

MultiPortal - Alpha Release

Installation Guide and Documentation

Important - Alpha Expiry	3
Important - VM ID	3
Alpha Release Information	3
Important Information	3
How You Can Help	3
System Requirements	4
Hardware Requirements	6
Prerequisites	6
Pre-installation checklist	6
1. A fresh install of Ubuntu	6
2. SSL Requirements	7
Installation Guide	8
Download MultiPortal	8
System Setup	8
Update Guide	9
Getting Started	9
MultiPortal Setup	9
Your first login to MultiPortal	9
Creating a Proxmox API User	10
Connecting your first Data Center	10
Adding a Storage Policy	13
Configuring Your VM ID Starting Point	14
MultiPortal Configuration	14
Documentation	14
Data Centers	14
Storage Policies	14
System Hierarchy, User Levels and Roles	15
Virtual Data Center	15
Networking	16
External Networking	16
Internal Networking	16
Console Server	16
API Documentation	16
Troubleshooting	17
SSL Certificate	17
Caddy Server Runtime Logs	19

Caddy Server Logs	20
Updating Caddy Configuration for Logging	20
Scripted Update	20
Error Logs	21
Known Issues	21
ISO Management	21
Release Notes	22
Overview of Changes	22
New Features	22
Bug Fixes & Improvements	22

Important - Alpha Expiry

If your Alpha has expired follow the steps outlined below in the Update Guide section.

Important - VM ID

Before creating your first VM, ensure you update the "Begin Proxmox VM ID At" setting to the next available ID in your Proxmox environment. This step is crucial to prevent the system from hanging while it attempts to find the next available ID.

Steps to Update:

1. Click on **Settings** in the left menu.
2. Click on **Global Configurations**.
3. Find "**Begin Proxmox VM ID At**" and set the ID (default is 1000).
4. Click **Save**.

You can now create your VMs.

Alpha Release Information

Please note that this version v0.5.0 is only intended for testing and evaluation purposes and should not be used in a production environment.

Important Information

- **Release Status:** This is an Alpha release, indicating that the application is in its early stages of development. Expect frequent updates and changes.
- **Expiration Date:** The Alpha release v0.5.0 has an alpha licence key applied and will be valid during the Alpha testing phase.
- **Usage Caution:** Due to the experimental nature of the Alpha release, there may be bugs, instability, or incomplete features. Use with caution and report any issues you encounter.

How You Can Help

Your feedback is invaluable to us during this Alpha testing phase. Please help us improve by reporting any bugs, usability issues, or suggestions for improvement.

On each page, you will find a feedback button. Feel free to use this button to provide feedback specific to the current page you're on.

System Requirements

The following table shows the recommended system requirements for running **MultiPortal**.

Requirement	Recommended
Proxmox VE	Release: 8.1 Version: 8.1.3
Operating System	Ubuntu 22.04
Web Server	CaddyServer
Database	MariaDB server
PHP Version	8.2
PHP Memory Limit	128MB
PHP Extensions	Fpm, common, curl, gd, mbstring, Mysql, opcache, xml, xmlrpc, imagick, zip
ionCube Loader®	12.0.1 or later for PHP 8.2
Additional Software	Git, Node.js, npm, composer
Networking MTU	9000

Note: The setup installation script will configure the underlying requirements if you have an up-to-date Ubuntu 22.04 server.

Hardware Requirements

The hardware requirements may vary based on the individual workload. However, a general recommendation is:

Requirement	Description
CPU	2 GHz or better
RAM	At least 4GB of RAM is recommended for optimal performance, but this may vary depending on the application's complexity and expected traffic.
Storage	At least 25GB free, large environments with multiple data centres and large numbers of VMs should consider increasing this to 100GB+

Prerequisites

Pre-installation checklist

- A fresh install of Ubuntu Server v22.04
- DNS records (FQDN) pointing to your Ubuntu (MultiPortal) server
- Port 443 is open to your Ubuntu (MultiPortal) server
- Direct access to the internet (Not using Proxy managers)

1. A fresh install of Ubuntu

The Alpha release of MultiPortal requires an up-to-date installation of Ubuntu 22.04, and a fresh installation is recommended.

The MultiPortal setup script currently can't handle when the system requires interaction after doing an update. To ensure that the script runs smoothly, please ensure that you have run the following commands before running the MultiPortal script:

```
sudo apt update
sudo apt upgrade
```

2. SSL Requirements

- MultiPortal will automatically generate its own valid SSL using LetsEncrypt but requires that it is accessible on port 443 with a valid DNS record (hostname) pointing to the server. The MultiPortal installation script will ask for this hostname.
 - *For example, if your FQDN for MultiPortal is multiportal.example.com then you must configure this as a DNS record and point it to your MultiPortal server and have it publicly accessible on port 443 on your firewall.*
 - **Note:** You can close port 443 after installation and once the SSL has been validated, but please note that future automatic SSL renewals will fail. *Future releases may allow for offline SSL installation.*
- MultiPortal must communicate with your Proxmox environments via a valid SSL certificate.
 - When configuring a Data Center within MultiPortal you must use a secure FQDN for example <https://proxmox.example.com>. Failure to do so will result in the console feature not working.
 - Your certificate Common Name (CN) and FQDN must match the instance you are connecting to.
 - Proxmox documentation on installing an SSL can be found at: https://pve.proxmox.com/wiki/Certificate_Management

Installation Guide

- [Installation Video of Installing MultiPortal on Ubuntu - Alpha Video Guide](#)

Download MultiPortal

To download MultiPortal run the following command

```
wget https://downloads.multiportal.io/multiportal-installation.tar
```

Once downloaded, extract the installation folder

```
tar -xvf multiportal-installation.tar
```

This will create a new directory called multiportal-installation, which contains multiportal and a setup.sh script, which you will use in System Setup.

System Setup

To set up the system for MultiPortal use, follow these steps:

1. Begin with a fresh installation of Ubuntu 22.04.
2. Change to the directory to where the multiportal-installation folder was extracted to
3. Make the setup file executable by running the following command:

```
chmod +x setup.sh
```

4. Execute the setup script with administrative privileges:

```
sudo ./setup.sh
```

5. Next, you will be asked to enter your domain name.
6. This will take a few minutes to install depending on your internet connection while it installs all the required dependencies
7. The script will generate output files to a designated folder.
8. Following this, the script will proceed to configure your Linux virtual machine.
9. Once the setup is complete, you can access your server instance through your web browser.

Update Guide

If you already have MultiPortal setup, and need to update your instance, follow these steps:

1. Follow the Download MultiPortal steps mentioned above
2. Change to the directory to where the multiportal-installation folder was extracted to
3. Make the update file executable by running the following command:

```
chmod +x update.sh
```

4. Execute the update script with administrative privileges:

```
sudo ./update.sh
```

5. Next, you will be asked to enter the domain name for your current MultiPortal instance for the update script to find your instance location.
6. The script will update your multiportal instance with the newer version.
7. Once the update is complete, you can access your server instance through your web browser.

Getting Started

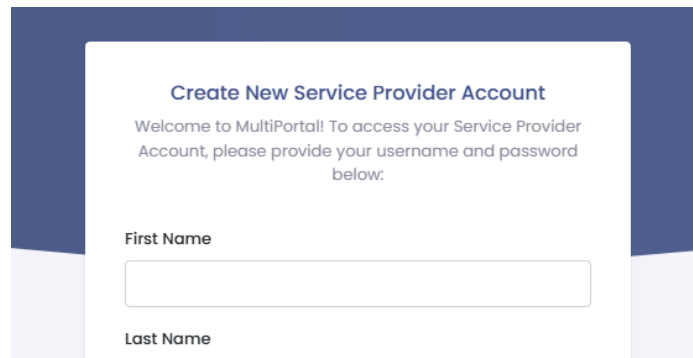
MultiPortal Setup

- [MultiPortal Setup - Alpha Video Guide](#)

Your first login to MultiPortal

Once you have completed the System Setup section, the hostname that you entered during setup will now be configured, allowing you to browse your application. Navigate to the FQDN you entered during installation (for example, <https://multiportal.example.com>).

Follow the instructions to create a new Service Provider account, which will act as your primary account for accessing MultiPortal.



Create New Service Provider Account

Welcome to MultiPortal! To access your Service Provider Account, please provide your username and password below.

First Name

Last Name

Creating a Proxmox API User

For MultiPortal to be able to access your Proxmox environment, you first need to create a new API user within your Proxmox environment.

To create an API user in Proxmox VE, follow these steps:

1. Log in to the Proxmox VE web UI.
2. Navigate to "Datacenter" from the left-hand navigation menu.
3. Select "Users" from the left sub-navigation menu.
4. Click on the "Add" button at the top of the main content area.
5. Enter the desired username as "API" and choose the realm as the Proxmox VE authentication server. Set and confirm a password for the user, then click "Add".
6. Now, navigate to "API Tokens" from the left sub-navigation menu.
7. Select "API@pve" as the username.
8. Enter a secret key into the "Token ID" field
9. Uncheck Privilege Separation, and click "Add".
10. Copy both the displayed Token ID and Secret to a text document for future use.
11. Close the dialogue box.
12. Proceed to "Roles" from the left sub-navigation menu.
13. Click on the "Create" button at the top of the main content area.
14. Name the new role "APIAdmin" and select all available privileges. Click "Create".
15. Next, go to "Permissions" from the left sub-navigation menu.
16. Select "Add User Permission" at the top of the main content area.
17. Set the path to "/", choose the "API@pve" user, and assign the role as "APIAdmin". Click "Add".

Connecting your first Data Center

After creating the Proxmox API user, you must integrate it into your MultiPortal installation.

Follow these steps:

1. Within MultiPortal, navigate to Settings -> Data Centers and click “Create Data Center”.
2. Fill in the address of your Proxmox environment. You must use a FQDN for the Address and API URL (e.g. <https://myproxmox.com:8006/>) By default, the API URL ends in /api2 unless specified otherwise in your Proxmox environment.

Please note: MultiPortal can only connect to a single Proxmox address, if you have multiple nodes in a cluster, we recommend using a reverse proxy (such as HAProxy) to balance the requests across all nodes.

<p>Proxmox Address</p> <p>The Proxmox address you want to connect to (eg https://myproxmox.com.au:8006/).</p> <input type="text"/>
<p>API URL</p> <p>The Proxmox API address (eg https://myproxmox.com.au:8006/api2).</p> <input type="text"/>

3. Next, you'll need to enter your Username and Password of the API User created in the previous section.
The username structure should be `username@pve`.

<p>Proxmox Username</p> <p>Created when setting up API credentials. This username is used to connect to the console of a VM.</p> <input type="text"/>
<p>Proxmox Password</p> <p>Created when setting up API credentials. This password is used to connect to the console of a VM.</p> <input type="text"/>

4. Your Token ID and Secret are what you copied in the last steps of creating the Proxmox API user.
Your Token ID follows the format: `username@pve!%secretkey%`.

Token ID This was the Token that was created when setting up the API credentials.
<input type="text"/>
Secret This was the Secret that was created when setting up the API credentials.
<input type="text"/>

After entering your Proxmox environment's details, click "Test API".

You will receive the message "Successfully Connected to the API Server" if everything is entered correctly.

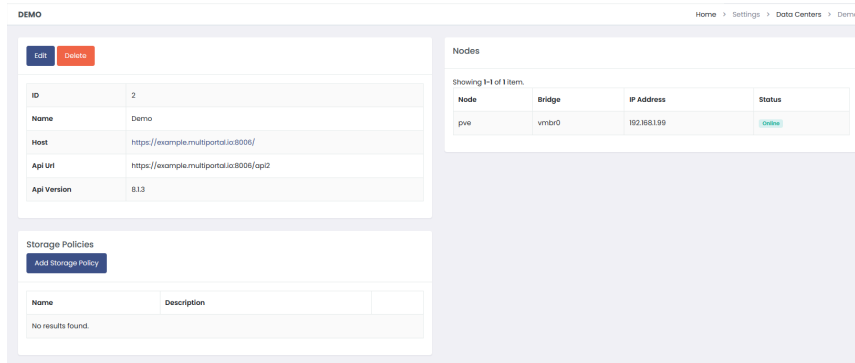
API Version The Proxmox API version. (This will populate after testing the connection).
<input type="text" value="8.1.3"/>
<input type="button" value="Test API"/> <input type="button" value="Save"/>
Successfully connected to the API server. Release: 8.1 Version: 8.1.3

Once you've confirmed connectivity, click Save.

Repeat the process for additional Proxmox environments.

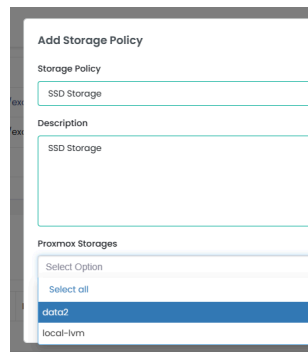
Adding a Storage Policy

After setting up a new Data Center in Multiportal, you'll be taken to the Data Center overview page. You'll find details about the nodes, storage, and any created Storage profiles here.

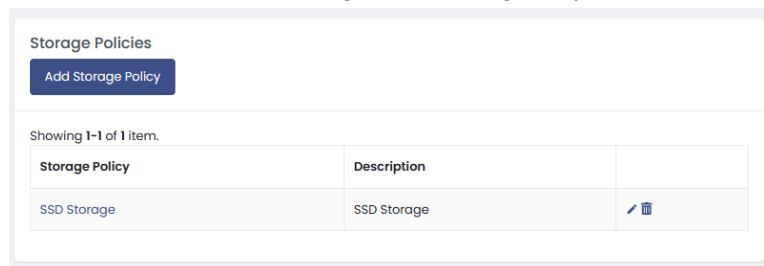


Before proceeding, you must create a Storage Policy for the Data Center. Storage Policies act as a friendly naming and grouping of underlying Proxmox storage. (*See the Documentation section below for more details*)

To create a Storage Policy, simply click "Add Storage Policy," give it a friendly name (Users will see this), and then select the storage volumes you'd like included within it.



Once created, you will now be able to assign this storage to your Virtual Data Centers.



Configuring Your VM ID Starting Point

Before creating your first VM, ensure you update the "Begin Proxmox VM ID At" setting to the next available ID in your Proxmox environment. This step is crucial to prevent the system from hanging while it attempts to find the next available ID.

Steps to Update:

1. Click on **Settings** in the left menu.
2. Click on **Global Configurations**.
3. Find "**Begin Proxmox VM ID At**" and set the ID (default is 1000).
4. Click **Save**.

You can now create your VMs.

MultiPortal Configuration

Following the initial setup of MultiPortal, the next step is to create a reseller, tenant, Virtual Data Center (VDC), and Virtual Machine.

Please follow the instructions in the video below to complete those steps

- [MultiPortal Configuration - Alpha Video Guide](#)

Documentation

Data Centers

Data Centers are the friendly name of your Proxmox environment. By default, you need to configure at least one Data Center, but you can create additional Data Centers for each Proxmox environment you want to connect into MultiPortal.

Storage Policies

Storage Policies are friendly groupings of storage available within Proxmox. For example, if you have several different storage volumes, you could group them based on performance.

- Slow Performance / SATA = Bronze Storage Policy
- Standard Performance / SAS = Silver Storage Policy

- High Performance / SSD = Gold Storage Policy

When a Tenant creates a virtual machine disk, they choose a storage policy to assign the disk, and the virtual disk is created on the least used storage volume within the Storage Policy.

Storage quota assignment is based on the Storage Policy when creating Virtual Data Centres.

For example, you may create a Virtual Data Center with a type of “Allocation” with 100GB from the above Bronze Storage Policy and 1000GB from the Gold Storage Policy. A virtual machine might then have two disks, one on each of the storage policies available or maybe both on a single storage policy.

System Hierarchy, User Levels and Roles

MultiPortal has three different levels of users.

- **Service Provider** - This is the top system administrator level
- **Reseller** - Resellers are the first customer layer designed to be used in wholesale environments.
- **Tenant** - Tenants are the second customer layer and below a Reseller. They also own the Virtual Data Centers.

MultiPortal ships with standard Roles but Service Providers can create and edit the roles from the administration section.

Virtual Data Center

A Virtual Data Center is a collection of resources and virtual machines that always belong to a Tenant and reside in a single Data Center.

There are two types of Virtual Data Centers

- **Allocation:** This type is where a quota is assigned. When the quota for CPU and RAM is reached Virtual Machines can no longer be powered in. However, Virtual Machines can still be created up until the allocated Storage Policy quota has been reached.
- **PAYG** - This type is the traditional cloud model where an unlimited quota is assigned and the system tracks the usage on an hourly basis for billing based on consumption. Storage Policies still need to be allocated however no quota can be assigned.

Networking

MultiPortal handles networking by using the SDN feature of Proxmox. It creates VLAN and VXLAN VNet as External and Internal networks.

Important: Switches and Proxmox environments should be configured with MTU 9000 to meet the requirements of VXLAN.

External Networking

Each external network adds a VLAN VNet in Proxmox allowing VLANs from the wider network to be connected directly to VMs in MultiPortal. This is typically used to connect machines such as virtual routers to WAN VLANs or a VM or Virtual Data Center to another network outside of MultiPortal.

Internal Networking

Each internal network creates a VXLAN VNet as an isolated private network. This is typically used to create an internal LAN network for virtual machines to talk to each other.

Console Server

The console server is an internal node application that is executed alongside MultiPortal, this creates a secure WebSocket connection to your Proxmox server. This is automatically started once the application has been installed and is checked every minute to ensure the server is running.

The server uses PM2, a node application monitoring tool to monitor and control the node application.

To manually check to see if the service is running, you can run the following:

```
sudo pm2 list
```

MultiPortal is designed to handle the console server itself, if you encounter any issues trying to connect to a VM via console, please report this via the feedback button on each page.

API Documentation

With the release of version 0.5.0, MultiPortal now includes an API that allows you to perform most actions available through the browser. This feature enables you to interact with your instance programmatically from other systems.

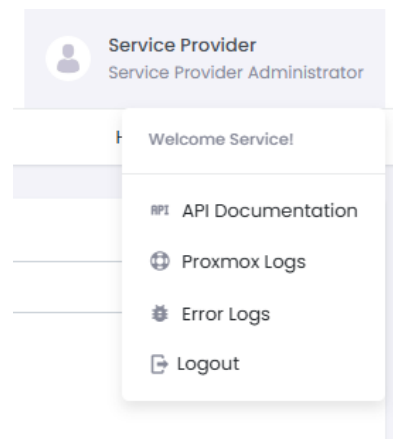
Getting Started:

1. Generate an OAuth Token:

- Navigate to the settings menu.
- Click on "OAuth Clients."
- Select "Generate OAuth Client" to create a new client. Note that the redirect URL is preset to '/'.

2. Access API Documentation:

- Click on the profile menu at the top right of the screen.
- Select "API Documentation."
- You will be redirected to the Swagger view of the API.



You can automatically import this documentation into Postman or any other tool you use for API interactions.

Troubleshooting

SSL Certificate

MultiPortal utilises CaddyServer to host the application and automatically generates an SSL certificate using LetsEncrypt. This process requires port 443 to be open and the Fully Qualified Domain Name (FQDN) to be correct.

The Caddyfile is located at `/etc/caddy/Caddyfile` and directly points to your installation folder at `/var/www/yourhostname`.

First, confirm whether CaddyServer is running correctly:

```
systemctl status caddy
```

```
● caddy.service - Caddy
   Loaded: loaded (/lib/systemd/system/caddy.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-04-11 21:34:03 UTC; 2h 44min ago
     Docs: https://caddyserver.com/docs/
   Main PID: 707 (caddy)
    Tasks: 13 (limit: 9387)
   Memory: 46.1M
     CPU: 2.190s
   CGroup: /system.slice/caddy.service
           └─707 /usr/bin/caddy run --environ --config /etc/caddy/Caddyfile
```

Caddy may take a few minutes to obtain your certificate during its initial run. It will continue attempting, but after several failed attempts, LetsEncrypt may block CaddyServer from obtaining a certificate for some time. The output of the preceding command will indicate whether it is currently blocked or successful.

You can manage the service using the start, stop, and restart commands. If CaddyServer is not running, MultiPortal will be unreachable.

Start Caddy

```
systemctl start caddy
```

Stop Caddy

```
systemctl stop caddy
```

Restart Caddy

```
systemctl restart caddy
```

Manually running caddy can provide a more detailed output when trying to troubleshoot your instance, to do this make sure caddy has been stopped and then run the following command

```
/usr/bin/caddy run --environ --config /etc/caddy/Caddyfile
```

The output will display INFO and WARN messages in the console

```
2024/04/12 00:46:48.832 INFO using provided configuration {"config_file": "/etc/caddy/Caddyfile"}
2024/04/12 00:46:48.837 WARN Caddyfile input is not formatted; run 'caddy fmt --overwrite' to fix i
2024/04/12 00:46:48.840 INFO admin admin endpoint started {"address": "localhost:2019", "enforce
2024/04/12 00:46:48.840 INFO http.auto_https server is listening only on the HTTPS port but has no
2024/04/12 00:46:48.840 INFO http.auto_https enabling automatic HTTP->HTTPS redirects {"serv
2024/04/12 00:46:48.840 INFO tls.cache.maintenance started background certificate maintenance
2024/04/12 00:46:48.845 INFO http enabling HTTP/3 listener {"addr": ":443"}
2024/04/12 00:46:48.846 INFO http.log server running {"name": "srv0", "protocols": ["hl", "
2024/04/12 00:46:48.846 INFO http.log server running {"name": "remaining_auto_https_redirec
2024/04/12 00:46:48.846 INFO http enabling automatic TLS certificate management {"domains": ["
2024/04/12 00:46:48.922 INFO autosaved config (load with --resume flag) {"file": "/root/.confi
2024/04/12 00:46:48.922 INFO serving initial configuration
2024/04/12 00:46:48.936 WARN tls storage cleaning happened too recently; skipping for now
6:48.936", "try_again_in": 86399.999999298}
2024/04/12 00:46:48.936 INFO tls finished cleaning storage units
```

Caddy Server Runtime Logs

To obtain the system logs for the Caddy server, run the following command:

```
journalctl -u caddy.service --since "2024-07-01 00:00:00" --until
"2024-07-01 23:59:59" > caddyLogs.log
```

This command will generate a log file named `caddyLogs.log` containing the journal entries for the Caddy service from the start of July 1, 2024, until the end of the day.

Adjust the date and time to collect the information within the required period.

Download this file from your server and send it to support when requested to help assist in troubleshooting.

Caddy Server Logs

The installation of MultiPortal is configured to output error messages from the Caddy server to a specific log file. This log file is located in the `/var/log/caddy` directory and is named according to your domain. For example, if your domain is `yourdomain.com`, the log file will be `/var/log/caddy/yourdomain.com.log`.

Download this file from your server and send it to support when requested to help assist in troubleshooting.

Updating Caddy Configuration for Logging

Original installations of MultiPortal did not have logging set up in the Caddy configuration for your instance. You can update the Caddyfile manually or run a script to do it for you.

1. Locate the Caddyfile:
The Caddyfile is located at `/etc/caddy/Caddyfile`.
2. Edit the Caddyfile:
Open the file in a text editor and add the following code at line 21 (replace `yourdomain.com` with the domain name you used for your MultiPortal installation):

```
log {  
  output file /var/log/caddy/yourdomain.com.log  
  level error  
}
```

Scripted Update

Alternatively, you can download and run the `caddyLogFixer.sh` script to automatically update your configuration.

1. Download the Script:

```
curl -O https://downloads.multiportal.io/scripts/caddyLogFixer.sh
```

2. Make the Script Executable:

```
chmod +x caddyLogFixer.sh
```

3. Run the Script:

```
./caddyLogFixer.sh
```

The script will prompt you for the hostname of your MultiPortal installation and will update the Caddyfile accordingly.

Error Logs

MultiPortal now includes an easy to access error log feature within the portal to assist with troubleshooting. When issues or errors occur, you may be asked to share this information with support.

To download the error logs:

1. Click on the profile menu at the top right of the screen.
2. Select "Error Logs" from the dropdown menu.
3. Click "Download" to save the logs to a file.

You can then share this file with support to help resolve the issue.

Known Issues

ISO Management

Uploading and Downloading ISOs

- **Requirement for ISO Storage:** When using the "Upload" or "Download from URL" functions in the ISOs catalogue, ensure that the selected storage has the "ISO image" content type enabled within Proxmox.
- **Multiple Storage Types:** You can assign multiple storage types to each storage policy. It's possible to add a separate Proxmox storage to existing storage policies if you have a separate storage location for ISOs.

Uploading ISOs

- **Form Reset Issue:** Some instances have experienced the Upload ISO form resetting after an ISO is uploaded. We are currently troubleshooting the cause of this issue.

Workaround for Form Reset:

- If you encounter the form reset issue after uploading an ISO, please follow these steps:
 1. Manually upload the ISO file to a public directory.
 2. Obtain the public link to the uploaded ISO file.
 3. Use the "Download from URL" function in the ISOs catalogue and paste the public link to download the ISO directly.

We apologise for the inconvenience and appreciate your patience as we work to resolve this issue.

Release Notes

Release Version: 0.5.0

Release Date: 24th July 2024

Overview of Changes

This release includes fixes for various bugs, feedback-based improvements, and task completions. It addresses issues related to VM creation, error handling, and performance enhancements.

New Features

1. Introduced the MultiPortal API.
2. Implemented task history tracking.
3. Enhanced ISO management.
4. Introduced the ability to customise the application's branding.
5. Added snapshot management functionality.
6. Added granular bandwidth settings at the storage policy level.
7. Added subnet details to external and internal networks.

Bug Fixes & Improvements

1. Improved ISO and hardware allocation.
2. Enhanced query performance throughout the system.
3. Improved page load speed for VDC.
4. Fixed login issue with no error message for invalid passwords.
5. Added alert for incomplete hardware attachment.

6. Fixed an issue when creating a VM failed if the ID was already in use.
7. Improved error handling during network creation.
8. Improve Proxmox resource overcommitment.
9. VM Create Form now correctly displays error messages.
10. Updated VDC and VM forms to display memory in GB instead of MB.
11. Addressed issue where VMs marked as unknown after moving to another host.
12. Resolved error that occurred when disabling a VDC and clicking 'save.'
13. Fixed MultiPortal issue where VMs migrated via the Proxmox portal showed incorrect status.
14. Fixed issue where the firewall was activated on NIC but not under options.
15. Resolved issues where certain hardware changes were ignored while the VM was running.
16. Improved logging efficiency.
17. Updated storage policies display at the VDC level.
18. Corrected storage calculations to account for boot order.
19. Resolved validation errors in new VDCs that caused loss of storage policy.
20. Enhanced handling of unavailable licence servers.
21. Fixed error encountered when creating an internal network.
22. Fixed error with PAYG totals showing a limit
23. Fixed error adding new network to VM with existing network: Null Firewall Parameter.