Restorepoint 5.4 User Guide

Release 2022

Restorepoint

Mar 07, 2022

CONTENTS

Revised: November 2021

CHAPTER

ONE

OVERVIEW

Restorepoint is a Disaster Recovery and Secure Configuration Management appliance for network devices such as routers, switches, proxies, and firewalls. Restorepoint can retrieve the configurations of your network devices automatically. It can also detect changes and compliance violations, and report these automatically to network administrators, all without any user intervention.

The process of adding new devices to Restorepoint is simple. The backup frequency can be set for each device individually or as a group. Once you have stored your device configurations on Restorepoint, restoring network devices when needed is straightforward, and could save you many hours of critical system downtime.

All backups, device configurations, and passwords are encrypted, and cannot be read by an unauthorised 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 web site for the latest updates to this list, which continues to grow.

CHAPTER

TWO

INSTALLING RESTOREPOINT

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.

2.1 Before you begin

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

- You have 1U of rack space available to install the appliance, with a standard 240V power socket (hardware appliance only)
- You have allocated a port on your Ethernet switch for the appliance (hardware appliance only)
- The appliance has a static IP address allocated to it.
- 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 that your ESX host has 4GB RAM available and 256GB available in the datastore where the virtual machine will be deployed.
- You have configured 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. See device-specific details in the Plugin Guide (**Help > Plugin Guide**).
- You have configured your mail server to allow Restorepoint to relay email.

2.2 Firewall Requirements

This section highlights the ports used to by clients connecting to Restorepoint, and by Restorepoint to network devices and other servers; your firewall policy may need to be modified for Restorepoint to function correctly.

2.2.1 Traffic from clients to Restorepoint

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

Table 1: Firewall requirements, inbound

2.2.2 Traffic from Restorepoint to network devices

Restorepoint connects to network devices in a variety of ways, according to the respective vendor documentation. Sometimes, devices use back-connections to transfer their configuration to Restorepoint. See the device-specific details in the Plugin Guide (**Help > Plugin Guide**).

2.2.3 Other traffic originating from Restorepoint

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

Table 2: Firewall requirements, outbound

2.3 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)

2.4 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. Choose a name for the virtual machine (or leave the default) 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 the **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.

2.5 IP address setup

To setup 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 enter the default user name (*admin*) and password (*admin*) for the device. Choose option 1 at the console menu:

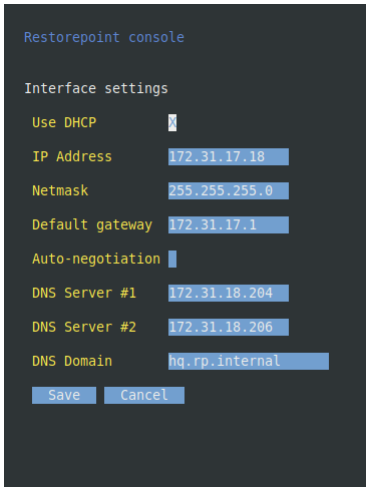


Fig. 2.1: Console Menu

3. Enter 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 may **exit** now.

You may now 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.

2.5.1 Alternative method for setting the IP address

It is possible to 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`.

2.6 Connecting to Restorepoint for the first time

After you have 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: because Restorepoint initially uses a self-signed certificate, your web browser will warn you of an invalid (untrusted) certificate. This is entirely normal, 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.

1. Login with the default username (*admin*) and default password (*admin*).
2. Restorepoint displays the End-User License Agreement as shown below. Read the terms of the Agreement, then click **I 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, tick 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 to which 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. Finally, click **Install**; at this point, Restorepoint will contact the update servers to verify the licence and download the device plugins; ensure that your firewall allows the required traffic (see *Firewall Requirements*).

2.7 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.

In order to enter the encryption password, use a browser to connect to the appliance and provide your administrator credentials as well as the encryption password, as indicated:

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

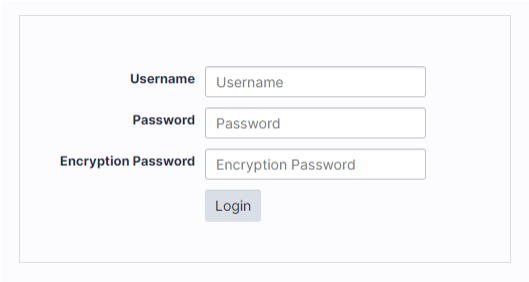


Fig. 2.2: Login screen after a reboot

CHAPTER

THREE

BASIC OPERATION

3.1 User Interface

All the pages in the Restorepoint web interface share some common features, which are shown below. (Fig. 3.1)

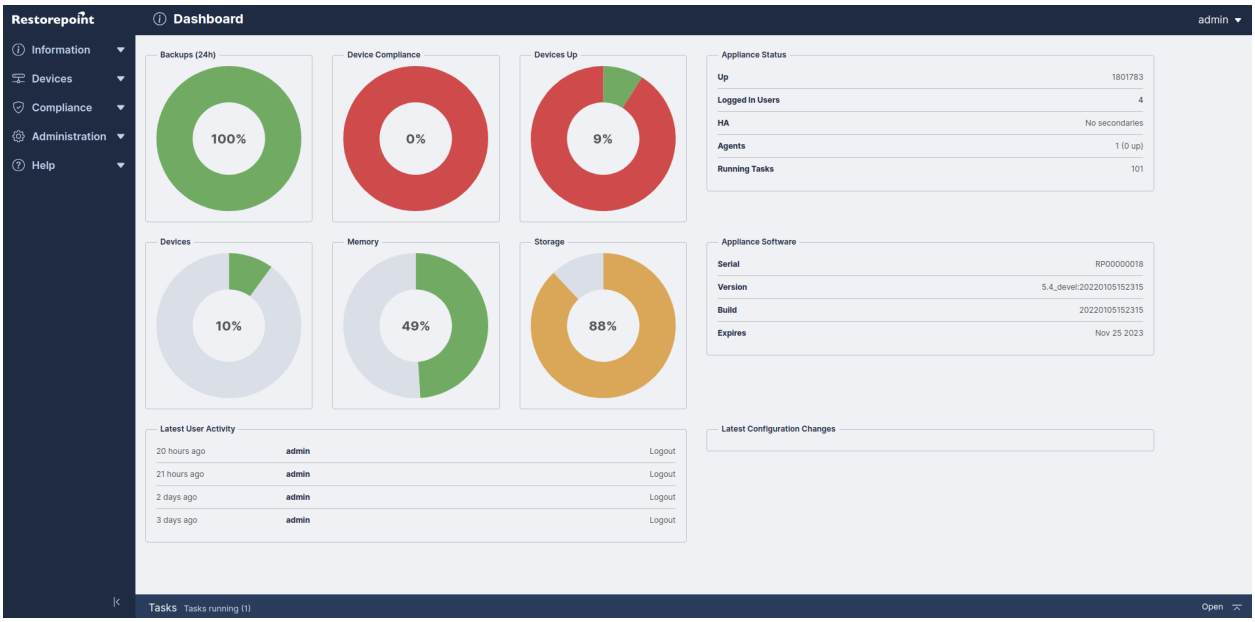


Fig. 3.1: Dashboard

These features include:

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

Tables, such as the **Device Management** page shown below. (Fig. 3.2), display a grey header. Column widths can be changed 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, as well as perform a full text search by typing in the **Search** field.

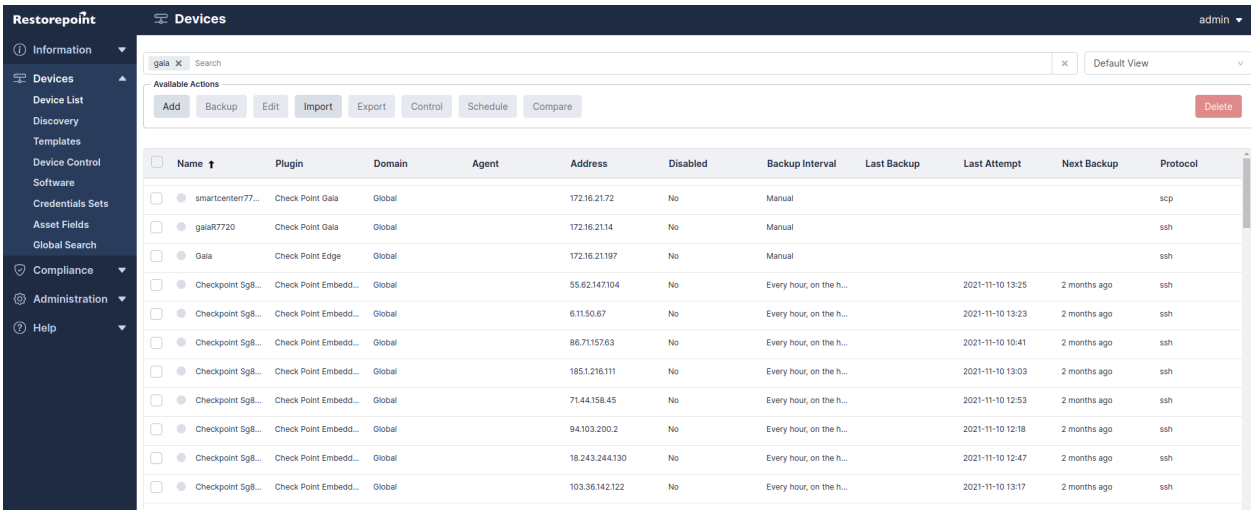


Fig. 3.2: Device list

3.1.1 My Account

Hovering over the username in the top-right corner offers two options. **Logout**, with a count of how many minutes until the user is automatically logged out, and **My Account**, which allows changing some user settings:

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

Note: When changing a password, you will need to specify the **Old Password** as well.

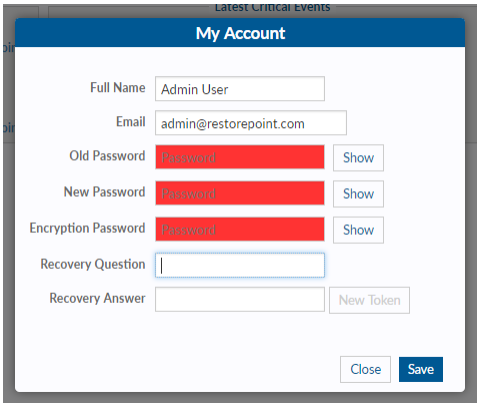


Fig. 3.3: My Account

These options are described in *Adding a new user*.

3.1.2 Activity Display

The Activity Display, shown below. (Fig. 3.4) shows a list of currently running tasks, and is shown on every page while tasks are in progress:

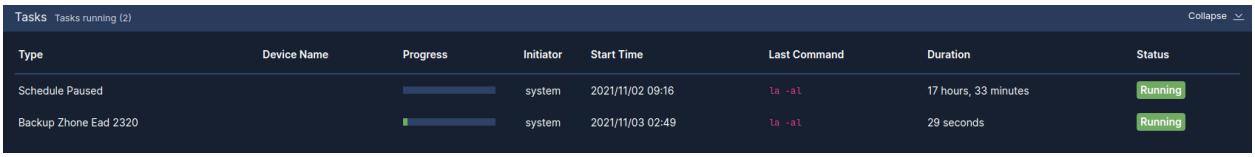


Fig. 3.4: Activity display

Clicking on the magnifying glass icon shows the Progress Log (Fig. 3.5), which displays detailed, real-time information about the running task:

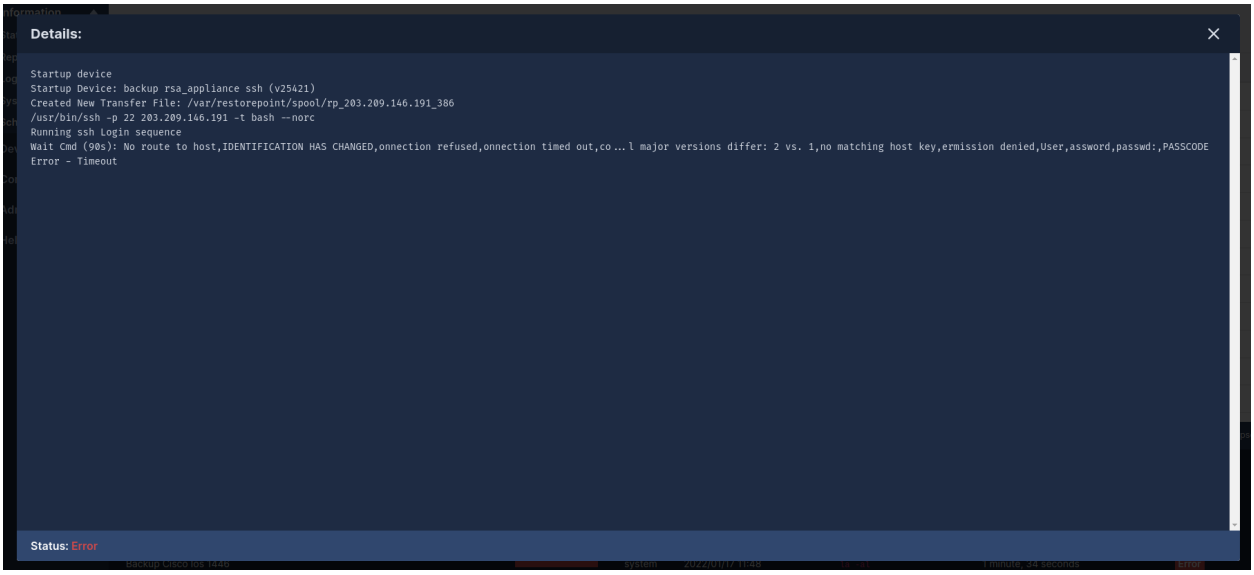


Fig. 3.5: Real-time progress log

3.1.3 Editing Views

Along with the built-in views, every data table in Restorepoint can have multiple customised views associated with it, accessed by clicking on the icon at the top left of the table, shown below. (Fig. 3.6) This allows you to re-order columns by clicking on the up/down arrows and show/hide columns using the checkboxes.

≡

Fig. 3.6: Data table view icon

Column orders, widths and display settings can be given a name and saved using the **Save** button. Saved Views can be deleted with the **Delete** button.

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

3.2 Encryption

All sensitive data, including device configurations, stored in Restorepoint is protected by encryption. Restorepoint encrypts data when it is written to disk, and decrypts it as it is read. Clear-text data is only ever held in volatile memory, and therefore 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 has been 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	After an administrator has provided 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.

As the entire Restorepoint database is encrypted, it is **vital** that administrators remember both their normal and encryption passwords, and keep their emailed password-recovery tokens safe. See *Connecting to Restorepoint after a reboot* and *Password Reset* for more information.

3.3 System Status Page

The System Status page, also known as the "**Dashboard**" (figure 3.7) gives an overview of the health of Restorepoint itself, and shows the number of devices being backed up. This is the default page shown whenever you first login to the system. You can display it at any time by clicking **Info** on the menu.

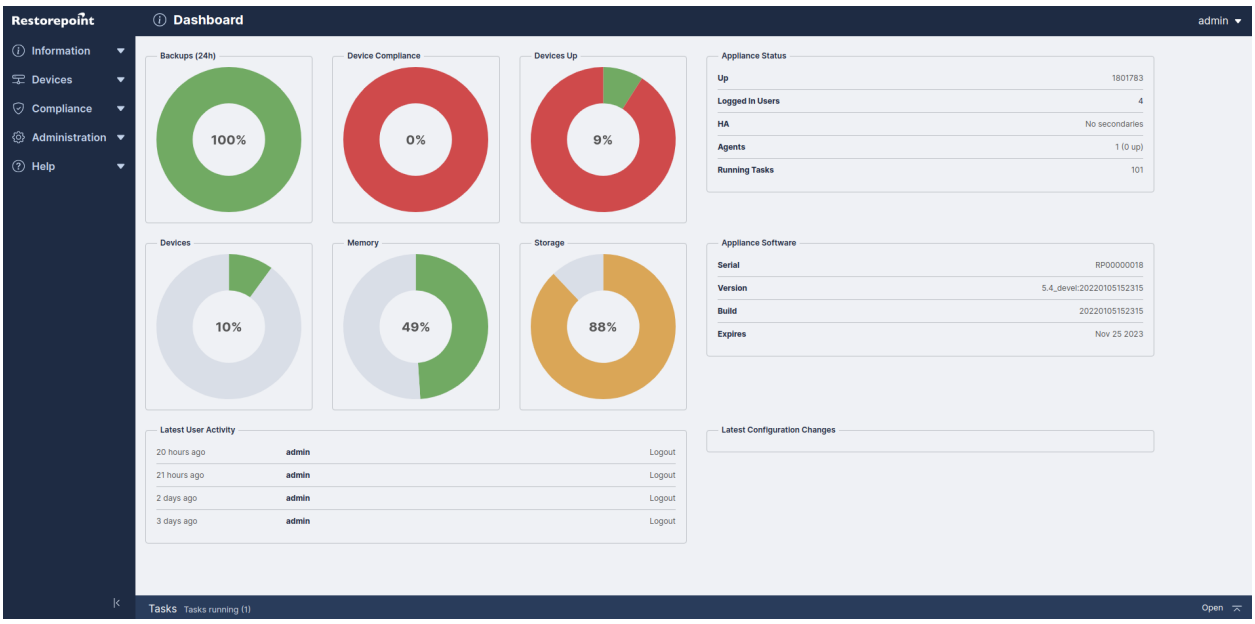


Fig. 3.7: Status page

The System Status page displays the following information:

Graphs:

Backups (24h)	scheduled, successful, and failed backups in the last 24 hours.
Device compliance	the number of compliant and non-compliant devices, as well as the number of devices with no policy assigned.
Device Baseline	the number of devices that are running a *baseline* configuration, the number that have a non-baseline configuration, and the number of devices with no baseline configuration set. See 4.6 *Configuration Baselines* for more information.
Devices Up	the number of devices that are currently monitored by and responding to Restorepoint. Clicking on the graph will give a moving average chart covering the past 24 hours.
Storage	the amount of disk space used and the total amount of disk space for the Restorepoint appliance.
Devices	the total number of devices configured on the appliance, and maximum allowed on your current licence.
Memory	the amount of RAM currently being used by the Restorepoint appliance, and the total amount of RAM available.
Network Activity	shows the current network activity, as seen by the Restorepoint appliance.
Load Average	the Load Average [https://en.wikipedia.org/wiki/Load_(computing)] of the Restorepoint appliance, over the last 30s.

Text panes:

Appliance Status	The uptime, number of logged in users, *High Availability* status (if enabled), *Agents* status (if enabled), and number of running tasks.
Appliance Software	The serial number, version, build number (including a link to the changelog for that version), and licence expiration date of the Restorepoint installation. This information is also available in the footer.
Latest user activity	Administrator logins/logouts, and other user-initiated operations.
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 allows displaying of real-time task details, as well as terminating a task.

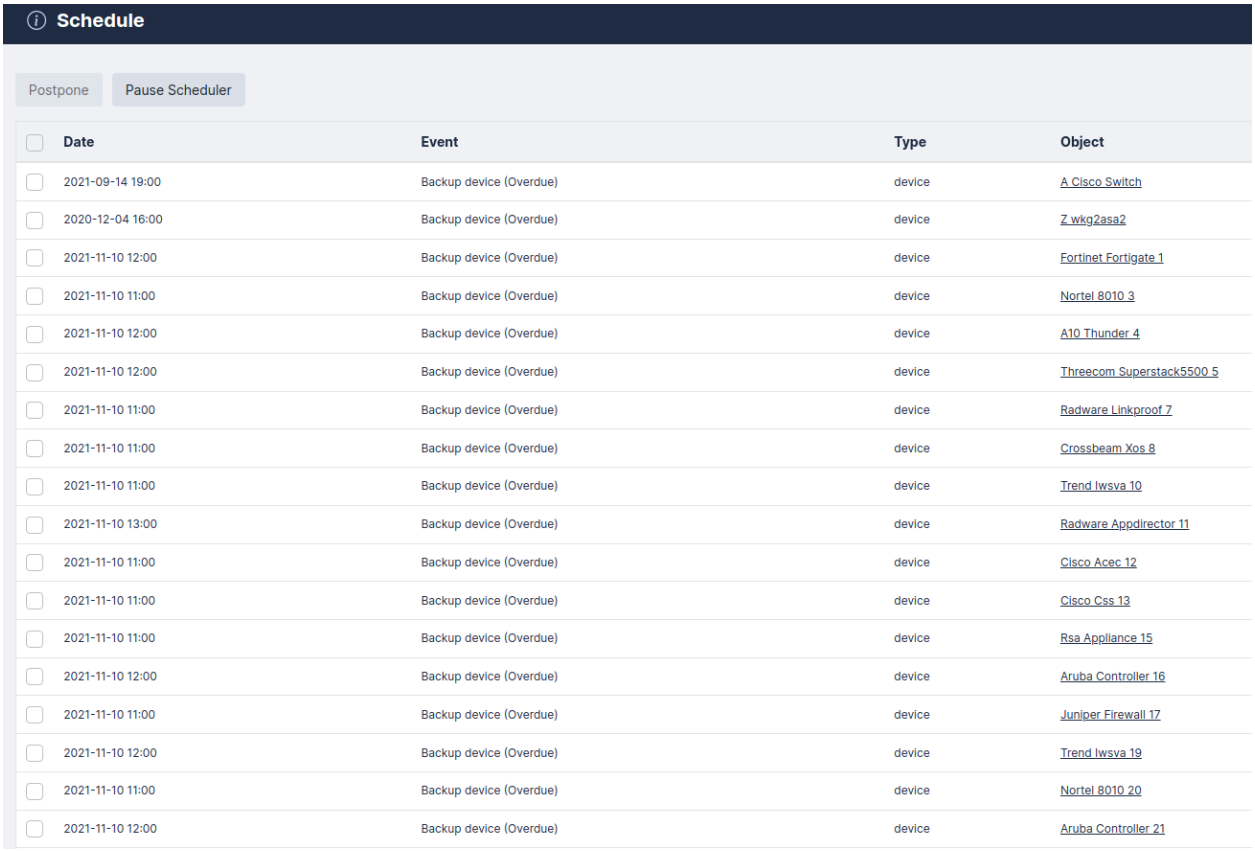
3.4 Scheduled tasks

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

- 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 from the schedule by ticking the relevant check box and clicking the **Postpone** button; this will effectively remove the next occurrence of a scheduled task.

The entire schedule can be halted by clicking the **Pause** button; no scheduled events will occur until the device is **Unpaused**.



Schedule

Postpone | Pause Scheduler

Date	Event	Type	Object
2021-09-14 19:00	Backup device (Overdue)	device	A Cisco Switch
2020-12-04 16:00	Backup device (Overdue)	device	Z wkg2asa2
2021-11-10 12:00	Backup device (Overdue)	device	Fortinet Fortigate 1
2021-11-10 11:00	Backup device (Overdue)	device	Nortel 8010 3
2021-11-10 12:00	Backup device (Overdue)	device	A10 Thunder 4
2021-11-10 12:00	Backup device (Overdue)	device	Threecom Superstack5500 5
2021-11-10 11:00	Backup device (Overdue)	device	Radware Linkproof 7
2021-11-10 11:00	Backup device (Overdue)	device	Crossbeam Xos 8
2021-11-10 11:00	Backup device (Overdue)	device	Trend Iwsva 10
2021-11-10 13:00	Backup device (Overdue)	device	Radware Appdirector 11
2021-11-10 11:00	Backup device (Overdue)	device	Cisco Acec 12
2021-11-10 11:00	Backup device (Overdue)	device	Cisco Css 13
2021-11-10 11:00	Backup device (Overdue)	device	Rsa Appliance 15
2021-11-10 12:00	Backup device (Overdue)	device	Aruba Controller 16
2021-11-10 11:00	Backup device (Overdue)	device	Juniper Firewall 17
2021-11-10 12:00	Backup device (Overdue)	device	Trend Iwsva 19
2021-11-10 11:00	Backup device (Overdue)	device	Nortel 8010 20
2021-11-10 12:00	Backup device (Overdue)	device	Aruba Controller 21

Fig. 3.8: Scheduled tasks

3.5 Adding devices to Restorepoint

Devices can be added to Restorepoint in three ways:

- Manually (Section *Adding a new device manually*)
- Importing a list from a CSV file (Section *Importing multiple devices using a CSV file*)
- Using automatic discovery (Section *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

3.5.1 Adding a new device manually

The way in which you configure a new device may vary slightly from one device to another. Please see the device specific information in the Plugin Guide (**Help > Plugin Guide**).

To create a new device, follow these steps:

1. Select **Devices** or **Device List** from the menu to display the **Device Management** page.

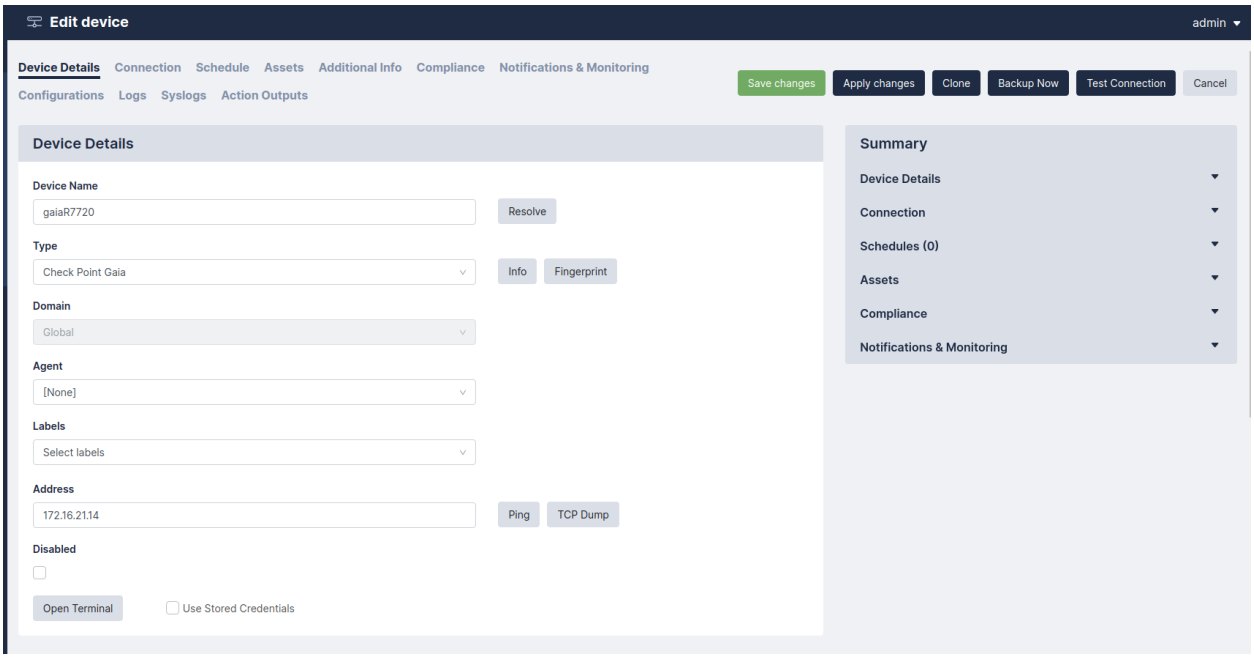


Fig. 3.9: Adding a new device

2. Click the **Add Device** button on the top left hand side of the page, to display the **Edit Device** page.

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, therefore manual changes to the IP address will be ignored.
Type	Select the device type from the quick entry list. You can also start typing in the field to filter the list. This list only shows the device types that are currently available on your license.
Domain	Choose the domain to which this device is assigned. This field is only present if Domain Administration is enabled on your appliance (see *Administration Domains*).
Agent	if the device is managed via an agent, choose the appropriate agent from the dropdown list.
Address	Enter the IP address for the device.
Open Terminal	This button opens a web-based virtual terminal to the device, to be used for troubleshooting. Ticking **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 Email	Enter the email address of the device administrator. By default, this field is filled with the notification email address defined in the system configuration page.
Email on Config Change	Select this option to automatically generate 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 option to send an email before a backup starts for this device. **Note:** this introduces a 1-minute delay before the backup starts.
Email On End Backup	Select this option to send an email when a backup completes. If this option is not selected, Restorepoint will only send a completion email if the backup fails, or if a configuration change is detected and **Email Config Change** is selected.
Syslog Change Detection	(if available): select this option for Restorepoint to automatically detect when a device is modified, and automatically retrieve its configuration. Please note that this feature is only available for specific devices. Please check the Plugin Guide (**Help > Plugin Guide**) for more information.
Log Transcript	Select this option to keep 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	Tick 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 option to monitor the device. See *Device monitoring* for details.

3. Select the **Connection** tab, then complete the following fields:

Protocol	Select the appropriate connection protocol for your device, such as telnet or SSH. The options available 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 colour will range from red to green to indicate the password strength, according to the policy set in the *Password Policies* page.
Use credentials	Instead of entering username and password, you can tick this box and select a **Credential Set**. Credential sets are re-usable username/password combinations that can be shared among different devices (See *Credential sets*).
Back-Connection NAT	Select this option 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	Tick this box if you wish to use SSH Public Key Authentication, instead of password-based authentication, when connecting to the device. Click **Show Keys** 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 this button.
Backup Port	If required for this device, enter the backup port to be used.

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

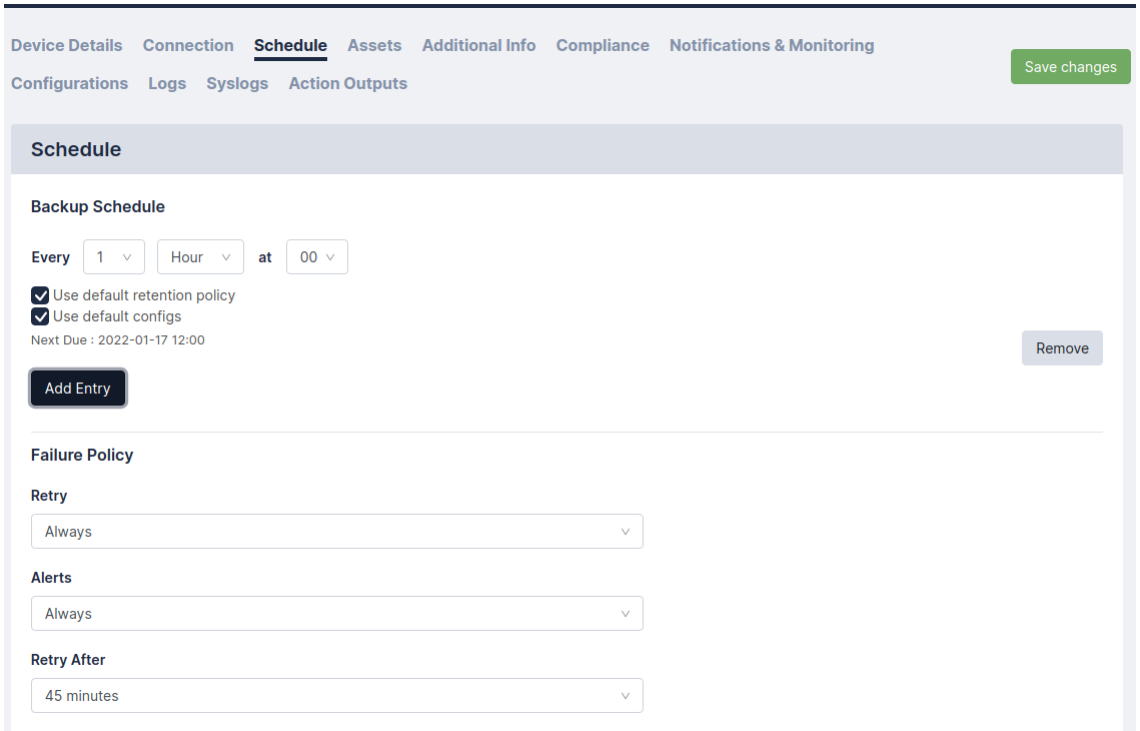


Fig. 3.10: Add schedule

For each schedule interval, you can override the config types to backup by ticking *any* of the **Config Type** tickboxes, or override the default retention policies by unticking **Use Default Policy**. You can also override the Failure Policy from this screen (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 (see *Asset Fields* for more details).

6. The **Additional Info** tab, if available, displays additional information retrieved from the device, such as licence details, routing table, and network interfaces. You can also have the output of a saved Action displayed here, using the **New Info Command** dropdown. See *Controlling a device*) for more information on creating Actions.
7. Click the **Compliance** tab to assign compliance policies to this device. Please see *Device Policies* for more information.
8. Click the **Save** button to finish creating the new device. Restorepoint displays the **Device Management** page showing the new device. (Fig. 3.11)

Fig. 3.11: Newly added 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. If the backup is completed successfully, the indicator next to the device name is green, and the date of the last backup is shown.

3.5.2 Importing multiple devices using a CSV file

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

When creating a comma-separated value (CSV) text file for 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	Device name (*required field*)
plugin	The device type, e.g. 'Cisco ASA' or 'cisco_asa'
protocol	The connection protocol, e.g. 'telnet' or 'ssh' (*required field*)
ip_address	The device IP address
username, password, password2	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

3.5.3 Device Discovery

The Restorepoint device discovery engine uses a variety of methods to discover hosts on your network that can be imported into 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; however, when you import a device, you will be able to override the detected type.

3.5.3.1 Discovery Setup

To configure discovery, follow these steps:

1. Select **Discovery** from the **Devices** menu to display the discovery setup page.
2. Add one or more network ranges (in CIDR notation) to be scanned to 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. (optional) Add one or more SNMP communities in use on your network: choose the SNMP version, enter a community string, then click the **Add** button.
5. If you wish to be notified of new device, tick the **Notify of New Devices** tickbox.
6. If you want to use the Cisco Discovery protocol (https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol), tick the **Use CDP** tickbox.
7. If you want to use the Link Layer Discovery protocol (https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol), tick the **Use LLDP** tickbox.
8. Choose a scan schedule.
9. Click **Update** to save your changes.
10. Click **Scan Now** to start the scan.

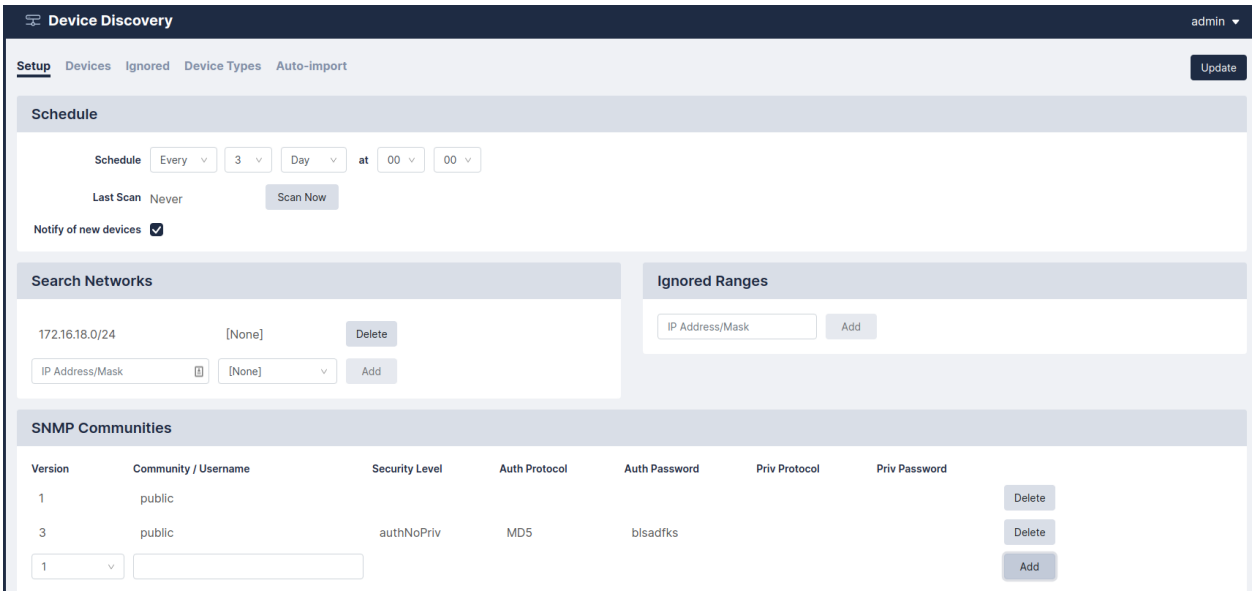


Fig. 3.12: Discovery setup

3.5.3.2 Discovered devices

At the end of the scan, a list of the discovered devices will be displayed:

Select one or more devices, then click **Import** to import them to the main device list. If only one device was selected, this will show the **New device** page with all the discovered information already filled in; after you review all the information and make any necessary changes, click **Save** to import the device. If multiple devices are selected, they will be imported without preview, however they will be marked as incomplete and displayed in red in the device list; you can then complete the configuration by adding the authentication details or modify any default parameters.

3.5.3.3 Ignored devices

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

3.5.3.4 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.

3.5.3.5 Automatic import

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

If you are using Domains, tick 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 to be used for imported devices; they can be based on detected device type, hostname, IP address range, or detected location.

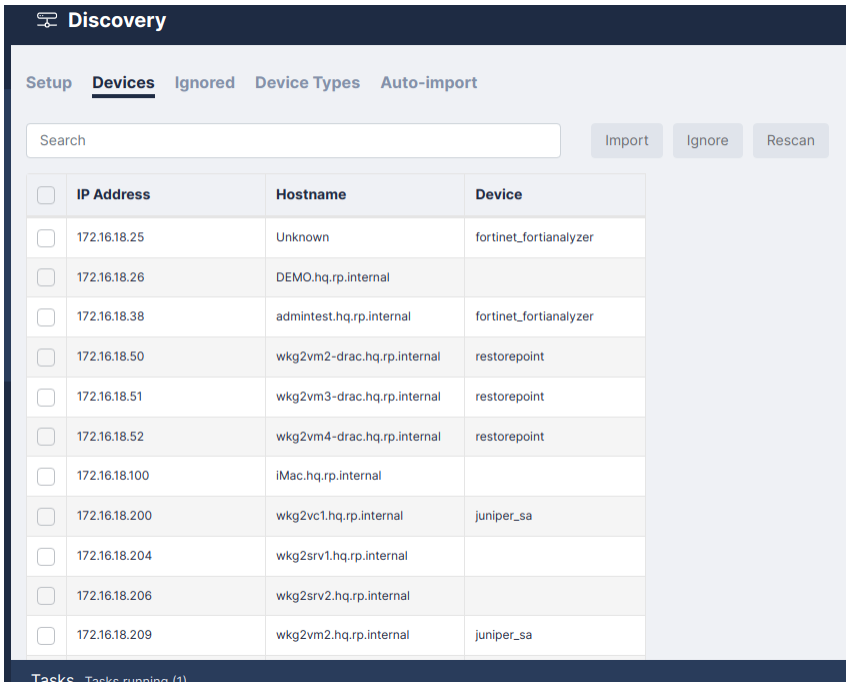


Fig. 3.13: Discovered devices

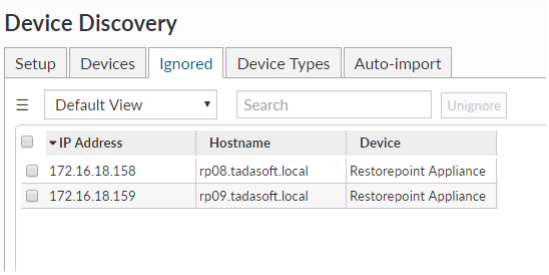


Fig. 3.14: Ignored devices image

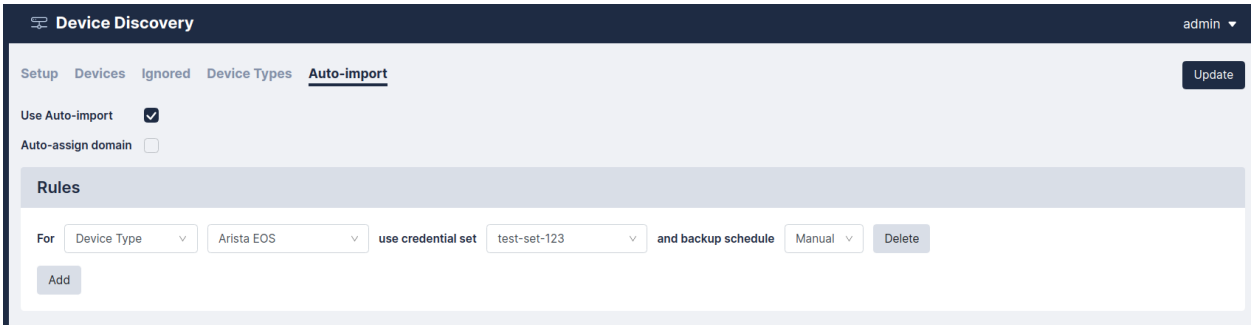


Fig. 3.15: Automatic device import

3.6 Running a manual backup

To run a manual backup, follow these steps:

1. Select **Devices** from the menu. Restorepoint displays the **Device Management** page.
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 in the **Edit Device** page.

3.7 Automatic Backup Scheduling

When a large number of devices are defined, choosing the backup schedule for each individual device can become a burdensome task. Restorepoint allows you to automatically schedule backups for a group of devices, by spreading the backups over a day, a week, or a month. To do so, 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. This allows you to run backups only at night, or during the weekend for example.

3.8 Exporting the device list

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

3.9 Editing an existing device

To edit an existing device, follow these steps:

1. Click on the relevant device name; Restorepoint displays the **Edit Device** page.
2. Make any required changes and click the **Save** button to apply them.

3.9.1 Editing multiple devices

By selecting a number of devices and clicking **Edit**, you can set values for whole groups of devices at once. The **Edit Device** screen will display *[Multiple]* for all values that are not common to the selected devices. Changing one of these and clicking **Update** will set that value for all devices.

This is particularly powerful when used with device grouping - for instance, all Cisco devices may be set to back up hourly by Grouping by Manufacturer, ticking the *Cisco* group checkbox (thus selecting all Cisco devices), selecting Hourly and clicking **Update**.

3.10 Deleting an existing device

To delete an existing device, follow these steps:

1. Select the device(s) you wish to remove.
2. Click **Edit**, and make sure that **Disabled** is set to *Yes*. This prevents accidentally deleting a device you have not disabled first.
3. Click the **Save** button to save your changes.
4. The devices you want to remove should still be selected. Click the **Delete** button.

3.11 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.

3.11.1 Enabling monitoring

To enable monitoring, bring up the relevant device Edit screen and:

1. Tick the **Monitor Device** check box
2. Select the **Type** of monitoring required. Normally, the device's TCP port used for backup is polled; if the *Ping* option is selected instead, ICMP Echo Request (ping) will be used instead.
3. Check **Email when down** to be notified 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 will be considered "down". This allows for temporary network interruptions to be ignored.

3.11.2 Displaying monitoring information

Hovering the mouse over the status information will bring up a graph of Round Trip Time between Restorepoint and the device, in 5 minute intervals.

Clicking on the **Uptime** information will show 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.

3.12 Configuration Templates

Templates are specially marked-up configurations that can be pushed to multiple devices, for instance during a large deployment of similarly configured devices. Each template can contain parameters, which are substituted for entered values for each device pushed to. For instance, a section may be marked "IP Address", and this will then be prompted for when pushing to devices.

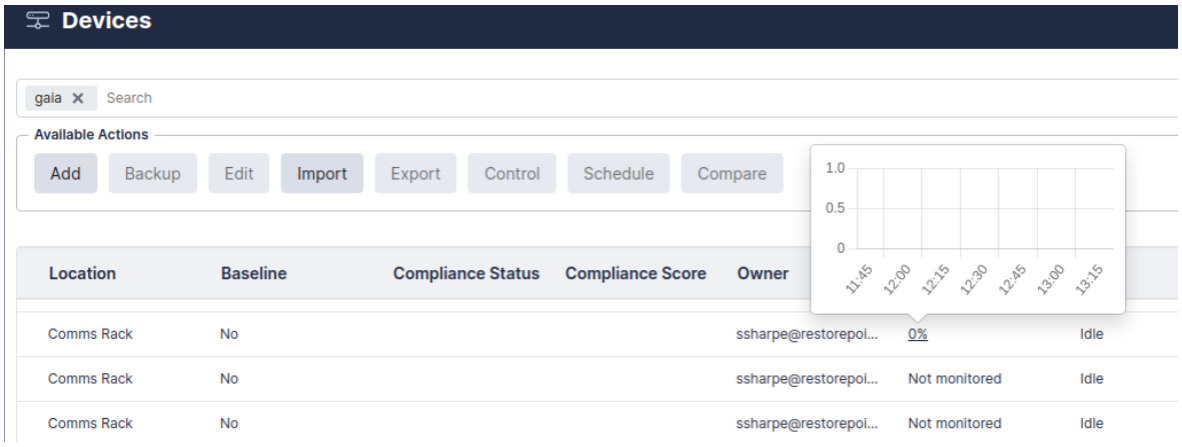


Fig. 3.16: Round-trip time graph

3.12.1 Creating and editing templates

1. Click **Add Template**, or click on an existing template name.
2. For new templates, select a device and configuration to base the template on.
3. Once loaded, highlight areas of the configuration to be substituted.
4. Click **Mark Variable** to name and store a highlighted value.
5. Once created, values can be renamed or deleted with the relevant buttons.
6. Click **OK** when done to save. If you don't provide a name and comment, they will be automatically generated.

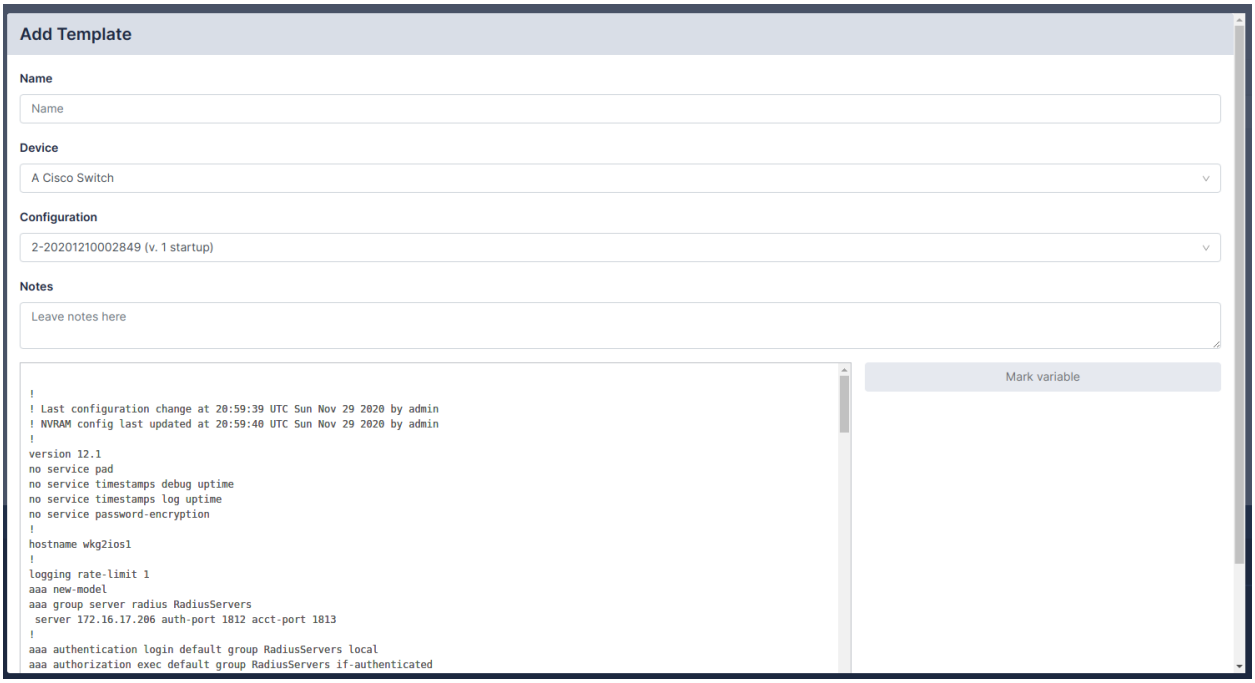


Fig. 3.17: Creating a template

3.12.2 Pushing templates

In order 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**.

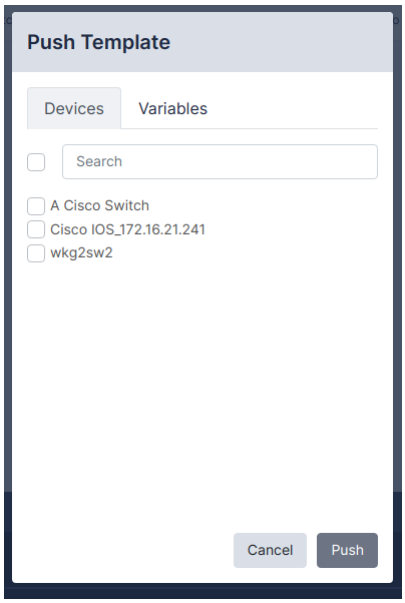


Fig. 3.18: Pushing a template

If the template has any parameters, Restorepoint will ask to enter their values, for each of the devices selected above:

Click **OK** to complete the operation.

3.13 Software management

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

3.13.1 Uploading and editing firmware images

1. Click **Import**, or click on an existing firmware name
2. For new firmware, select the file from your hard drive using the **Browse** button.
3. Fill in the **Device Type** and **Description** fields
4. Click **Save** when done to save/upload.

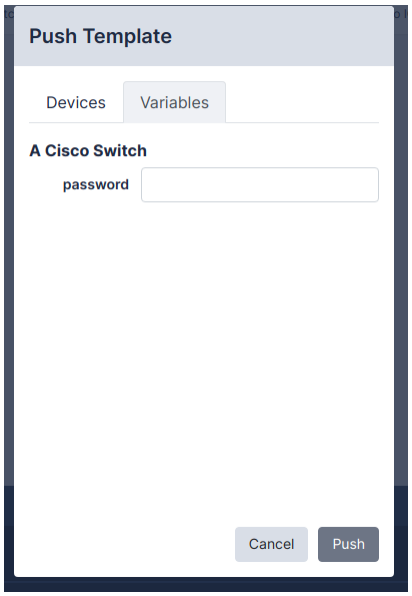


Fig. 3.19: Entering template parameters

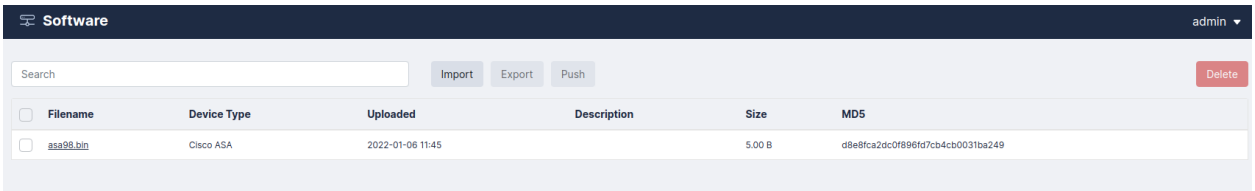


Fig. 3.20: Software images

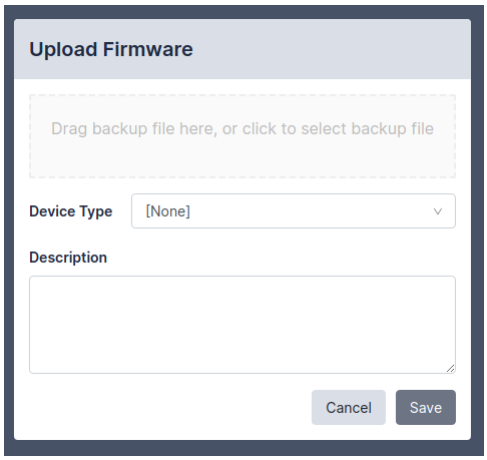


Fig. 3.21: Uploading a firmware image

3.13.2 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.

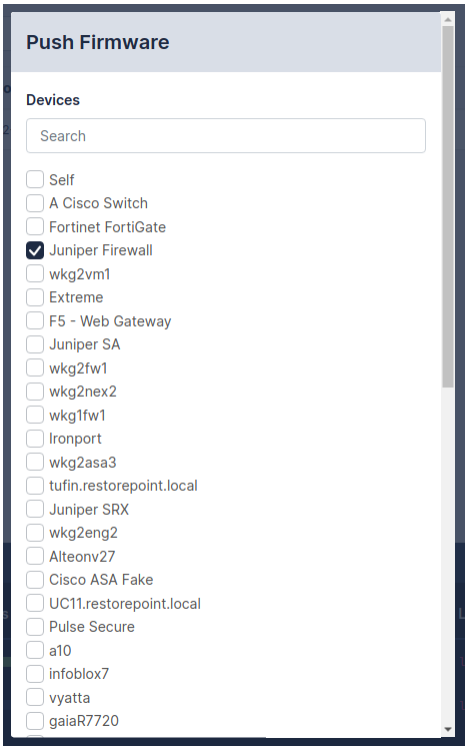


Fig. 3.22: Device firmware upgrade

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

3.13.3 Credential sets

Restorepoint can use predefined **Credential Sets** to authenticate to a device, in place of individual usernames and passwords; this is particularly useful if several devices share the same authentication credentials. To use this feature:

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** when done to save.

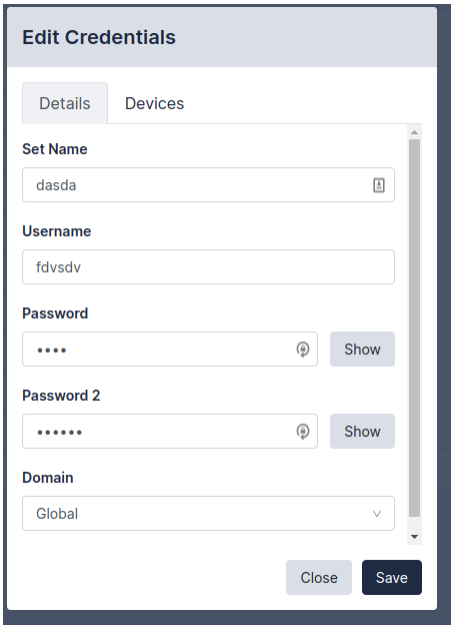


Fig. 3.23: Adding a credential set

3.13.4 Using Credential sets

In order to authenticate to a device using an existing credential set, leave the authentication details empty, tick **Use Credentials**, and then select the correct credential set. Click **Save** when done.

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

3.14 Asset Fields

In addition to the built-in Asset Management fields, you can also define custom fields. To do this got to **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, this will trigger an automatic email to the device's owner when the date specified is reached. Expiry date is also used in reports.

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

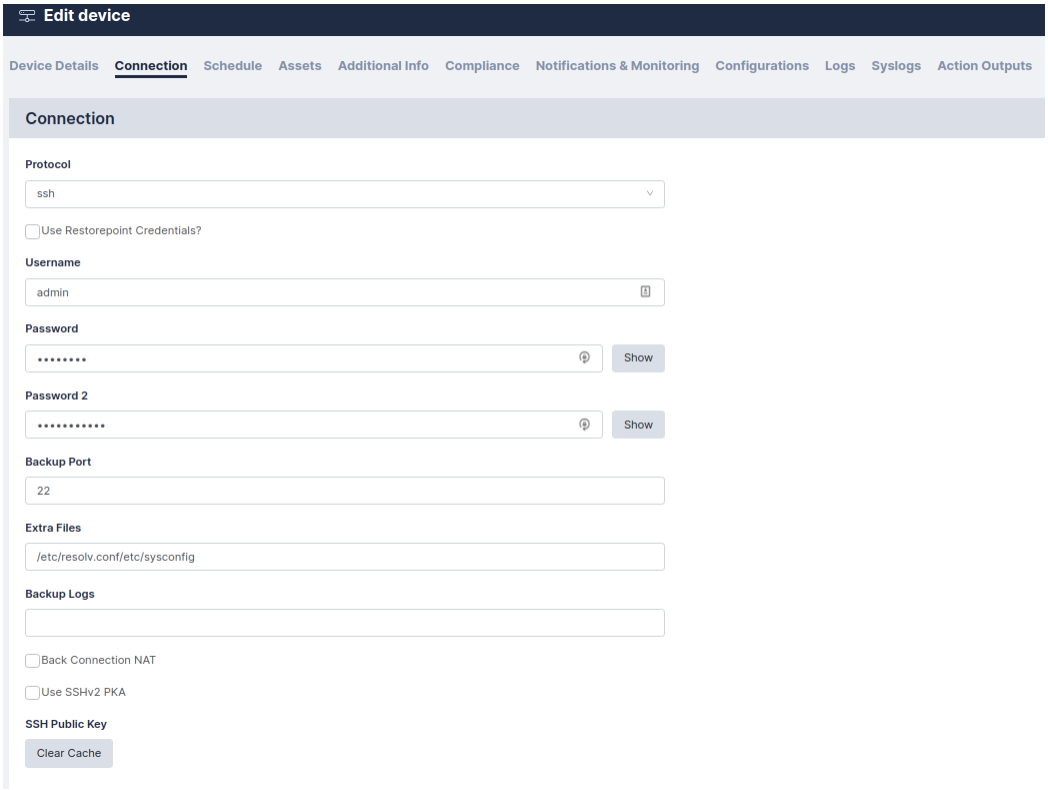


Fig. 3.24: Applying credential sets

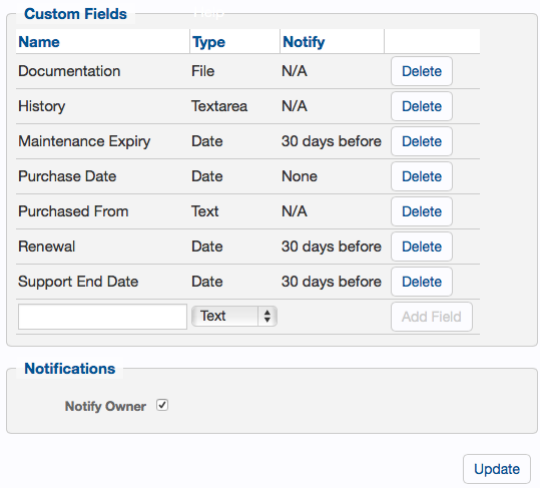


Fig. 3.25: Custom asset fields

3.15 Global Search

Restorepoint supports searching the full text of configuration backups for a keywords, from the **Devices > Global Search** page.

Enter your search term in the **Search for** box, select the devices you would like to search, and click **Go**. You can also choose to **Limit** the search to a given timeframe, to avoid generating more results than needed.

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. Clicking the name of the device configuration will open the configuration at the point that a match was found.

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

3.16 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 in the **last backup** column corresponding to the device, or clicking on 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.

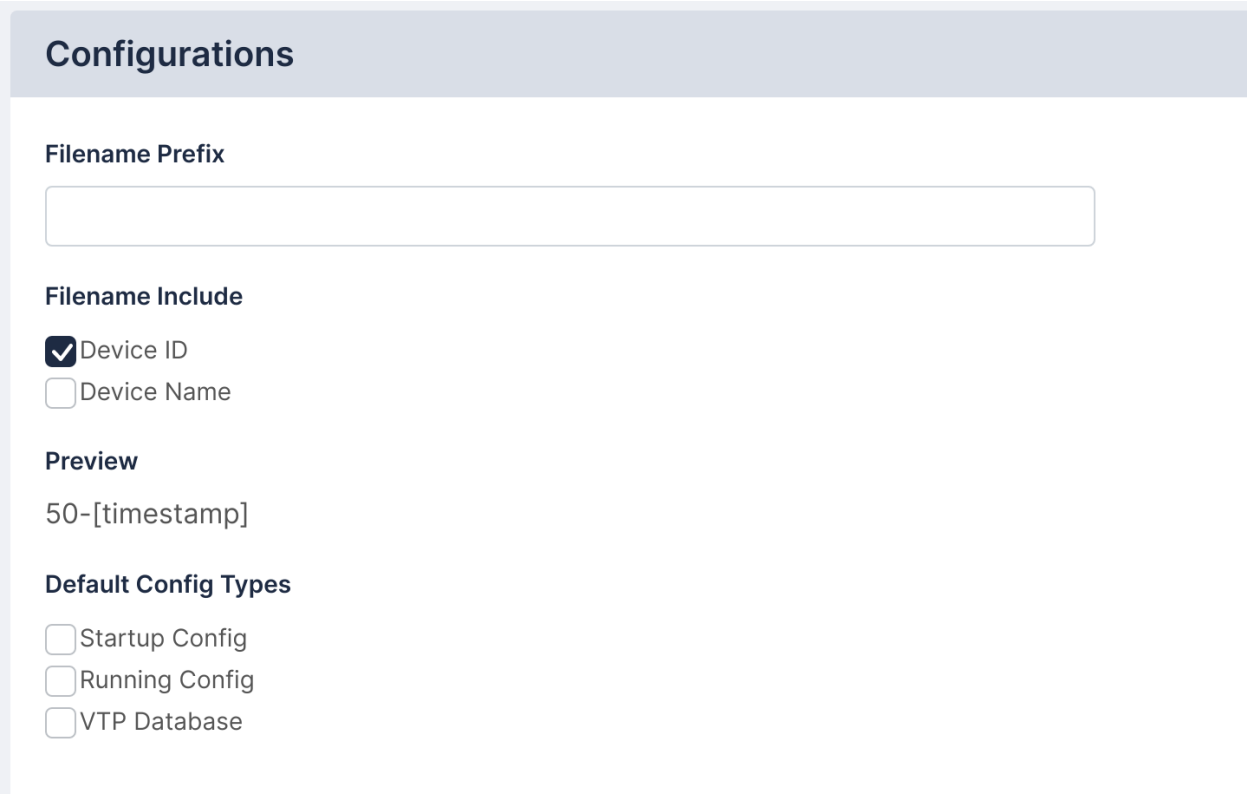


Fig. 3.26: Selecting device configuration types

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:

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.

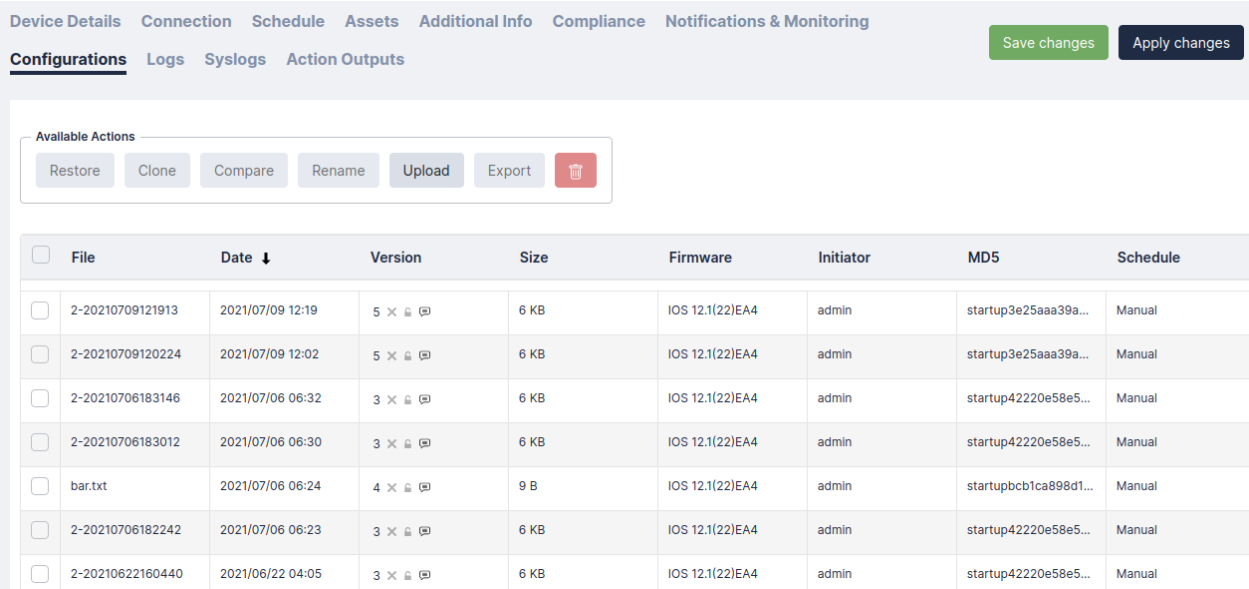


Fig. 3.27: Configuration list for a Cisco IOS

View	**There are three available modes:** 1. **Default View:** Restorepoint will display 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 a version of a configuration that has been set as a baseline. To set a version as baseline, click 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. See *Configuration Baselines*, for more information.
Retaining a version	You may wish to retain a configuration indefinitely (a *milestone* configuration), overriding 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 colour . 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 those devices whose configuration is a text file or a tar/tgz archive of text files. To compare two configurations, select two items using the check box 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, highlighting differences; inserted lines will be displayed in blue, changed lines 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 check box to its left 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 check box to its left 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.

3.17 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.

From this page, you can copy this file to your local machine by clicking the **Export** button. From there, 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. Restorepoint now holds the edited configuration file, which you can push to the device by using the **Restore** button.

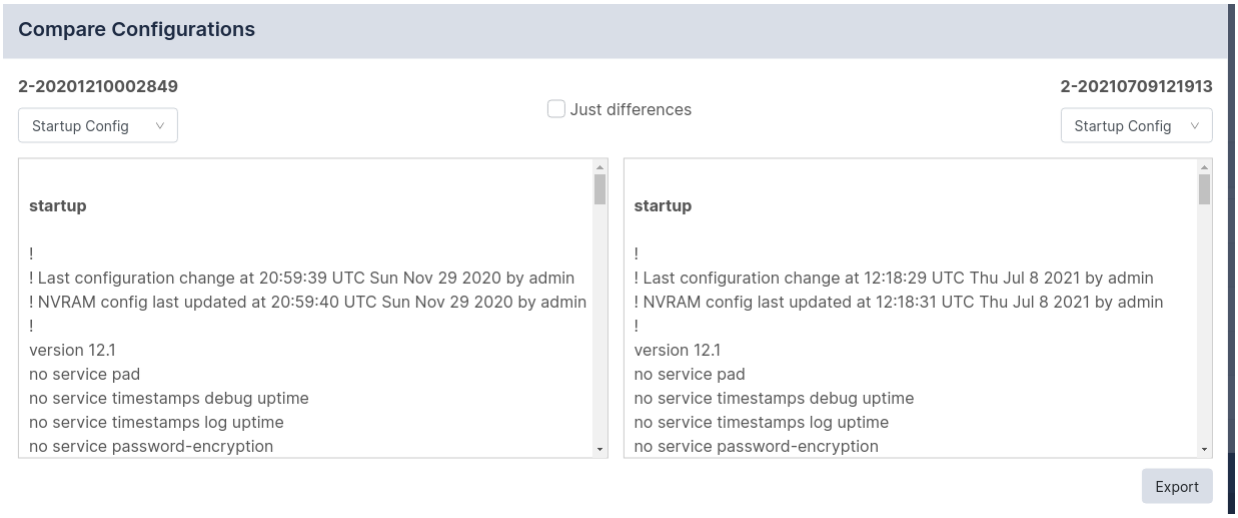


Fig. 3.28: Examining configuration changes

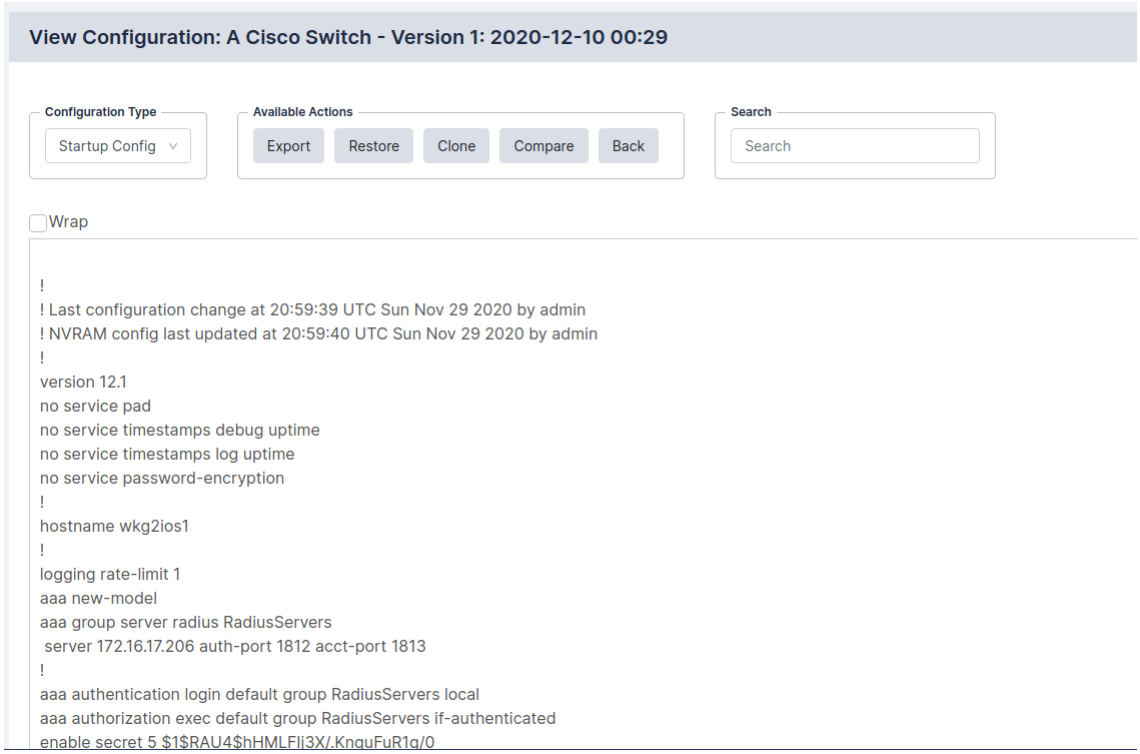


Fig. 3.29: Viewing a plain text configuration (Cisco switch)

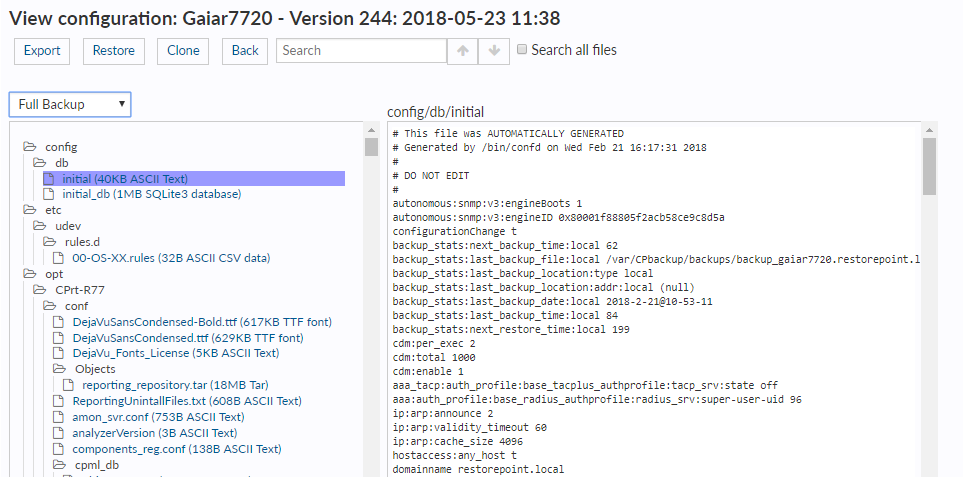


Fig. 3.30: Viewing a file within a TGZ configuration (Check Point Gaia)

3.18 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 the action to be performed when the last allowed failure occurs (either revert to the set schedule, or disable further backups).
- Finally, choose when to be notified of a failure.

3.19 Restoring to an existing device

To restore a device, follow these steps:

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 ticking its check box and click **Restore**. Restorepoint prompts you to confirm the restore operation. Depending on the device type, you may be prompted for additional options.

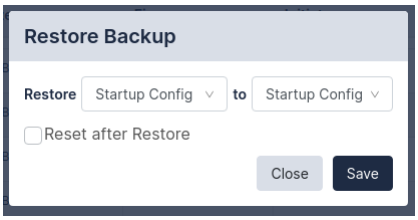


Fig. 3.31: Restoring a configuration

4. If the restore operation fails, this will be reflected 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.

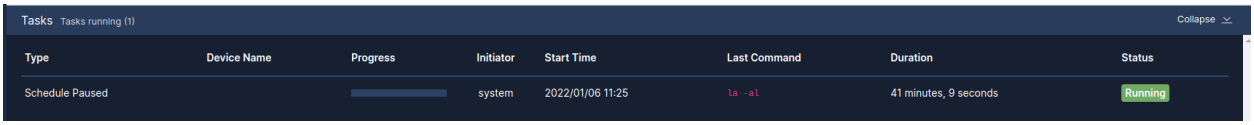


Fig. 3.32: Magnifying Glass

3.20 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 to need clear the SSH cache in Restorepoint in the **Connection** tab of **Device Management**.

3.21 Cloning

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

CHAPTER

FOUR

COMPLIANCE

Restorepoint enables you to create policies that can be used to verify that your devices comply with corporate or regulatory guidelines:

- *Device Policies*
- *Password Policies*
- *Configuration Baselines*

4.1 Device Policies

Use the **Compliance > Device Policies** page to create configuration compliance policies and assign them 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 they contain a certain phrase or Regular Expressions, or if they match an existing device template. If the tests fail, a compliance violation occurs 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.

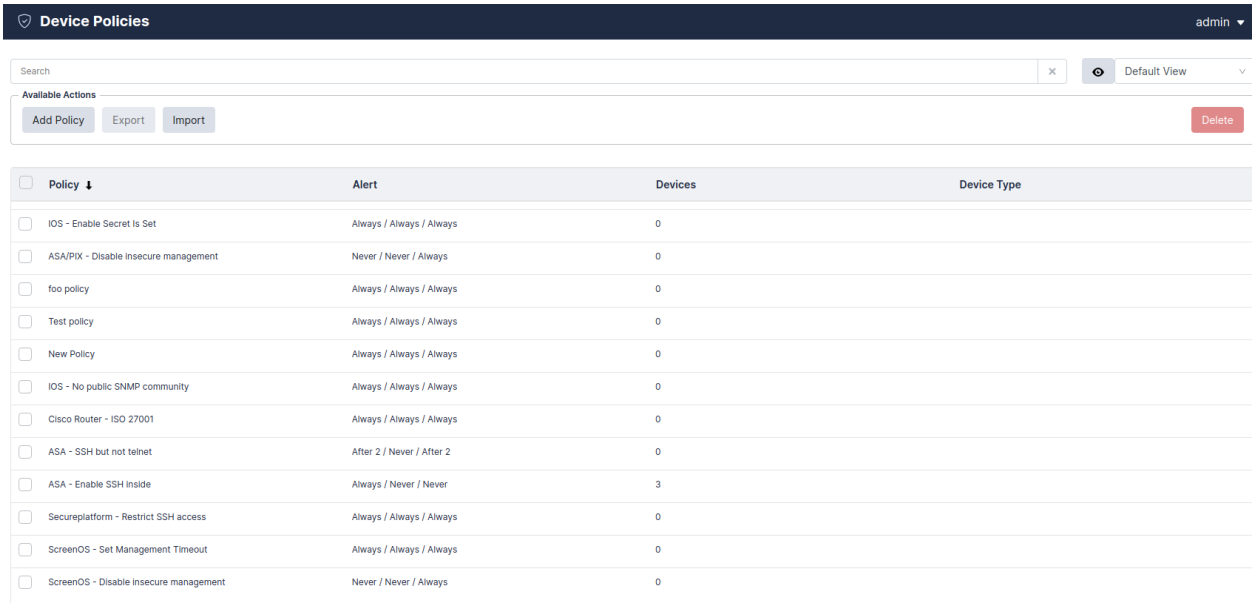


Fig. 4.1: Configuration policies

4.1.1 Creating a Policy

Click on the **Add Policy** button to create a new policy, or **Import** to import a previously exported policy:

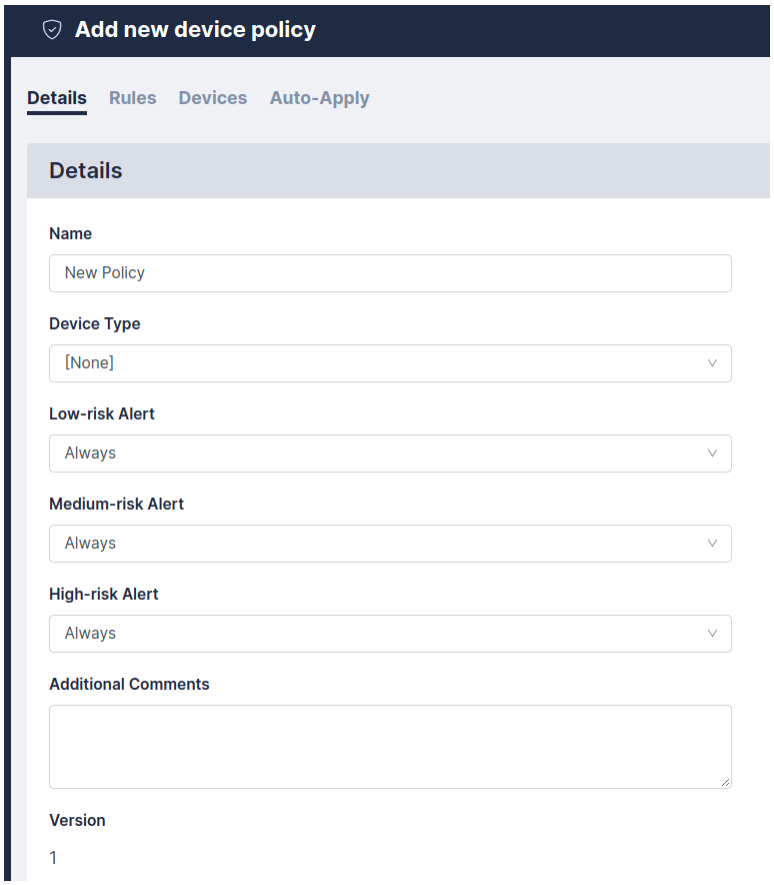


Fig. 4.2: New policy

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

4.1.2 Alert Criteria

Individual rules can be given a risk level, either **Low** , **Medium** or **High**. For each level, a trigger point can be set, determining whether or not an alert is generated. This ranges from **Never**, through 2, 3, 4 or 5 violations, to **Always**. For instance, you may want an alert only if 3 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.

4.1.3 Rules

Rules are defined and added to a policy with the **Add rule** button. Each rule consists of several parts:

Rule name	A label which 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, this pull-down is used to select an existing device template. Templates are defined in the **Devices** menu.
Match type	Phrase or (Perl-flavoured) *Regular Expressions*.
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 defined, a rule can be edited, removed, cloned, or (like the whole policy) tested against an existing backup using the appropriate buttons.

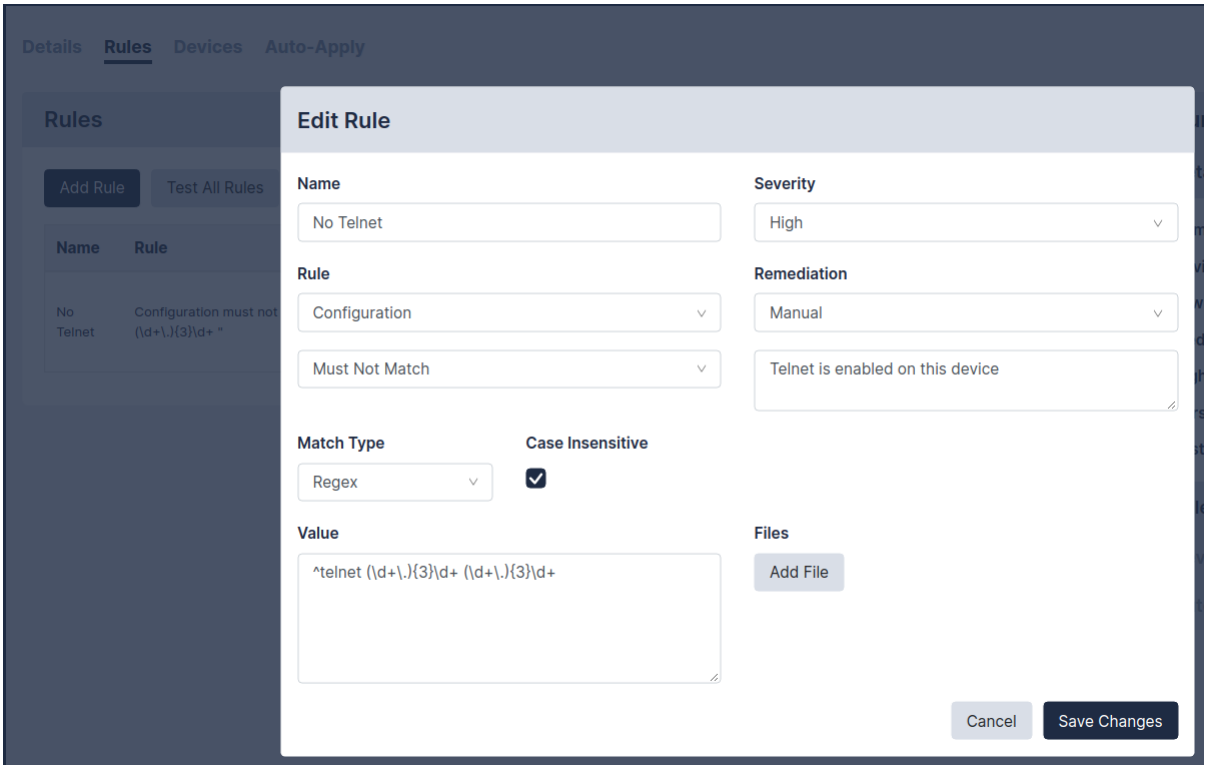


Fig. 4.3: Adding a new rule to a policy

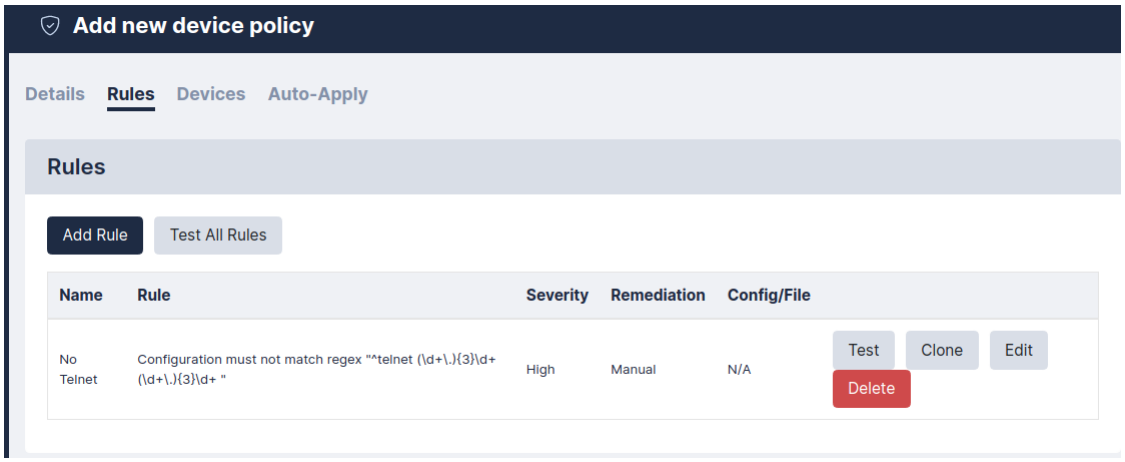


Fig. 4.4: Newly added rule

4.1.4 Remediation

Remediation is an action to be performed when a compliance rule is not met, generally intended to rectify the violation. The following remediation types can be configured:

Manual	In this case, the remediation text will simply be appended to the notification email, signifying that the recipient should take the appropriate action.
Command	This will execute one of the stored **Actions** on the device (see 7.1 *Controlling a device*).
Automatic	This setting will treat the text specified in the textbox as a command and execute it 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 part in brackets is a match for an IP address. If this rule is violated, the configuration can be remedied using the phrase:

```
unset telnet $1
```

In this case, the brackets in the rule will capture the IP address, and fill it in when the command is performed, expanding to

```
unset telnet 1.2.3.4
```

if that was the matched IP address.

4.1.5 Devices

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

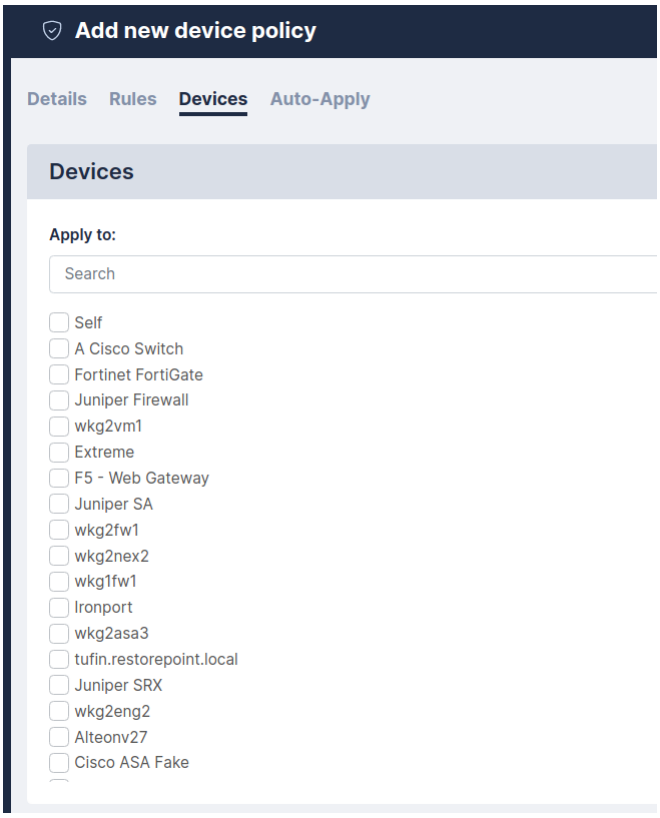


Fig. 4.5: Applying a policy to multiple devices

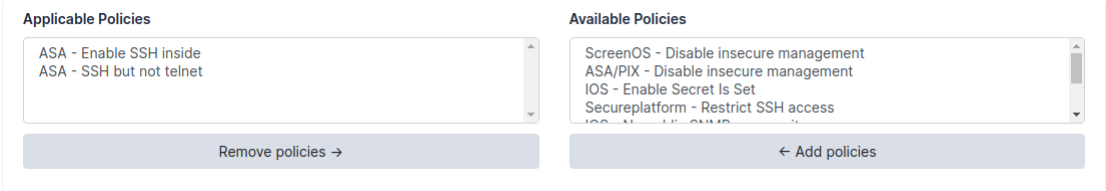


Fig. 4.6: Applying a policy from the device page

4.2 Regular Expressions

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

Most characters can be used in a regular expression; however, 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 instance:

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

There are some useful abbreviations for common character classes, in particular:

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

For instance, `\d\d:\d\d:\d\d` would match a time in a hh:mm:ss format.

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

4.3 Lua Functions

In Restorepoint, you can now 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 instance, `addmessage("Hello")` with a remediation text of `$1 World!` would produce the 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.`

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

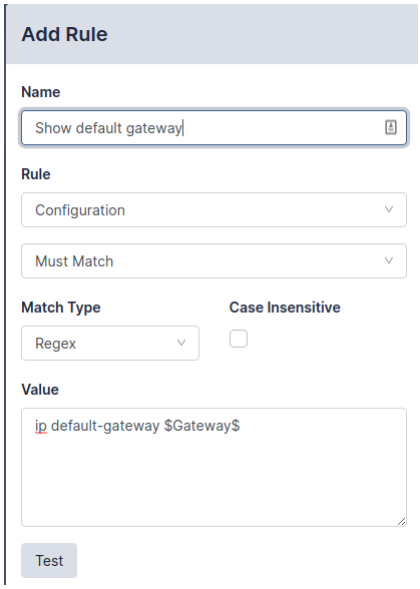


Fig. 4.7: Using variables in a rule

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

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

4.5 Password Policies

Password policies allow you to configure various rules for enforcing password strength, for both devices and users. These settings are used in the *strength meter* displayed in all password fields : the background of the field will change colour, from red for an unacceptable password, to yellow for a weak password, to green for a good password. Password Strength reports are available from the Reports page (see *Reporting* for more information).

The following rules can be used:

Minimum length	Minimum number of characters for a password to be accepted.
Good Length	Recommended number of characters to be considered *good*.
No Common	Password cannot be simple to guess, such as *1234* or *password*.
No Dictionary	Password cannot be a dictionary word, such as *backup* or *admin*.
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 `^`.

4.6 Configuration Baselines

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

CHAPTER

FIVE

REPORTING

A number of reports can be produced from the Restorepoint data. These can either be run on an ad-hoc basis, or scheduled and emailed to an authorised user.

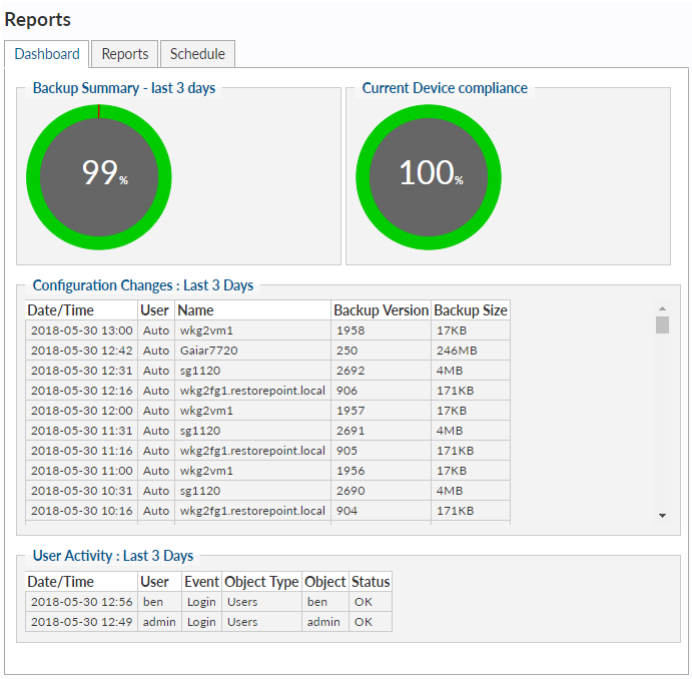


Fig. 5.1: Report dashboard

Initially, the Reports page shows the **Dashboard** tab, a summary of the last 72 hours' activity. This includes:

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

Rather than a report being composed of a single page, multireports are comprised of several individual report pages. The dropdown in the top left corner of the **Reports** tab shows the currently selected multireport.

5.1 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 (type, format, period, sorting, and filters), and click the **Run** button to generate a report. If the **New Tab** checkbox is ticked, 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.

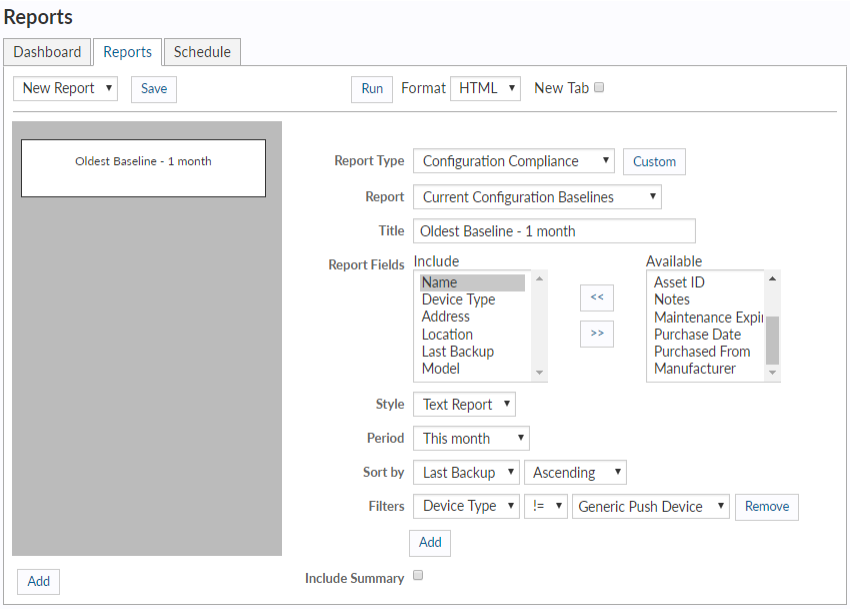


Fig. 5.2: Creating a report

5.1.1 Report formats

Reports can be produced in the following formats:

- HTML
- CSV
- PDF
- XML

Graphs can be produced in PDF or HTML format. In general, the *graph* types show summary data, while the *report* types show full details.

Note: if created from the browser, reports are produced either on-screen or as a downloadable file. When emailed, the reports are sent as attachments.

5.1.2 Report types

The following report page types are available:

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.

Once you have created a report type, you can save that configuration for later reuse by using the **Custom** button - this adds an entry to the **Custom Reports** report type.

5.1.3 Periods

Where relevant, reports can be produced for the following periods:

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

5.1.4 Sort By

Which column the generated table will be sorted by, on your report.

5.1.5 Filters

You can add filters to a report to limit to 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.

5.2 Scheduling a report

To schedule a report to run automatically:

1. Click the **Reports** tab.
2. Select the report parameters, then click the **Schedule** button.
3. Select a schedule for the report from the pull-down menus (shown below).
4. Enter the email address that will receive the report.
5. Click **Save**.

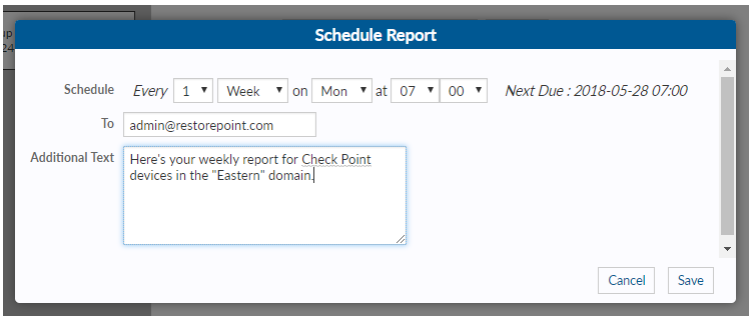


Fig. 5.3: Adding a new scheduled report

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

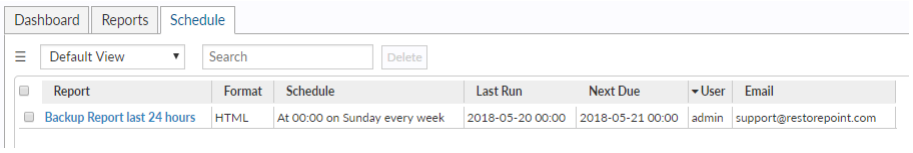


Fig. 5.4: Scheduled reports tab

CHAPTER

SIX

MANAGING USERS

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

Restorepoint supports three levels of user access:

Admin	Super User; has full control (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; can perform device backups and restores, but cannot modify devices, users, or appliance settings.
View Only	Monitor Operator; can only view existing backups, access logs, and verify that the system is operating normally.

6.1 Listing Logged-in users

A list of currently Logged-in users can be obtained from **Administration > Users**, in the **Logged-in Users** tab. The number of Logged-in users is also displayed on the dashboard (**Info > Status**).

6.2 Adding a new user

To add or modify administrators, select **Administration > Users**. Administrator passwords and encryption passwords by default must be at least 8 characters long. See *Password Policies* for more information.

To add a new user, follow these steps:

1. Select **Users** from the menu. Restorepoint displays the **User Management** page.
2. Click **Add User**. Restorepoint displays the **New User** page as shown below. (Fig. 6.1)
3. Complete the following 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	Tick this box to prevent the user from logging in.
Allowed Networks	Allows the user to connect to Restorepoint only from certain subnets, if set. Enter an IP range (in CIDR format) in the IP Address/Mask box, and click **Add**.

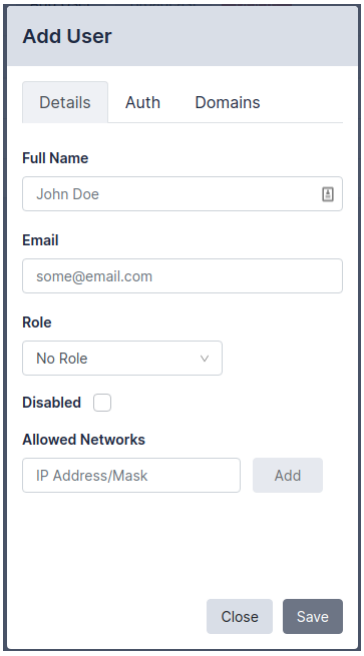


Fig. 6.1: Adding a new user

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. 6.2):

Username	Enter the new username (usernames may be up to 16 characters long)
Password	Enter the password for the new user (passwords must be between 8 and 24 characters long by default). The field colour will range from red to green to indicate the password strength, according to the policy set in the **Password Policies** page (see *Password Policies*).
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. The field colour will range from red to green to indicate the password strength.
Email activation link	This 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, without you needing to be aware of it.
Expire Password	Allows you to override the global password expiry rules for this user. See *Timeouts* for the global password expiry settings.
Use RADIUS	Tick this box 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.

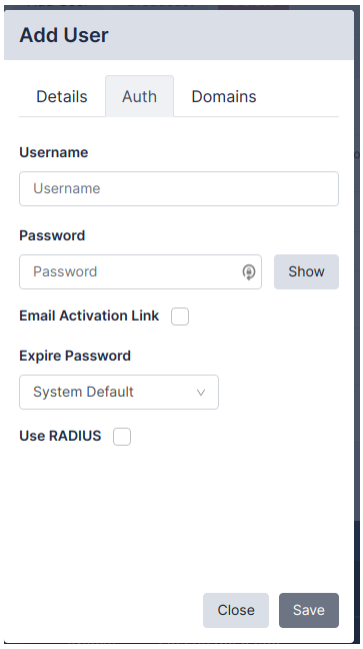


Fig. 6.2: Adding authentication details

5. Click on the **Save** button to complete adding the user to the system. Restorepoint displays the updated Users page, as shown in the image below (Fig. 6.3)

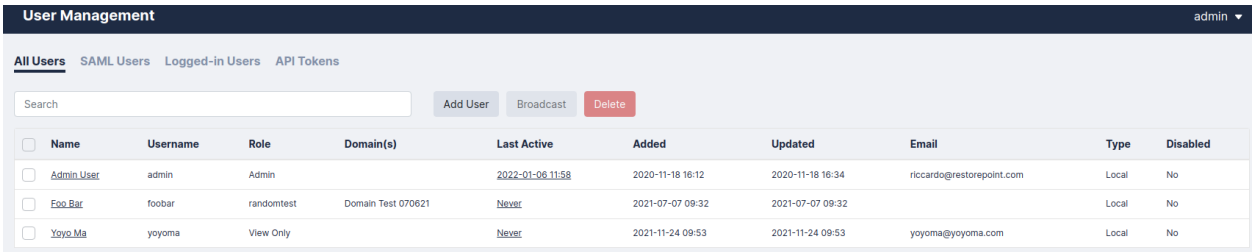


Fig. 6.3: Administrator list

When the new administrator first logs in, they will be prompted to configure a password recovery question and answer. Please see *Password Reset* for more information.

6.3 Editing an existing user

To edit the details of an existing user, follow these steps:

1. Select **Users** from the menu.
2. Click on the user you wish to edit.
3. Amend as needed and then click on the **Save** button to apply the changes.

When editing an *Admin*-level user, you'll see two additional boxes on the Auth tab:

- **Recovery Question/Answer**: Set a Recovery Question / Answer to allow password recovery.

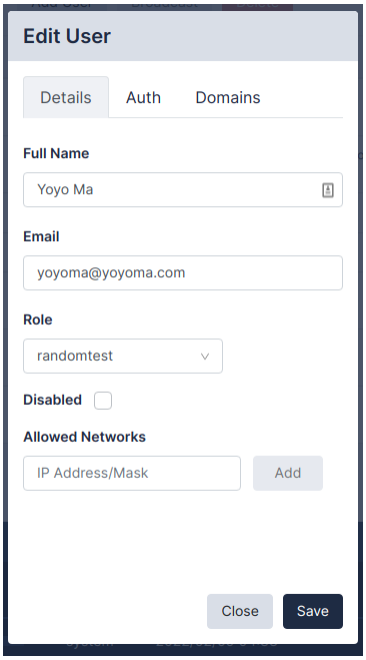


Fig. 6.4: Editing an existing user

- **New Token**: Generates and emails a new recovery token to the user. This will allow them to recover their encryption password if forgotten. Please see *Password Reset* for more information.

6.4 Broadcasting to users

Restorepoint allows for sending a notification message to a user (or group of users). Select the users 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 (explained below), and how long the message should persist for.

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 as registered on the appliance.

6.5 Deleting a user

To delete one or more existing users, follow these steps:

1. Tick the checkboxes next to the users you wish to remove.
2. Click on the **Delete** button.

6.6 Password Reset

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

6.6.1 Password recovery configuration

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

- A password recovery question and related answer; for security reasons, these should be only known to the administrator.
- The administrator's email address.

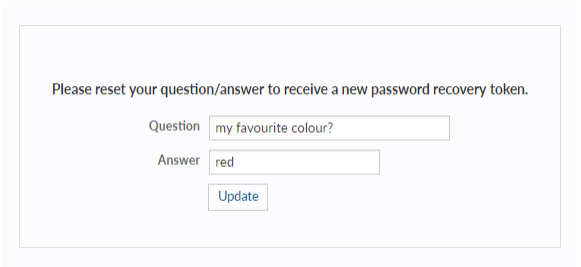


Fig. 6.5: Security question and answer

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

6.6.2 Recovery Procedure

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

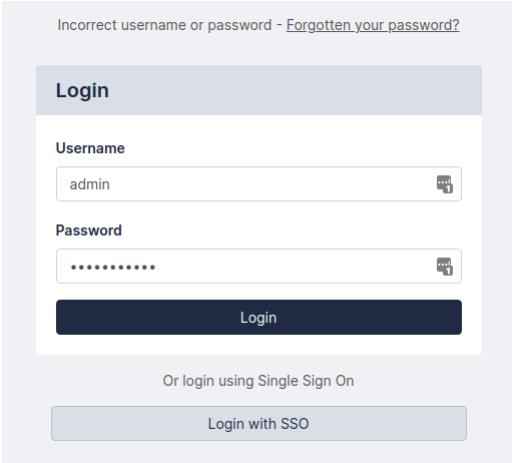


Fig. 6.6: Forgotten password link

Click on **Forgotten password?** to start the password recovery procedure; the system will ask for your recovery token and recovery answer; enter the required details and click **Recover**

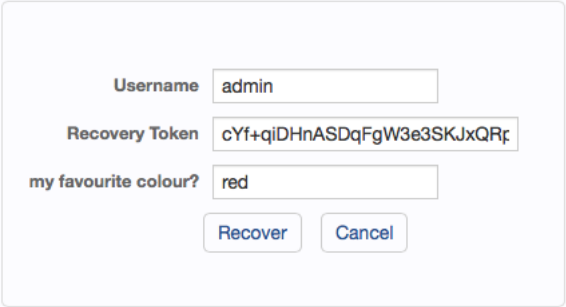


Fig. 6.7: Password recovery

If you have lost your recovery token, you can issue a new one from the **Edit User** (Fig 6.4) screen. 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**

6.7 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 granular, custom roles, which specify in detail which product elements are accessible to the user. This feature is only available with an Enterprise licence.

In order to define a custom role, proceed as follows:

1. Select **User Roles** from the **Administration** menu. Restorepoint displays the **User Roles** page.
2. Click **Add Role**, and fill in a name for the role.
3. Select the actions which are allowable for this role.
4. Click the **Users** tab to assign this role to one or more existing users.
5. Click **Save** to apply the changes.

Once added, a Role is immediately available in the **Role** dropdown in the **Edit User** page. Note that any changes to custom roles take effect immediately upon save.

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

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

Reports	
Backup	Enables backup reports
Config	Enables configuration reports
Assets	Enables assets reports
Compliance	Enables compliance reports
Admin	Enables administration reports
Monitor	Enables monitoring reports
Dashboard	Enables dashboard reports
Modify	Enables modifying and scheduling reports

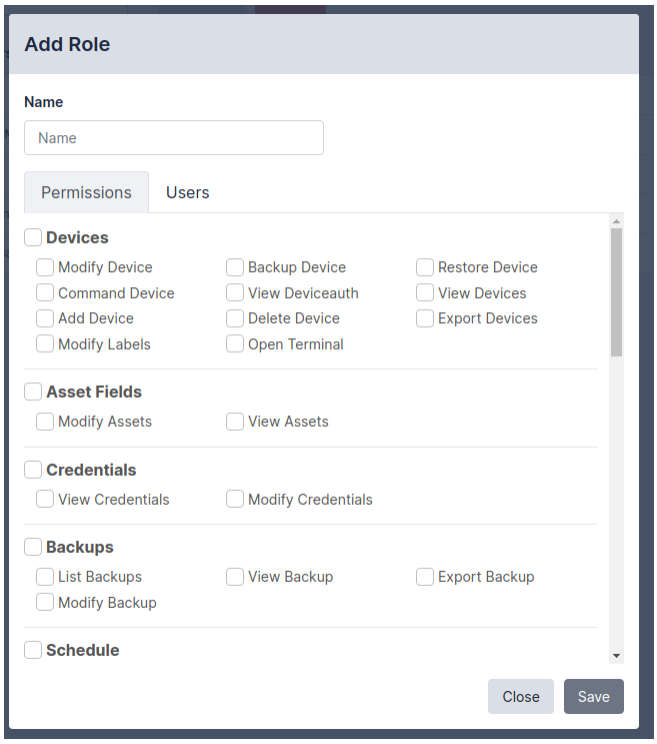


Fig. 6.8: Adding a custom administrator role

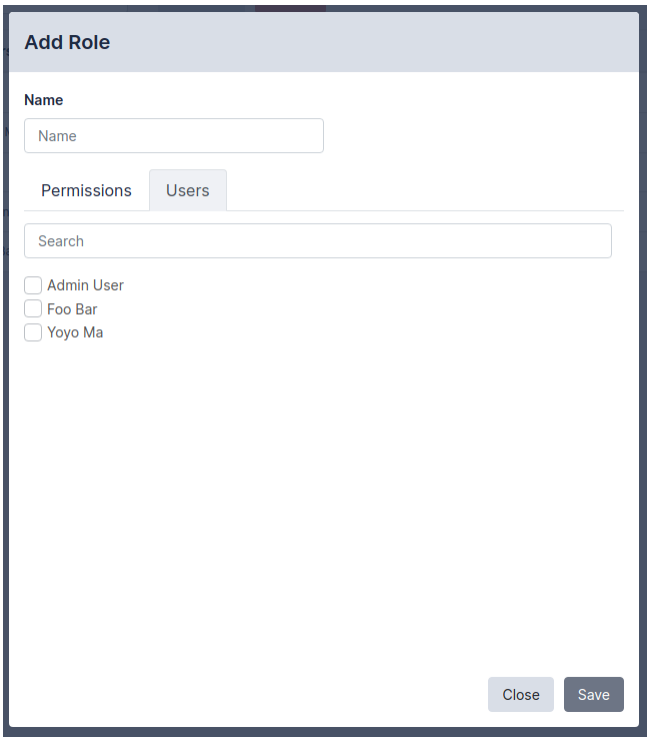


Fig. 6.9: Assigning a role to an administrator

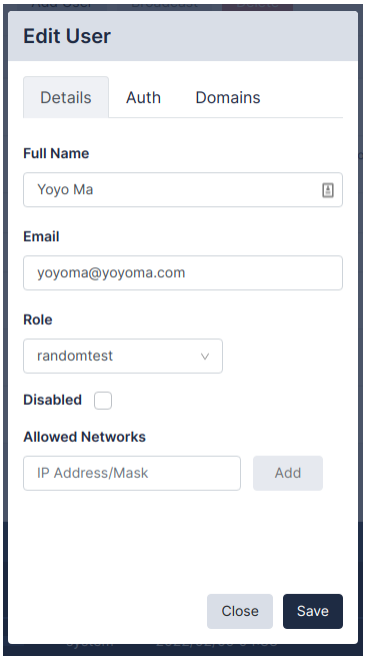


Fig. 6.10: Assigning a custom role by editing an administrator

Logs	
View Logs	Enables viewing of the system log
View Syslogs	Enables viewing of device syslogs

Devices	
View	Enables viewing of the device list and device details (excluding authentication details)
View Auth	Enables viewing of device authentication details
Backup	Enables device backup operations
Command	Enables device remote control

Configurations	
List	Enables viewing of device configuration list
Export	Enables exporting of device configuration
Restore	Enables restoring a configuration to a device

Templates	
List	Enables viewing of the template list
Push	Enables pushing templates to devices

Firmware	
Push	Enables pushing firmware images to devices

Assets	
List	Enables viewing of custom asset fields

Compliance Rules	
Apply	Enables applying compliance rules to devices

System	
Archive	Enables system archive operations

Users	
View	Enables viewing of the user list and user details (excluding authentication details)
View Auth	Enables viewing of user authentication details

6.8 Authentication Servers

6.8.1 RADIUS Authentication

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

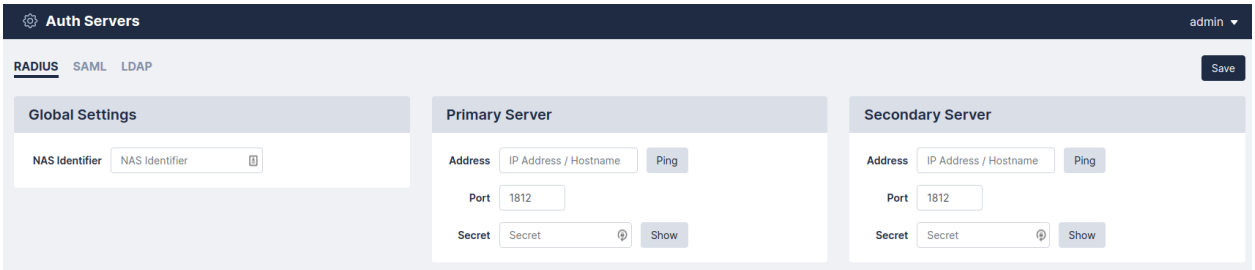


Fig. 6.11: RADIUS configuration

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.	

6.8.2 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 *dc=company,dc=com*.	
User Search	**Base DN**	for example, *cn=users,dc=company,dc=local*
	Username Field	what LDAP field to use as the Restorepoint login id, for instance *uid* or *samAccountName*.
Group Search	**Base DN**	for example, *cn=security groups,dc=company,dc=local*.
	Search String	the group search filter, for instance *objectClass=Group* or *objectClass=posixGroup*, 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, *cn=Administrator,cn=Users,dc=company,dc=local*.
	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	

Please note that LDAP Users will need to be assigned a role from the **Administration > Users > LDAP Users** tab before they can log in.

CHAPTER

SEVEN

DEVICE CONTROL

7.1 Controlling a device

Restorepoint allows you to send a CLI command to a device or group of devices and capture the output of the command. This is a very convenient tool 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**.

This dialogue box appears:

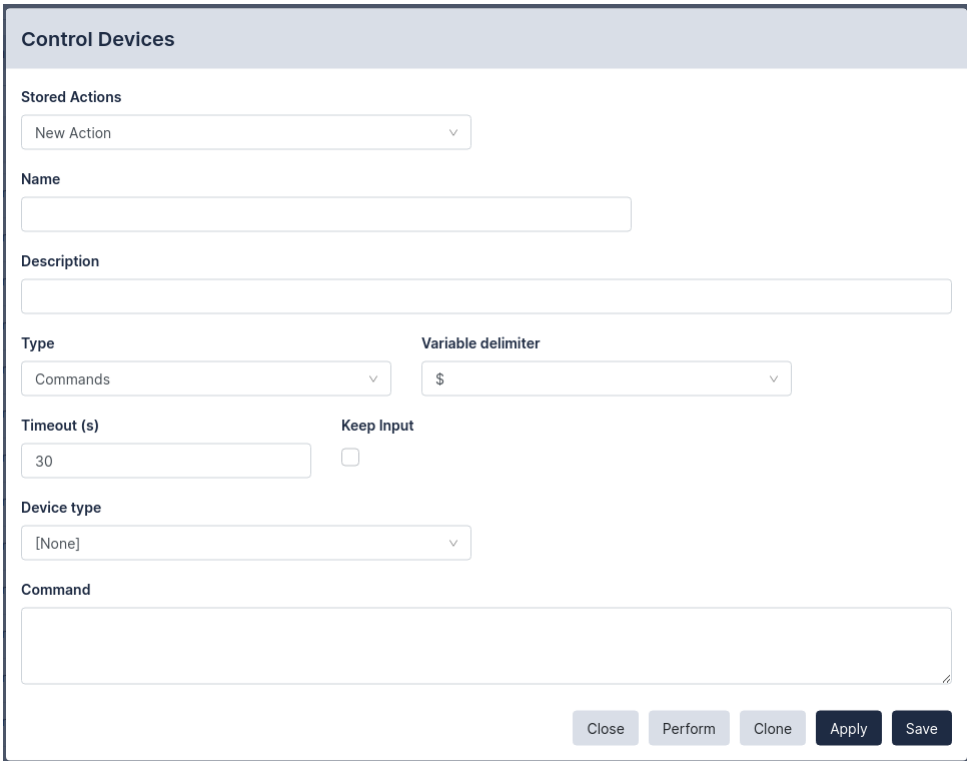


Fig. 7.1: Device control

Select **New Action** from the pull-down menu, then enter the commands in the text area. Device Control Actions can also be defined from the **Device Control** menu entry, by clicking the **New Action** button.

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 (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.

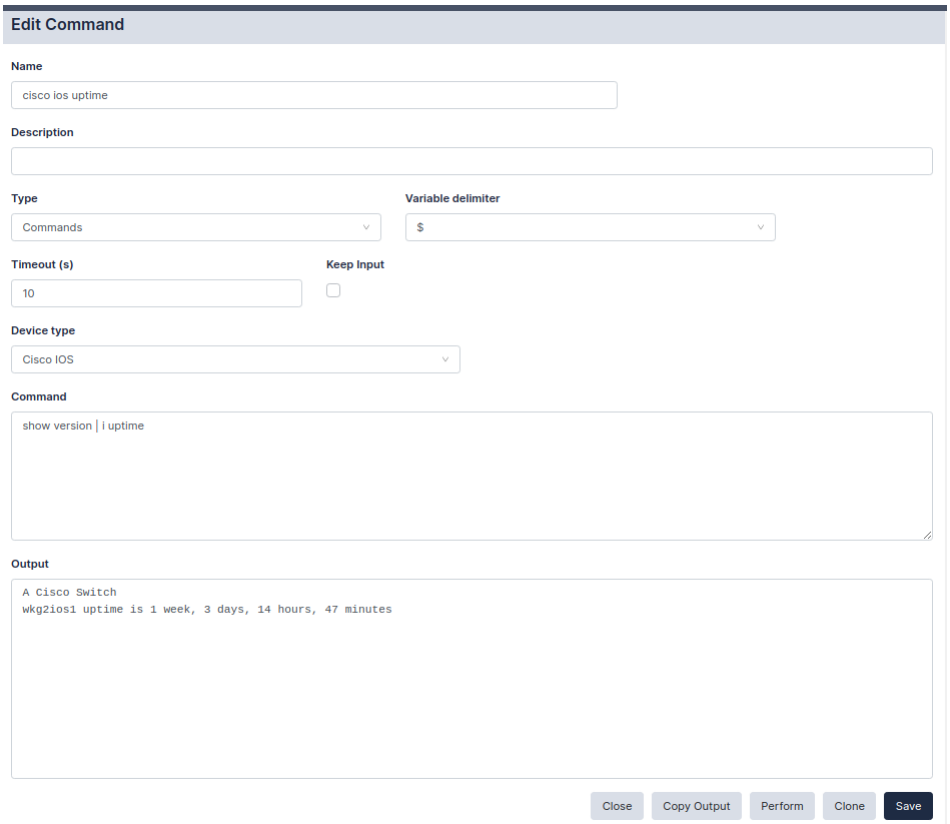


Fig. 7.2: Control output

7.1.1 Using Parameters

Actions can be parameterised 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:

```
set admin password $password$
```

After clicking **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`).

7.2 Scheduled Actions

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

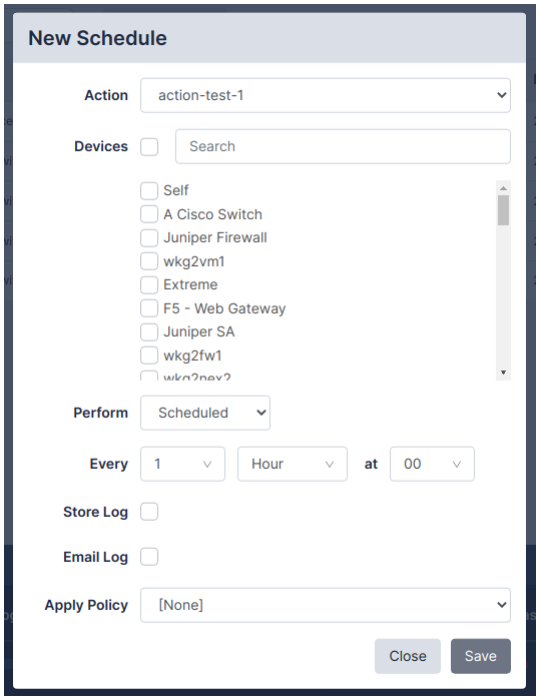


Fig. 7.3: Scheduling an action

1. Choose the **Action** to be performed.
2. Choose the device or devices on which to perform the action.
3. Choose a frequency, either **Scheduled** or **Once At** and a time interval or date.
4. Tick **Store Log** if you want to keep the output of the action.
5. Tick **Email Log** and enter an email address if you want to email the output of an action after execution.
6. Optionally, choose a compliance policy to apply to the output of the action (see *Device Policies*).
7. Click **Save**; the scheduled action page is displayed.

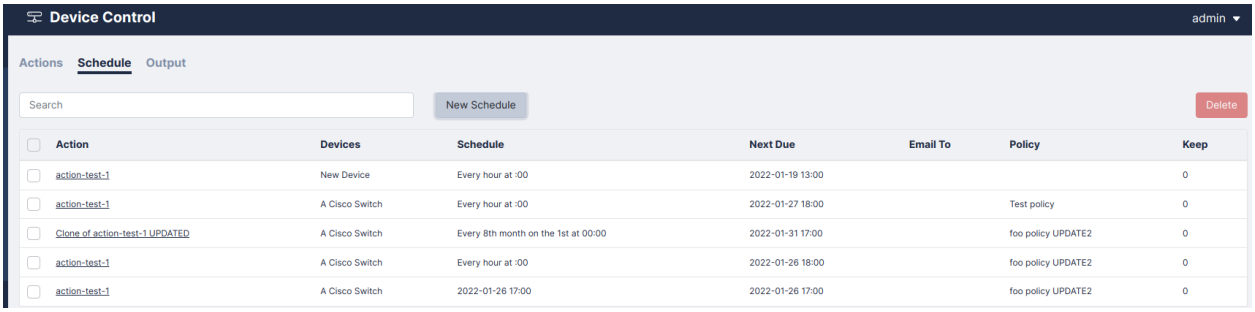


Fig. 7.4: Scheduled Actions page

Note: scheduled Actions cannot contain parameters.

CHAPTER

EIGHT

LUA APPLETS

Device Control features an additional, more powerful way to interact with devices, using the Lua programming language. Rather than just sending a single command to a device, Lua provides control structures loops, conditionals, match functions etc. This provides the ability to perform more complex tasks, including making decisions based on the output produced by the device.

In order to create a Lua action, proceed as usual but select **Type > Lua** from the pull down menu.

The syntax is straightforward, and it does not require any specific programming experience or knowledge of markup languages like XML; more information about Lua can be found at https://www.lua.org/docs.html.

8.1 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.

Also, standard Lua commands such as `string.match`, `string.gsub`. and `string.trim` may be useful.

Note that you do not need to write any code to connect and authenticate to the device; Restorepoint will do that for you.

However, there are some restrictions when it comes to making Lua scripts. Users are not permitted to run any "os" or "system" function. This restriction is in place to maintain the security of your Restorepoint appliance.

8.2 Examples

8.2.1 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)
```

8.2.2 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
```

8.2.3 IP Spoofing (ScreenOS)

For ScreenOS, you could do something like this 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
```

8.2.4 IP Spoofing (Palo Alto)

The same check, 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%-spoof:%s+enabled: yes') then
       print('Zone '..k..': antispoofing enabled')
    else
       print('Zone '..k..': antispoofing disabled')
    end
 end
```

CHAPTER

NINE

FILE STORAGE

9.1 File Servers

This page, accessed from the **Administration > Storage** menu item, allows you to save file storage configurations in Restorepoint. These can be used in the **Archive** or **Logs** page, or for automated configuration export from Restorepoint.

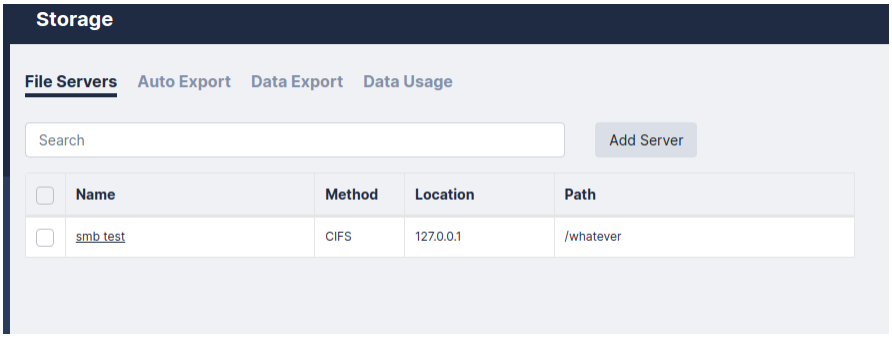


Fig. 9.1: File Storage

For each fileserver, you can define the following:

Name	A memorable name for the fileserver
Protocol	Select CIFS (Windows Server), FTP, SCP or SFTP from the drop down menu
Server IP	Enter IP address and port of the remote server
Path	Enter the full path on the remote server; for example, */home/user1* (FTP) or *share1directory2subdirectory3* (CIFS)
Username	Enter Username. This will be an FTP user, or a valid windows user if using CIFS
Password	Enter password
Use NTLMv2 (CIFS Only)	Tick this box if using CIFS with the NTLMv2 authentication protocol

9.2 Auto Export

For each policy, you can define the following:

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

There are also some options you can choose for your new policy:

Use GPG	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, */home/user1* (FTP) or *share1directory2subdirectory3* (CIFS).
Disabled	If this tickbox is selected, the policy will not run. This allows for temporarily disabling an auto-export policy.

9.3 Data Export

This page allows you to export a selection of device configurations on-demand.

Configurations	**No configs**, only the **Most Recent** version of the config, or **All Configs**.
Data	Allows you to include the device's **Logs**, and/or the **Device Data** in your export.
For	This allows you to pick the devices or domains to export.
As	You can export the configs as *TGZ* or *ZIP* archives, or directly export the individual config files.
Chunk Size	If you've selected an archive format, you can choose to create archive files of a specific size, rather than one large file.
To	Specify 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**.

9.4 Data Usage

This menu shows some 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 taken up by Restorepoint's search index (used primarily for the *Global Search* function).
Cache Size	Space taken up 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, but you can also manually **Clear Cache** if you'd like.
Debug Size	Space used for Restorepoint debugging logs, such as Appliance Debug Logs. The Appliance Debug Logs will be cleared if a new Debug Log is started, but there is a button on this page to **Clear Debug** if this file gets too large.

CHAPTER

TEN

AGENTS

Agents allow a Restorepoint appliance to manage devices located on a remote or otherwise disjoint network, not directly routable by Restorepoint, without the need of 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, enabling backups of devices on remote sites.

An Agent can be deployed as a Virtual or Hardware appliance on the remote network; the Agent provides faster 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 licence.

10.1 Agent Firewall Requirements

An agent initiates and maintains an SSH connection to the master Restorepoint appliance in order 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.

10.2 Agent Installation

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

10.3 Initial Setup

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

1. Open the virtual machine console in your Virtual Infrastructure client.
2. At the login prompt, enter the default user name (*admin*) and password (*admin*) for the agent.
3. Follow the prompts to change the agent shell password.
4. Choose the option **IP Address Configuration** at the console menu:
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.

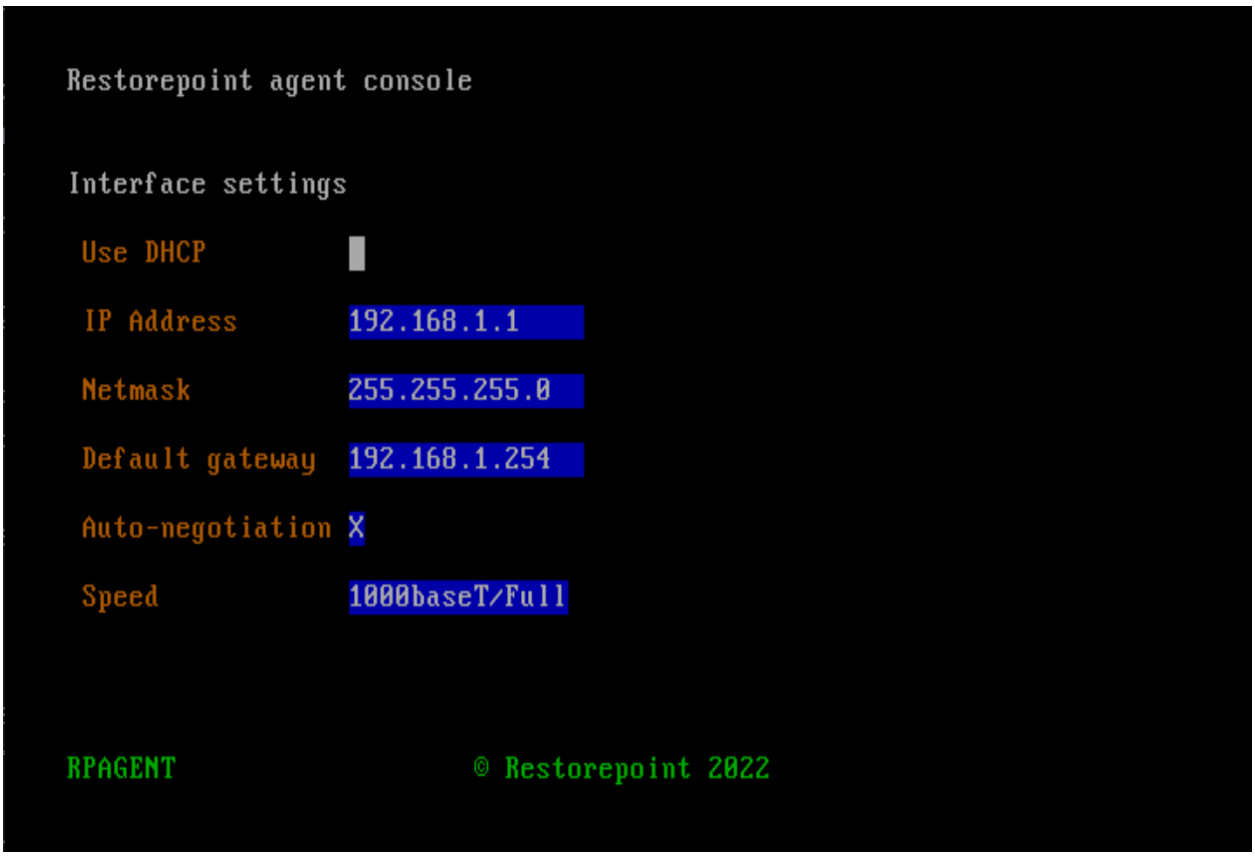


Fig. 10.1: Setting the agent IP address

7. Next, choose the option **Initial Restorepoint Master Setup**:

Fig. 10.2: Setting up the connection to the master

8. 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).

10.4 Adding an agent to Restorepoint

In order to add a configured agent to Restorepoint, go to **Administration > Agents** and click **Add Agent**. This dialog will appear:

Enter the following details:

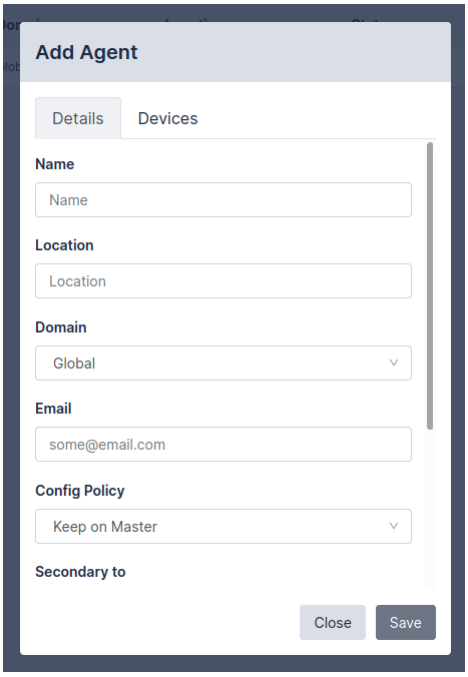


Fig. 10.3: Adding an agent

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. See *Administration Domains* for more information.
Email (optional)	The person responsible for the upkeep of the agent.
Alert on disconnect	If ticked, will send an email alert if the agent goes offline. If the **Email** field is not filled in, the default notification address is used.
Alert on reconnect	If ticked, will send an email alert 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 filled in once the agent has connected successfully for the first time. Note that currently, only one agent can be set up at a time.

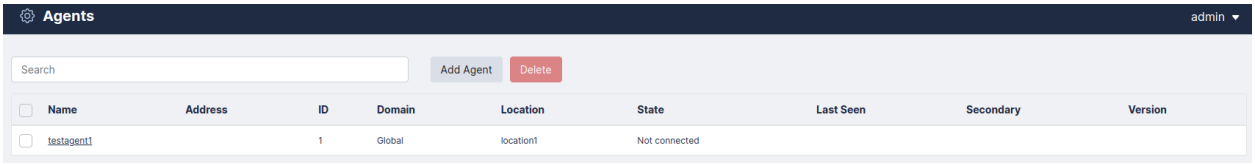


Fig. 10.4: Agent list

10.5 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. In order to do so, follow these steps:

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

Note: do not use the option **Initial Restorepoint Master Setup** to set the new master IP address; doing so would invalidate the master-agent authentication and would require re-pairing the agent to the master Restorepoint appliance.

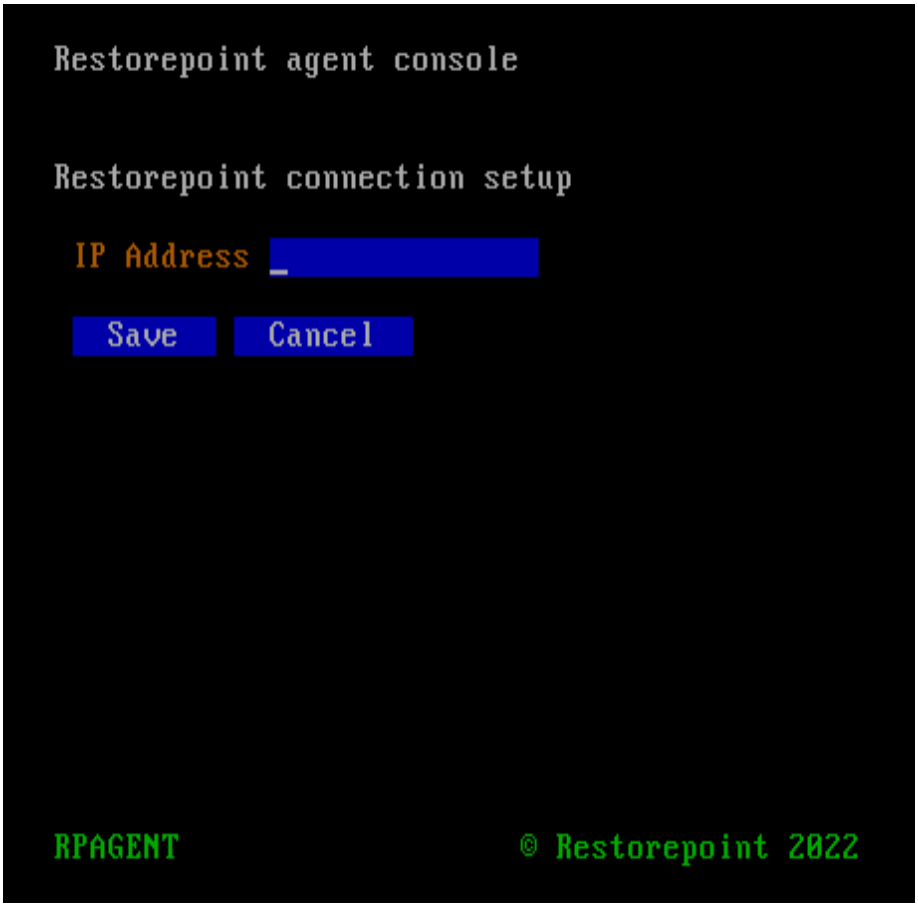


Fig. 10.5: Changing the master IP address

10.6 Remote operations using agents

Once an agent is configured, you can perform any operation (backup, restore, control etc.) on a device via the agent. This mean that the Restorepoint appliance will not connect directly to the device, but it will instead instruct the agent to perform the operation on its behalf.

In order 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 pull-down menu as shown:

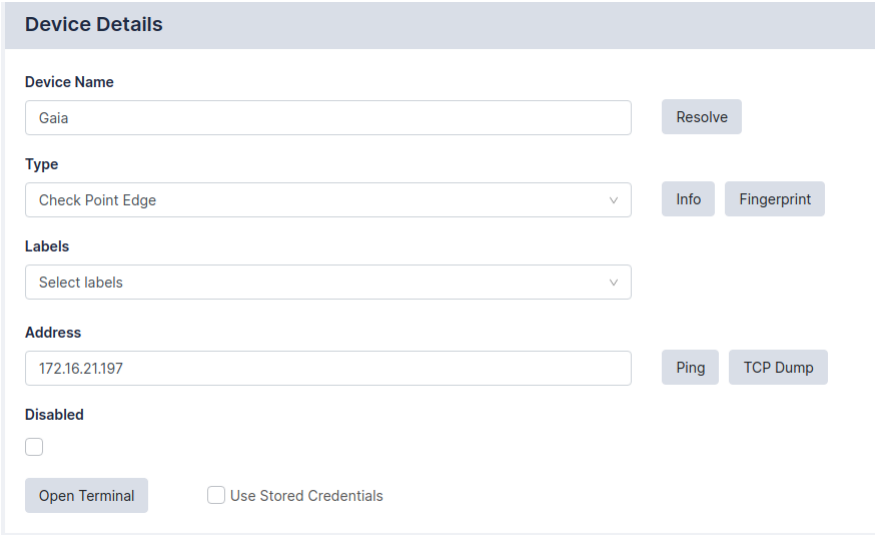


Fig. 10.6: Reaching a device via an Agent

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

10.7 Managing Agents

From the **Administration > Agents** page, a list of the paired agents can be seen. If you click on the name of an Agent, you will be able to edit the settings for an agent.

These include the **Name**, **Location**, **Domain**, **Email**, whether to **Alert on Disconnect/Reconnect**, or allow you to factory **Reset** the Agent for re-pairing. There is also a series of options for Debugging agent connections.

Debug > Start works similarly to Appliance Debugging, where it records a debug log that can be seen with 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 for remote management of an agent. This option will give a port number; connecting to that port on your Restorepoint master appliance will redirect to the agent, so that trickier issues can be diagnosed.

CHAPTER

ELEVEN

ADMINISTRATION DOMAINS

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

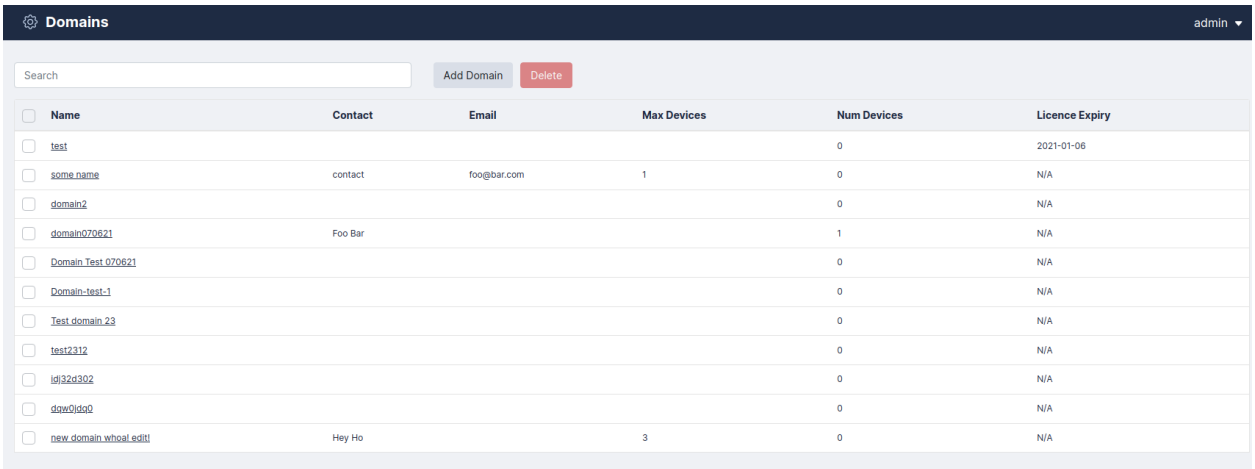
A typical use is for Service Providers managing multiple customers, or large enterprises with separate teams, where it is essential to restrict the scope of administrators to a subset of network devices.

Domains are only available with an Enterprise licence.

11.1 Managing domains

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

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



Name	Contact	Email	Max Devices	Num Devices	Licence Expiry
test				0	2021-01-06
some name	contact	foo@bar.com	1	0	N/A
domain2				0	N/A
domain070621	Foo Bar			1	N/A
Domain Test 070621				0	N/A
Domain-test-1				0	N/A
Test domain 23				0	N/A
test2312				0	N/A
idj32d302				0	N/A
dqw0jdq0				0	N/A
new domain whoal edit!	Hey Ho		3	0	N/A

Fig. 11.1: Domain list

To add a new domain, follow these steps:

1. Click **Add Domain**. Restorepoint displays the New Domain page.
2. Complete the following details:

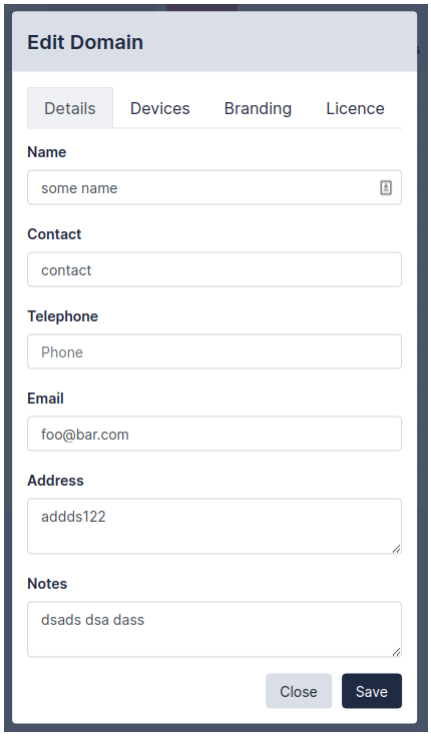


Fig. 11.2: New domain

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

3. Click the **Devices** tab to use the device selector and add devices to the domain. In addition, 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 (see *Network Address Translation (NAT)* for more information). This setting can in turn be overridden by the device-specific setting.
   - The exact devices that are part of the new domain.
4. Click the **Branding** tab (optional) to customise 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 optimal 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 for users in this domain
Remove Help Menu	Disallows access to the help for users in this domain

5. Click the **Licence** tab (optional) to restrict the domain to expire on a certain date. Click **Enforce Licence** to

enable the function, and choose the date.

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

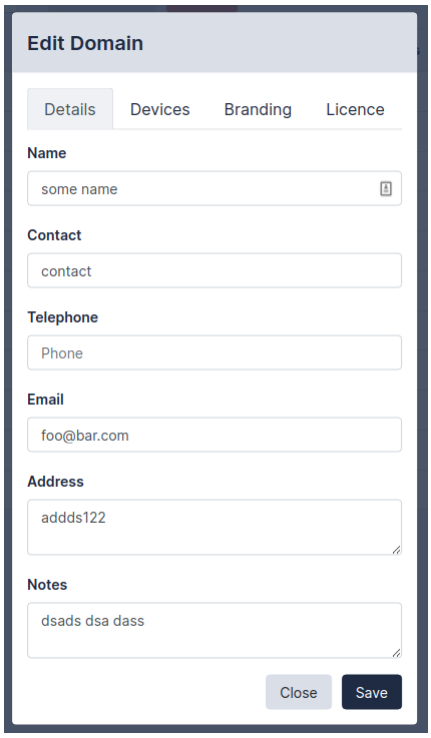


Fig. 11.3: Adding devices to a domain

6. Click **Save** to complete the task; the system will return to the domain list.

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

11.2 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, irrespective of which domain the devices are assigned to; logs and status page 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:
	• create/modify/delete devices in any domain
	• create/modify/delete global and domain administrators
	• initiate backups/restores
	• change the appliance configuration
	• 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

For additional flexibility, custom user roles can also be defined (see *Custom User Roles*).

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

11.3 Adding a new domain user

To add a new domain user, follow these steps:

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 details:

Full Name	Enter the full name of the user.
User-name	Enter the new username (up to 16 characters).
Pass-word	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)

Encryp-tion 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:

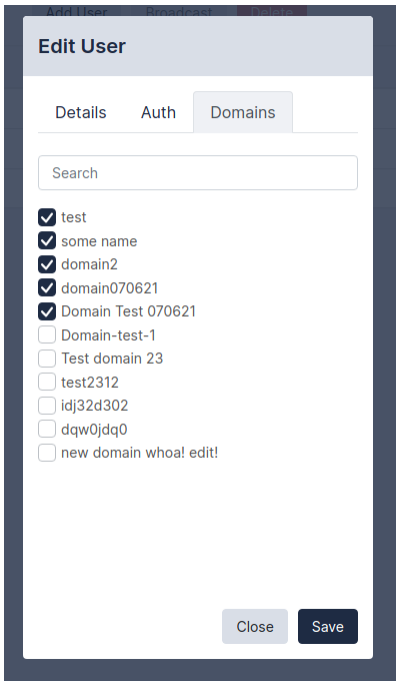


Fig. 11.4: Restricting a user to a specific domain

4. Click the **Update** button to complete the operation; Restorepoint will display the updated **Users** page:

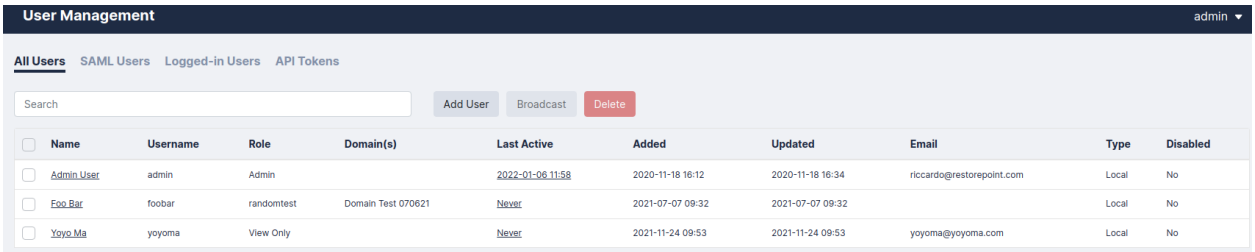


Fig. 11.5: User list

11.4 Editing devices

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

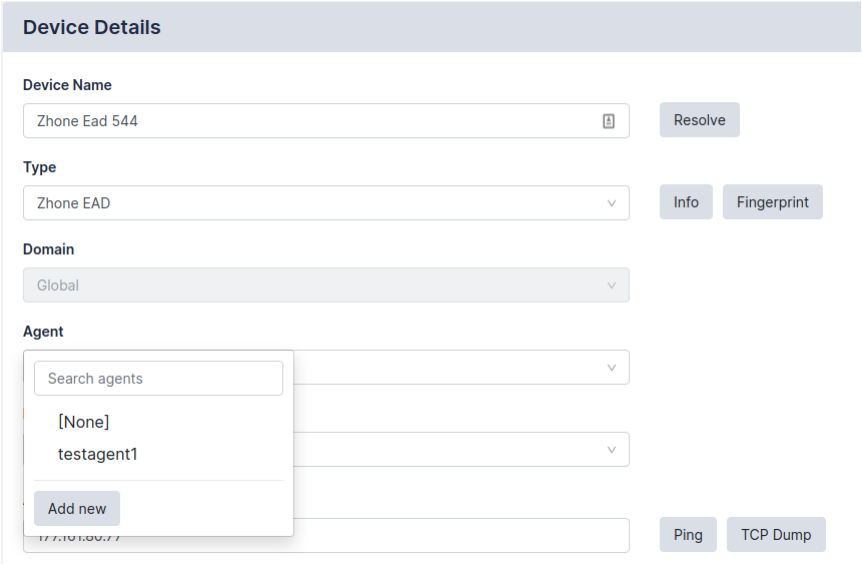


Fig. 11.6: Assigning a device to a domain

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

CHAPTER

TWELVE

LOGS

The Logs page provides detailed information about system activity.

12.1 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 had the action performed.
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 *localhost*.

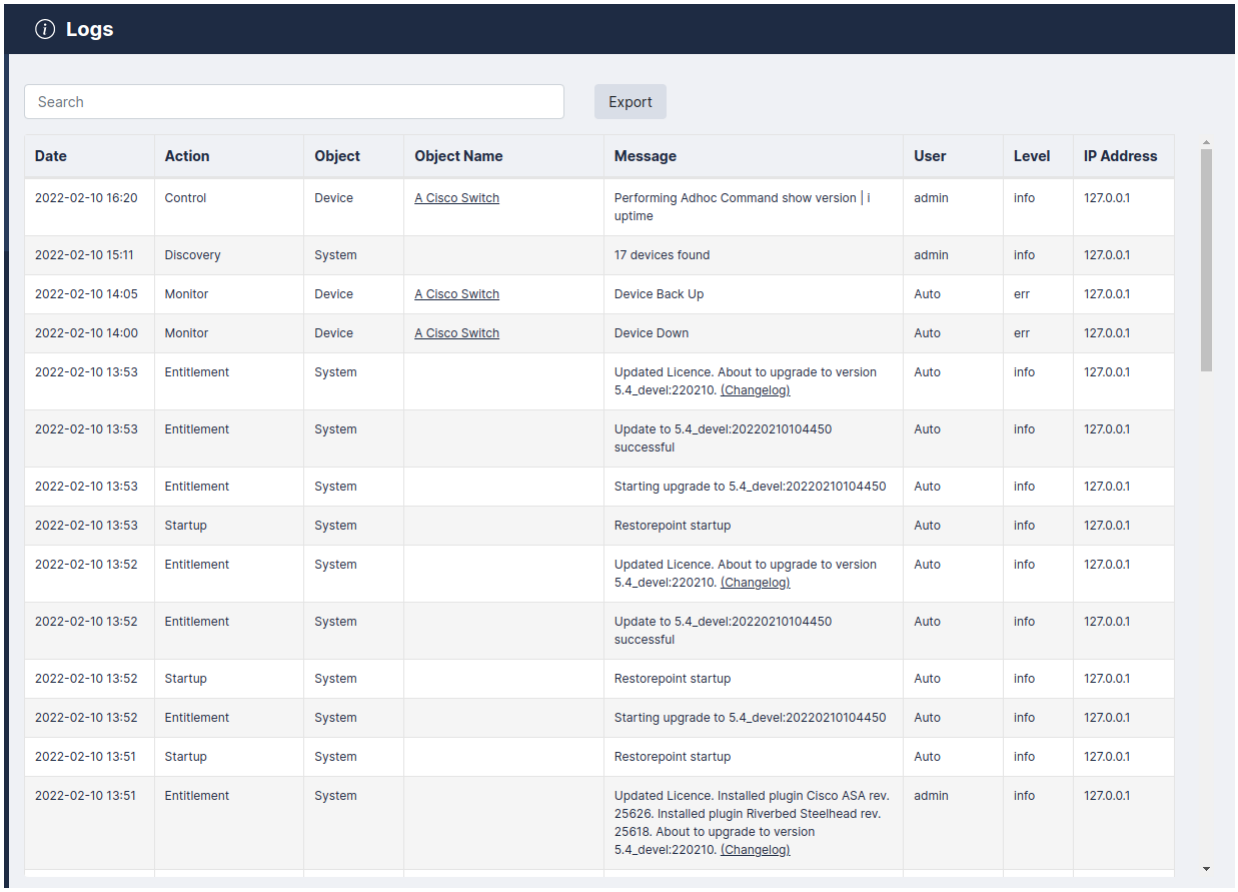
Use the **Export** button to export the event log as a CSV file.

Entries in the system log will be deleted according with the retention policy set in the *Log Settings and Alerts* page.

12.2 Syslog

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

Date/Time	Displays the specific 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 *localhost*



Logs

Search

Export

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

Fig. 12.1: Log page

CHAPTER

THIRTEEN

APPLIANCE ADMINISTRATION

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

13.1 System Settings

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

13.1.1 Network settings

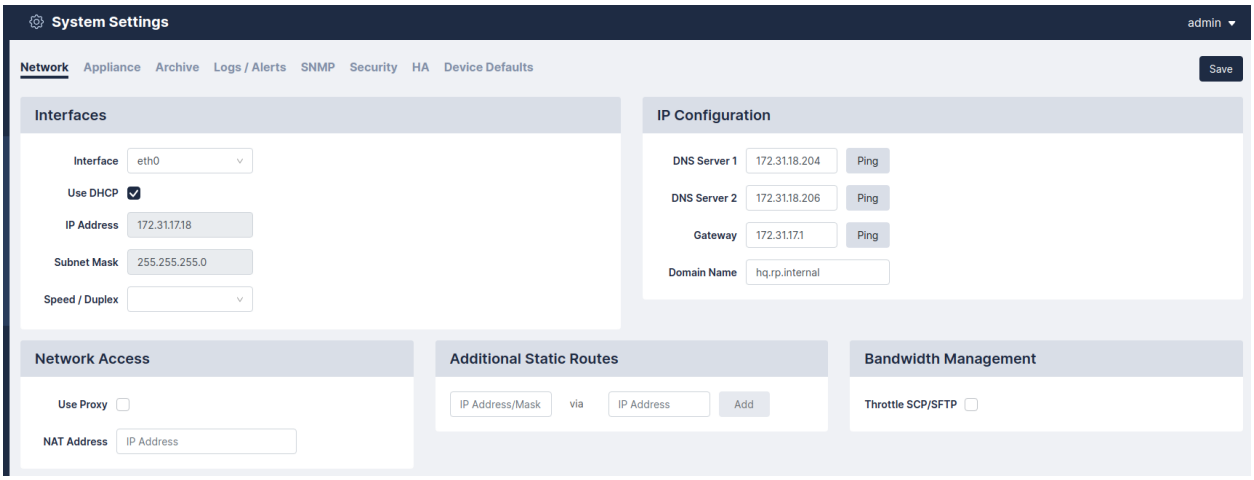


Fig. 13.1: Network settings

13.1.1.1 Network Interfaces

Use the pull-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.

13.1.1.2 Primary / Secondary Interface

Use the **Network** tab to set or update the network address for Restorepoint. The initial settings are usually entered when you first set up your appliance. Select your **Interface** first, and then apply your settings. The fields are as follows:

Use DHCP	If you use DHCP for your interface, the other options will be disabled.
IP Address	The IP address of the Restorepoint appliance.
Subnet Mask	The subnet mask associated with the IP address.
Speed/Duplex	The link speed and duplex can be specified here.

13.1.1.3 IP Configuration

DNS Server	The DNS server address for your network. The DNS server must be able to resolve public names (for example, *support.restorepoint.com*), otherwise the appliance cannot retrieve software updates and license details.
DNS Server 2 (optional)	A second DNS server.
Gateway	The default gateway for your network. You can **Ping** these servers to check connectivity.
Domain Name	Default domain name.

Click the **Save** button to apply any changes.

13.1.1.4 Network Access

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

- IP address of the proxy server.
- Proxy port.
- Username/password, if your proxy requires authentication; leave blank otherwise.

  Use the **Test Proxy** button to verify that the configuration is correct.

13.1.1.5 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, proceed as follows:

- On your firewall, create a 1:1 NAT mapping (often referred to as Static NAT or Mapped IP) to translate the IP address of Restorepoint to a public/routable IP address.
- 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 also needs to be selected in any device which is accessed by Restorepoint through NAT (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.

13.1.1.6 Additional Static Routes

If the devices to be added to Restorepoint are located on different networks, you may need to define additional static routes. The fields are as follows:

- **IP Address / Mask length**: enter the network address/netmask (in CIDR notation).
- **Via IP address**: enter the destination gateway IP address.
- Click **Add**.
- Click the **Save** button to apply changes.

To remove a static route:

- Click **Delete** next to the static route you want to remove.
- Click the **Save** button to apply changes.

13.1.1.7 Bandwidth Management

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

13.1.2 Appliance Operations

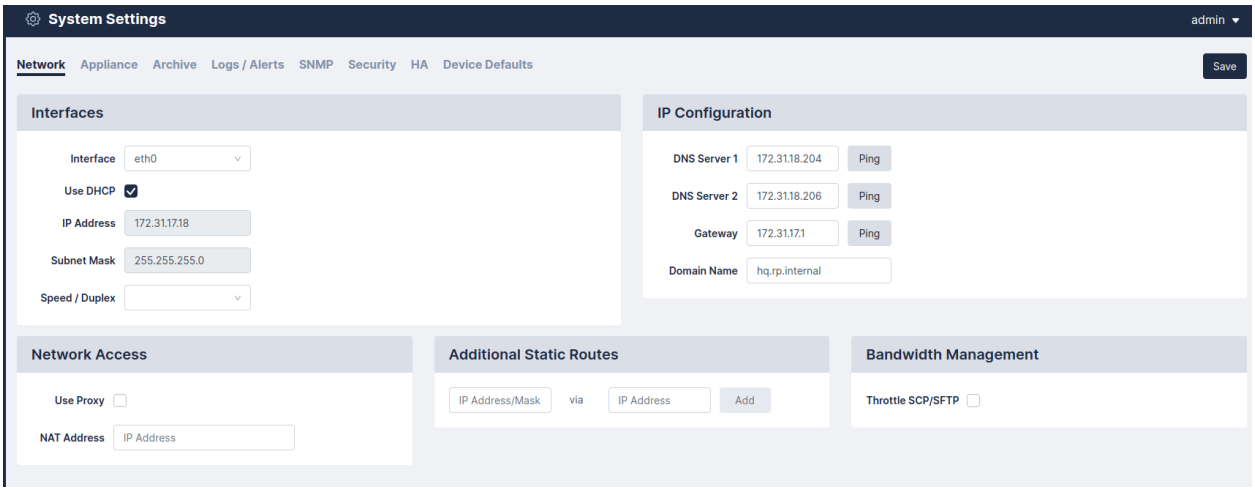


Fig. 13.2: Appliance operations

13.1.2.1 Platform

Restart software	Restarts the Restorepoint daemon. 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	Clicking **Start** enables 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* (see *Firewall Requirements* for notes on firewall configuration).
Open Console	Generates an appliance debug file that may help Technical Support diagnose your issue. **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. **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	What Restorepoint should do when returning from a power-off state, if it should *Run Due Backups*, and treat any missed backups as Overdue, or *Recalculate Schedules* and just return to the normal backup schedule.

13.1.2.2 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 the best results, the logo should be exactly 30 pixels tall and up to 150 pixels wide, and no more than 40KB in size. Clicking **Revert** will return the logo to the default Restorepoint logo.

You can customise the user interface for Domain users in the Domains page (see *Managing domains*).

13.1.2.3 Software Updates

See *System Updates*.

13.1.2.4 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*.

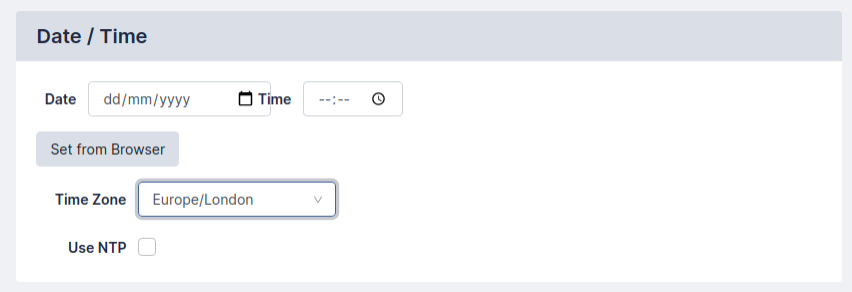


Fig. 13.3: Date and time configuration

13.1.3 System Archive

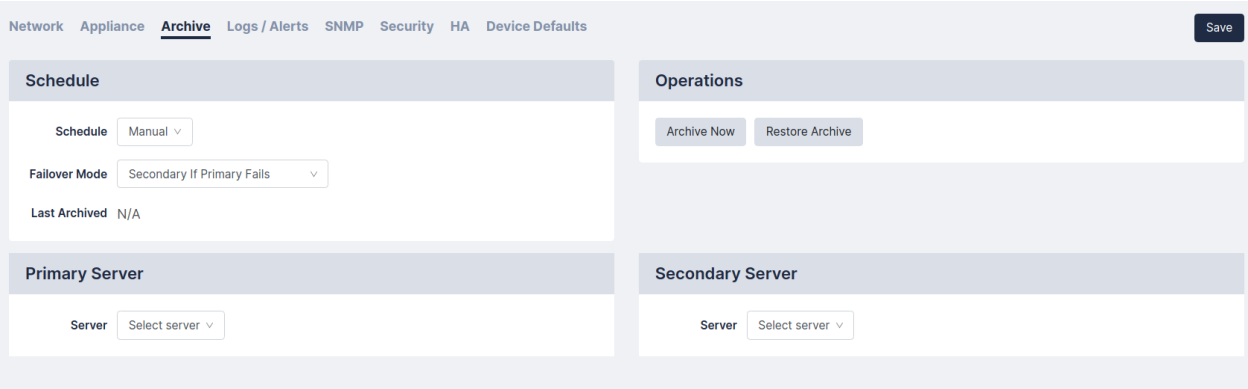


Fig. 13.4: Archive configuration

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

13.1.3.1 Taking an archive

You can define the following settings for archiving:

Frequency	Select Manual, Daily, Weekly or Monthly from the drop down menu.	
Policy	Selects the behaviour when two servers are defined:	
	Use both servers if defined	creates an archive on both servers
	Use secondary only if primary fails	creates an archive on the primary server; only uses the secondary if the primary is unavailable.
On Failure	If the scheduled archive fails for any reason, you may want to have the archive operation wait until the next scheduled operation (*Revert to Schedule*), *Retry after ``x`` hours*, or stop attempting to archive the system automatically (*Set to Manual*).	

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

For each Archive Server, you can define the following:

Retain	Enter the maximum number of archives to keep on the remote server. When this number is reached, older archives will be removed.
Type	What each archive should contain. A *Full Archive* 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 the **Save** button to apply changes.
- Click the **Archive Now** button to start a manual archive operation.

13.1.3.2 Restoring from an archive

Restoring from an archive allows you to quickly recover from a failure; for instance, when installing a replacement appliance after a hardware problem. In order to restore the appliance from an archive, proceed as follows:

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 that you will need the password and encryption password for the *admin* account in order to complete the operation.

13.1.3.3 Workstation DB Archives

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

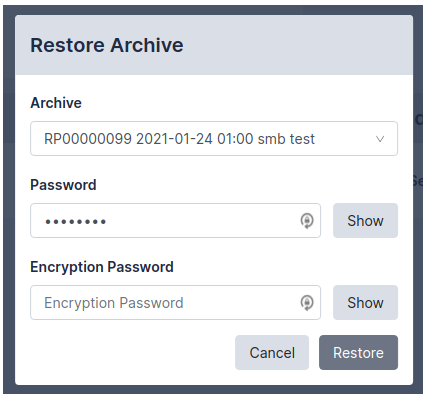


Fig. 13.5: Choosing an archive to restore

13.1.4 Log Settings and Alerts

Use the log settings and alerts section to define your default log retention policy, and the email address for system error notifications. The fields are as follows:

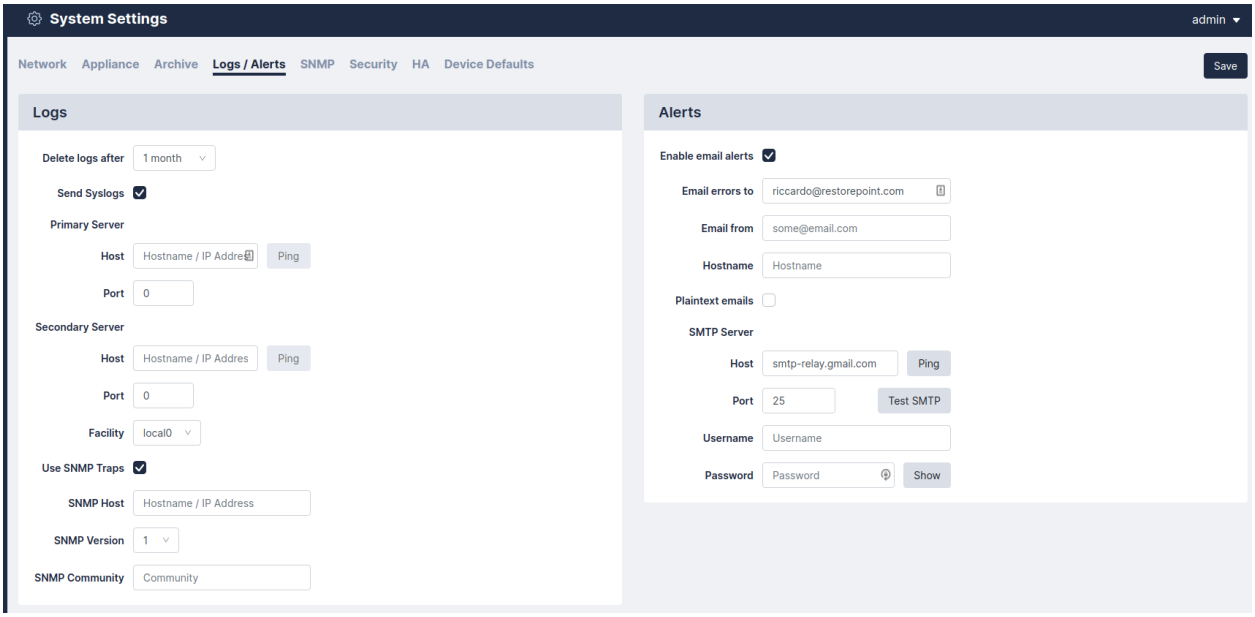


Fig. 13.6: Logs and notification settings

Delete logs after	Events older than this value are permanently deleted from the system. The default value is one month.
Send Syslogs	Tick this box 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	Tick this box 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	An email address for notifications.
Email errors from	The sender email address to be used for notifications.
SMTP Server/Port	The IP address of your mail server. Your mail server must be configured to allow Restorepoint to relay to internal and external recipients.
SMTP User-name/Password	If your SMTP server requires authentication, use this fields to enter the necessary credentials.
Plain-text Emails	Tick this box if you prefer plain text emails instead of HTML.
Prevent Email alerts	Tick this box if you wish to suppress all email notifications.

Click the **Save** button to apply changes.

13.1.5 SNMP

If your network has a Network Management System, you can use SNMP to perform some basic monitoring of the Restorepoint appliance. Restorepoint supports SNMP v1, v2c, and v3. In order to configure SNMP, proceed as follows:

- Choose which SNMP versions should be enabled by clicking on 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, a username must be defined. Depending on the SNMP v3 security level chosen, additional integrity/encryption passwords and integrity/encryption algorithms will need to be specified.

Click the **Save** button to apply changes.

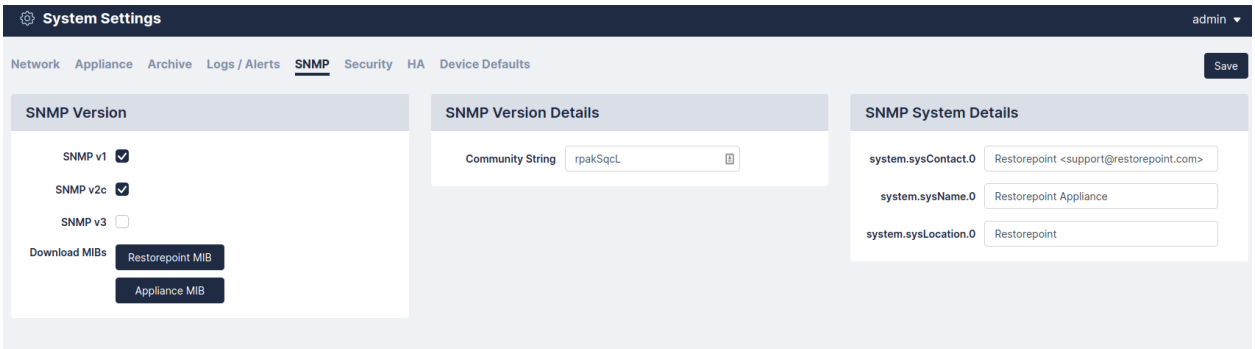


Fig. 13.7: SNMP configuration

13.1.6 Security

The **Security** tab allows you to configure various global settings to mandate a higher level of network security for the Restorepoint appliance. Setting some of these options may cause compatibility problems with legacy devices and clients.

13.1.6.1 Protocol Versions

This section allows you to specify the minimum version of TLS used by the Restorepoint UI, and when communicating with devices. You can also prevent Restorepoint from falling back to SSHv1, if TLS is unavailable.

13.1.6.2 Services

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

13.1.6.3 HTTPS Certificate

Click the **Change** button to modify the HTTPS certificate used by Restorepoint. This dialog appears:

The **Type** dropdown 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.

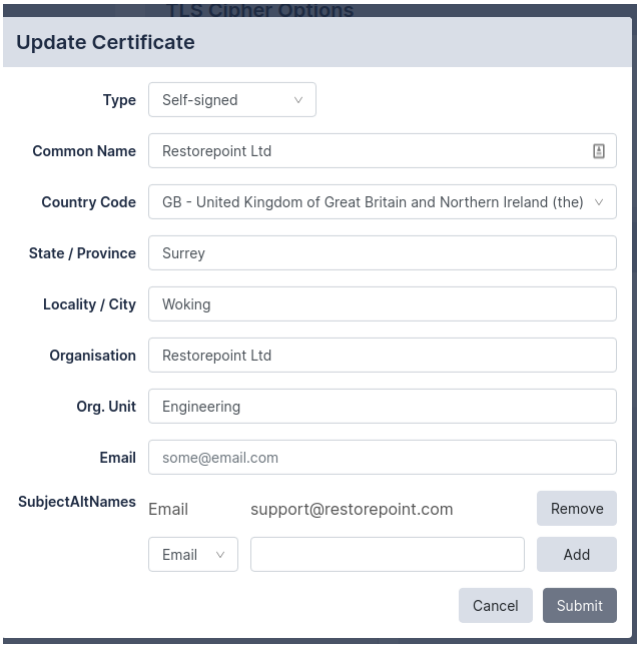


Fig. 13.8: HTTPS Certificate dialog

13.1.6.4 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 *60 minutes*.
Console Timeout	How long to keep a session for the VM Console open without an action. Default value is *15 minutes*.
Expire User Passwords	Allows you to automatically force users to change their password after a given length of time. This setting can be overridden on a per-user basis (See *Managing Users* for more information).

13.1.6.5 Admin Allowed Networks

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

13.1.7 High Availability

High Availability (HA) provides a way to minimise 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 instance, just after a backup is retrieved from a device) and by performing full synchronisations on a regular basis.

Should the primary member become unavailable because of hardware failure, other network problem, or 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.

13.1.7.1 HA Requirements

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

13.1.7.2 Creating a cluster

To create a cluster, on the primary appliance:

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

On the secondary Restorepoint appliance:

1. Click **Join Cluster**.
2. Enter the same shared secret used on the Primary.
3. Enter the IP Address of the Primary appliance.
4. Click **Save**. The cluster will now perform the initial full sync.

Once the cluster has been created, this screen can also be used to monitor the status of the cluster, or leave the cluster.

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

The **Leave Cluster** button can be used to break the cluster; all synchronisation will stop, the two appliances will keep the existing configuration and carry on independently.

CHAPTER

FOURTEEN

LABELS

There is a new feature called Labels. Labels will mainly be used to filter and group devices.

Labels can be created by users and can be confined to a specific domain. When a new device is created, or an existing device is editted, then it is possible to set the Labels for that device. There is a field called Labels in the Device Details that contains a drop down box of all the available Labels. There is also an option in this drop down box to define new Labels, by selecting "Add new".

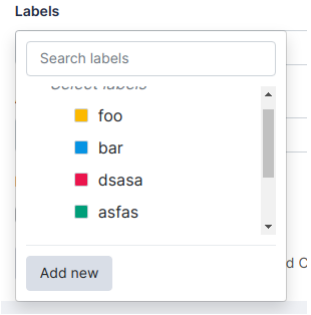


Fig. 14.1: Labels

These options are described in *Adding a new user*.

The following link is to 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 particular office, a user always works with a particular 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 only the relevant devices are seen by the user

CHAPTER

FIFTEEN

SAML

A “Single Sign On” (SSO) option has now been made available via SAML authentication.

The configuration for this is found in the following location:

Administration > Auth Servers > SAML tab

In the SAML tab there are 2 fieldsets:

1. Service Provider Settings
2. Identity Provider Settings

Fig. 15.1: Fieldsets

To set up SAML, complete the following steps:

1. Take the “ACS URL” and “Entity ID” values that appear in the Service Provider Settings
2. Put these values into whatever the relevant part of your SAML IdP is. 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. Press Save. This will upload the metadata to Restorepoint, which should then handle everything from then on

Now that SAML is setup, a new button will appear on the login page called “Login with SSO”. This button can be clicked on without entering any values into any 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

SIXTEEN

SYSTEM UPDATES

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 plugin updates
- Licence updates.

Ensure that your firewall is configured correctly to allow system updates (see *Firewall Requirements* for notes on firewall configuration).

16.1 Disabling automatic updates

Although we strongly recommend that all updates are automatically applied, you may wish to override this behaviour by ticking **Disable Automatic Version Upgrades**.

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

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, allowing you to force an update manually.

16.2 Manual updates

If Restorepoint is deployed on an isolated network and cannot connect to the update server, it can still be updated manually. If this is the case, **This appliance is not connected to the Internet** should be ticked. Clicking **Manual Upgrade** displays instructions 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 licence details) must be manually performed by the administrator.

CHAPTER

SEVENTEEN

GETTING HELP

Click the **Help** menu to display the Restorepoint contextual help for the 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**).

17.1 Error messages

17.1.1 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 typically happens because the device has been replaced. If this is the case, edit the device in question and click **Clear Cache** near **SSH Public Key**.

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 for 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 re-occurring 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: ensure 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: ensure 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.

17.1.2 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: log in 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. Ensure that no firewall is 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 used, 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 ticking **This appliance is not connected to the Internet** in the **System** page.

Licence expired

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

Solution: contact your Restorepoint Account Manager.

17.2 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 with the *admin* account and select **System Shell**.

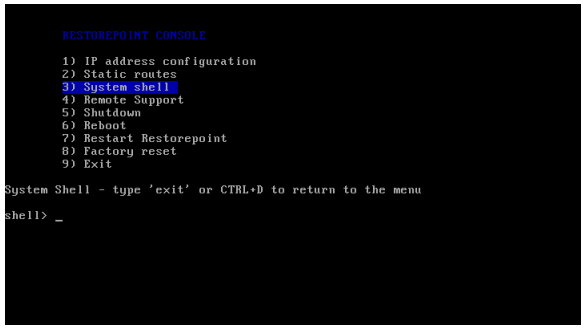


Fig. 17.1: System shell

The commands available are:

help	Lists the available commands.
ping	Sends an ICMP Echo Request packet to a network host.
traceroute	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.

17.3 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** the information stored on the appliance, not just the system settings. In particular:

- The encryption key will be destroyed
- 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 : in order 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:

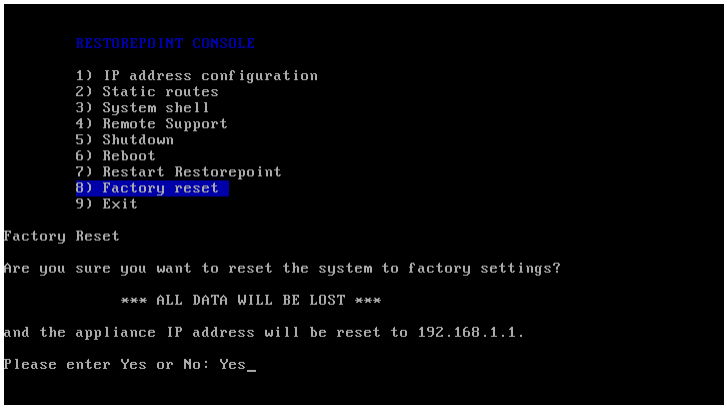


Fig. 17.2: Factory reset procedure

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.

17.4 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

Ensure 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, ensure 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

Make sure 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 allow to relay email to your SMTP server. You will also need to have specified a valid email account which notifications are sent to.

Scheduled tasks are not running

Make sure 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 endeavour 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).

17.5 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 UK time Monday to Friday, excluding UK public holidays. Technical support is also available through your reseller.

17.6 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 licence.

CHAPTER

EIGHTEEN

COPYRIGHT AND CONTACT INFORMATION

18.1 Copyright Notice

18.2 Trademarks

18.3 Contact Details


```
Restorepoint Ltd
Unit 4, Tannery House
4 Tannery Lane
Send
Woking
Surrey GU23 7EF
United Kingdom
```

Telephone: +44 844 571 8120

General Enquiries: info@restorepoint.com

Sales Enquiries: sales@restorepoint.com

Support Enquiries: support@restorepoint.com