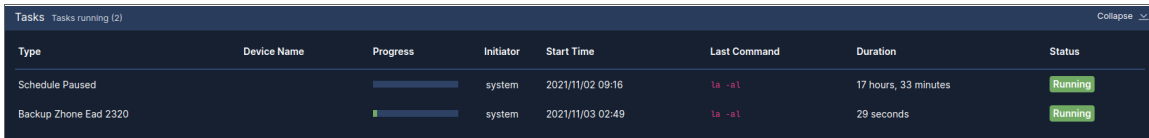
- Full Name:
- Email:
- Old Password:
- New Password:
- Encryption Password:
- Recovery Question:
- Recovery Answer:

At the bottom right, there are two buttons: and .

For more information on the **My Account** options, see [Adding a new user](#).

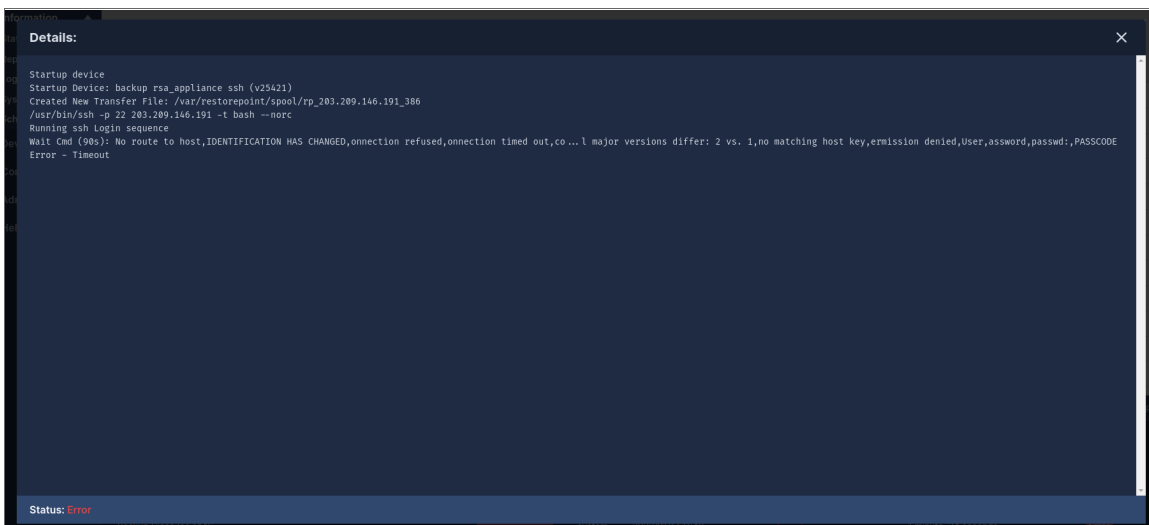
Activity Display

The Activity Display, shown below, displays a list of tasks that are currently running. This list is displayed on every page while tasks are in progress:



Type	Device Name	Progress	Initiator	Start Time	Last Command	Duration	Status
Schedule Paused		<div style="width: 100%;"></div>	system	2021/11/02 09:16	la -al	17 hours, 33 minutes	Running
Backup Zhone Ead 2320		<div style="width: 100%;"></div>	system	2021/11/03 02:49	la -al	29 seconds	Running

You can click on the magnifying glass icon to show the Progress Log, which displays real-time information about the running task:



```
Details:
Startup device
Startup Device: backup rsa_appliance ssh (v25421)
Created New Transfer File: /var/restorepoint/spool/rp_203.209.146.191_386
/usr/bin/ssh -p 22 203.209.146.191 -t bash --norc
Running ssh Login sequence
Wait Cmd (90s): No route to host,IDENTIFICATION HAS CHANGED,connection refused,connection timed out,co...l major versions differ: 2 vs. 1,no matching host key,emission denied>User,assword,passwd:;PASSCODE
Error - Timeout
Status: Error
```

Editing Views

In addition to the built-in views, every data table in Restorepoint can have multiple customized views. You can access these by clicking on the icon at the top left of the table shown below. You can use this icon to reorder columns by clicking the up/down arrows and selecting the checkbox to show/hide columns.



You can define a name and save column orders, widths, and display settings using the **Save** button. You can delete Saved views using the **Delete** button.

NOTE: Views stored in your browser's local storage are only available on the browser and workstation where they were set. If you clear your browser storage, you will clear any saved views.

Encryption

All sensitive data, including device configurations, stored in Restorepoint is protected by encryption. Restorepoint encrypts data when it is written to a disk and decrypts it as it is read. Cleartext data is only held in volatile memory. Therefore, the data disappears when the appliance is shut down or rebooted, rendering data theft impossible without a valid encryption key.

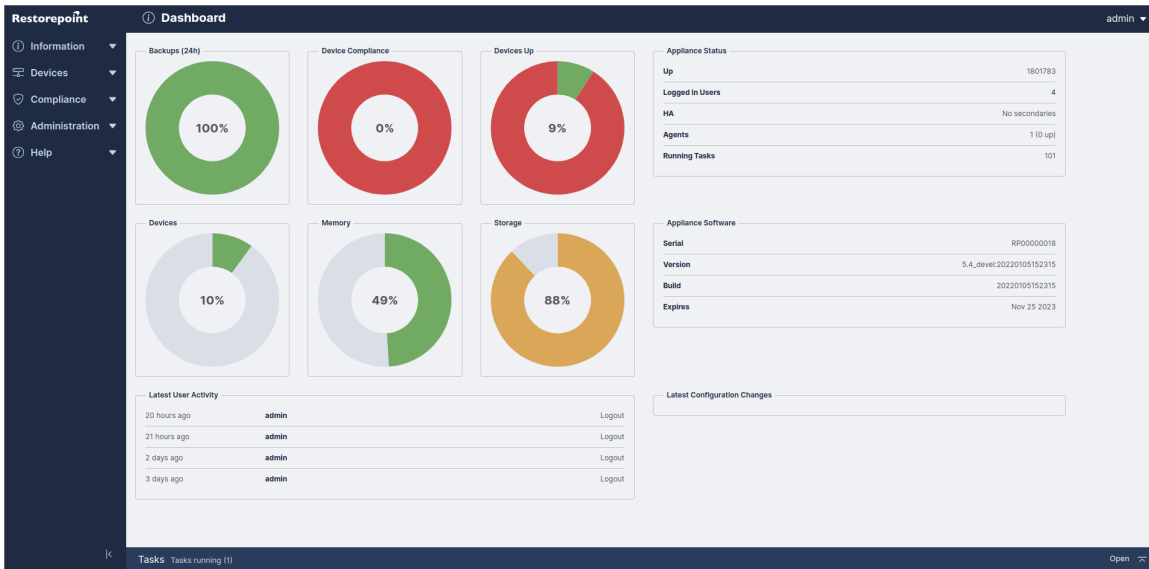
Restorepoint has two operational states:

Locked state	When the appliance is powered up and no encryption password was entered by an administrator. In this state, Restorepoint cannot read its own database and therefore cannot perform any operations. An administrator must log in and provide the encryption password to unlock the database.
Normal state	Once an administrator provides the encryption password at login, all system functions are enabled. Subsequent administrator logins will not require an encryption password until the appliance is powered down or rebooted.

The entire Restorepoint database is encrypted. Therefore, it is **vital** that administrators remember both their normal and encryption passwords. Administrators must also keep their emailed password-recovery tokens safe. For more information, see [Connecting to Restorepoint After a Reboot](#) and [Password Reset](#).

System Status Page

The System Status page or **Dashboard**, displays an overview of the health of Restorepoint and displays the number of devices being backed up. The following image is the default page when you first login to Restorepoint. You can display it at any time by clicking **Info** on the menu.



Graphs:

Backups (24h)	The scheduled, successful, and failed backups in the last 24 hours.
Device compliance	The number of compliant and non-compliant devices, and the number of devices with no policy assigned.
Device Baseline	The number of devices that are running a <i>baseline</i> configuration, non-baseline configuration, and no baseline configuration set. For more information, see Configuration Baselines .
Devices Up	The number of devices that are currently being monitored and responding to Restorpoint. If you click on the graph, a moving average chart covering the past 24 hours is displayed.
Storage	The amount of disk space used and the total amount of disk space for the Restorpoint appliance.
Devices	The total number of devices configured on the appliance, and the maximum devices allowed on your current licence.
Memory	The amount of RAM currently being used by the Restorpoint appliance and the total amount of RAM available.
Network Activity	The current network activity, as seen by the Restorpoint appliance.
Load Average	The Load Average [https://en.wikipedia.org/wiki/Load_(computing)] of the Restorpoint appliance, over the last 30s.

Text panes:

Appliance Status	The uptime, number of logged in users, <i>High Availability</i> status (if enabled), <i>Agents</i> status (if enabled), and number of running tasks.
Appliance Software	The serial number, version, build number (including a link to the change log for that version), and license expiration date of the Restorpoint installation. This information is also available in the footer.
Latest user	Administrator logins/logouts, and other user-initiated operations.

activity	
Latest critical events	Any backup failures, bad logins, or other important information.
Latest Configuration Changes	Any devices that have reported modified configurations.
Activity display	Appears on the left-hand side if any background processes are running. It also displays real-time task details and terminating a task details.

Scheduled Tasks

The **Info > Schedule** page displays the upcoming scheduled tasks, including the next backup for each of the devices configured in Restorepoint. Each item displays the following:

- The date and time when the next task is due.
- The task type (backup, discovery, archive, etc.).
- The device, user, or system configuration object to which the task refers.

Any scheduled event can be postponed and remove the next occurrence of a scheduled task by selecting the relevant checkbox and clicking the **Postpone** button.

The entire schedule can be paused by clicking the **Pause** button. If you click the **Pause** button, no scheduled events will occur until the device is **Unpaused**.

Schedule				
<input type="button" value="Postpone"/> <input type="button" value="Pause Scheduler"/>				
<input type="checkbox"/>	Date	Event	Type	Object
<input type="checkbox"/>	2021-09-14 19:00	Backup device (Overdue)	device	A Cisco Switch
<input type="checkbox"/>	2020-12-04 16:00	Backup device (Overdue)	device	Z_wkg2asa2
<input type="checkbox"/>	2021-11-10 12:00	Backup device (Overdue)	device	Fortinet Fortigate_1
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Nortel 8010_3
<input type="checkbox"/>	2021-11-10 12:00	Backup device (Overdue)	device	A10 Thunder_4
<input type="checkbox"/>	2021-11-10 12:00	Backup device (Overdue)	device	Threecom Superstack5500_5
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Radware Linkproof_7
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Crossbeam Xos_8
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Trend lwsva_10
<input type="checkbox"/>	2021-11-10 13:00	Backup device (Overdue)	device	Radware Appdirector_11
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Cisco Acec_12
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Cisco Ccs_13
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Rsa Appliance_15
<input type="checkbox"/>	2021-11-10 12:00	Backup device (Overdue)	device	Aruba Controller_16
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Juniper Firewall_17
<input type="checkbox"/>	2021-11-10 12:00	Backup device (Overdue)	device	Trend lwsva_19
<input type="checkbox"/>	2021-11-10 11:00	Backup device (Overdue)	device	Nortel 8010_20
<input type="checkbox"/>	2021-11-10 12:00	Backup device (Overdue)	device	Aruba Controller_21

Adding Devices to Restorepoint

You can add devices to Restorepoint using three methods:

- Manually (For more information, see [Manually Adding a New Device](#))
- Importing a list from a CSV file (For more information, see [Importing Multiple Devices Using a CSV File](#))
- Using automatic discovery (For more information, see [Device Discovery](#))

The **Device List** menu allows you to:

- Display all the existing backups for a device
- Compare the configurations of two devices

The **Discovery** menu allows you to:

- Define the networks you wish to scan
- Schedule a periodic network scan
- Import discovered devices into the main device list

Manually Adding a New Device

How you configure a new device may vary slightly from one device to another. Please see device specific information in the Plugin Guide ([Help > Plugin Guide](#)).

To create a new device:

1. Navigate to the **Device Management** page (Devices > Device List).

2. Click the **Add** button on the top left hand corner of the page. The **Add device** page appears. Complete the following fields:

Device Name	Enter a name for the device up to 64 characters long. If the name is defined in your DNS, you can click the Resolve button to automatically fill the IP Address field. Restorepoint will keep the IP address up to date with your DNS and manual changes to the IP address will be ignored.
Type	Select the device type. You can start typing in the Select plugin field to filter the list. This list only displays the device types that are currently available on your license.
Domain	Select the domain that the device is assigned to. This field is only present if Domain Administration is enabled on your appliance. For more information, see Administration Domains .
Agent	If the device is managed via an agent, select the appropriate agent from the dropdown list.
Address	Enter the IP address for the device.
Open Terminal	You can click this button to open a web-based virtual terminal to the device that you can use for troubleshooting. Selecting Restorepoint Credentials uses the credentials you have defined on the Connection tab, otherwise you will need to provide your own credentials for logging into the device. For more complex terminal use, ask your account manager about Restorepoint Universal Console .
Owner	Enter the email address of the device administrator. By default, this field is filled with the notification

Email	email address defined on the System Configuration page.
Email on Config Change	Select this checkbox to automatically trigger an email notification to the device owner when a device configuration change is detected. This option is not available for all device types.
Email On Start Backup	Select this checkbox to automatically trigger an email notification before a backup starts for this device. This notification creates a 1-minute delay before the backup starts.
Email On End Backup	Select this checkbox to automatically trigger an email notification when a backup completes. If this checkbox is not selected, Restorepoint will only send an email notification if the backup fails, or if a configuration change is detected and Email Config Change is selected.
Syslog Change Detection	If available on your Restorepoint system, select this checkbox for Restorepoint to automatically detect when a device is modified and automatically retrieve its configuration. Note that this feature is only available for specific devices. For more information, see the Plugin Guide (Help > Plugin Guide).
Log Transcript	Select this checkbox to create a full transcript log for this device for debugging purposes. A transcript log is automatically saved if the backup fails, so this is rarely needed.
Types	Select the types of configurations to backup for this device.
Filename Prefix	Optionally enter a custom filename prefix for the device configuration files, and check the relevant fields to include. A preview of the filename will appear in the Preview field.
Monitor	Select this checkbox to monitor the device. For more information, see Device Monitoring .

3. Select the **Connection** tab and complete the following fields:

Protocol	Select the appropriate connection protocol for your device, such as telnet or SSH. The options may vary depending on the device type.
Username	Enter the administrator account username for the target system.
Password	Enter the password associated with the administrator account. For some devices you may need to enter more than one password. The field color ranges from red to green to indicate the password strength, according to the policy set in the Password Policies page.
Use credentials	You can select this checkbox and select a Credential Set instead of entering a username and password. Credential sets are reusable username/password combinations that can be shared among different devices (See Credential sets).
Back-Connection NAT	Select this checkbox if Restorepoint accesses this device through a NAT router or firewall. This option will only be displayed if the device requires back-connections and if Use NAT is selected in the System page. If a NAT IP Address is configured here, it will override the corresponding Domain (Section Administration Domains) and System (Section Network Address Translation (NAT)) settings.
Use SSHv2 PKA	Select this checkbox if you want to use SSH Public Key Authentication instead of password-based authentication when connecting to the device. Click the Show Keys button to display Restorepoint's public SSH keys.
Clear cache	If you have replaced a device, Restorepoint may refuse to connect to it because it will detect that the device key has changed and display a connection error; this is a security feature of SSH. In order to override this feature, click the Clear Cache button.
Backup Port	If required for your device, enter the backup port you want to use.

4. Select the **Schedule** tab (figure 3.10) to configure the backup schedule for the device, then click **Add Entry** to add one or more backup intervals.

The screenshot shows a web interface for configuring a device's backup schedule. At the top, there are navigation tabs: Device Details, Connection, **Schedule** (selected), Assets, Additional Info, Compliance, and Notifications & Monitoring. Below these are sub-tabs: Configurations, Logs, Syslogs, and Action Outputs. A green 'Save changes' button is in the top right. The main content area is titled 'Schedule' and contains a 'Backup Schedule' section. This section includes a frequency selector set to 'Every 1 Hour at 00', two checked checkboxes for 'Use default retention policy' and 'Use default configs', and a 'Next Due' date of '2022-01-17 12:00'. There is an 'Add Entry' button and a 'Remove' button. Below the backup schedule is a 'Failure Policy' section with three dropdown menus: 'Retry' (set to 'Always'), 'Alerts' (set to 'Always'), and 'Retry After' (set to '45 minutes').

For each schedule interval, you can override the config types to backup by selecting any of the **Config Type** checkboxes, or override the default retention policies by unselecting **Use Default Policy**. You can also override the Failure Policy on this page. For more information, see [Backup failures](#).

5. Click the **Assets** tab to enter optional Asset Management details for the device.

By default, these include:

- Asset ID
- Firmware Version
- History
- Serial Number
- Location
- Notes
- Manufacturer
- Model

Custom fields can be added in the Custom Asset Fields page. For more information, see [Asset Fields](#).

- The **Additional Info** tab, if available, displays additional information retrieved from the device, such as license details, routing table, and network interfaces. You can also display the output of a saved Action on this page using the **New Info Command** dropdown. For more information on creating Actions, see [Controlling a device](#).
- Click the **Compliance** tab to assign compliance policies to this device. For more information, see [Device Policies](#).
- Click **Save** to finish creating the new device. The **Device List** page appears and the new device.



Select the device and click the **Backup** button to perform a manual backup, if required. The backup progress and completion will be shown in the Activity Display. If the backup is completed successfully, the indicator next to the device name is green, and the date of the last backup is added to the display.

Importing Multiple Devices Using a CSV File

If you need to add a large number of devices, you can click the **Import** button and select a comma-separated values (.CSV) file, that contains the device details.

When you create a comma-separated value (CSV) text file to import, include a line at the top of the file to indicate the columns for the attributes you want to import; the order is irrelevant. For example:

```
name,plugin,protocol,ip_address,username,password,password2,backup_port,keep_
backup,owner,serial_no,asset_id,location,notes
```

where:

name	The device name (<i>required field</i>)
plugin	The device type, e.g. 'Cisco ASA' or 'cisco_asa'
protocol	The connection protocol, e.g. 'telnet' or 'ssh' (<i>required field</i>)
ip_address	The device IP address
username, password, password2	The login credentials for the device
backup_port	The port to use to connect to the device, if required
keep_backup	The backup retention policy (days)
owner, serial_no, asset_id, location, notes	Optional fields

Device Discovery

The Restorepoint device discovery engine uses a variety of methods to discover hosts on your network that can be imported to the main device list. You can also be notified by email of new devices that are installed on your network.

NOTE: Device discovery is not guaranteed to discover all the relevant devices on your network. Firewalls or the device configuration itself may negatively affect the discovery process. Similarly, the device type may not always be detected correctly. When you import a device, you are able to override the detected type.

Discovery Setup

To configure discovery, follow these steps:

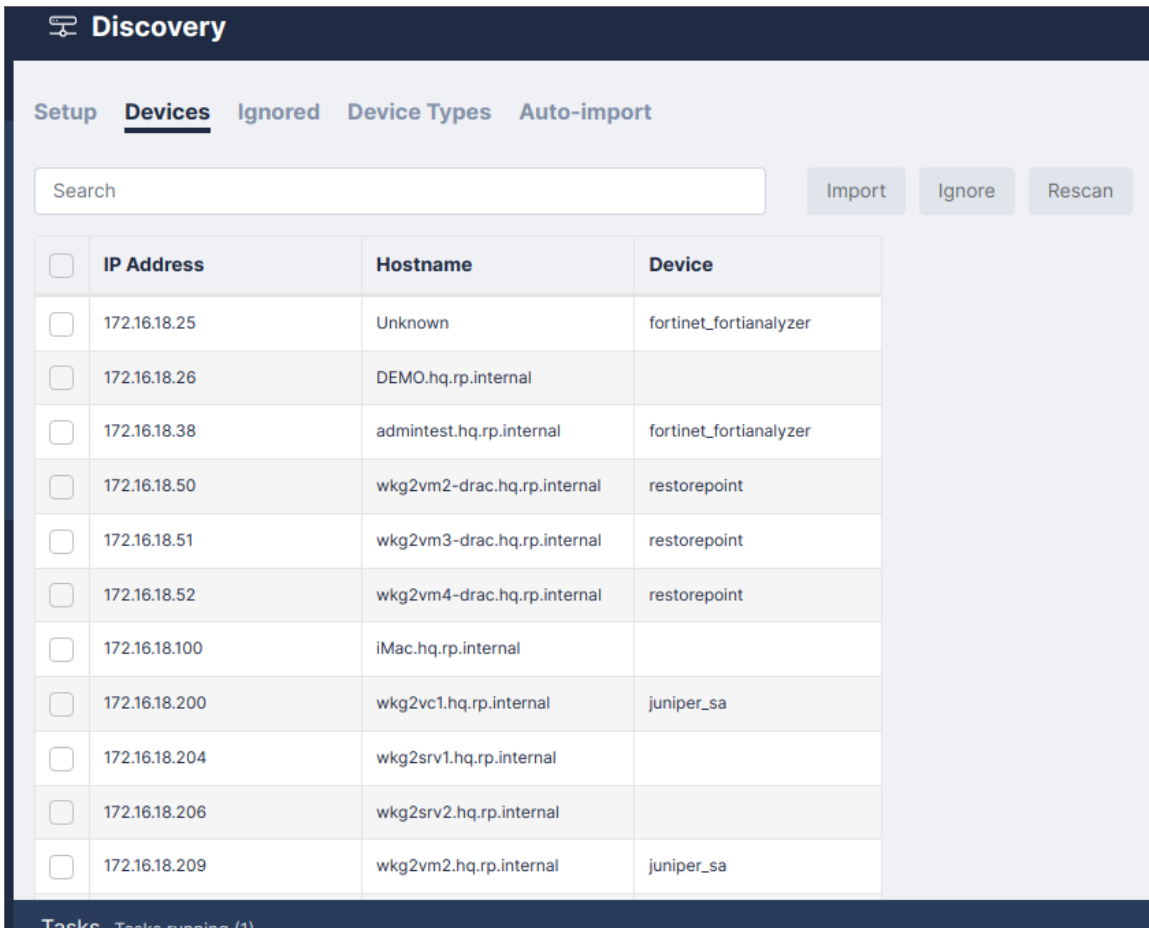
1. Select **Discovery** from the **Devices** menu. The discovery setup page appears.
2. Add one or more network ranges (in CIDR notation) to scan on the **Search Networks** list, for example: 10.20.0.0/16.
3. If you do not wish to scan a particular range, for example 10.20.10.0/24, add this to the **Ignored Ranges** list.
4. You can optionally add one or more SNMP communities in use on your network: choose the SNMP version, enter a community string, and then click the **Add** button.
5. If you want to be notified of a new device, select the **Notify of New Devices** checkbox.
6. If you want to use the [Cisco Discovery protocol](https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol) (https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol), select the **Use CDP** checkbox.
7. If you want to use the [Link Layer Discovery protocol](https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol) (https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol), select the **Use LLDP** checkbox.
8. Choose a scan schedule.
9. Click **Update** to save your changes.
10. Click **Scan Now** to start the scan.

The screenshot shows the 'Device Discovery' setup page. At the top, there are tabs for 'Setup', 'Devices', 'Ignored', 'Device Types', and 'Auto-import'. The 'Setup' tab is active. Below the tabs, there is a 'Schedule' section with a dropdown for 'Every', a number '3', a dropdown for 'Day', and a time 'at 00:00'. There is a 'Last Scan' dropdown set to 'Never' and a 'Scan Now' button. A checkbox for 'Notify of new devices' is checked. Below this is the 'Search Networks' section with a table showing '172.16.18.0/24' and '[None]'. There is an 'Add' button and a 'Delete' button. Below that is the 'Ignored Ranges' section with an input field for 'IP Address/Mask' and an 'Add' button. At the bottom is the 'SNMP Communities' section with a table:

Version	Community / Username	Security Level	Auth Protocol	Auth Password	Priv Protocol	Priv Password	
1	public						Delete
3	public	authNoPriv	MD5	blsadfks			Delete
1							Add

Discovered Devices

At the end of a discovery scan, a list of discovered devices is displayed:



The screenshot shows a web interface titled "Discovery" with a navigation menu including "Setup", "Devices", "Ignored", "Device Types", and "Auto-import". The "Devices" tab is active. Below the navigation is a search bar and three buttons: "Import", "Ignore", and "Rescan". A table lists discovered devices with columns for "IP Address", "Hostname", and "Device". Each row has a checkbox on the left. The table contains 12 rows of data.

<input type="checkbox"/>	IP Address	Hostname	Device
<input type="checkbox"/>	172.16.18.25	Unknown	fortinet_fortianalyzer
<input type="checkbox"/>	172.16.18.26	DEMO.hq.rp.internal	
<input type="checkbox"/>	172.16.18.38	admintest.hq.rp.internal	fortinet_fortianalyzer
<input type="checkbox"/>	172.16.18.50	wkg2vm2-drac.hq.rp.internal	restorepoint
<input type="checkbox"/>	172.16.18.51	wkg2vm3-drac.hq.rp.internal	restorepoint
<input type="checkbox"/>	172.16.18.52	wkg2vm4-drac.hq.rp.internal	restorepoint
<input type="checkbox"/>	172.16.18.100	iMac.hq.rp.internal	
<input type="checkbox"/>	172.16.18.200	wkg2vc1.hq.rp.internal	juniper_sa
<input type="checkbox"/>	172.16.18.204	wkg2srv1.hq.rp.internal	
<input type="checkbox"/>	172.16.18.206	wkg2srv2.hq.rp.internal	
<input type="checkbox"/>	172.16.18.209	wkg2vm2.hq.rp.internal	juniper_sa

Select one or more devices, then click **Import** to import them to the main device list. If only one device was selected, the **New device** page appears with all the discovered information automatically populated. After you review all of the information and make any necessary changes, click **Save** to import the device. If multiple devices are selected, they will be imported without preview. The devices are marked as incomplete and displayed in red in the device list. You can then complete the configuration by adding authentication details or by modifying any default parameters.

Ignored Devices

The **Ignored devices** screen displays a list of devices that will be ignored in future scans. To remove devices from the ignore list, select the devices then click **Un-ignore**.

Device Discovery

Setup Devices Ignored Device Types Auto-import

☰ Default View Search Unignore

<input type="checkbox"/>	IP Address	Hostname	Device
<input type="checkbox"/>	172.16.18.158	rp08.tadasoft.local	Restorepoint Appliance
<input type="checkbox"/>	172.16.18.159	rp09.tadasoft.local	Restorepoint Appliance

Device Types

The **Device Type Override** screen allows you to force discovery scans to import a device as a certain type based on a hostname pattern.

Automatic Import

Select the **Use Auto-Import** checkbox to automatically import discovered devices into the device list.

If you are using Domains, select the **Auto-assign Domain** checkbox to automatically add a discovered device to a domain based on its IP address.

Next, add one or more auto-import rules. Rules determine the credentials and backup schedule that are used for imported devices. The rules can be determined by detected device type, hostname, IP address range, or detected location.

Device Discovery admin

Setup Devices Ignored Device Types **Auto-import** Update

Use Auto-import

Auto-assign domain

Rules

For Device Type Arista EOS use credential set test-set-123 and backup schedule Manual Delete

Add

Running a Manual Backup

To run a manual backup:

1. Select **Devices** from the menu. The **Device List** page appears.
2. Select the devices you want to back up and click **Backup Now**.

You can also run a manual backup by clicking the **Backup Now** button on the **Edit Device** page.

Automatic Backup Scheduling

To automatically schedule backups for a large group of devices by spreading the backups over a day, a week, or a month. To automatically schedule backups, select the relevant devices on the **Devices** screen, and click the **Schedule** button. Select the desired time interval, and the daily Start/End time and/or the Start/End day. For example, you to run backups only at night, or during the weekend.

Exporting the Device List

Click the **Export** button to save the device database in a CSV file.

Editing an Existing Device

To edit an existing device:

1. Click on the relevant device name. The **Edit Device** page appears.
2. Make any required changes and click the **Save** button.

Editing Multiple Devices

You can apply values for multiple devices at once by selecting the devices and clicking **Edit**. The **Edit Device** screen displays *[Multiple]* for all values that are not common to the selected devices. You can change a value for all the devices by editing the field and clicking **Update**.

You can use this feature in addition to device grouping - for instance, all Cisco devices may be set to back up hourly by Grouping by Manufacturer, selecting the Cisco group checkbox to select all Cisco devices, selecting Hourly, and clicking **Update**.

Deleting an Existing Device

To delete an existing device:

1. Select the device(s) you want to remove.
2. Click **Edit**, and ensure that the **Disabled** field is set to Yes to prevent accidentally deleting a device you have not disabled.
3. Click **Save**.
4. The devices you want to remove are selected. Click **Delete**.

Device Monitoring

Restorepoint can monitor devices by periodically checking that the TCP port used for backup (for example, telnet or SSH) is accepting connections, or by sending ICMP Echo Requests (pings) to the device. Monitoring is disabled by default and can be enabled or disabled for each individual device.

Enabling Monitoring

To enable monitoring, open the relevant device **Edit** screen:

1. Select the **Monitor Device** checkbox
2. Select the **Type** of monitoring required. Normally, the device's TCP port used for backup is polled; if the *Ping* option is selected, the ICMP Echo Request (ping) will be used.
3. You can select **Email when down** to send an email notification if the device appears to be down. You can also choose to receive **Email when up**.
4. If the device fails to respond after the number of attempts specified in the **Fail after** box, it is considered "down".

Displaying Monitoring Information

You can hover over status information to display a Round Trip Time graph between Restorepoint and the device, in 5 minute intervals.

The screenshot shows the 'Devices' management interface. At the top, there is a search bar with 'gala' entered. Below the search bar are several action buttons: Add, Backup, Edit, Import, Export, Control, Schedule, and Compare. A table lists devices with columns for Location, Baseline, Compliance Status, Compliance Score, and Owner. A tooltip graph is displayed over the 'Compliance Status' column of the first device, showing a Round Trip Time graph with a y-axis from 0 to 1.0 and an x-axis with time intervals from 11:45 to 13:15. The graph shows a single data point at 12:00 with a value of 0.0, and the status is '0%'.

Location	Baseline	Compliance Status	Compliance Score	Owner
Comms Rack	No	0%		ssharpe@restorepol...
Comms Rack	No	Not monitored		ssharpe@restorepol...
Comms Rack	No	Not monitored		ssharpe@restorepol...

Clicking **Uptime** will display the monitoring graph for the device.

You can select any other monitored device from the dropdown at the top of the page to display its graphs.

Configuration Templates

Templates are configurations that can be pushed to multiple devices. For example, during a large deployment of similarly configured devices. Each template can contain parameters, which are substituted for entered values for each device. For example, a section may be marked “IP Address”, and the field will be applied when pushed to devices.

Creating and Editing Templates

1. Navigate to the Template page (Devices > Templates). Click **Add**, or click on an existing template name.
2. For new templates, select a device and configuration to base the template on.
3. After your template has loaded, select the configuration fields that you want to be substituted.
4. Click **Mark Variable** to name and store a highlighted value.
5. Once your template is created, the template values can be renamed or deleted with the relevant buttons.
6. Click **OK**. If you don't provide a name and comment, a name and comment will be automatically generated.

The screenshot shows the 'Add Template' form with the following fields and content:

- Name:** A text input field.
- Device:** A dropdown menu showing 'A Cisco Switch'.
- Configuration:** A dropdown menu showing '2-20201210002849 (v. 1 startup)'.
- Notes:** A text area with the placeholder 'Leave notes here'.
- Code Editor:** A text area containing the following configuration commands:

```
!  
! Last configuration change at 20:59:39 UTC Sun Nov 29 2020 by admin  
! NVRAM config last updated at 20:59:40 UTC Sun Nov 29 2020 by admin  
!  
version 12.1  
no service pad  
no service timestamps debug uptime  
no service timestamps log uptime  
no service password-encryption  
!  
hostname wkg2ios1  
!  
logging rate-limit 1  
aaa new-model  
aaa group server radius RadiusServers  
server 172.16.17.206 auth-port 1812 acct-port 1813  
!  
aaa authentication login default group RadiusServers local  
aaa authorization exec default group RadiusServers if-authenticated
```
- Mark variable:** A button located to the right of the code editor.

Pushing Templates

To push a template to a device, select the template from the **Template Management** page. Choose one or more devices using the device selector, and click **Push**.

Push Template

Devices Variables

Search

A Cisco Switch

Cisco IOS_172.16.21.241

wkg2sw2

Cancel Push

If the template has any parameters, you must enter the values for each of the devices selected above:

Push Template

Devices Variables

A Cisco Switch

password

Cancel Push

Click **OK** to complete the operation.

Software Management

Restorepoint can be used as a repository for device firmware/software that allows you to upload files like firmware images and ISO images to the appliance. Software images can also be pushed to supported devices.

Filename	Device Type	Uploaded	Description	Size	MD5
<input type="checkbox"/> asa98.bin	Cisco ASA	2022-01-06 11:45		5.00 B	d8e8fca2cdc0f896fd7cb4c0031ba249

Uploading and Editing Firmware Images

1. Click **Import**, or an existing firmware name.
2. For new firmware, click the **Browse** button and navigate to the file from your hard drive.
3. Supply values in the **Device Type** and **Description** fields.
4. Click **Save**.

Upload Firmware

Drag backup file here, or click to select backup file

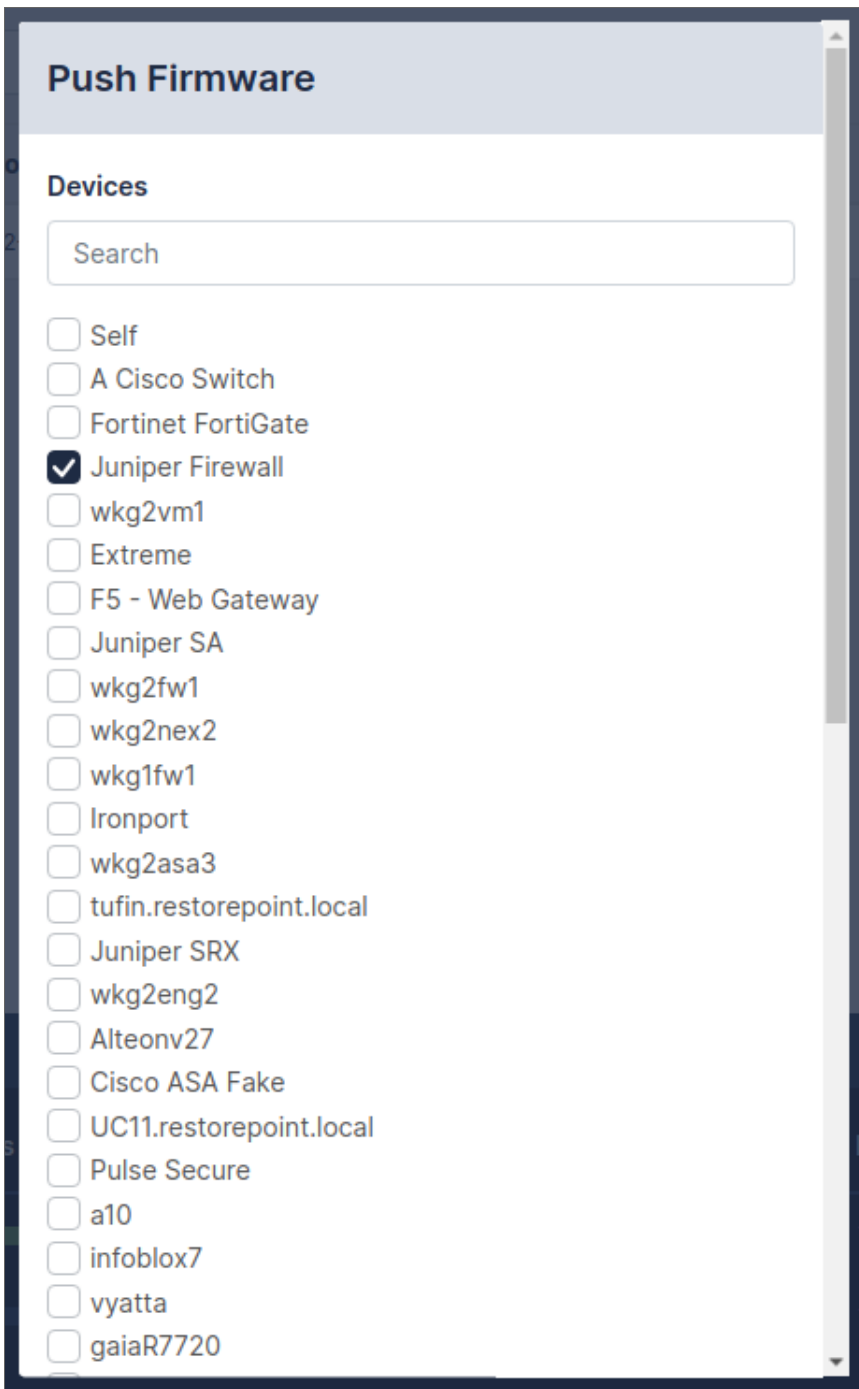
Device Type [None] ▼

Description

Cancel
Save

Pushing Firmware

Restorepoint can upgrade the firmware of a supported device using an image stored in the repository. Select a firmware image using the tickboxes, then click **Push**. Select the device from the menu, then click **Push** again; Restorepoint will perform the upgrade procedure recommended by the device vendor.



Please check the Plugin Guide (**Help > Plugin Guide**) for a list of devices that support this function.

Credential Sets

Restorepoint can use predefined **Credential Sets** to authenticate to a device instead of individual usernames and passwords. Credential Sets are useful if several devices share the same authentication credentials. To create a Credential Set:

1. Select **Credential Sets** from the **Devices** menu.
2. Click **Add Set**, or click on an existing Credential Set name.
3. Give the Set a name, then fill in the authentication details .
4. Select a **Domain** from the pull-down menu to restrict the scope of this set to a particular domain; otherwise choose **Global** to make this set available to all domains.
5. Click **OK**.

Edit Credentials

Details Devices

Set Name
dasda

Username
fdvsdv

Password
..... Show

Password 2
..... Show

Domain
Global

Close Save

Using Credential Sets

To authenticate to a device using an existing credential set, leave the authentication details empty, check **Use Credentials**, and then select the correct credential set. Click **Save**.

Edit device

Device Details **Connection** Schedule Assets Additional Info Compliance Notifications & Monitoring Configurations Logs Syslogs Action Outputs

Connection

Protocol
ssh

Use Restorepoint Credentials?

Username
admin

Password
..... Show

Password 2
..... Show

Backup Port
22

Extra Files
/etc/resolv.conf/etc/sysconfig

Backup Logs

Back Connection NAT

Use SSHv2 PKA

SSH Public Key
Clear Cache

To see what devices are currently using a given Credential set, click the name on the **Devices > Credential Sets** page, and navigate to the **Devices** tab.

Asset Fields

In addition to the built-in Asset Management fields, you can also define custom fields. To do this, navigate to the Assets Fields page (**Devices > Asset Fields**). Custom fields can be of type **Date**, **Text** (single-line), **Textarea** (multiple-line), and **File**.

Once defined, date fields can be set to give an **Expiry Notification**:

- 60 days before
- 30 days before
- When Reached

If set, an email is automatically sent to the device's owner on the specified expiration date. Expiry date is also used in reports.

Custom Fields

Name	Type	Notify	
Documentation	File	N/A	Delete
History	Textarea	N/A	Delete
Maintenance Expiry	Date	30 days before	Delete
Purchase Date	Date	None	Delete
Purchased From	Text	N/A	Delete
Renewal	Date	30 days before	Delete
Support End Date	Date	30 days before	Delete

Text
Add Field

Notifications

Notify Owner

Update

Any custom fields defined in this page become immediately available in the **Assets** page of all devices managed by Restorepoint.

Global Search

Restorepoint can search the full text of configuration backups for a keyword from the Global Search page (**Devices > Global Search**).

Enter your search term in the **Search for** box, select the devices you would like to search, and click **Go**. To avoid excessive results, you can choose to **Limit** the search to a given timeframe.

If the keyword (or keywords, if more than one is entered) are found in a device configuration, it will be listed in the right-hand panel. If you click the name of the device configuration, the device configuration page will open.

Global searches are case-insensitive and do not support wildcards.

Viewing the List of Configurations for a Device

You can access the list of configurations for a device from the **Device Management** page by clicking the **last backup** column of the corresponding device, or by clicking the **Configurations** tab when you edit the device.

A configuration may contain more than one file. For example, a Cisco IOS device has a start-up and a running configuration; you can choose which configurations should be backed up in the **Device Details** page.

Configurations

Filename Prefix

Filename Include

Device ID
 Device Name

Preview

50-[timestamp]

Default Config Types

Startup Config
 Running Config
 VTP Database

If a device supports firmware identification, Restorepoint will display the firmware version detected at the time of backup, next to each configuration. A sample list is shown below:

[Device Details](#) | [Connection](#) | [Schedule](#) | [Assets](#) | [Additional Info](#) | [Compliance](#) | [Notifications & Monitoring](#)

[Configurations](#) | [Logs](#) | [Syslogs](#) | [Action Outputs](#)

Available Actions

☐	File	Date ↓	Version	Size	Firmware	Initiator	MD5	Schedule
<input type="checkbox"/>	2-20210709121913	2021/07/09 12:19	5 ×	6 KB	IOS 12.1(22)EA4	admin	startup3e25aaa39a...	Manual
<input type="checkbox"/>	2-20210709120224	2021/07/09 12:02	5 ×	6 KB	IOS 12.1(22)EA4	admin	startup3e25aaa39a...	Manual
<input type="checkbox"/>	2-20210706183146	2021/07/06 06:32	3 ×	6 KB	IOS 12.1(22)EA4	admin	startup42220e58e5...	Manual
<input type="checkbox"/>	2-20210706183012	2021/07/06 06:30	3 ×	6 KB	IOS 12.1(22)EA4	admin	startup42220e58e5...	Manual
<input type="checkbox"/>	bar.txt	2021/07/06 06:24	4 ×	9 B	IOS 12.1(22)EA4	admin	startupbcb1ca898d1...	Manual
<input type="checkbox"/>	2-20210706182242	2021/07/06 06:23	3 ×	6 KB	IOS 12.1(22)EA4	admin	startup42220e58e5...	Manual
<input type="checkbox"/>	2-20210622160440	2021/06/22 04:05	3 ×	6 KB	IOS 12.1(22)EA4	admin	startup42220e58e5...	Manual

Restorepoint keeps track of configuration changes by assigning a version ID to each unique configuration retrieved from a device. Identical configurations are not stored multiple times.

View	<p>There are three available views:</p> <ol style="list-style-type: none"> 1. Default View: A list of all the configurations retrieved from the device. 2. Group by: This view groups the configurations by File, Size, Firmware version, Initiator, or configuration version.
-------------	--

	3. Version Changes: This view does not display consecutive entries with the same version ID, and therefore highlights configuration changes.
Baseline version	The checkmark shows the baseline version of a configuration. To set a baseline version, select the checkmark. The checkmark will become solid. Restoring a non-baseline configuration version to a device with a baseline configuration version will cause a compliance alert. For more information, see Configuration Baselines .
Retaining a version	You may want to retain a configuration indefinitely (a <i>milestone</i> configuration), that overrides your configured retention policy. For example, a backup taken just before a device upgrade. To retain a configuration, click the padlock icon next to the file name; the padlock will become solid. To undo this action, click the padlock icon again.
Adding comments	You can add a comment to a configuration by clicking the grey note icon next to the relevant configuration. Enter your comment in the pop-up dialog box and click OK; the icon will change color. To remove a comment, click the icon, delete the text, and click OK.

NOTE: the above options apply to a configuration version, rather than an individual backup.

Compare configurations	The Compare option is only available for the devices with text file or a tar/tgz archive of text files configurations. To compare two configurations, select two items using the checkbox to the left of the item, and click Compare . If the configurations are archives, Restorepoint will expand the archives and compare the individual files. Restorepoint will display the chosen configuration files side by side and highlight the differences; inserted lines will be displayed in blue and changed lines will be displayed in red. When Only differences is selected, Restorepoint will not display lines which are identical in both files, except those preceding or following a change. Note: Some devices embed a timestamp or fingerprint in the configuration every time a backup is performed. Wherever possible, Restorepoint ignores lines that only differ by such fingerprints when comparing configurations, so that only relevant changes are displayed.
Delete a configuration	Select a configuration using the checkbox and click Delete . This operation is usually only required to delete a milestone configuration (one you have chosen to retain indefinitely), because old configurations are automatically removed according to the retention policy.
Restore a configuration	To restore a configuration, select a configuration using the checkbox and click Restore . Additional options may be displayed, for instance which configuration type should be restored, or whether the device should be reset to complete the operation.
Upload Backup	This option allows you to upload a new device configuration file to Restorepoint from your PC.
Export Backup	You can export a device configuration from Restorepoint through your browser, email, make it available for FTP/TFTP/SFTP collection by a device, or export it to one of your pre-configured file servers.

Compare Configurations

2-20201210002849
 Just differences
2-20210709121913

Startup Config ▾

```

startup
!
! Last configuration change at 20:59:39 UTC Sun Nov 29 2020 by admin
! NVRAM config last updated at 20:59:40 UTC Sun Nov 29 2020 by admin
!
version 12.1
no service pad
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption

```

Startup Config ▾

```

startup
!
! Last configuration change at 12:18:29 UTC Thu Jul 8 2021 by admin
! NVRAM config last updated at 12:18:31 UTC Thu Jul 8 2021 by admin
!
version 12.1
no service pad
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption

```

[Export](#)

Backup File Operations

If a device configuration is a plain text file or a tar/tgz archive of text files, you can view the configuration contents by clicking the relevant tab or file name in the configuration page. If the configuration is an archive of text files, Restorepoint will attempt to unpack the archive and display each individual file. If the configuration is a binary file, or if the file is too large, Restorepoint will not display the contents.

View Configuration: A Cisco Switch - Version 1: 2020-12-10 00:29

Configuration Type

Startup Config ▾

Available Actions

[Export](#) [Restore](#) [Clone](#) [Compare](#) [Back](#)

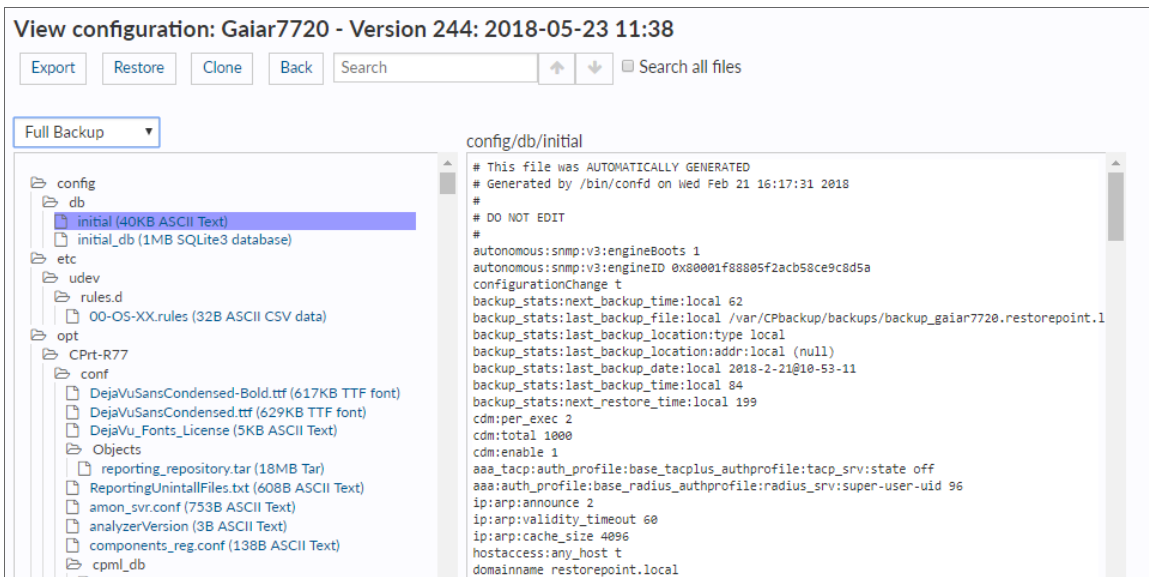
Search

Wrap

```

!
! Last configuration change at 20:59:39 UTC Sun Nov 29 2020 by admin
! NVRAM config last updated at 20:59:40 UTC Sun Nov 29 2020 by admin
!
version 12.1
no service pad
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption
!
hostname wkg2ios1
!
logging rate-limit 1
aaa new-model
aaa group server radius RadiusServers
server 172.16.17.206 auth-port 1812 acct-port 1813
!
aaa authentication login default group RadiusServers local
aaa authorization exec default group RadiusServers if-authenticated
enable secret 5 $1$RAU4$hHMLFJi3X/.KnquFuR1q/0

```



From this page, you can copy this file to your local machine by clicking the **Export** button. After you export the file, you can use a text editor to edit the backup file, and then upload it back to Restorepoint using the **Upload Backup** button on the **Configurations** tab. You can push the edited configuration file to the device by clicking the **Restore** button.

Backup Failures

By default, after a device fails to back up, Restorepoint will retry the operation every hour until it succeeds, and it will send an error notification by email on every failed attempt. This behaviour can be modified by changing the **Failure Policy**, configured in the device **Schedule** tab:

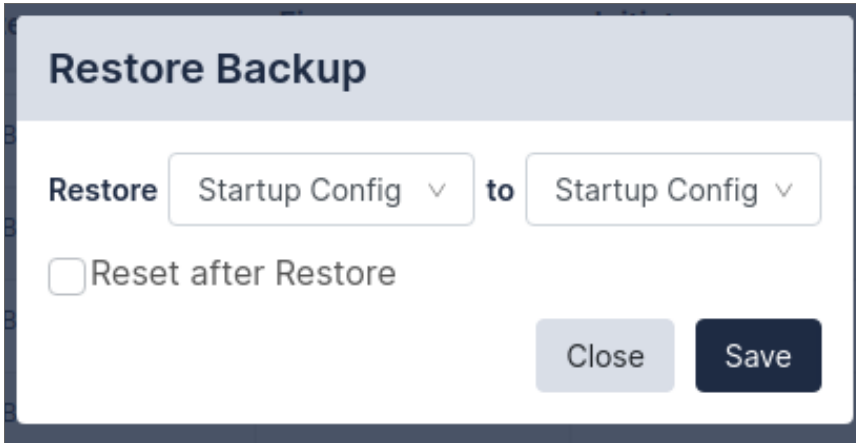
- From the **Retry** pull-down, choose how many times to retry a failed backup. Backups are attempted every hour.
- Next, choose whether to revert to the set schedule or disable further backups when the last allowed failure occurs.
- Finally, choose when to be notified of a failure.

Restoring to an Existing Device

To restore a device:

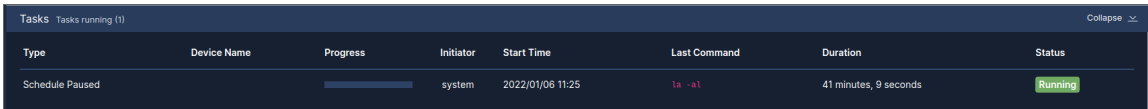
1. Select **Devices** from the menu. Restorepoint displays the **Device Management** page.
2. Click the entry in the **Last Backup** column next to the device you want to restore. Restorepoint displays all the available configurations.
3. Select a configuration by selecting its checkbox and click **Restore**. Restorepoint prompts you to confirm the

restore operation. Depending on the device type, you may be prompted for additional options.



The image shows a 'Restore Backup' dialog box. It has a title bar with the text 'Restore Backup'. Below the title bar, there is a 'Restore' label followed by a dropdown menu set to 'Startup Config'. This is followed by the word 'to' and another dropdown menu also set to 'Startup Config'. Below these options is a checkbox labeled 'Reset after Restore' which is currently unchecked. At the bottom right of the dialog are two buttons: 'Close' and 'Save'.

4. If the restore operation fails, you will see an activity in the activity display. You can click on the magnifying glass icon next to the progress bar to show a real-time progress log, which will aid in determining the cause of the failure. There is also a **Transcript** in the **Logs** tab for failed backups, which contains the details of the conversation with the device.



The image shows a 'Tasks' table with the following data:

Type	Device Name	Progress	Initiator	Start Time	Last Command	Duration	Status
Schedule Paused		<div style="width: 50%;"></div>	system	2022/01/06 11:25	ta -a1	41 minutes, 9 seconds	Running

Restoring to a New Device

When a device is replaced, for instance due to failure, the following conditions must be met:

- The new device must run the same software version as the original.
- The new device must be configured with the same IP address and authentication details as the old device. Alternatively, you can temporarily change the IP addresses or credentials stored on Restorepoint to match those of the new device.
- If Restorepoint connects to the device using SSH, you may need to clear the SSH cache in Restorepoint in the **Connection** tab of **Device Management**.

Cloning

The **Clone** button restores a configuration to a device that is different than the original, which produces a duplicate of the original device. This operation should be used with caution, as it may produce a duplicate IP address on your network.

Chapter

4

Compliance

Overview

You can use Restorepoint to create policies to verify that your devices comply with corporate or regulatory guidelines.

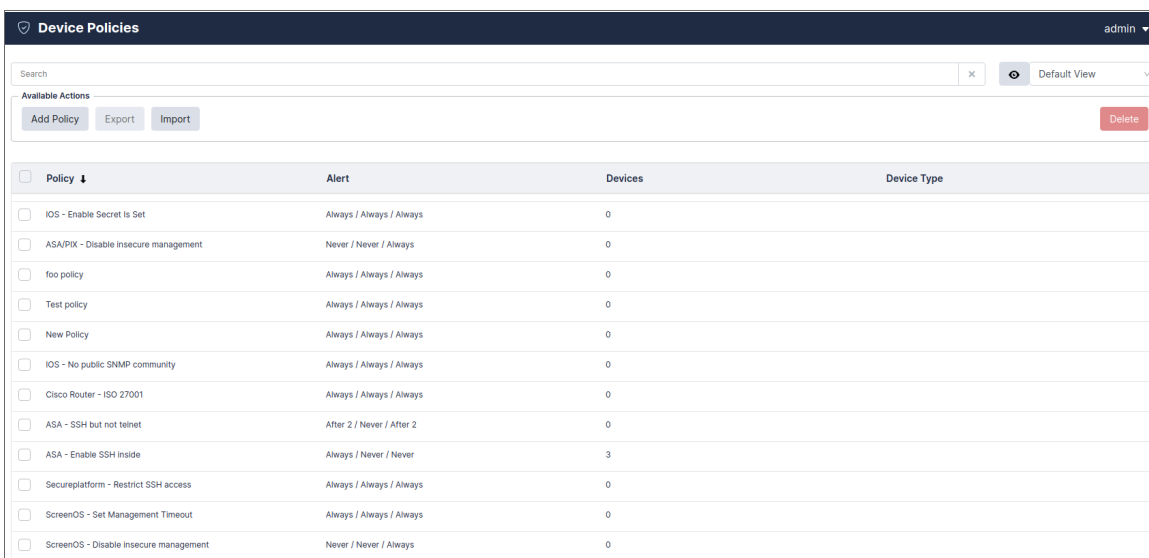
This section covers the following topics:

<i>Device Policies</i>	45
<i>Password Policies</i>	53
<i>Configuration Baselines</i>	53

Device Policies

Use the **Compliance > Device Policies** page to create configuration compliance policies and assign the policies to devices. Policies are groups of one or more rules. A rule is a pattern that is applied to configurations or device firmware version to test whether the configurations or firmware contain a certain phrase or Regular Expressions, or if they match an existing device template. If the tests fail, a compliance violation is triggered and an email alert is sent to the device owner.

Configuration Policies can be configured for devices that have a text configuration file or a TGZ archive of text configuration files.



The screenshot shows the 'Device Policies' management page. At the top, there is a search bar and a 'Default View' dropdown. Below this are buttons for 'Add Policy', 'Export', 'Import', and 'Delete'. The main content is a table with the following columns: Policy (with a checkbox), Alert, Devices, and Device Type. The table lists 14 policies with their respective alert settings and device counts.

<input type="checkbox"/>	Policy ↓	Alert	Devices	Device Type
<input type="checkbox"/>	IOS - Enable Secret Is Set	Always / Always / Always	0	
<input type="checkbox"/>	ASA/PIX - Disable Insecure management	Never / Never / Always	0	
<input type="checkbox"/>	foo policy	Always / Always / Always	0	
<input type="checkbox"/>	Test policy	Always / Always / Always	0	
<input type="checkbox"/>	New Policy	Always / Always / Always	0	
<input type="checkbox"/>	IOS - No public SNMP community	Always / Always / Always	0	
<input type="checkbox"/>	Cisco Router - ISO 27001	Always / Always / Always	0	
<input type="checkbox"/>	ASA - SSH but not telnet	After 2 / Never / After 2	0	
<input type="checkbox"/>	ASA - Enable SSH inside	Always / Never / Never	3	
<input type="checkbox"/>	Secureplatform - Restrict SSH access	Always / Always / Always	0	
<input type="checkbox"/>	ScreenOS - Set Management Timeout	Always / Always / Always	0	
<input type="checkbox"/>	ScreenOS - Disable Insecure management	Never / Never / Always	0	

Creating a Policy

Click **Add Policy** to create a new policy or click **Import** to import a previously exported policy:

✓ Add new device policy

Details Rules Devices Auto-Apply

Details

Name

Device Type

Low-risk Alert

Medium-risk Alert

High-risk Alert

Additional Comments

Version

1

To copy a policy, open the existing policy and click **Clone**.

Alert Criteria

Individual rules can be given a risk level, either **Low** , **Medium** or **High**. For each level, a trigger point can be set, to determine whether or not to generate an alert. This ranges from **Never**, through two, three, four, or five violations, to **Always**. For example, you may want an alert only if three or more low-risk rules are broken, but always if a single high-risk fails. You can also specify a **Device Type** that the policy will apply to, and add a **Comment** to explain the purpose of the policy.

Rules

Click **Add rule** to define and add a rule to a policy. Supply values in the following fields:

Rule name	A label that is used to identify a rule in a report or email
Rule Type	Whether the rule applies to a configuration, software version, runtime command, or the output of a scheduled action

Requirement	Must Match/Must Not Match/Must Match Template
Template	If Must Match Template is selected, you can use this drop down menu to select an existing device template. Templates are defined in the Devices menu.
Match type	Phrase or (Perl-flavoured) <i>Regular Expressions</i> .
Pattern	The pattern to be matched
Severity	Low, Medium or High
Remediation type	Manual, Automatic, or Command (see Remediation below)
Applicable File	For multi-file configurations, e.g., TGZ archives

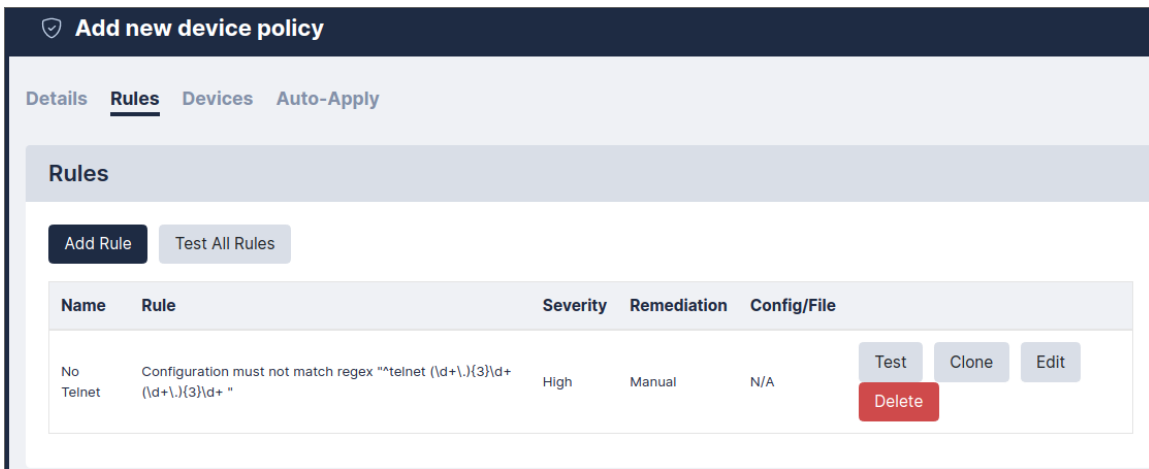
The **Phrase** match type matches any (case sensitive) number of characters, including multi-line. The **Regex** match type (see *Regular Expressions*) takes a Perl-flavoured regular expression, and applies it to the whole configuration, or firmware string.

Once a rule is defined, it can be edited, removed, cloned, or tested against an existing backup using the appropriate buttons.

The screenshot displays the 'Edit Rule' configuration page. On the left, there is a sidebar with 'Rules' selected, showing a table with columns 'Name' and 'Rule'. The main area is titled 'Edit Rule' and contains several sections:

- Name:** A text input field containing 'No Telnet'.
- Severity:** A dropdown menu set to 'High'.
- Rule:** A dropdown menu set to 'Configuration'.
- Remediation:** A dropdown menu set to 'Manual'.
- Match Type:** A dropdown menu set to 'Regex'.
- Case Insensitive:** A checked checkbox.
- Value:** A text area containing the regular expression: `^telnet (\d+\.)\{3\}\d+ (\d+\.)\{3\}\d+`.
- Files:** A section with an 'Add File' button.

At the bottom right, there are 'Cancel' and 'Save Changes' buttons.



Remediation

You can use remediation when a compliance rule is not met, generally intended to rectify the violation. The following remediation types can be configured:

Manual	The remediation text is appended to the notification email to signify that the recipient should take the appropriate action.
Command	One of the stored Actions on the device (see Controlling a device) is executed.
Automatic	The text specified in the textbox is used as a command and executed on the device.

If the rule match type is **Regex**, the remediation can make use of the **Capture** feature, whereby parts of the pattern in brackets can be captured and then referred to in the remediation text (as \$1, \$2, etc.). For example, a rule may state that a configuration must not contain the regex:

```
set telnet (\d+\.\d+\.\d+\.\d+)
```

Where the command in brackets is a match for an IP address. If this rule is violated, the configuration can be remedied using the phrase:

```
unsettelnet$1
```

In this case, the brackets in the rule will capture the IP address, and apply it when the command is performed. The rule is then expanded:

```
unsettelnet1.2.3.4
```

if that was the matched IP address.

Devices

Each policy can be assigned to, or removed from devices by selecting the relevant checkboxes. Alternatively, this can be done from individual devices in the **Edit Device** page.

Add new device policy

Details Rules **Devices** Auto-Apply

Devices

Apply to:

Search

- Self
- A Cisco Switch
- Fortinet FortiGate
- Juniper Firewall
- wkg2vm1
- Extreme
- F5 - Web Gateway
- Juniper SA
- wkg2fw1
- wkg2nex2
- wkg1fw1
- Ironport
- wkg2asa3
- tufin.restorepoint.local
- Juniper SRX
- wkg2eng2
- Alteonv27
- Cisco ASA Fake

Applicable Policies	Available Policies
ASA - Enable SSH inside ASA - SSH but not telnet	ScreenOS - Disable insecure management ASA/PIX - Disable insecure management IOS - Enable Secret Is Set Secureplatform - Restrict SSH access
Remove policies →	← Add policies

Regular Expressions

A regular expression specifies a set of strings as a pattern, rather than a list. For example, the pattern `C(o|a)s?t` matches the strings `Cot`, `Cat`, and `Cast`, but not `Coast`. Restorepoint uses Perl-flavor Regular Expressions.

Most characters can be used in a regular expression. Some characters, called *metacharacters*, have special meanings:

- `()` denote grouping: `(a|b)b` matches `ab` and `bb`
- `|` denotes an alternative (see above)
- `^` matches the beginning of a line
- `$` matches the end of a line
- `.` matches any character
- `+` denotes one or more occurrences of the previous character: `a+b` matches `ab`, `aab`, `abb`, but not `b`
- `*` denotes zero or more occurrences of the previous character: `a*b` matches `b`, `ab`, `aab`, `aaab`
- `?` denotes zero or one occurrences of the previous character: `a?b` matches `b` and `ab`, but not `aab` or `aaab`

Character classes are matches for sets of possible characters, rather than just a single character. For example:

- `[bcr]at` matches `bat`, `cat` and `rat`
- `-` can be used as a range operator in a character class. For example, `[a-g]` matches any character from `a` to `g`

There are some abbreviations for common character classes:

- `\d` matches a digit
- `\s` matches whitespace (a space or a tab)
- `\w` matches a word character (alphanumeric or a `_`)

For example, `\d\d:\d\d:\d\d` matches time in a `hh:mm:ss` format.

For more information and examples of regular expressions, see the [reference guide](http://www.regularexpressions.info/reference.html) (<http://www.regularexpressions.info/reference.html>).

Lua Functions

You can use Restorepoint to define rules using Lua functions. For information on using Lua to run commands on your devices, see [Lua Applets](#).

Available functions for compliance rules are:

- `nextline()` returns the next line of text
- `getline(n)` returns the given line of text
- `numlines()` returns the number of lines
- `addmessage(m)` allows you to replace a series of variables in the remediation text. For example, `addmessage("Hello")` with a remediation text of `$1World!` would output `Hello World!`. The next `addmessage` call would replace `$2`, and so on.

This function checks that the number of lines containing `configure` matches the lines containing `port`:

```
num1 = 0
num2 = 0
line, next = nextline()
```

```
while next do
  if line:match("configure") then num1 = num1+1 end
  if line:match("port") then num2 = num2+1 end
  line, next = nextline
end

if num1 > num2 then addmessage("more")
else if num2 < num1 then addmessage("less") end
return num1 == num2
```

Remediation Text: Config contains \$1 configures than ports.

Variable Definitions

Items defined in this section can be used in compliance rules as variable replacements, referenced with the `$replace$` format, where `replace` is the variable you have defined. This enables you to use a variable as shorthand for configuration elements, that are likely to be referenced multiple times.

For example, if you create a definition for *Gateway*, and assign it a **Value** of `192.168.0.1`, you can then use it in a compliance rule, as shown below:

Add Rule

Name

Show default gateway

Rule

Configuration

Must Match

Match Type **Case Insensitive**

Regex

Value

`ip default-gateway $Gateway$`

Test

This rule will be expanded to `ip default-gateway 192.168.0.1`. If the gateway address changes, update the **Value** in the *Gateway* variable definition and all rules that use the `$Gateway$` variable will be automatically updated.

NOTE: A variable name can only consist of letters, numbers, and the underscore character `_`. If the value contains escape sequences (such as `\n`), the sequence must be double-escaped (`\\n`).

Password Policies

You can use password policies to configure various rules to enforce password strength for devices and users. These settings are used in the **strength meter** that is displayed in all password fields : the background of the field will change color, from red for an unacceptable password, to yellow for a weak password, to green for a good password. Password Strength reports are available on the Reports page (see Reporting for more information).

You can use the following rules:

Minimum length	Minimum number of characters for a password to be accepted
Good Length	Recommended number of characters to be considered <i>good</i>
No Common	Password cannot be simple to guess, such as <i>1234</i> or <i>password</i>
No Dictionary	Password cannot be a dictionary word, such as <i>backup</i> or <i>admin</i>
Must Mix Case	Passwords must contain a mixture of lower and upper case letters
Must Use Numbers	Passwords must contain numbers as well as letters
Must Use Symbols	Passwords must contain non-alphanumeric symbols, such as \$ or ^

Configuration Baselines

Configuration versions can be marked as *Baseline* by clicking the *checkmark* symbol in the Version column of the **Configurations** tab. When you perform subsequent backups, an email notification is sent if the configuration differs from a baseline version. This allows you to quickly check if the current configuration is an approved version.

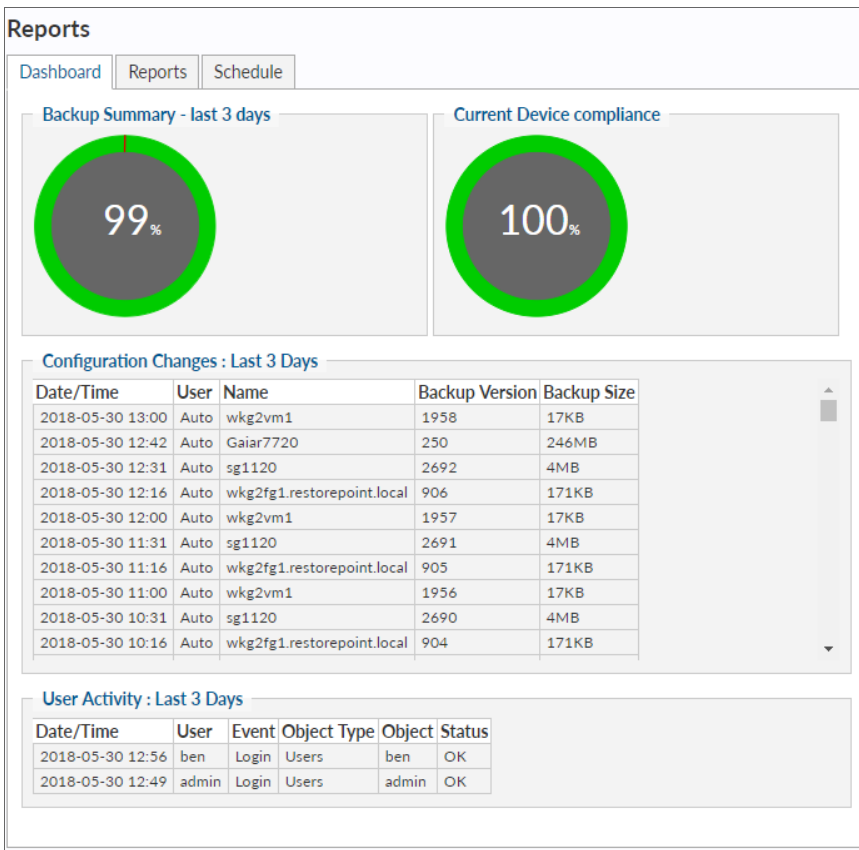
Chapter

5

Reports

Overview

This chapter describes how you can run reports in Restorepoint. You can run reports as needed or you can schedule reports to be emailed to an authorized user.



On the **Dashboard** tab (Information > Reports > Dashboard), a default report displays summary activity information from the past 72 hours. This includes:

- Backup summary
- Compliance Violations recorded
- Failed Device Backups
- Configuration Changes
- User activity

You can display reports between multiple individual reports pages, also called multireports. The dropdown in the top left corner of the **Reports** tab displays the multireport that is currently selected.

This section covers the following topics:

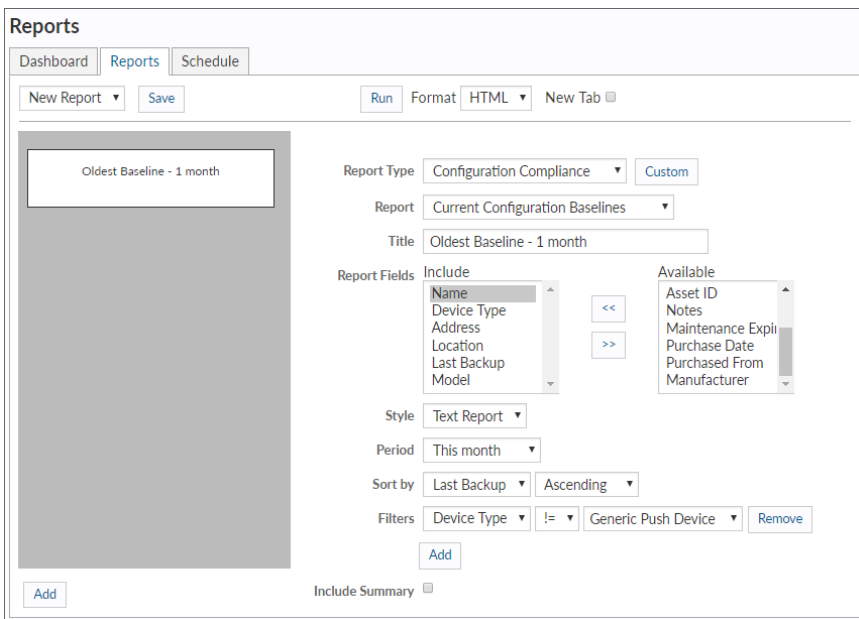
Creating a Report	56
Scheduling a Report	57

Creating a Report

To create a new multireport, select *New Report* from the top-left dropdown. This opens a new multireport, with one report page added. From here, you can set the parameters of the report page, and then click the **Run** button to generate a report. If the **New Tab** checkbox is selected, the report will open in a new browser tab.

To add additional report pages, click the **Add** button in the lower left hand corner.

You can also **Clone** or **Delete** an existing multireport.



The screenshot shows the 'Reports' configuration interface. At the top, there are tabs for 'Dashboard', 'Reports', and 'Schedule'. Below the tabs, there are buttons for 'New Report', 'Save', 'Run', 'Format' (set to 'HTML'), and 'New Tab'. The main area is divided into two sections. On the left, there is a preview area showing a report titled 'Oldest Baseline - 1 month'. On the right, there are configuration options: 'Report Type' (Configuration Compliance), 'Report' (Current Configuration Baselines), and 'Title' (Oldest Baseline - 1 month). Below these are 'Report Fields' with 'Include' and 'Available' lists. The 'Include' list contains Name, Device Type, Address, Location, Last Backup, and Model. The 'Available' list contains Asset ID, Notes, Maintenance Expi, Purchase Date, Purchased From, and Manufacturer. There are '<<' and '>>' buttons between the lists. Below the lists are 'Style' (Text Report), 'Period' (This month), 'Sort by' (Last Backup, Ascending), and 'Filters' (Device Type, !=, Generic Push Device, Remove). At the bottom, there are 'Add' and 'Include Summary' checkboxes.

Report Formats

Reports can be produced in the following formats:

- HTML
- CSV
- PDF
- XML

Graphs can be produced in PDF or HTML format. The *graph* type reports displays summary data and the *report* type displays full details.

Note: If you create a report from a browser, the report is produced either on-screen or as a downloadable file. If you create and export the report to email, the reports is sent as an attachment.

Report Types

The following report page types are available and display the following information:

Backups	Successful/failed backups performed within a given period, backup schedule etc.
Configurations	Configuration changes within a given period.
Assets	Inventory and user-defined asset fields reports.
Compliance	Configuration compliance, password strength for devices and administrators
Administration	User activity, modification to devices, device credentials
Monitoring	Device uptime reports.

After you create a report type, you can save that configuration to reuse it by clicking the **Custom** button. An entry will then be added to the **Custom Reports** report type.

Periods

Where relevant, reports can be created for the following time periods:

- Last 24 Hours
- This Week
- This Month
- This Year
- Since a given hour/day/week/month/year
- A given date range

Sort By

Determines which column the generated table on your report will be sorted by.

Filters

You can add filters to a report to limit or exclude a specific Domain, Location, Device Type, or Device. A device must match *all* filters to be included in the report.

Add Summary adds a count of the number of Rows/Devices in the report to the beginning of the document.

Scheduling a Report

To schedule a report to run automatically:

1. Click the **Reports** (Information > Reports > Reports) tab.
2. Select the report parameters, then click the **Schedule** button.

3. Select a schedule for the report from the drop-down lists.
4. Enter the email address that will receive the report.
5. Click **Save**.

Schedule Report

Schedule Every 1 Week on Mon at 07:00 Next Due : 2018-05-28 07:00

To admin@restorepoint.com

Additional Text Here's your weekly report for Check Point devices in the "Eastern" domain

Cancel Save

The report will then be displayed in the **Scheduled Reports** table, on the **Schedule** tab, along with any other reports that are already scheduled. To remove a report, select the checkbox next to it and click the **Delete** button.

Report	Format	Schedule	Last Run	Next Due	User	Email
<input type="checkbox"/> Backup Report last 24 hours	HTML	At 00:00 on Sunday every week	2018-05-20 00:00	2018-05-21 00:00	admin	support@restorepoint.com

Chapter

6

Managing Users

Overview

This chapter describes how you can add administrators to Restorepoint and configure administrator roles.

Restorepoint supports three levels of user access:

Admin	Super User who has full access (can create/modify/delete devices and users, initiate backups/restores and change the appliance configuration). Admins also have an encryption password that allows Restorepoint to transition from the locked state to the normal state.
Backup	Backup Operator who can perform device backups and restores, but cannot modify devices, users, or appliance settings.
View Only	Monitor Operator who can only view existing backups, access logs, and verify that the system is operating normally.

This section covers the following topics:

<i>Listing Logged-in Users</i>	60
<i>Adding a New User</i>	60
<i>Editing an Existing User</i>	63
<i>Broadcasting to Users</i>	64
<i>Deleting a User</i>	65
<i>Password Reset</i>	65
<i>Custom User Roles</i>	66
<i>Authentication Servers</i>	71

Listing Logged-in Users

You can view a list of currently logged in users in the **Logged-in Users** tab (**Administration > Users > Logged-in Users**). The number of Logged-in users is also displayed on the dashboard (**Info > Status**).

Adding a New User

To add or modify administrators, navigate to the Users page (**Administration > Users**). Administrator passwords and encryption passwords, by default, must be at least 8 characters long. For more information, see [Password Policies](#).

To add a new user:

1. Navigate to the Users page (**Administration > Users**). The **User Management** page appears.
2. Click **Add User**. The **New User** page appears:

Add User

Details Auth Domains

Full Name
John Doe

Email
some@email.com

Role
No Role

Disabled

Allowed Networks
IP Address/Mask

3. Complete the following fields on the **Details** tab:

Full Name	Enter the full name of the user
Email	Enter the user's email address
Role	Select the privilege level from the drop-down list. See below for the privileges associated with each admin level.
Disabled	Select this checkbox to prevent the user from logging in.
Allowed Networks	If set, this field allows the user to connect to Restorepoint only from certain subnets. Enter an IP range in CIDR format in the IP Address/Mask box, and click Add .

Privileges Add users/ devices; modify system	View Only N	Backup N	Admin Y
---	-------------	----------	---------

Table 3 : Default Administrator privilege levels (simplified)

4. On the [Auth Tab \(Fig. 47\)](#):

Username	Enter the new username. Usernames may be up to 16 characters long.
Password	Enter the password for the new user. By default, passwords must be between 8 and 24 characters long. The field color will range from red to green to indicate the password strength, according to the policy set in the Password Policies page. For more information, see Password Policies .
Encryption Password	This field appears if an <i>Admin</i> -level administrator is selected. The encryption password must be between 8 and 24 characters long, and must be different from the administrator password. The field color will range from red to green to indicate the password strength.
Email activation link	This field allows you to set up a user without specifying a password. The user will receive an activation email to let them set their own password.
Expire Password	This field allows you to override the global password expiry rules for this user. See Timeouts for the global password expiry settings.
Use RADIUS	Select this checkbox if you want the user to authenticate against an external RADIUS server. See RADIUS Authentication on how to configure a RADIUS server.

NOTE: Administrators authenticating using RADIUS or LDAP cannot decrypt the system after a reboot.

Add User

Details
Auth
Domains

Username

Password

Show

Email Activation Link

Expire Password

System Default v

Use RADIUS

Close
Save

5. Click **Save**. The updated **Users** page appears:

User Management
admin v

All Users
SAML Users
Logged-in Users
API Tokens

Add User
Broadcast
Delete

<input type="checkbox"/>	Name	Username	Role	Domain(s)	Last Active	Added	Updated	Email	Type	Disabled
<input type="checkbox"/>	Admin User	admin	Admin		2022-01-06 11:58	2020-11-18 16:12	2020-11-18 16:34	riccardo@restorepoint.com	Local	No
<input type="checkbox"/>	Foo Bar	foobar	randomtest	Domain Test 070621	Never	2021-07-07 09:32	2021-07-07 09:32		Local	No
<input type="checkbox"/>	Yoyo.Ma	yoyoma	View Only		Never	2021-11-24 09:53	2021-11-24 09:53	yoyoma@yoyoma.com	Local	No

When the new administrator first logs in, they will be prompted to configure a password recovery question and answer. For more information, see [Password Reset](#).

Editing an Existing User

To edit the details of an existing user:

1. Navigate to the Users page (**Administration > Users**).
2. Click on the name of the user that you want to edit.

3. Edit the user as needed and then click **Save**.

The screenshot shows the 'Edit User' dialog box with the following fields and controls:

- Full Name:** Text input containing 'Yoyo Ma'.
- Email:** Text input containing 'yoyoma@yoyoma.com'.
- Role:** Dropdown menu showing 'randomtest'.
- Disabled:** A checkbox that is currently unchecked.
- Allowed Networks:** A section containing a text input for 'IP Address/Mask' and an 'Add' button.
- Buttons:** 'Close' and 'Save' buttons at the bottom right.

When editing an Admin-level user, there are two additional boxes on the **Auth** tab:

- **Recovery Question/Answer:** Set a Recovery Question / Answer for password recovery.
- **New Token:** Generates and emails a new recovery token to the user. This allows the user to recover their encryption password, if forgotten. For more information, see [Password Reset](#).

Broadcasting to Users

You can use Restorepoint to send a notification message to a user or group of users. Select checkbox next to the users you want to message and click **Broadcast**. This opens the Broadcast Dialog, where you can enter the **Text** of the message, the **Type** of message to send, and how long the message should persist.

A *UI* message type appears as a pop-up in the User's UI session. If the user is not currently logged in, the message will appear when they log in to the appliance until the **Persist** time is reached. An *Email* message type will send the notification to the User's email address registered on the appliance.

Deleting a User

To delete one or more existing users:

1. Select the checkboxes of the users you want to remove.
2. Click **Delete**.

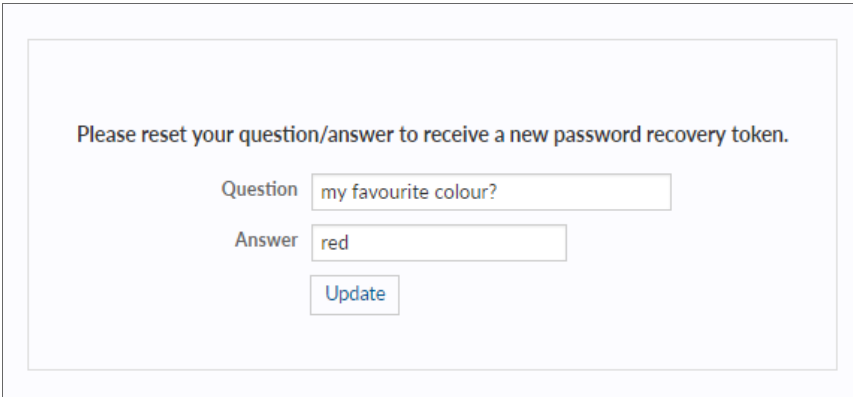
Password Reset

Restorepoint provides a password reset mechanism based on two-factor authentication.

Password Recovery Configuration

During the initial configuration procedure, or when an administrator logs in for the first time, the following information must be set:

- A password recovery question and related answer. For security reasons, only an administrator should know these.
- The administrator's email address.



The screenshot shows a web form for configuring password recovery. The form has a light blue background and is enclosed in a thin grey border. At the top, it says "Please reset your question/answer to receive a new password recovery token." Below this, there are two input fields: "Question" with the text "my favourite colour?" and "Answer" with the text "red". Below the answer field is a blue "Update" button.

Restorepoint will then email a **recovery token**, which can be used by the administrator to reset their password and encryption password, if the administrator knows the recovery question and answer.

Recovery Procedure

When logging on with an incorrect password for the given account, Restorepoint will display the **Forgotten password** link:

Incorrect username or password - [Forgotten your password?](#)

Login

Username
admin

Password
.....

Login

Or login using Single Sign On

Login with SSO

Click **Forgotten password?** to start the password recovery procedure. You will be prompted to enter your recovery token and recovery answer. After you enter the required information, click **Recover**.

Username admin

Recovery Token cYf+qIDHnASDqFgW3e3SKJxQRf

my favourite colour? red

Recover Cancel

If lose your recovery token, you can issue a new one from the **Edit User** page. If you change your password recovery question or enter your answer, a new recovery token will be sent. You can also issue a new recovery token by clicking **New Token**

Custom User Roles

In addition to the standard built-in administrator roles (**Admin**, **Backup**, and **View Only**), which cannot be edited, it is possible to define custom roles that define which product elements are accessible to the user. This feature is only available with an Enterprise license.

In order to define a custom role:

1. Navigate to the **User Roles** page (**Administration > User Roles**).
2. Click **Add Role**, and enter a name for the role.

3. Select the allowed actions for this role.

Add Role

Name

Permissions **Users**

Devices

<input type="checkbox"/> Modify Device	<input type="checkbox"/> Backup Device	<input type="checkbox"/> Restore Device
<input type="checkbox"/> Command Device	<input type="checkbox"/> View Deviceauth	<input type="checkbox"/> View Devices
<input type="checkbox"/> Add Device	<input type="checkbox"/> Delete Device	<input type="checkbox"/> Export Devices
<input type="checkbox"/> Modify Labels	<input type="checkbox"/> Open Terminal	

Asset Fields

<input type="checkbox"/> Modify Assets	<input type="checkbox"/> View Assets
--	--------------------------------------

Credentials

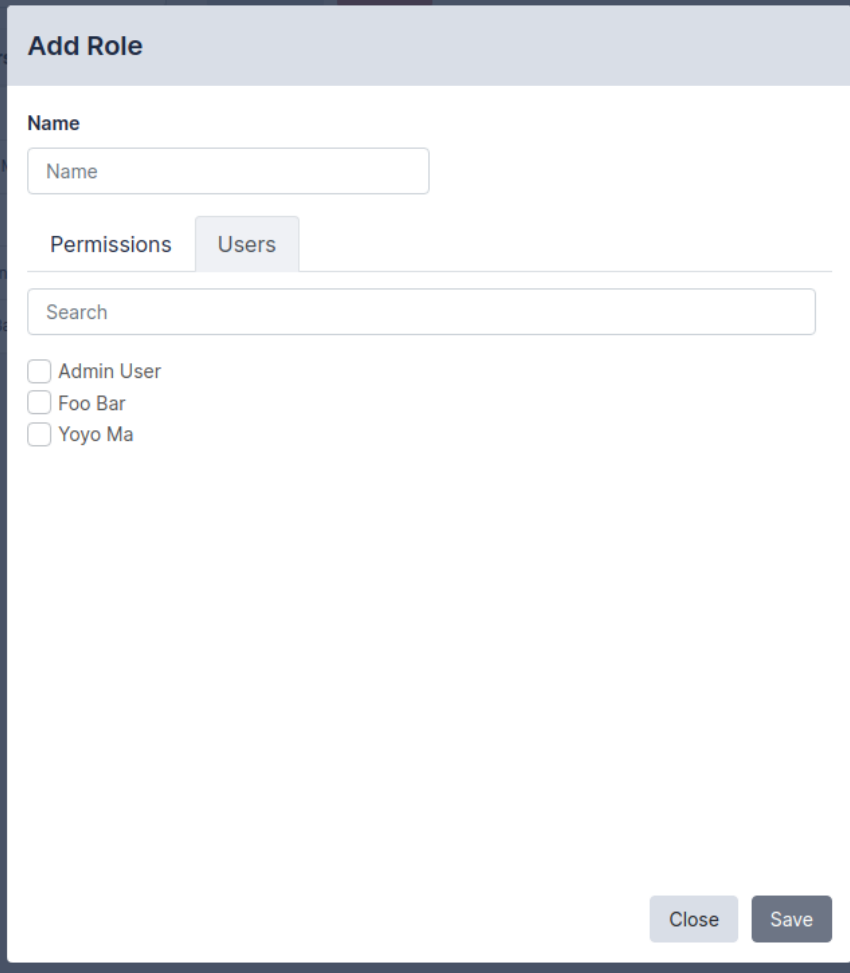
<input type="checkbox"/> View Credentials	<input type="checkbox"/> Modify Credentials
---	---

Backups

<input type="checkbox"/> List Backups	<input type="checkbox"/> View Backup	<input type="checkbox"/> Export Backup
<input type="checkbox"/> Modify Backup		

Schedule

4. Click the **Users** tab to assign this role to one or more existing users.



The screenshot shows a dialog box titled "Add Role". At the top, there is a "Name" label and a text input field containing the word "Name". Below this, there are two tabs: "Permissions" and "Users", with "Users" being the active tab. Under the "Users" tab, there is a "Search" label and a text input field. Below the search field, there are three list items, each with an unchecked checkbox: "Admin User", "Foo Bar", and "Yoyo Ma". At the bottom right of the dialog, there are two buttons: "Close" and "Save".

5. Click **Save**.

After you add a role, it is immediately available in the **Role** drop-down on the **Edit User** page. Note that any changes to custom roles take effect immediately upon save.

For example, you can create a user role called *Compliance Officer* that can only create and modify compliance rules, and apply those to devices.

Edit User

Details
Auth
Domains

Full Name

Email

Role

randomtest
▼

Disabled

Allowed Networks

Add

Close
Save

In addition to the global **View** (read-only) and **Modify** (read-write) permissions, you can allow the following actions:

Reports	
Backup	Allows backup reports
Config	Allows configuration reports
Assets	Allows assets reports
Compliance	Allows compliance reports
Admin	Allows administration reports
Monitor	Allows monitoring reports
Dashboard	Allows dashboard reports
Modify	Allows users to modify and schedule reports

Logs	
View Logs	Allows users to view the system log
View Syslogs	Allows users to view the device syslogs

Devices	
View	Allows users to view the device list and device details (excluding authentication details)
View Auth	Allows users to view device authentication details
Backup	Allows device backup operations
Command	Allows device remote control

Configurations	
List	Allows users to view the device configuration list
Export	Allows users to export device configurations
Restore	Allows users to restore a configuration to a device

Templates	
List	Allows users to view the template list
Push	Allows users to push templates to devices

Firmware	
Push	Allows users to push firmware images to devices

Assets	
List	Allows users to view custom asset fields

Compliance Rules	
Apply	Allows users to apply compliance rules to devices

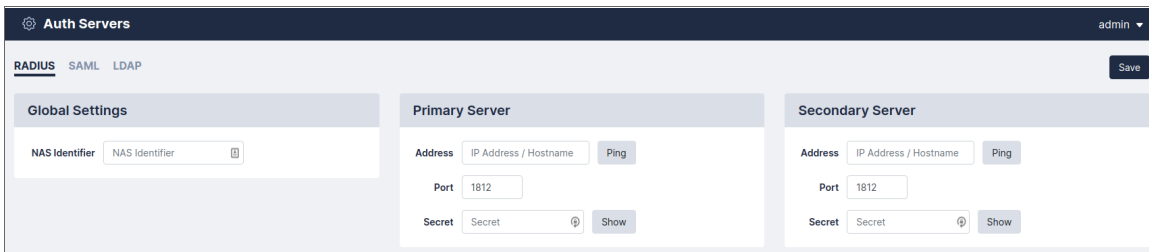
System	
Archive	Allows system archive operations

Users	
View	Allows user to view the user list and user details (excluding authentication details)
View Auth	Allows users to view user authentication details

Authentication Servers

RADIUS Authentication

Here you can configure parameters for authenticating administrators via RADIUS. If **Use RADIUS** is selected for a user, Restorepoint will use RADIUS instead of the internal authentication database. Restorepoint supports the PAP and CHAP (not MS-CHAP) authentication protocols.



NAS Identifier	a string identifying Restorepoint to the RADIUS server	
Primary Server	Address	IP address of the RADIUS server
	Port	UDP port used by the RADIUS server (usually 1812)
	Secret	a string shared between Restorepoint and the RADIUS Server
Secondary Server (optional)	A second RADIUS server, configured as above.	

LDAP Authentication

This section can be used to connect to an LDAP (Active Directory) user authentication server.

Base DN	The top-level LDAP DN. This is usually (but not always) the DNS domain name, such as <i>dc=company,dc=com</i> .	
User Search	Base DN	for example, <i>cn=users,dc=company,dc=local</i>
	Username Field	what LDAP field to use as the Restorepoint login id, for instance <i>uid</i> or <i>samAccountName</i> .
Group Search	Base DN	for example, <i>cn=security groups,dc=company,dc=local</i> .
	Search String	the group search filter, for instance <i>objectClass=Group</i> or <i>objectClass=posixGroup</i> , depending on the directory type.

Primary Server	Address	IP address of the LDAP server.
	Port	UDP port used by the LDAP server (usually 389). LDAP over SSL may use 636. Use 3268 to query the Active Directory Global Catalogue (useful for multi-domain forests).
	Bind DN	the DN to bind the LDAP with. For instance, gbh.
	Bind Password	the bind password for the LDAP Server.
	Use TLS	allows you to require encrypted connections to the LDAP Server.
Secondary Server (optional)	A secondary LDAP server	

NOTE: LDAP users will need to be assigned a role from the **Administration > Users > LDAP Users** tab before they can log in.

Chapter

7

Device Control

Overview

This chapter describes how you can use Restorepoint to send a command-line interface (CLI) command to a device or group of devices and capture the output of the command. This tool can be used to perform a task concurrently on a group of devices.

This section covers the following topics:

<i>Controlling a Device</i>	74
<i>Using Parameters</i>	76
<i>Scheduled Actions</i>	76

Controlling a Device

You can use Restorepoint to send a CLI command to a device or group of devices and capture the output of the command. This tool can be used to perform a task concurrently on a group of devices, such as changing the administrator password. To use this function, select the relevant device(s) and click **Control**.

The dialogue box appears:

Control Devices

Stored Actions
New Action

Name
[Text Input]

Description
[Text Input]

Type
Commands

Variable delimiter
\$

Timeout (s)
30

Keep Input

Device type
[None]

Command
[Text Area]

Close Perform Clone Apply Save

Select **New Action** from the drop-down menu, then enter the commands in the text area. Device Control Actions can also be defined from the **Device Control** page (Devices > Device Control), by clicking **New Action**.

If required, you can **Save** these commands as an **Action** for later execution, or for use in **Compliance Remediation**.

Stored Actions can also be scheduled. For more information, see [Scheduled Actions](#).

Click **Perform** to execute the commands. Restorepoint will display the output of the commands for each of the selected devices. Device Control outputs are stored in the **Output** tab of the Device Control page.

Edit Command

Name

Description

Type **Variable delimiter**

Timeout (s) **Keep Input**

Device type

Command

Output

```
A Cisco Switch
wkg2ios1 uptime is 1 week, 3 days, 14 hours, 47 minutes
```

This section covers the following topics:

Using Parameters

You can use action parameters for different devices, using the format `$`parameter`$`, where `$` is the **Variable Delimiter** you've set for your Action. For instance, to change the admin password for a number of ScreenOS devices, select the devices and enter the command:

```
setadminpassword$password$
```

After you click **Perform**, you will be asked for a replacement string for each device. An unlimited number of parameters can be replaced this way.

NOTE: A parameter can only consist of letters, numbers, and the underscore character `_`. If the replacement string contains escape sequences (such as `\n`), they must be double-escaped (`\\n`).

Scheduled Actions

Actions can be scheduled and run automatically. Click on the **Schedule** tab in the Device Control page, then click **New Schedule**:

New Schedule

Action

Devices

- Self
- A Cisco Switch
- Juniper Firewall
- wkg2vm1
- Extreme
- F5 - Web Gateway
- Juniper SA
- wkg2fw1
- wkn2nev2

Perform

Every **at**

Store Log

Email Log

Apply Policy

1. Select the **Action**.
2. Select the device or devices on which to perform the action.
3. Select a frequency, either **Scheduled** or **Once At** and a time interval or date.
4. If you want to keep the output of the action, select the **Store Log** checkbox.
5. If you want to email the output of an action after execution, select the **Email Log** check box and enter an email address.
6. Optionally, select a compliance policy to apply to the output of the action. For more information, see [Device Policies](#).
7. Click **Save** and the scheduled action page is displayed.

Device Control admin ▾

Actions Schedule Output

Search New Schedule Delete

<input type="checkbox"/>	Action	Devices	Schedule	Next Due	Email To	Policy	Keep
<input type="checkbox"/>	action-test-1	New Device	Every hour at :00	2022-01-19 13:00			0
<input type="checkbox"/>	action-test-1	A Cisco Switch	Every hour at :00	2022-01-27 18:00		Test policy	0
<input type="checkbox"/>	Clone of action-test-1 UPDATED	A Cisco Switch	Every 8th month on the 1st at 00:00	2022-01-31 17:00		foo policy UPDATE2	0
<input type="checkbox"/>	action-test-1	A Cisco Switch	Every hour at :00	2022-01-26 18:00		foo policy UPDATE2	0
<input type="checkbox"/>	action-test-1	A Cisco Switch	2022-01-26 17:00	2022-01-26 17:00		foo policy UPDATE2	0

NOTE: Scheduled Actions cannot contain parameters.

Chapter

8

Lua Applets

Overview

Device Control features a more powerful way to interact with devices using the Lua programming language. Instead of sending a single command to a device, Lua offers control structures loops, conditionals, match functions, etc. Using Lua, you can perform more complex tasks, including making decisions based on the device output.

To create a Lua action, navigate to the Device Control page (Devices > Device Control) and click New Action. Then select **Type > Lua** from the drop-down menu.

The syntax is straightforward, and it does not require any specific programming experience or knowledge of markup languages like XML. For more information about Lua, see <https://www.lua.org/docs.html>.

This section covers the following topics:

<i>Restorepoint Built-in Functions</i>	80
<i>Examples</i>	80

Restorepoint Built-in Functions

The following functions can be used in a Lua applet:

- `timeout (seconds)` - set the maximum timeout when waiting for device output
- `sleep (seconds)` - do nothing for the given number of seconds.
- `send (command)` - send `command` to the device
- `wait (string)` - wait for `timeout` seconds for `string` from the device
- `sendget (command, output)` - combined `send/wait`
- `before ()` - used after `wait()` or `sendget()`; it contains the output from the device up to the expected string.
- `print (string)` - displays the value of `string`
- `splitlines (string)` - split a multi-line string (for example, the output of a command) into an array of lines.

Other standard Lua commands that may be useful include, `string.match`, `string.gsub`, and `string.trim`.

NOTE: You do not need to write any code to connect and authenticate to the device. Restorepoint will automatically connect and authenticate the device for you.

CAUTION: Users are not permitted to run any “os” or “system” functions when making Lua scripts. This restriction is in place to maintain the security of your Restorepoint appliance.

Examples

Show Version (Cisco)

A basic example is to display the output of the `show version` command on a Cisco switch:

```
timeout (20)
send('show version')
wait('#')
out=before()
print(out)
```

The `send ()` & `wait ()` commands can also be combined into a `sendget ()`:

```
timeout (20)
sendget("show version", "#")
out=before()
```



```
print(out)
```

Show Interface (Cisco)

The following is a more complex example using control structures. It runs `show interfaces` on a Cisco switch and checks that all interfaces that are not connected (line protocol is down) are also administratively down. Note that everything after `--` is a comment, and is not executed:

```
timeout(20) -- set the timeout to 20 seconds
sendget("terminal length 0", "#") -- send command to the device, and
-- wait for the prompt
sendget('show interfaces', '#')
out = before() -- set "out" to the output
lines = splitlines(out) -- split the output lines into array
for k,v in pairs(lines) do -- loop over each line, and
-- set k=number and v=text
    int,st1,st2 = v:match(
        "^(%S+Ethernet[0-9/]+) is ([a-z ]+), line protocol is ([a-z]+)"
    ) -- extract the interface name,
-- interface status, and the
-- line protocol status
    if int ~= nil and
        ( st1 ~= 'administratively down' and st2 == 'down' ) then
        print("Interface "..int.." is disconnected but not shutdown")
    end
end -- end loop
```

IP Spoofing (ScreenOS)

For ScreenOS, use the following script to check for ip-spoofing:

```
timeout(5)
sendget("set console page 0", ">")
sendget("get zone | inc L3", ">")
ret = before()
sendget("get config | inc ip-spoofing", ">")
conf = before()
for zone in ret:gmatch(" [0-9]+ (.-)%s+Sec") do
    if conf:match('zone "'..zone.." screen ip%-spoofing') then
        print('Zone '..zone..' : antispoofing enabled')
    else
        print('Zone '..zone..' : antispoofing disabled')
    end
end
```

IP Spoofing (Palo Alto)

You can use the following script to check for ip-spoofing, but for Palo Alto devices:

```
timeout(5)
sendget("set cli pager off", ">")
sendget("set cli config-output-format set", ">")
waitprompt()
sendget("configure", "#")
send("show zone")
sleep(1)
waitlast("#")
ret = before()
sendget("exit", ">")
tbl = {}
for key in ret:gmatch("set zone (.-) ") do
    tbl[key] = true
end
for k, _ in pairs(tbl) do
    send('show zone-protection zone '..k)
    sleep(1)
    waitlast('>')
    ret = before()
    if ret:match('discard%-ip%-spoofer:%s+enabled: yes') then
        print('Zone '..k..'': antispoofing enabled')
    else
        print('Zone '..k..'': antispoofing disabled')
    end
end
```

Chapter

9

File Storage

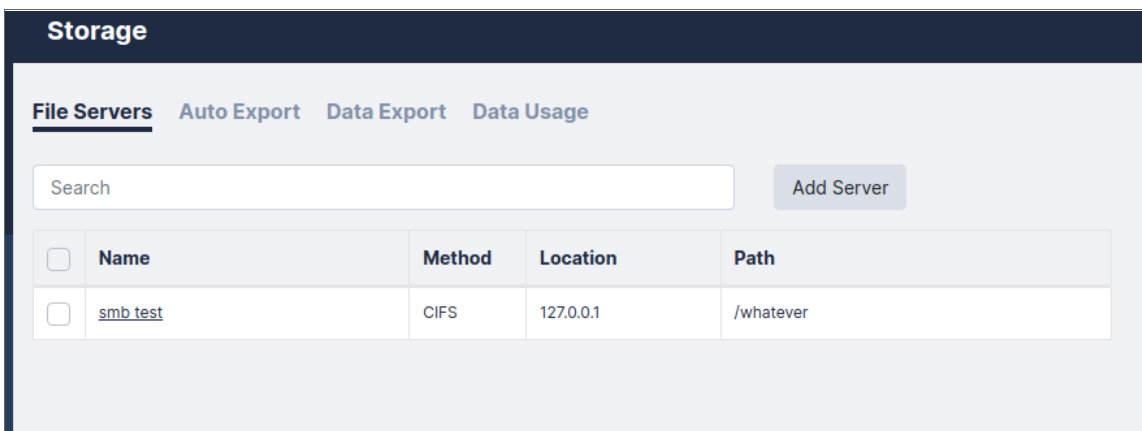
Overview

This chapter describes how to use File Storage in Restorepoint. You can use the Storage page (**Administration > Storage**) to save file storage configurations in Restorepoint. These can be used in the **Archive** or **Logs** page, or for automated configuration export from Restorepoint.

This section covers the following topics:

<i>File Servers</i>	84
<i>Auto Export</i>	84
<i>Data Export</i>	85
<i>Data Usage</i>	85

File Servers



For each file server, you can define the following fields:

Name	A name for the file server.
Protocol	Select CIFS (Windows Server), FTP, SCP or SFTP from the drop down menu.
Server IP	The IP address and port of the remote server.
Path	The full path on the remote server. For example, <i>/home/user1</i> (FTP) or <i>share1 directory2subdirectory3</i> (CIFS).
Username	The username. This will be an FTP user, or a valid windows user if using CIFS.
Password	The password for the associated username.
Use NTLMv2 (CIFS Only)	If you are using CIFS with the NTLMv2 authentication protocol, you can select this checkbox.

Auto Export

For each policy, you can define the following fields:

Server	The fileserver to store the exported configurations. You can also define a new server by using the <i>[New Server]</i> option - see File Servers for details on the configuration.
Policy	When to automatically export configurations to your external server. Always Export will export when the backup is complete, Only Export new Versions will export when the backup is complete and the version number of the backup has changed, and Export before automatic deletion will export only the backups that are due to be removed from the Restorpoint appliance.

There are additional options you can apply to your new policy:

Use GPG	Users must enter a passphrase to securely encrypt the exported configurations before transfer to your external server.
----------------	---

Include Domain/Device Name	The filename / path on the remote server will contain the domain name/device name. For example, <code>/home/user1</code> (FTP) or <code>share1directory2subdirectory3</code> (CIFS).
Disabled	If this checkbox is selected, the policy will not run. This options allows you to temporarily disable an auto-export policy.

Data Export

You can use this page to export device configurations on-demand.

Configurations	No configs , only the Most Recent version of the config, or All Configs .
Data	Includes the device's Logs , and/or the Device Data in your export.
For	The devices or domains to export.
As	The format to export the configurations. They can be exported as <i>TGZ</i> or <i>ZIP</i> archives, or directly export the individual config files.
Chunk Size	If you've selected an archive format, you can choose the size to create the archive files.
To	The server to store the exported configurations. See File Servers for more details. Alternately, you can choose to export device configurations directly to your workstation, via the Browser .

Data Usage

The Data Usage page displays statistics on the storage disk of your Restorepoint appliance.

Total Disk Size	The size of the encrypted volume that Restorepoint uses to store device configurations and settings.
Total Used	How much of that volume's space is used.
Backup size	Space used by device configurations.
Index size	Space used by Restorepoint's search index (used primarily for the Global Search function).
Cache Size	Space used by the Restorepoint cache. This is usually device configurations that needed to be extracted for viewing or comparisons. Restorepoint will automatically remove this cache, if needed. You can also manually clear the cache and click Clear Cache to clear the cache.
Debug Size	Space used by Restorepoint debugging logs, such as Appliance Debug Logs. Appliance Debug Logs are cleared if a new Debug Log is started. You can manually clear the Appliance Debug Logs and click Clear Debug .

Chapter

10

Agents

Overview

Agents allow a Restorepoint appliance to manage devices located on a remote or otherwise disjoint network, not directly routable by Restorepoint, without complex firewall changes, Network Address Translation, or VPNs. For instance, a Service Provider can set up a central Restorepoint appliance and deploy agents on customer networks and enable device backups on remote sites.

An Agent can be deployed as a Virtual or Hardware appliance on the remote network. The agent provides fast operations by locally performing all the tasks that would typically require extensive network interaction. Configurations, logs, etc. are processed locally by the agent, and uploaded to the master Restorepoint appliance.

NOTE: Device firmware updates via agents are not yet supported.

Agents are only available with an Enterprise license.

This section covers the following topics:

<i>Agent Firewall Requirements</i>	87
<i>Agent Installation</i>	87
<i>Adding an Agent to Restorepoint</i>	89
<i>Changing the Master IP Address</i>	91
<i>Remote Operations Using Agents</i>	92
<i>Managing Agents</i>	93

Agent Firewall Requirements

An agent initiates and maintains an SSH connection to the master Restorepoint appliance to receive tasks to execute, upload and download device configurations, task output and logs, and download software updates.

Your firewall policy must allow SSH traffic (TCP port 22) from the agent to the master for an agent to function correctly.

Agent Installation

An agent virtual appliance is deployed in a similar manner to a Restorepoint appliance (see the section on [Restorepoint Virtual Appliance](#)). Agents are kept up-to-date with software updates via the connection to the master appliance.

Initial Setup

To setup an agent, you must configure the network parameters and the details of the connection to the master:

1. Open the virtual machine console in your Virtual Infrastructure client.
2. In the login prompt, enter the default username (*admin*) and password (*admin*) for the agent.
3. Follow the prompts to change the agent shell password.

4. Select **IP Address Configuration** at the console menu:

```
Restorepoint agent console

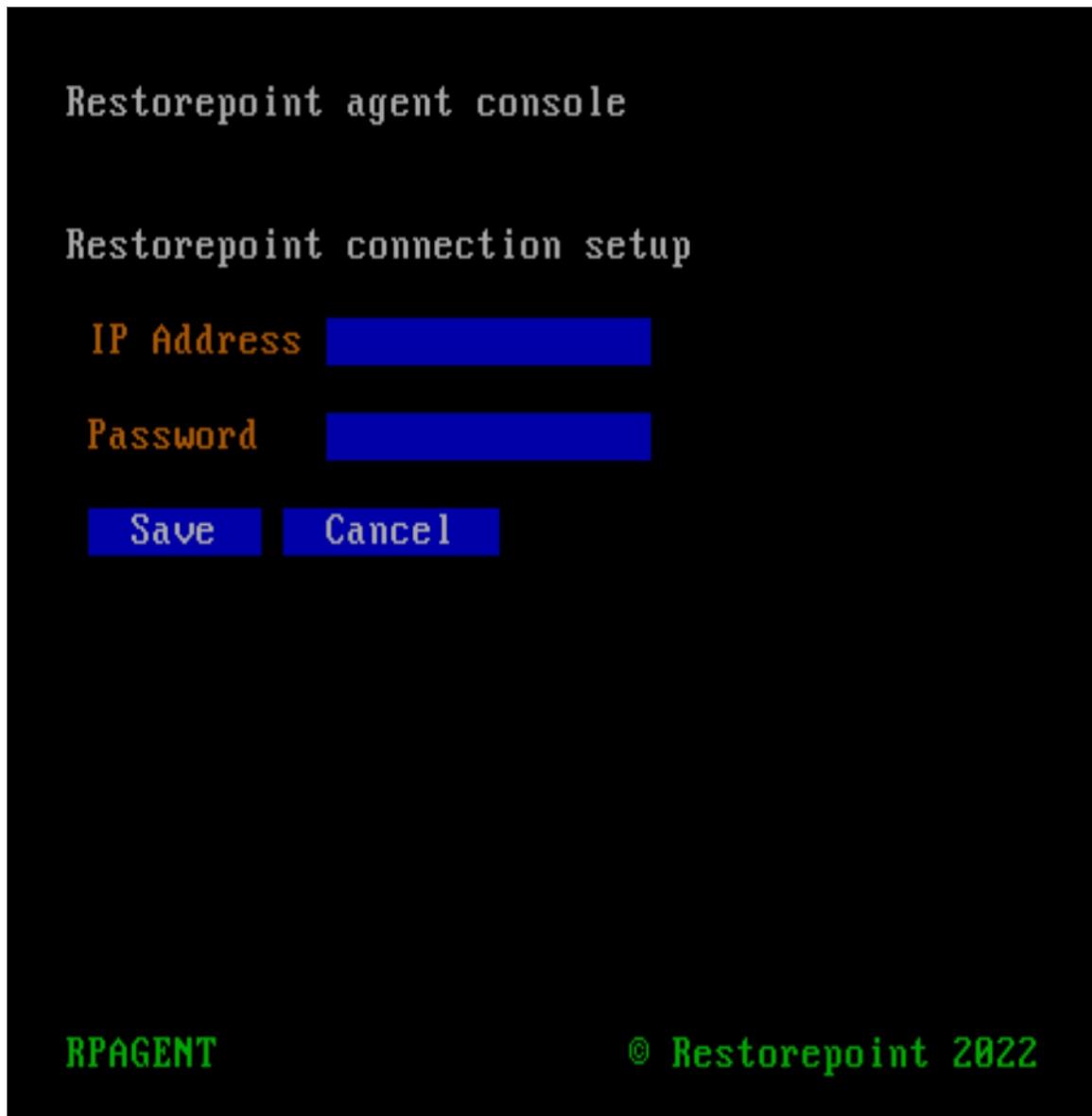
Interface settings

Use DHCP      
IP Address    192.168.1.1
Netmask       255.255.255.0
Default gateway 192.168.1.254
Auto-negotiation X
Speed         1000baseT/Full

RPAGENT                © Restorepoint 2022
```

5. Enter the settings for IP address, Netmask, Default gateway, and Primary DNS server as prompted.
6. Enter y to confirm the settings. If the settings are applied successfully, the console menu will be redisplayed.

- Next, select **Initial Restorepoint Master Setup**:



- Enter the IP address of the master Restorepoint appliance, and a one-time password to verify the Agent to the master (only used for initial pairing).

Adding an Agent to Restorepoint

To add a configured agent to Restorepoint, navigate to the Agents page (**Administration > Agents**) and click **Add Agent**. The following dialog appears:

Add Agent

Details Devices

Name

Name

Location

Location

Domain

Global

Email

some@email.com

Config Policy

Keep on Master

Secondary to

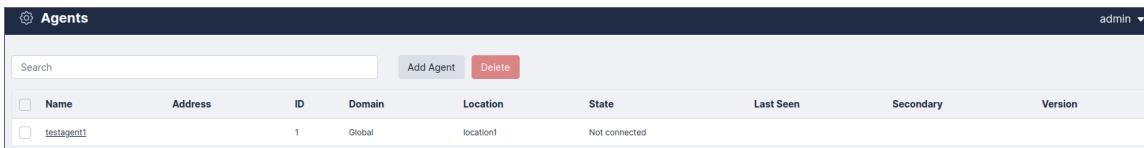
Close Save

Enter the following details:

Name	A name for the agent.
Location	Where the agent is located. Pick an existing location, or enter a new one.
Domain (optional)	The domain of the devices that this agent will manage. For more information, see Administration Domains .
Email (optional)	The email for the user that is responsible for the upkeep of the agent.
Alert on	If selected, an email alert will be sent if the agent goes offline. If the Email field is not filled in, the

disconnect	default notification address is used.
Alert on reconnect	If selected, an email alert will be sent if the agent comes back online. If the Email field is not filled in, the default notification address is used.
Password	The one-time password entered in the agent setup.

After the agent is added, Restorepoint will display the agent list. The address and port will be automatically filled in once the agent has connected successfully for the first time. Note that only one agent can be set up at a time.



Changing the Master IP Address

If the IP address of the master Restorepoint appliance changes, any agents connected to that master need to be reconfigured with the new master details. To reconfigure an agent with the new master details:

1. SSH to the agent (or open the virtual machine console).
2. Log in using the agent's *admin* account.
3. Select **Change Restorepoint Master IP address** in the console menu, and apply the new master IP address.

NOTE: Do not use the option **Initial Restorepoint Master Setup** to set the new master IP address. If you use this option, it invalidates the master-agent authentication and would require re-pairing the agent to the master Restorepoint appliance.



Remote Operations Using Agents

Once you configure an agent, you can perform any operation (backup, restore, control etc.) on a device via the agent. The Restorepoint appliance will not connect directly to the device, the appliance will instruct the agent to perform the operation on its behalf.

To move an existing device to an agent, select one or more devices from the **Device Management** List, and click **Edit**, then select the correct Agent in the drop-down menu as shown:

Device Details

Device Name

Resolve

Type

Check Point Edge ▼

Info

Fingerprint

Labels

Select labels ▼

Address

Ping

TCP Dump

Disabled

Open Terminal

 Use Stored Credentials

Operations using agents are completely transparent for the user. For instance, bulk operations can be started for agent-managed and directly-managed devices simultaneously.

Managing Agents

You can view a list of the paired agents from the **Administration > Agents** page. To edit an agent's settings, click the name of the agent.

The settings include the **Name, Location, Domain, Email**, whether to **Alert on Disconnect/Reconnect**, or allow you to factory **Reset** the Agent for re-pairing. There are additional settings for Debugging agent connections.

Debug > Start works similarly to Appliance Debugging. It records a debug log that can be viewed using the **Debug > View** button.

Debug > Info collects and displays a series of system information from the Agent, such as RAM usage, Disk usage, and Uptime.

Debug > Remote allows remote management of an agent. This option will displays a port number. You can connect to that port on your Restorepoint master appliance to redirect to the agent so that trickier issues can be diagnosed.

Chapter

11

Administration Domains

Overview

Administration Domains allow you to organize devices into separate domains and delegate their management to Domain Administrators.

Service Providers typically use this feature to restrict the scope of administrators to a subset of network devices.

Domains are only available with an Enterprise license.

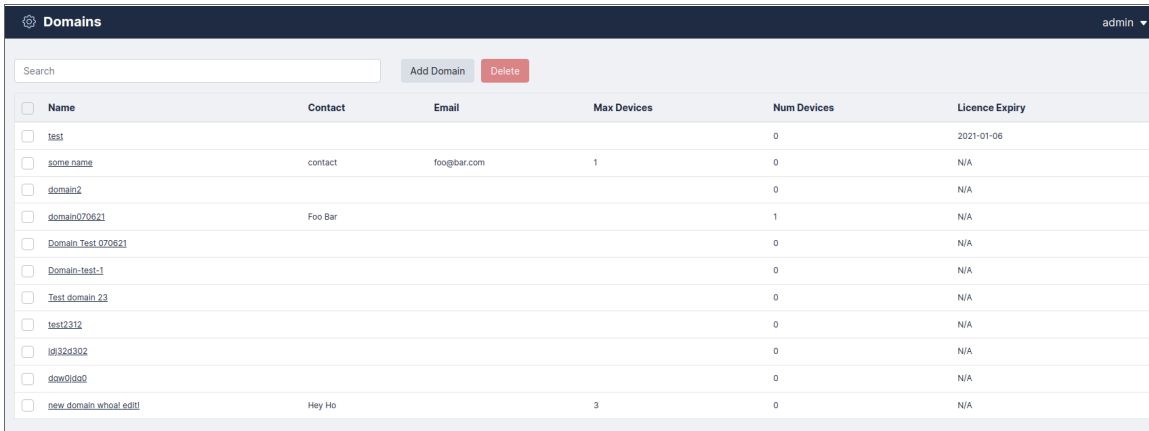
This section covers the following topics:

<i>Managing Domains</i>	95
<i>Administrator Roles</i>	97
<i>Adding a New Domain User</i>	98
<i>Editing Devices</i>	101

Managing Domains

The **Domain Management** page allows you to create, modify, and delete Administration Domains. This page is only displayed if you are logged in as a Global Administrator.

Click **Administration > Domains** on the menu to display the domain list:



<input type="checkbox"/>	Name	Contact	Email	Max Devices	Num Devices	Licence Expiry
<input type="checkbox"/>	test				0	2021-01-06
<input type="checkbox"/>	some name	contact	foogbar.com	1	0	N/A
<input type="checkbox"/>	domain2				0	N/A
<input type="checkbox"/>	domain070621	Foo Bar			1	N/A
<input type="checkbox"/>	Domain.Test.070621				0	N/A
<input type="checkbox"/>	Domain-test-1				0	N/A
<input type="checkbox"/>	Test domain 23				0	N/A
<input type="checkbox"/>	test2312				0	N/A
<input type="checkbox"/>	test23302				0	N/A
<input type="checkbox"/>	gwer01992				0	N/A
<input type="checkbox"/>	new domain whoal edit!	Hey Ho		3	0	N/A

To add a new domain:

1. Click **[Add Domain]**. The **New Domain** page appears:

Edit Domain

Details Devices Branding Licence

Name

Contact

Telephone

Email

Address

Notes

Close Save

2. Complete the following details:

Name	Enter a name for the domain (e.g., Customer Name, Business Unit, etc.).
Contact (optional)	Enter the name of the main contact for the domain.
Telephone (optional)	Enter a contact telephone number.
Email (optional)	Enter a contact email.
Address (optional)	Enter a customer or Business Unit address.
Notes (optional)	Enter any additional information.

3. Click the **Devices** tab to use the device selector and add devices to the domain. Additionally, you can configure the following:
- **Max. devices:** the maximum permitted number of devices that can be added to this domain.
 - One or more IP address ranges that are allowed for this domain.
 - A domain-wide NAT IP address, which overrides the system-wide setting. For more information, see [Network Address Translation \(NAT\)](#). This setting can be overridden by the device-specific setting.
 - The devices that are part of the new domain.
4. Click the **Branding** tab (optional) to customize the top left-hand side corner image that will be displayed to a Domain Administrator. Click **Choose File** to locate a suitable image file on your PC. For best results, the logo should be exactly 100 pixels wide and up to 100 pixels tall, and no more than 40KB in size.

Remove Licence Info	Hides the expiration date for users in this domain.
Remove Serial Number	Hides the appliance serial number for users in this domain.
Remove Help Menu	Disables access to help for users in this domain.

5. Click the **License** tab (optional) to restrict the domain to expire on a certain date. Click **Enforce License** to enable the function, and choose a date.

Disable Schedule	Stops all scheduled jobs for this domain when a defined date is reached.
Prevent User Login	Disables users of this domain from accessing the appliance when a defined date is reached.

6. Click **Save**. The system returns to the domain list.

To edit an existing domain, click the name of the domain.

Administrator Roles

If Administration Domains are enabled, administrators have either a global or a domain scope:

Global Users	Have visibility and can operate on all the devices on the system, regardless of the domain the devices are assigned to. Logs and status pages display information about all the devices defined on the system.
Domain Users	Users with at least one domain set. Their visibility is restricted to devices in their own domain(s). Logs and status pages only display information on the devices in the selected domain(s).

Restorepoint supports six built-in user roles:

Global Admin	A "Super User" that has full control on any aspect of the appliance:
	<ul style="list-style-type: none">• create/modify/delete devices in any domain
	<ul style="list-style-type: none">• create/modify/delete global and domain administrators
	<ul style="list-style-type: none">• initiate backups/restores
	<ul style="list-style-type: none">• change the appliance configuration
	<ul style="list-style-type: none">• an encryption password that allows Restorepoint to transition from the lock-down state to the normal state
Global Backup	Backup Operator; can perform backups/restores of devices in any domain, but cannot modify devices, users, or appliance configuration.
Global View Only	Monitor Operator; can only view existing backups and verify that the system is operating normally.
Domain Admin	Has full control of devices and users in their domain. Does not have visibility of devices in other domains, cannot modify the appliance configuration, or transition the appliance from lock-down state to normal state. Logs and status screens only display information related to the domain.
Domain Backup	Can perform backups/restores of devices in their domain.
Domain View Only	Can only view existing backups, access logs, and status information of devices in their domain.

You can also define custom user roles. For more information, see [Custom User Roles](#).

You can use the **Users** page to add or delete administrator or modify their password, scope, or permissions.

Adding a New Domain User

To add a new domain user:

1. Select **Administration > Users** from the menu. Restorepoint displays the **User Management** page.
2. Click **Add User**. Restorepoint displays the **New User** page as shown:

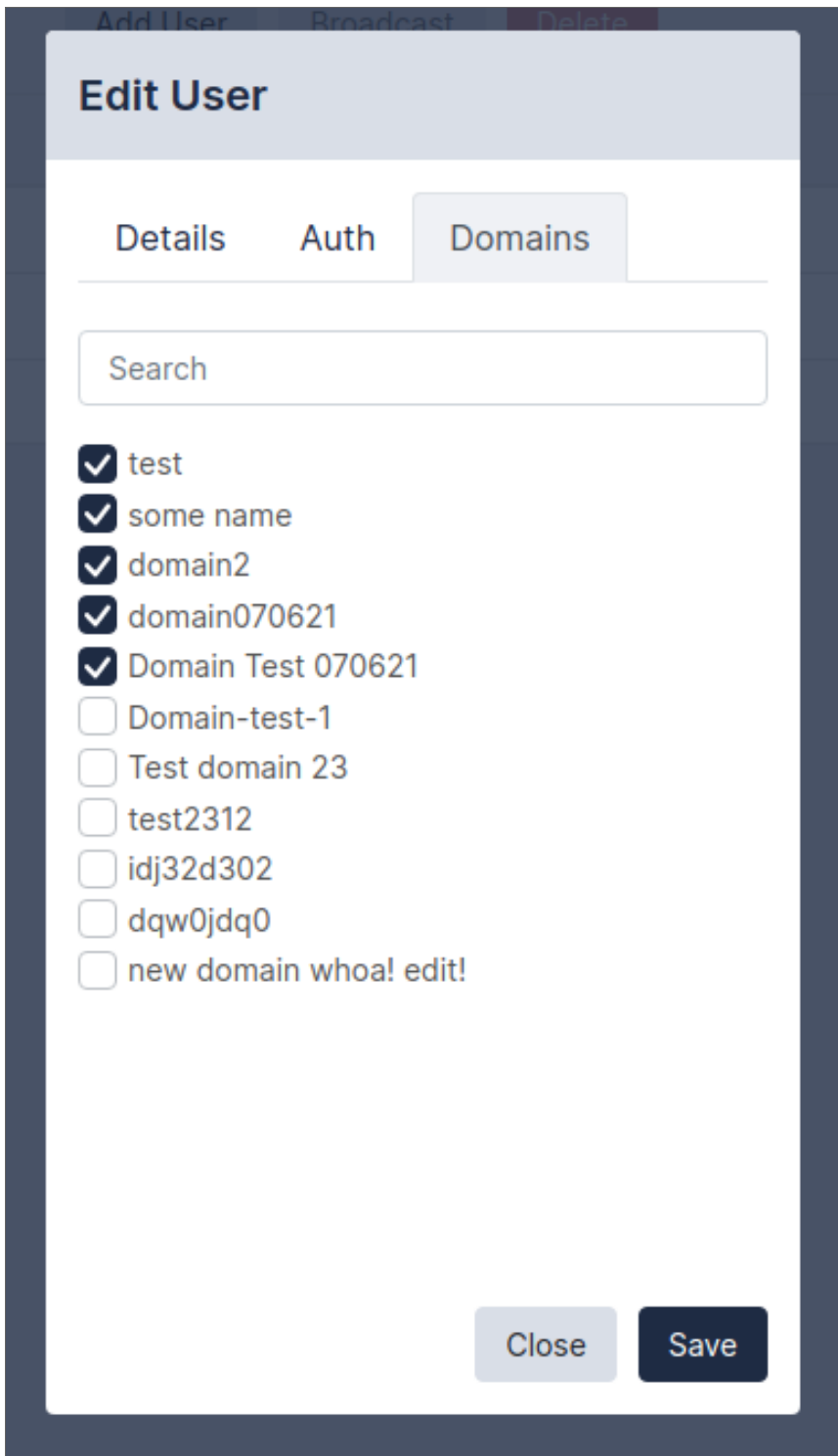
3. Complete the following fields:

Full Name	Enter the full name of the user.
Username	Enter the new username (up to 16 characters).
Password	Enter the password for the new user (passwords must be between 8 and 24 characters long).
Role	Select the privilege level from the drop-down list. See for the privileges associated with each admin level.

Privileges	View Only	Backup	Admin
View devices/configurations	Y	Y	Y
Run device operations	N	Y	Y
Add users/devices; modify system	N	N	Y

Table 4 : Default Administrator privilege levels (simplified)

Encryption Password	This field appears if an Admin-level administrator is selected. The encryption password must be between 8 and 24 characters long and must be different from the administrator password.
Domains	Assign the user to one or more domains to restrict the user's scope:



4. Click **Update**. The updated **Users** page appears:

User Management										
admin										
All Users SAML Users Logged-in Users API Tokens										
Search										
Add User Broadcast Delete										
<input type="checkbox"/>	Name	Username	Role	Domain(s)	Last Active	Added	Updated	Email	Type	Disabled
<input type="checkbox"/>	Admin User	admin	Admin		2022-01-06 11:58	2020-11-18 16:12	2020-11-18 16:34	riccardo@restorepoint.com	Local	No
<input type="checkbox"/>	Foo Bar	foobar	randomtest	Domain Test 070621	Never	2021-07-07 09:32	2021-07-07 09:32		Local	No
<input type="checkbox"/>	Yoyoma	yoyoma	View Only		Never	2021-11-24 09:53	2021-11-24 09:53	yoyoma@yoyoma.com	Local	No

Editing Devices

If Administration Domains are enabled, you can use the **Domain** drop-down menu in the **Edit Device** modal to move a device from a domain to another.

Device Details

Device Name

Zhone Ead 544 Resolve

Type

Zhone EAD Info Fingerprint

Domain

Global

Agent

Search agents

[None]

testagent1

Add new

177.101.80.77 Ping TCP Dump

The domain selector will only be displayed if you are logged on as a Global Administrator.

Chapter

12

Logs

Overview

The **Logs** page displays detailed information about system activity.

This section covers the following topics:

<i>Event Log</i>	103
<i>Syslog</i>	104

Event Log

These are the log messages for user activity, device operations, and system messages. A typical entry displays:

Date	The specific time of an event.
Action	The event type
Object	The device, user, or system configuration object to which the event refers.
Object Name	The device, user, or server that an action was performed on.
Message	The status, return, or error message associated with the event.
User	The user associated with the event (or Auto for scheduled events).
Status	OK or Error
IP Address	The IP Address that is associated with the event, or <i>localhost</i> .

The screenshot shows a web interface for viewing logs. At the top left, there is an information icon and the word "Logs". Below this is a search input field and an "Export" button. The main area contains a table with the following columns: Date, Action, Object, Object Name, Message, User, Level, and IP Address. The table lists various system events such as device discovery, monitoring, license updates, and system upgrades.

Date	Action	Object	Object Name	Message	User	Level	IP Address
2022-02-10 16:20	Control	Device	A Cisco Switch	Performing Adhoc Command show version I uptime	admin	Info	127.0.0.1
2022-02-10 15:11	Discovery	System		17 devices found	admin	info	127.0.0.1
2022-02-10 14:05	Monitor	Device	A Cisco Switch	Device Back Up	Auto	err	127.0.0.1
2022-02-10 14:00	Monitor	Device	A Cisco Switch	Device Down	Auto	err	127.0.0.1
2022-02-10 13:53	Entitlement	System		Updated Licence. About to upgrade to version 5.4_devel:220210. [Changelog]	Auto	info	127.0.0.1
2022-02-10 13:53	Entitlement	System		Update to 5.4_devel:20220210104450 successful	Auto	info	127.0.0.1
2022-02-10 13:53	Entitlement	System		Starting upgrade to 5.4_devel:20220210104450	Auto	info	127.0.0.1
2022-02-10 13:53	Startup	System		Restorepoint startup	Auto	info	127.0.0.1
2022-02-10 13:52	Entitlement	System		Updated Licence. About to upgrade to version 5.4_devel:220210. [Changelog]	Auto	info	127.0.0.1
2022-02-10 13:52	Entitlement	System		Update to 5.4_devel:20220210104450 successful	Auto	info	127.0.0.1
2022-02-10 13:52	Startup	System		Restorepoint startup	Auto	info	127.0.0.1
2022-02-10 13:52	Entitlement	System		Starting upgrade to 5.4_devel:20220210104450	Auto	info	127.0.0.1
2022-02-10 13:51	Startup	System		Restorepoint startup	Auto	info	127.0.0.1
2022-02-10 13:51	Entitlement	System		Updated Licence. Installed plugin Cisco ASA rev. 25626. Installed plugin Riverbed Steelhead rev. 25618. About to upgrade to version 5.4_devel:220210. [Changelog]	admin	Info	127.0.0.1

Use the **Export** button to export the event log as a CSV file.

Entries in the system log will be deleted according to the retention policy set on the [Log Settings and Alerts](#) page.

Syslog

The following messages are logged to the Restorepoint syslog service by both the appliance itself and any devices configured to log to it.

Date/Time	Date/time of an event
Process	Syslog Process
Level	Syslog level (Alert, Critical, Error, Warning, Notice, or OK, corresponding to severity levels 1 - 6).
Message	Status/Error message associated with the event.
Facility	Syslog Facility
Source	The IP Address that is associated with the event or <i>localhost</i> .

Chapter

13

Appliance Administration

Overview

The **System Settings** page allows you to configure appliance-related settings, such as networking parameters and date/time settings.

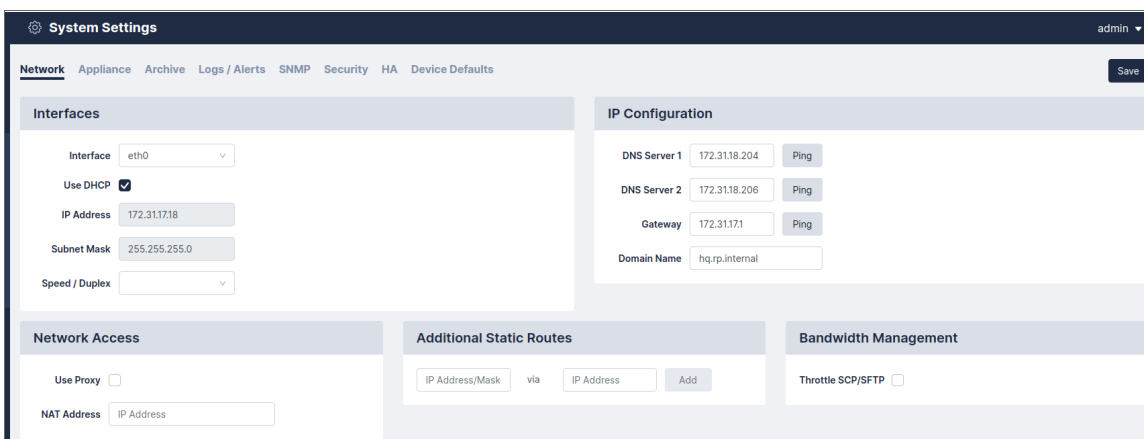
This section covers the following topics:

<i>System Settings</i>	106
------------------------------	-----

System Settings

To access the **System Settings** page, expand the **Administration** menu and select **System Settings**.

Network Settings



Network Interfaces

Use the drop-down menu to override the default auto-detect setting of the Ethernet interface(s). Click **Save** to apply the change. There will be a short delay while the new settings are applied. If Restorepoint fails to detect a link after the change, it will revert to the previous setting.

Primary / Secondary Interface

Use the **Network** tab (Administration > System Settings > Network) to set or update the network address for Restorepoint. The initial settings are entered when you first set up your appliance. Select your **Interface** first and then supply values in the following fields:

Use DHCP	Select this checkbox if you use DHCP for your interface and the other options will be disabled.
IP Address	Enter the IP address of the Restorepoint appliance.
Subnet Mask	Enter the subnet mask associated with the IP address.
Speed/Duplex	Select the link speed and duplex from the drop-down list.

IP Configuration

DNS Server	The DNS server address for your network. The DNS server must be able to resolve public names (for example, <i>support.restorepoint.com</i>), otherwise the appliance cannot retrieve software updates and license details.
DNS Server	A second DNS server.

2 (optional)	
Gateway	The default gateway for your network. You can Ping these servers to check connectivity.
Domain Name	The default domain name.

Click **Save**.

Network Access

Restorepoint needs Internet access (HTTP/HTTPS) to retrieve software and plugin updates. If a proxy is required for Internet access, select **Use Proxy**, and supply the following information:

- IP address of the proxy server.
- Proxy port.
- Username/password, if your proxy requires authentication. Otherwise, leave this field empty. Use the **Test Proxy** button to verify that the configuration is correct.

Network Address Translation (NAT)

Restorepoint may use back-connections (typically TFTP or FTP) to backup certain devices. If Restorepoint is accessing a device using back connections through a NAT router or firewall, back-connections will fail because the device will attempt to connect to the original, untranslated IP address. To avoid this problem:

1. On your firewall, create a 1:1 NAT mapping (often referred to as Static NAT or Mapped IP) to translate the Restorepoint IP address to a public/routable IP address.
2. Enter the public IP address for Restorepoint in the **NAT Address** box. The system-wide NAT IP address defined here can be overridden in the Domain settings, or in each individual device's settings.

The **Back-connection NAT** option needs to be selected in any device that is accessed by Restorepoint through NAT. For more information, see [Adding a new device manually](#).

Restorepoint supports multiple NAT addresses. The NAT IP address defined in this page can be overridden by the Domain or Device NAT IP setting.

Additional Static Routes

If the devices that you want to add to Restorepoint are located on different networks, you may need to define additional static routes. To define a static route:

1. **IP Address / Mask length:** Enter the network address/netmask (in CIDR notation).
2. **Via IP address:** Enter the destination gateway IP address.
3. Click **Add**.
4. Click **Save**.

To remove a static route:

1. Click **Delete** next to the static route you want to remove.
2. Click **Save**.

Bandwidth Management

You may limit the amount of network bandwidth Restorepoint uses by selecting **Throttle SCP/SFTP** and specifying a speed (in kbps).

Appliance Operations

The screenshot shows the 'System Settings' interface for network configuration. The 'Network' tab is active, showing several sections:

- Interfaces:** Shows configuration for the 'eth0' interface, including 'Use DHCP' (checked), 'IP Address' (172.31.17.18), 'Subnet Mask' (255.255.255.0), and 'Speed / Duplex'.
- IP Configuration:** Shows DNS Server 1 (172.31.18.204), DNS Server 2 (172.31.18.206), Gateway (172.31.17.1), and Domain Name (hq.rp.internal).
- Network Access:** Includes 'Use Proxy' (unchecked) and 'NAT Address'.
- Additional Static Routes:** A table for adding routes with columns for 'IP Address/Mask', 'via', and 'IP Address', and an 'Add' button.
- Bandwidth Management:** Includes a checkbox for 'Throttle SCP/SFTP'.

Platform

Restart software	Restarts the Restorepoint domain. May leave the system in an unstable state, use when directed by Restorepoint support.
Abort all tasks	Aborts all currently-running tasks. May leave network devices in an unstable state.
Reboot	Enables you to reboot your Restorepoint appliance. However, try to Restart software first.
Shutdown	Enables you to shutdown and power off your Restorepoint appliance. This is the safest way to shut down your Restorepoint appliance. Wherever possible, avoid using the front panel buttons to reset or shutdown Restorepoint.
Remote Support	Click Start to enable Technical Support to securely connect to your Restorepoint appliance for troubleshooting. To stop the remote support tunnel, click the Stop button on this page, or click the running task in the Activity Display , and click Stop Remote Support to terminate the secure connection. Note: This feature requires that your firewall allows SSH connections (TCP port 22) from Restorepoint to support.restorepoint.com . For notes on firewall configuration, see Firewall Requirements for notes on firewall configuration.
Open Console	Generates an appliance debug file that may help Technical Support diagnose your issue. Click Start to start the debug, retrace your steps, and then click Stop Debug . A link to download the debug log will appear next to this button.
Debug	Generates an appliance debug file that may help Technical Support diagnose your issue. Click Start to start the debug, retrace your steps, and then click Stop Debug . A link to download the debug log will appear next to this button.

After Power On	Defines what Restorepoint should do when returning from a power-off state. If Restorepoint should <i>Run Due Backups</i> , and treat any missed backups as <i>Overdue</i> , or <i>Recalculate Schedules</i> and just return to the normal backup schedule.
-----------------------	--

Branding

Restorepoint can display your logo in the top left-hand side corner, instead of the default one. Click **Change** and then **Browse** to locate a suitable image file on your PC. For best results, the logo should be exactly 30 pixels tall and up to 150 pixels wide, and no more than 40KB in size. Click **Revert** to return the logo to the default Restorepoint logo.

You can customize the user interface for Domain users in the Domains page. For more information, see [Managing domains](#).

Software Updates

See [System Updates](#).

Date and Time

Use the selectors to set the date, time, and world time zone on the appliance. You can also enable the [Network Time Protocol \(NTP\)](#) (https://en.wikipedia.org/wiki/Network_Time_Protocol) and enter up to two NTP servers, such as *pool.ntp.org*.

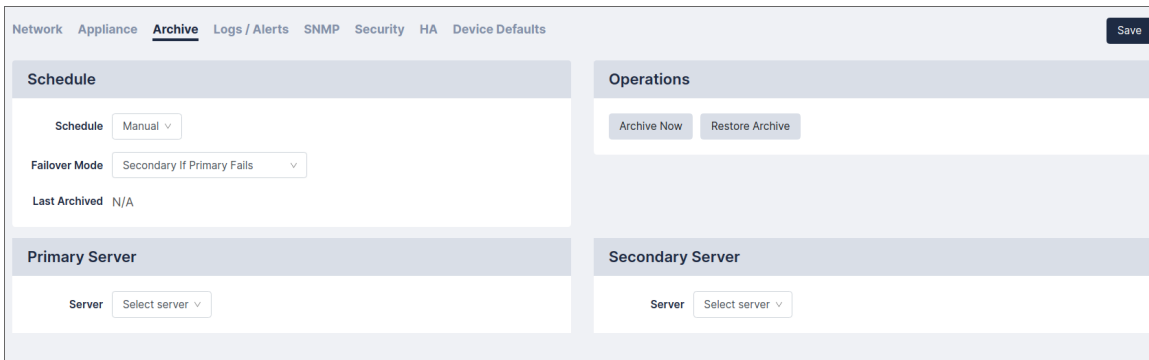
Date / Time

Date Time

Time Zone

Use NTP

System Archive



You can prepare for disaster recovery scenarios by archiving the Restorepoint configuration from the **Administration > System Settings > Archive** tab. Archiving the Restorepoint configuration allows you to back up the Restorepoint appliance automatically to up to two remote servers, including all device configurations stored on Restorepoint.

Taking an Archive

You can define the following settings for archiving:

For Primary and Secondary Archive servers, you can use a pre-defined server, or select *[New Server]* to enter the details for a server that you have not defined. For details on how to define a file server, See [File Storage](#).

For each Archive Server, you can define the following:

Retain	Enter the maximum number of archives to keep on the remote server. You reach this number, older archives will be removed.
Type	Define what each archive should contain. A <i>Full Archive</i> is a complete disaster-recovery backup. You can also choose to only save the most recent 1 to 5 configurations for each device, or only the Restorepoint database (only Restorepoint settings, no configuration backups).

- Click **Save**.
- Click **Archive Now** to start a manual archive operation.

Restoring from an Archive

Restoring from an archive allows you to quickly recover from a failure. For example, when installing a replacement appliance after a hardware problem. To restore the appliance from an archive:

1. Click the **Restore Archive** button on the **System Archive** page to display the list of available archives.
2. Select the archive to be restored.
3. Click **Restore**.

NOTE: You will need the password and encryption password for the *admin* account in order to complete the operation.

Restore Archive

Archive

RP00000099 2021-01-24 01:00 smb test

Password

..... Show

Encryption Password

Encryption Password Show

Cancel Restore

Workstation DB Archives

You can also a database-only export/import to a workstation instead of a fileserver. While not suitable for most disaster recovery scenarios, it allows for a quick migration of your Restorepoint settings from one appliance to another. You can use the **Export/Import DB Archive** buttons to save the Restorepoint database through your browser and reimport a previously saved database.

Log Settings and Alerts

You can use the log settings and alerts section to define your default log retention policy and the email address for system error notifications. Navigate to the Logs/Alerts page (Administration > System Settings > Logs/Alerts) and supply values in the following fields:

Delete logs after	Enter a maximum age for events. Events older than this value are permanently deleted from the system. The default value is one month.
Send Syslogs	Select this checkbox to forward all log messages to an external syslog server. Log entries will still be available by clicking on Info > Logs or Info > Syslogs . If you use a syslog server, you will need to enter its IP address and choose the syslog facility. Note that the facility setting only applies to forwarded Restorepoint logs, not forwarded operating system events.
Use SNMP Traps	Select this checkbox to forward log messages as SNMP traps to a Network Management Server (NMS). You will need to enter the NMS IP Address, the SNMP Version, and the community string.
Email errors to	Enter an email address for notifications.
Email errors from	Enter a sender email address to be used for notifications.
SMTP Server/Port	Enter the IP address of your mail server. Your mail server must be configured to allow Restorepoint to relay to internal and external recipients.
SMTP Username/Password	If your SMTP server requires authentication, enter the necessary credentials in this field.
Plain-text Emails	Select this checkbox if you prefer plain text emails instead of HTML.
Prevent Email alerts	Select this checkbox if you wish to suppress all email notifications.

Click **Save**.

SNMP

If your network has a Network Management System, you can use SNMP to perform some basic monitoring of your Restorepoint appliance. Restorepoint supports SNMP v1, v2c, and v3. Navigate to the SNMP page (Administration > System Settings > SNMP) to configure SNMP and supply values in the following fields:

- Select which SNMP versions should be enabled by selecting the relevant checkbox.
- If you enable SNMP v1 or v2c, you must enter a **Community String** in the appropriate field.
- If you enable SNMP v3, you must define a username. Depending on the SNMP v3 security level, you may need to enter additional integrity/encryption passwords and integrity/encryption algorithms.

Click **Save**.

The screenshot shows the 'System Settings' interface with the 'SNMP' tab selected. The page is divided into three main sections:

- SNMP Version:** Contains checkboxes for 'SNMP v1' (checked), 'SNMP v2c' (checked), and 'SNMP v3' (unchecked). Below these are two buttons: 'Restorepoint MIB' and 'Appliance MIB'.
- SNMP Version Details:** Features a 'Community String' input field with the value 'rpakSqcL' and a small icon to its right.
- SNMP System Details:** Contains three input fields: 'system.sysContact.0' with the value 'Restorepoint <support@restorepoint.com>', 'system.sysName.0' with the value 'Restorepoint Appliance', and 'system.sysLocation.0' with the value 'Restorepoint'.

The top navigation bar includes 'Network', 'Appliance', 'Archive', 'Logs / Alerts', 'SNMP', 'Security', 'HA', and 'Device Defaults'. A 'Save' button is located in the top right corner.

Security

The **Security** tab (Administration > System Settings > Security) allows you to configure various global settings to mandate a higher level of network security for the Restorepoint appliance. Applying some of these settings may cause compatibility problems with legacy devices and clients.

Protocol Versions

The Protocol tab allows you to specify the minimum version of TLS that the Restorepoint UI can use and can communicate with devices. You can also prevent Restorepoint from falling back to SSHv1, if TLS is unavailable.

Services

You may wish to disable some functionality of Restorepoint for reasons such as PCI Compliance.

HTTPS Certificate

Click **Change** to modify the HTTPS certificate used by Restorepoint. The following dialog appears:

TLS Cipher Options

Update Certificate

Type

Common Name

Country Code

State / Province

Locality / City

Organisation

Org. Unit

Email

SubjectAltNames

Email

The **Type** drop-down will show you the different options available:

Self-Signed	Generates a self-signed HTTPS certificate with the current keypair.
New Key	Allows you to generate a new private/public keypair of the given length.
Create CSR	Allows you to generate a Certificate Signing Request, which your Certificate Authority (CA) will need to produce a signed certificate.
Upload Certificate	Once you have a signed certificate from the CA, you can upload it here.
Upload All	Alternatively, if you have a key/certificate pair already from your CA, you can upload both of them here.

Timeouts

UI Timeout	How long a user may stay logged-in to the Restorepoint UI without making a change or initiating an action. Default value is <i>60 minutes</i> .
Console Timeout	How long to keep a session for the VM Console open without an action. The default value is <i>15 minutes</i> .
Expire User	Allows you to automatically force users to change their password after a given length of time. This

Passwords	setting can be overridden on a per-user basis. For more information, see Managing Users .
------------------	---

Admin Allowed Networks

This tab allows you to set a range of IPs (in CIDR format) that administrator accounts can connect from. For a per-user setting, see the section on [Managing Users](#).

High Availability

High Availability (HA) provides a way to minimize the effects of hardware failure, by configuring two Restorepoint appliances in a cluster.

Under normal operating conditions, the primary cluster member is active and the secondary is in standby mode; the active appliance performs all network operations, and replicates all settings and device configurations to the standby appliance. Restorepoint replicates data both incrementally (for example, just after a backup is retrieved from a device) and by performing full synchronizations on a regular basis.

If the primary member becomes unavailable because of a hardware failure, other network problem, or from losing power, the secondary member will automatically become Active, and carry on as normal. If the primary recovers, it will automatically take over from the secondary and become active.

HA does not require the appliance to be installed on the same network, as long as the traffic requirements are met (see below).

Software updates and upgrades are managed at the cluster level; updating the active appliance will automatically update the standby appliance.

HA Requirements

- HA is a separately licensed feature.
- Only appliances of the same model can be clustered and appliances must be running the same software version.
- Cluster members must be able to communicate over HTTPS to exchange heartbeat information and data synchronization. TCP/443 traffic should be permitted bidirectionally between the appliances.

Creating a Cluster

To create a cluster, on the Primary Restorepoint appliance:

1. Click **Create Cluster**.
2. Type a password to be used between appliances in the cluster.
3. Click **Save**.

On the secondary Restorepoint appliance:

1. Click **Join Cluster**.
2. Enter the same password you entered on the Primary appliance.

3. Enter the IP Address of the Primary appliance.
4. Click **Save**. The cluster will perform the initial full sync.

After the cluster is created, this screen can be used to monitor the status of the cluster or to leave the cluster.

- **Role** displays which position the appliance takes in the cluster (*Primary* or *Secondary*).
- The **Member Status** displays if the current appliance is *Active* or *Standby*.
- The **Cluster Status** displays the status of the Secondary appliance on the Primary or the amount of time between heartbeat synchronizations on the Secondary.

You can use the **Leave Cluster** button to break the cluster. When you click Leave Cluster, all synchronization will stop, the two appliances will keep the existing configuration, and the appliances will carry on independently.

Chapter

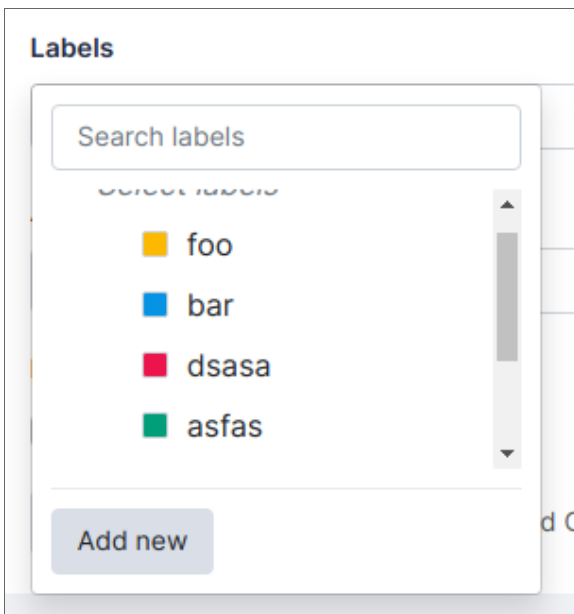
14

Labels

Overview

You can use Labels to filter and group devices.

Labels can be created by users and confined to a specific domain. When you create a new device or edit an existing device, you can set Labels for that device. The Device Details field contains a drop-down list of the available Labels. You can define new Labels by selecting “Add new”.



These options are described in [Adding a new user](#).

See the following link for the API used to create labels:

https://restorepoint.dev/api.html#operation/create_label

To understand Labels better, it is best to use a real world example:

In a office, a user consistently works with a set of devices because these devices are in that office. A label can be assigned to these devices, for example, the name of the office. This label can then be used to filter the devices in the Device Table so that the user can only see the relevant devices.

Chapter

15

SAML

Overview

A “Single Sign On” (SSO) option is available via SAML authentication.

You can configure SSO in SAML tab:

Administration > Auth Servers > SAML

In the SAML tab there are 2 fieldsets:

1. Service Provider Settings
2. Identity Provider Settings



To set up SAML:

1. Note the “ACS URL” and “Entity ID” values that appear in the Service Provider Settings.
2. Enter these values into the relevant part of your SAML IdP. This will generate some IdP Metadata.

3. This IdP Metadata (usually some XML) needs to be entered into the IdP Metadata field in the Identity Provider Settings.
4. Click Save. The metadata is then uploaded to Restorepoint.

Now that SAML is setup, a new button will appear on the login page called "Login with SSO". You can click this button without entering values in the other fields and it will either:

- redirect the user to their SAML IdP to login
- log them in to Restorepoint if the user already has a valid SAML SSO session

Chapter

16

System Updates

Overview

System updates are managed centrally by Restorepoint from the **Administration > System Settings > Appliance** tab. By default, the appliance checks and automatically installs any available software upgrades and updates, including:

- System software updates
- Device plug in updates
- License updates

Ensure that your firewall is configured correctly to allow system updates. For information on firewall configuration, see [Firewall Requirements](#).

Disabling Automatic Updates

Although Restorepoint strongly recommends that all updates are automatically applied, you can override this behavior by selecting **Disable Automatic Version Upgrades**.

Minor software updates that do not change the user interface or modify any Restorepoint functions are still downloaded and automatically applied, unless you select **Disable Automatic Minor updates**.

The **Force Check** button checks for any available updates and installs them automatically by default. If any updates are available, the **Upgrade Now** button appears which allows you to manually force an update.

Manual Updates

If Restorepoint is deployed on an isolated network and cannot connect to the update server, it can be manually updated. If you manually update the system, you should select **This appliance is not connected to the Internet**. If you click **Manual Upgrade**, instructions are displayed on how to download an update package using a computer with an internet connection and upload it to the appliance. Note that when this option is enabled, all update and upgrade operations (including enabling software features or applying new license details) must be manually performed by the administrator.

Chapter

17

Getting Help

Overview

Click **Help** to display Restorepoint documentation for your current page.

You can also click **Help > Help Index** to access the HTML userguide, download a PDF copy, or access the Plugin Guide (**Help > Plugin Guide**).

This section covers the following topics:

<i>Error Messages</i>	124
<i>Using the System Shell</i>	126
<i>Factory Reset</i>	127
<i>Frequently Asked Questions</i>	128
<i>Contacting Technical Support</i>	129
<i>Support Portal</i>	129

Error Messages

Errors During Backup Operations

Connection timeout

Possible causes:

1. Restorepoint can't connect to the device using the specified protocol.

Solution: Check that the protocol is correct and that there is connectivity to the device (e.g., no firewall is blocking the required ports). If the device uses back-connections, also check that this is not blocked, and/or NAT is correctly configured on Restorepoint. Check **Help > Plugin Guide** to verify the connectivity requirements for this particular device.

2. The device is not sending the expected output to Restorepoint within the allocated time.

Solution: Check that you have selected the correct plugin and that the device firmware/operating system is supported by Restorepoint.

Connection failed: Device SSH key has changed

Restorepoint has detected that device's SSH key has changed

Solution: This error typically occurs because the device has been replaced. If the device has been replaced, edit the device and click **Clear Cache**.

Timeout waiting for username prompt

Restorepoint can connect to the device but did not receive a username prompt.

Solution: Check that you are using the correct plug-in. If the device is not configured to prompt a username, leave the Username field empty in the device definition.

Timeout waiting for password prompt

Restorepoint can connect to the device but did not receive a password prompt.

Solution: Check that you are using the correct plug-in and that the device username and password are correct.

Timeout waiting for device prompt

Restorepoint can connect to the device but did not receive the device CLI prompt.

Solution: Check that you are using the correct plug-in and that the device username and password are correct.

Error creating backup

Restorepoint can connect to the device but is not able to create a backup on the device. This can be caused by a number of circumstances, usually a lack of available disk space.

Solution: Connect to the device manually from your PC or from the Restorepoint system shell and attempt to create a backup to determine the cause of the error.

Error transferring backup

Restorepoint can connect to the device and create a backup on the device but is not able to transfer it back. This is usually due to a firewall blocking a required port (e.g., TFTP) between Restorepoint and the device. If your device has a large backup file (several Mbytes) and you are backing up over a WAN, this error message can be caused by a timeout during file transfer.

Solution: Check the Plugin Guide (**Help > Plugin Guide**) and ensure that the TCP or UDP ports required by your device are not blocked by any firewalls.

Incorrect checksum after transfer

Wherever possible, Restorepoint calculates an MD5 checksum of the backup file before and after transfer to ensure the integrity of the file. If the checksum changes, this indicates that the file got corrupted in transit.

Solution: Retry the backup. An isolated error of this type may indicate a problem on the network (e.g., faulty switches or cables). A reoccurring error may be caused by a large backup file and/or a slow network, where only part of the file is transferred. Try and reduce the size of the backup if possible; use SCP or FTP instead of TFTP wherever possible.

Wrong parameter found at . ^ . position

Solution: Check that you have specified the correct unit when backing up a 3Com 5500 switch.

Error backing up the device/Could not hold conversation with device

Although a failure will normally generate a specific error message, you may occasionally encounter a generic error.

Solution: Check that the device credentials are correct, that you are using the correct device plug-in, and that the required TCP/UDP traffic is allowed between Restorepoint and the device. If you are still unsuccessful, contact Technical Support.

Other Messages

Cryptfs not mounted

The encrypted storage was not mounted correctly after a reboot. This may happen if the appliance is powered off without a clean shutdown.

Solution: Login with your username, password, and encryption password. Restorepoint will attempt to check and mount the encrypted storage. If you keep receiving this message every few minutes, contact Technical Support.

Couldn't connect to update server

Restorepoint needs to communicate to the update server (`support.restorepoint.com`) to check whether new software or device plug-ins are available.

Solution: Check the following:

1. Check that the DNS servers configured in the **System** page are correct and are working properly
2. Check that a firewall is not blocking HTTPS traffic from Restorepoint to `support.restorepoint.com`.
3. If Restorepoint uses a proxy to access the internet, check that the correct proxy username and password are being used and that the password for the proxy user account has not expired.
4. If Restorepoint is located on a network without internet access, disable automatic updates by selecting **This appliance is not connected to the Internet** in the **System** page.

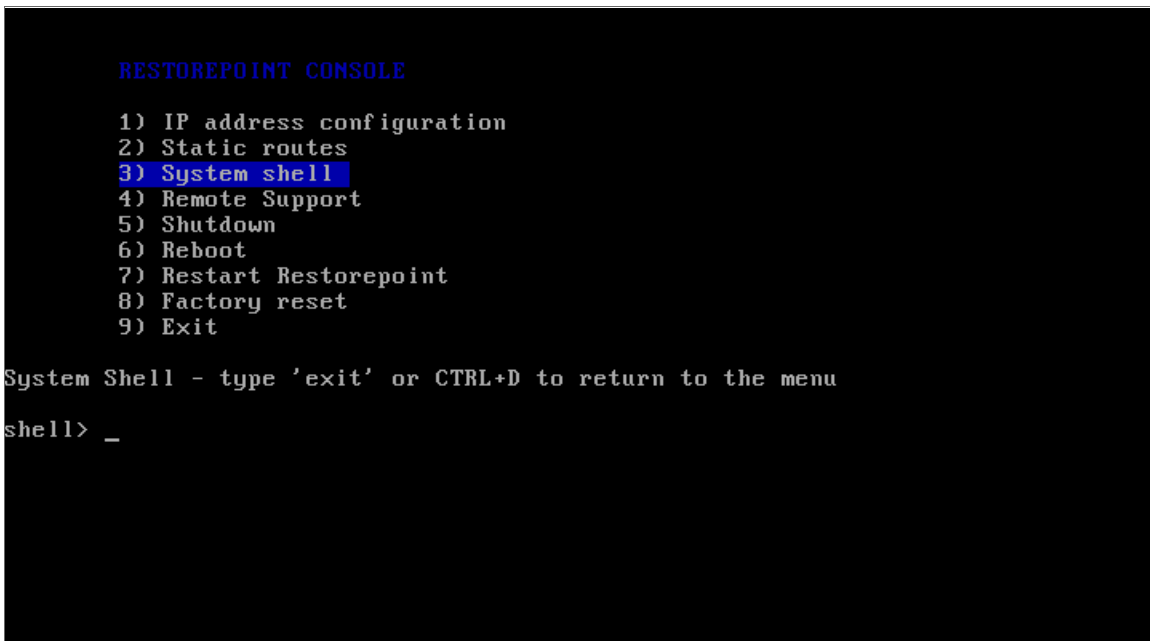
License expired

Your license has expired and your appliance is no longer obtaining software updates.

Solution: Contact your Restorepoint Account Manager.

Using the System Shell

The system shell provides some useful command line network tools that can be used to troubleshoot connectivity problems. To start the system shell, log in to the Restorepoint console using an *admin* account and select **System Shell**.



```
RESTOREPOINT CONSOLE
1) IP address configuration
2) Static routes
3) System shell
4) Remote Support
5) Shutdown
6) Reboot
7) Restart Restorepoint
8) Factory reset
9) Exit

System Shell - type 'exit' or CTRL+D to return to the menu
shell> _
```

The available commands are:

help	Lists the available commands.
ping	Sends an ICMP Echo Request packet to a network host.
tracert	Displays the route packets take to a network host.
nslookup	Query a DNS name server.
telnet	Connect to a host using the TELNET protocol.
ssh	Connect to a host using the SSH protocol.
tcpdump	Displays the network traffic.
exit	Returns you to the main menu.

Ensure that you are familiar with these tools before using the system shell.

Factory Reset

If you need to reset your Restorepoint appliance to factory settings, you can follow the factory reset procedure. Note that the factory reset will permanently erase **ALL** of the information stored on the appliance, not just the system settings. In particular:

- The encryption key will be deleted.
- All the device data (configuration and backups) will be erased.
- All the administrators (except *admin*) will be deleted.
- All plugins will be deleted.
- System settings will be reset to their default values.
- The password for the *admin* user will be reset to `admin`.

Note : To reset the appliance, you must have the admin password. If you need to reset Restorepoint and you do not know the admin password, contact Technical Support.

To start the factory reset procedure:

1. Log in as *admin* on the Restorepoint console.
2. Choose the **Factory reset** option.
3. Confirm that you understand and accept that your data will be lost and enter *Yes*, otherwise enter *No* to abort:

```
RESTOREPOINT CONSOLE

1) IP address configuration
2) Static routes
3) System shell
4) Remote Support
5) Shutdown
6) Reboot
7) Restart Restorepoint
8) Factory reset
9) Exit

Factory Reset

Are you sure you want to reset the system to factory settings?

*** ALL DATA WILL BE LOST ***

and the appliance IP address will be reset to 192.168.1.1.

Please enter Yes or No: Yes_
```

The system will then erase the database and reset the system settings to their default values. This can take some time, depending on how much data is stored on the appliance. Do not shut down or power off the system before the reset has completed or you may damage the appliance. Restorepoint will automatically shut down at the end of the procedure.

Frequently Asked Questions

I have forgotten my encryption password

See [Connecting to Restorepoint after a reboot](#) and [Password Reset](#) for more information.

I cannot connect to the web interface

Check that you have network connectivity. The power and network LEDs on the front panel of your Restorepoint appliance should be lit. If you are in an environment using a proxy server, check that you are connecting to the device on port 443, or that your browser is set to bypass connection to the device.

I cannot add a device

Check that the model and firmware version of the device you are adding is on the list of supported devices. The list of supported devices can be found in the Plugin Guide ([Help > Plugin Guide](#)).

I do not get notifications

Verify that you have connectivity to the SMTP server specified in the **Logs/Alerts** tab of the **System Settings** page and that Restorepoint is able to relay email to your SMTP server. You need to specify a valid email account that notifications are sent to.

Scheduled tasks are not running

Check that the task is not paused in the **Info > Schedule** page.

I have a device that is not supported but would like to see support for it

Contact Technical Support and let us know the vendor, product, model, and version of the device. Wherever possible, Restorepoint will endeavor to add support for your device.

I still need assistance and require remote support

If you are having problems and need a support engineer from Restorepoint to help troubleshoot the issue, click the **Remote Support** option on the Restorepoint appliance to create an SSH tunnel to our support server which allows a support engineer to assist you. Alternatively, our support team can set up a web session with you (WebEx, join.me, GoToMeeting, or similar).

Contacting Technical Support

You can contact Restorepoint Support at support@restorepoint.com, or by telephone at **+44 844 571 8120**. Telephone support is available 9:00 to 17:30 GMT or 5:00 to 13:30 EST Monday to Friday, excluding [UK public holidays](#). Technical support is also available through your reseller.

Support Portal

You can open a support ticket at any time using the Restorepoint Customer Support Portal at <http://support.restorepoint.com>. Access to the portal requires registration and a valid software license.

Chapter

18

Copyright and Contact Information

Overview

Copyright Notice

Copyright © 2008 - 2022 Restorepoint Ltd. This document and any information therein are confidential and copyright property of Restorepoint Ltd and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Restorepoint Ltd retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Trademarks

Restorepoint is a trademark of Restorepoint Ltd. All Rights Reserved. All other trademarks and registered trademarks appearing in this document are the property of their respective owners, and are used for identification purposes only.

Contact Details

Telephone: +44 844 571 8120

General Inquiries: info@restorepoint.com

Sales Inquiries: sales@restorepoint.com

Support Inquiries: support@restorepoint.com

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010