Student: Willie de Klerk

Year: 3

Student No: 20230254

Module: WIL730

Document: Reflection Report

WIL Mentor: Hennis de Klerk

Declaration of Authenticity

A critical aspect of any assignment is *authenticity*. Because you are completing much of the work for the assignments *unsupervised*, the examiner must be convinced that it is all your work. For this reason, you must complete the *Declaration of Authenticity* provided in the study guide and have it counter-signed by your manager, mentor, or lecturer.

NB	The declaration of authenticity is a legal document, and if found that you have made a false declaration, then not only will your results be declared null and void, but you could also have criminal charges brought against you. It is not worth taking the risk!

Please complete the declaration of authenticity below for all assignments:

DECLARATION OF AUTHENTICITY

I _____WILLIE DE KLERK_____ hereby

declare that the contents of this assignment are entirely my work except for the following documents: (List the documents and page numbers of work in this portfolio that were generated in a group)

Activity	Date
WIL730/630	**2025/09/01**

Signature: _____ Recoverable Signature X Willie de Klerk Student (20230254) Signed by: 7e38ac48-8902-42d6-b32e-8740bcbddb0d _____ **Date:** _2025/09/01__

Table of Contents

CTU Training Solutions WIL Placement Notice

At the time of writing in 2025, CTU Training Solutions does not provide Higher Education Diploma Network Design & Administration students with placement opportunities to complete their work integrated learning at a company.

Network design students, myself included were informed that we should find our own companies willing to accommodate us for 80 hours of work integrated learning in our second and third-year studies. This is a catch 22 situation, since we are required to complete work integrated learning in our second and third-year studies. If we do not complete our work integrated learning module, we are unable to obtain our diploma, regardless of what our marks are for the rest of our subject modules.

If you are able to help change this situation by offering short-term mentorship or guidance to students, please contact CTU Training Solutions. +27 18 290 5340

Description of work experience and intended learning outcomes.

WIL730 Mentor

I completed my work integrated learning module remotely under mentorship of Hennis de Klerk.

Hennis de Klerk is a Network Specialist and IT administrator at Your Computer Man with 26+ years of experience. His daily responsibilities include IT network and server infrastructure planning and deployment for seven newspapers across the South African landscape.

With his guidance, expertise and patience I deployed and configured various applications that can be utilized during daily business operations in a business environment. Despite having the same last name, we are not family.

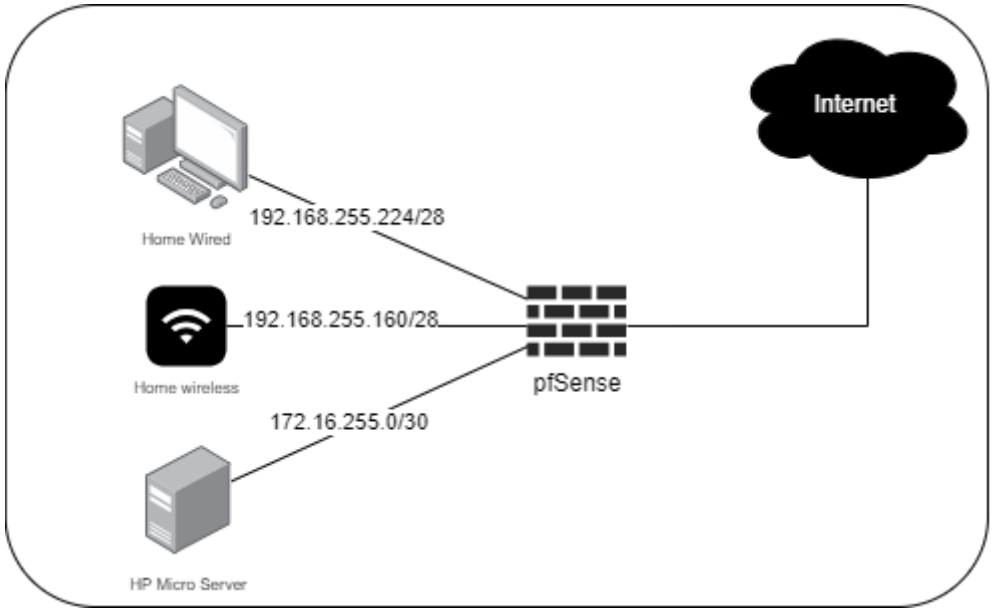
Tasks delegated to me

Some of the tasks delegated to me included:

1. Installing and configuring an open source, enterprise grade storage solution on a HP Micro Server.
2. Installing Cloudflared and a proxy solution used for containerized applications hosted on TrueNAS.
3. Deployment of NextCloud.
4. Installing and utilizing the Community Edition of Portainer.
5. Setting up Authentication through OAuth with Microsoft Entra ID to enhance security on portainer.

Network Layout

In this segment I will be describing my home network and the firewall rules that I have configured to maintain network security. Additionally, I will be performing connectivity testing between the server and my home network, as well as the server and the internet to validate my firewall configuration.

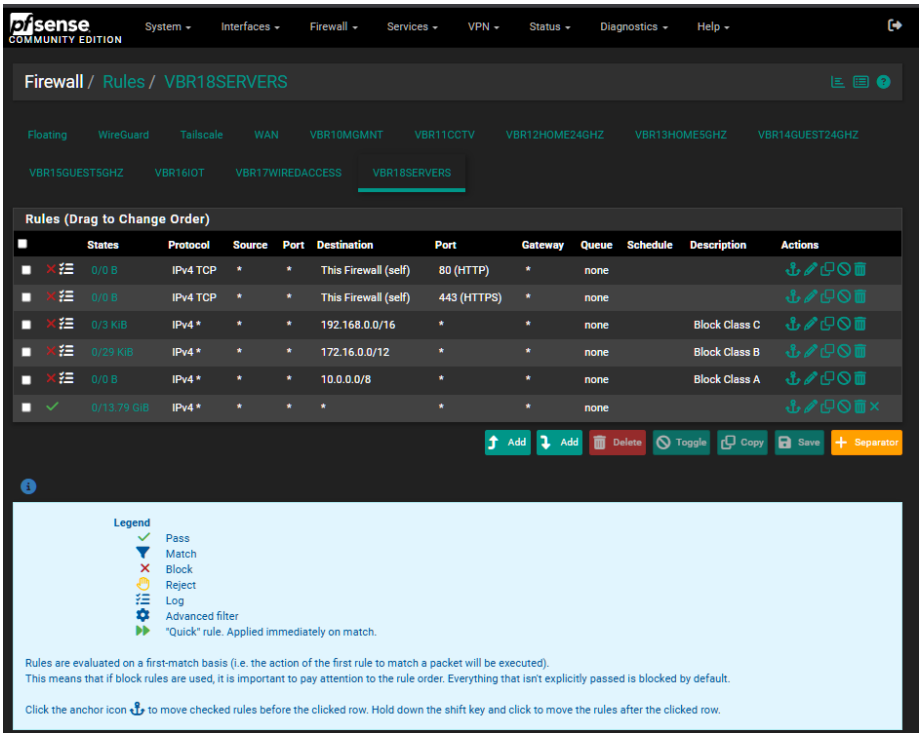


1 Simplified home network layout

To refresh your memory I suggest the subnetting deep dive with Kevin Wallace. (Kevin Wallace Training, LLC, 2023)

Firewall Configuration

Firewall Rules

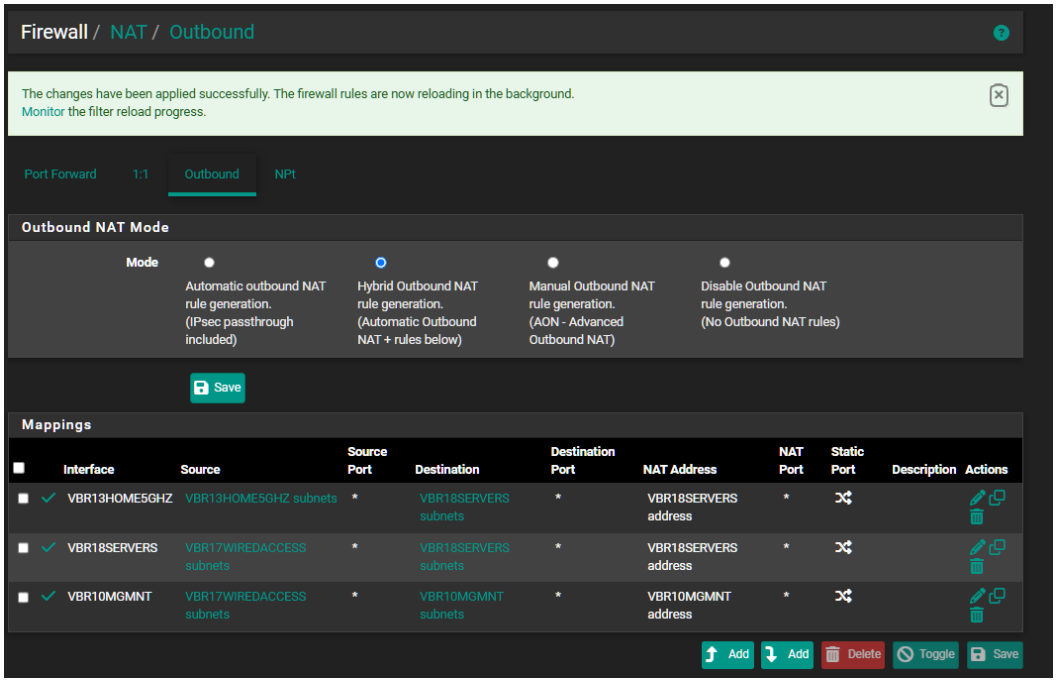


2 Firewall rules configured on the interface on which the micro server is connected to my home network.

(docs.netgate.com, 2025)

I am blocking connections to the Class A, B and C private addressing spaces. (www.iana.org, 2025) This will prevent anyone from entering my home network when they connect from the internet through the cloudflared container and cloudflare tunnel on the HP Microserver.

Network Address Translation (NAT)



3 Outbound Network Address translation mappings.

The mappings above allow me to access the server from my home network, without the server knowing the actual source IP address is from my home wired or wireless network. In a business environment this would have the benefit of allowing us to utilize the full bandwidth of local interfaces securely.

An example related to bandwidth:

My ISP provides me with a 50mb/s, full duplex, symmetric connection. My home network has 1gb/s LAN ethernet ports. Without the NAT rules, I would only be able to access the server at 50mbp/s (I can do 50 upload and download at the same time).

With the NAT rules, I can do close to the full 1gb/s upload and download at the same time. In a business environment where there may be staff located on premises, this would allow more people to work at the same time.

Result of the firewall configuration

```
willie@truenas:~$ ping 192.168.255.226 -c 5 -v
ping: sock4.fd: 3 (socktype: SOCK_RAW), sock6.fd: 4 (socktype: SOCK_RAW), hints.ai_family: AF_UNSPEC

ai->ai_family: AF_INET, ai->ai_canonname: '192.168.255.226'
PING 192.168.255.226 (192.168.255.226) 56(84) bytes of data.

--- 192.168.255.226 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4076ms

willie@truenas:~$ # With the command issued above, I am testing connectivity between the server and my home network.
willie@truenas:~$ # Ping works with ICMP echo request and reply packets, the server sent out five requests but
willie@truenas:~$ # it did not receive a single reply, with 100% packet loss since I am blocking instead of
willie@truenas:~$ # rejecting the connection from being made.
willie@truenas:~$ # 20230254@ctucareer.co.za
willie@truenas:~$
```

4 Testing connectivity between the server and my home network, from the server to a device on the home network. The rules work as intended if packet loss is 100%

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/

PS C:\Users\willie> ping 172.16.255.2

Pinging 172.16.255.2 with 32 bytes of data:
Reply from 172.16.255.2: bytes=32 time=1ms TTL=63
Reply from 172.16.255.2: bytes=32 time=1ms TTL=63
Reply from 172.16.255.2: bytes=32 time=1ms TTL=63
Reply from 172.16.255.2: bytes=32 time=1ms TTL=63

Ping statistics for 172.16.255.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\willie>
```

5 Testing connectivity between the server and my home network, from a home network device to the server. The outbound NAT works as intended if the packet loss is 0%

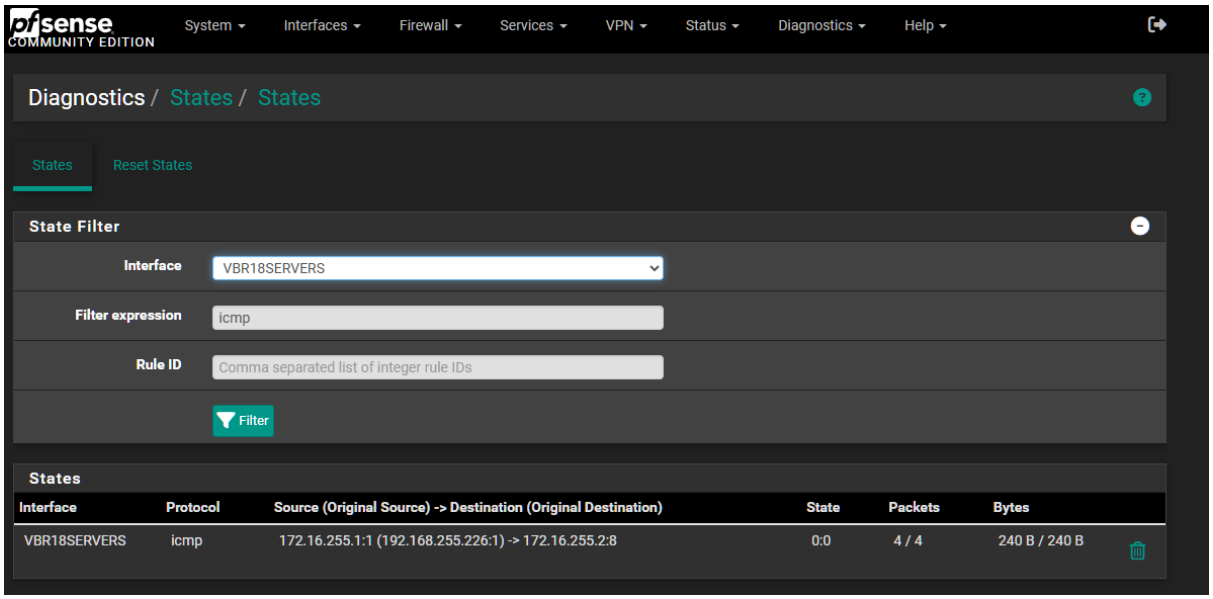


Figure 6 Connection States in pfSense, indicating that the network address translation is working as intended.

```
willie@truenas:~$ ping google.com -c 5 -v
ping: sock4.fd: 3 (socktype: SOCK_RAW), sock6.fd: 4 (socktype: SOCK_RAW), hints.ai_family: AF_UNSPEC

ai->ai_family: AF_INET, ai->ai_canonname: 'google.com'
PING google.com (172.217.170.142) 56(84) bytes of data.
64 bytes from tzjnba-ae-in-f14.1e100.net (172.217.170.142): icmp_seq=1 ident=35785 ttl=116 time=9.09 ms
64 bytes from tzjnba-ae-in-f14.1e100.net (172.217.170.142): icmp_seq=2 ident=35785 ttl=116 time=9.65 ms
64 bytes from tzjnba-ae-in-f14.1e100.net (172.217.170.142): icmp_seq=3 ident=35785 ttl=116 time=9.32 ms
64 bytes from tzjnba-ae-in-f14.1e100.net (172.217.170.142): icmp_seq=4 ident=35785 ttl=116 time=9.39 ms
64 bytes from tzjnba-ae-in-f14.1e100.net (172.217.170.142): icmp_seq=5 ident=35785 ttl=116 time=11.5 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 9.090/9.783/11.466/0.859 ms
willie@truenas:~$ # Testing internet connectivity with a ping test.
willie@truenas:~$ # Internet connectivity is needed to download application images and to create the
willie@truenas:~$ # cloudflare tunnel that is used in combination with the proxy to access the apps
willie@truenas:~$ # hosted on TrueNAS with docker containers.
willie@truenas:~$
```

7 Testing connectivity to internet services from the server.

Tasks

In this section I am describing the tasks that have been assigned to me, as described in the introduction.

Task 1: Installing an open source, enterprise grade storage solution.

As part of my first task, I was asked to install the TrueNAS Community edition operating system on an HP ProLiant Micro Server. TrueNAS is open source, easy to install and to get it up and running. It provides the ability to provide a business of any size with a reliable network attached storage solution. It has easy integration with apps such as the WordPress app.

Tools and Platforms used

Software

1. Etcher – I used etcher to create the installation media.
2. Truenas.iso – I used TrueNAS version 25.04.0

Hardware

1. Generic USB drive

***8** USB drive used for installation media*

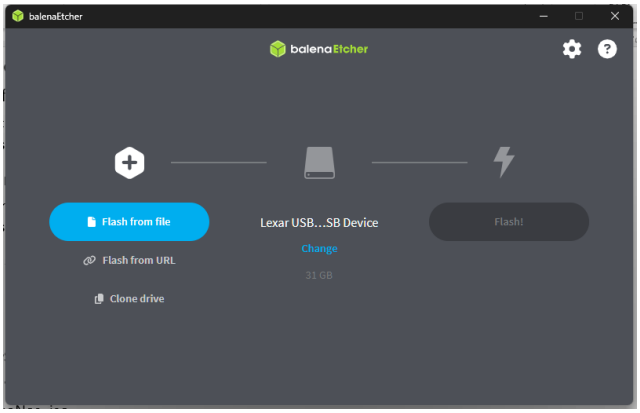
I used a Lexar 32gb usb drive for my installation media. Available from takealot.com.

2. HP MicroServer

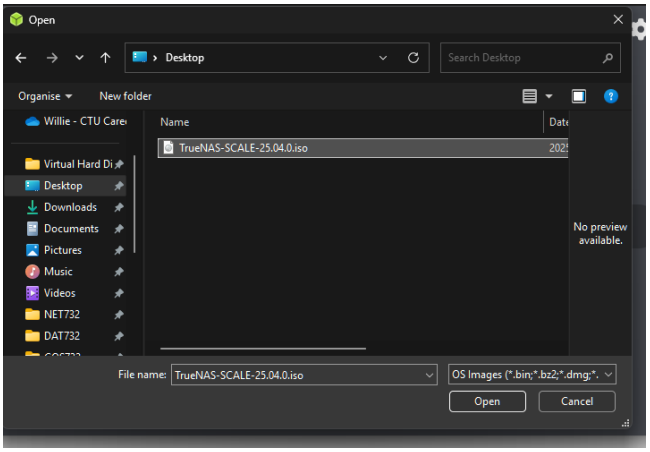
9 HP Micro Server

Creating the Installation Media with Etcher

Step 1: Select Flash From file

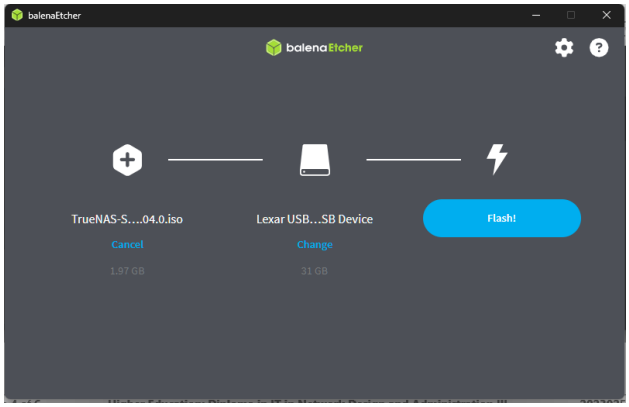


10 Etcher Software

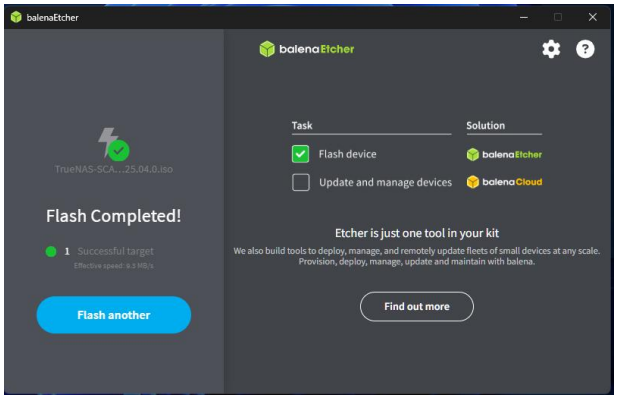


11 Selecting the iso file.

Step 2: Click Flash button



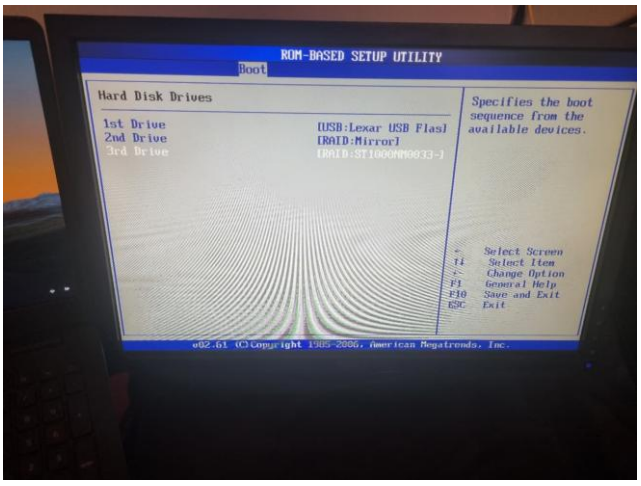
***12** Clicking Flash Button*



13 Creation of Installation media completed

Installing TrueNAS

Checking the drive configuration in bios



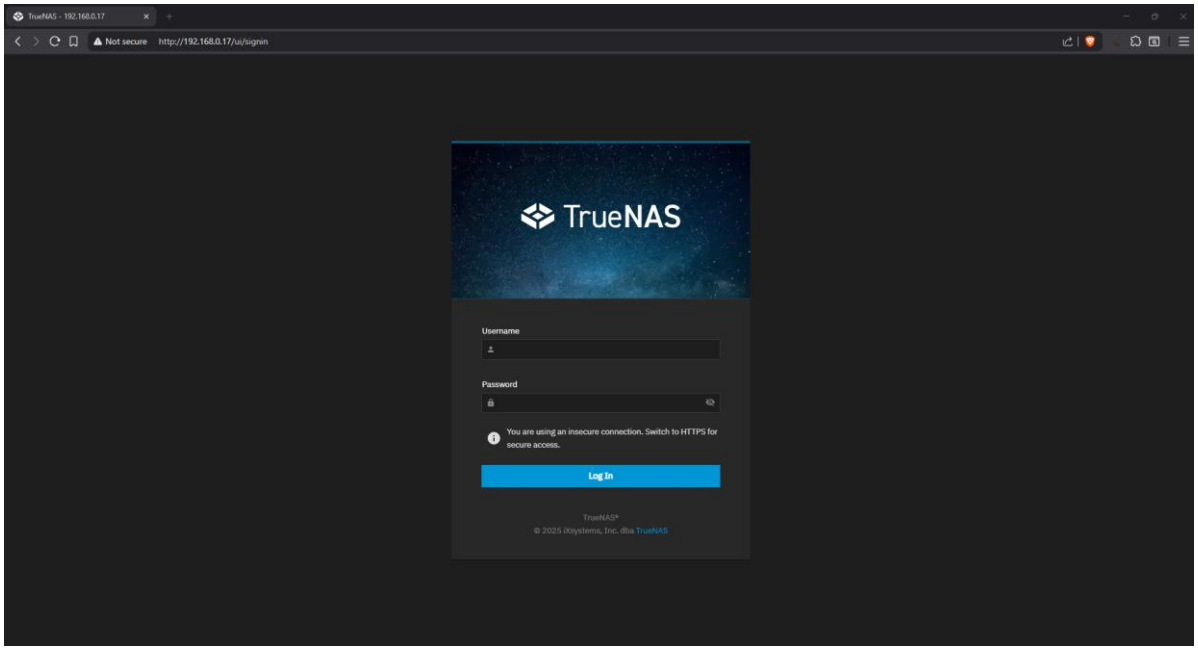
***14** Server hard disk configuration*

The Server is currently populated with two 1tb hard drives, this is confirmed through the information showed in the bios. The controller should not be in Raid Mode. (www.truenas.com,2024)

Installation process

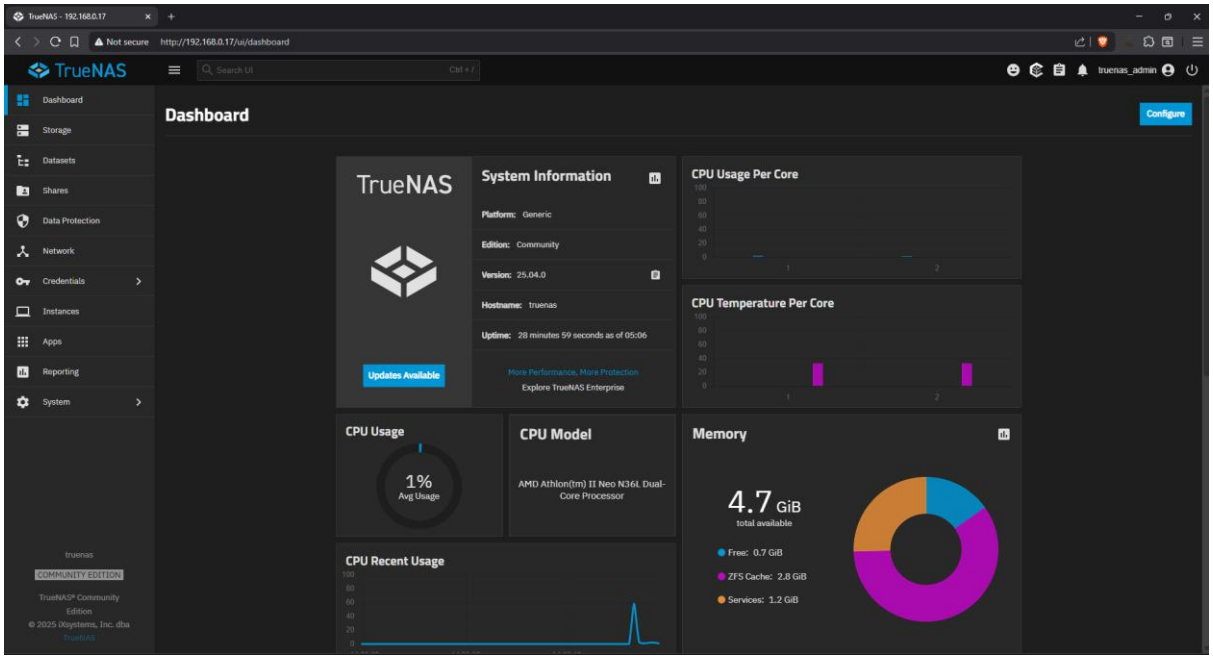
I captured pictures of the installation process, but they are of unsatisfactory quality. At a high level the process involved multiple steps:

1. Selecting to boot the TrueNAS installer. (If you wait long enough it will automatically boot)
2. Choosing to update/install TrueNAS
3. Selecting the installation disk, which should be the correct drive of the raid.
4. Configuring a truenas_admin password.
5. Selecting to reboot & removing installation media.



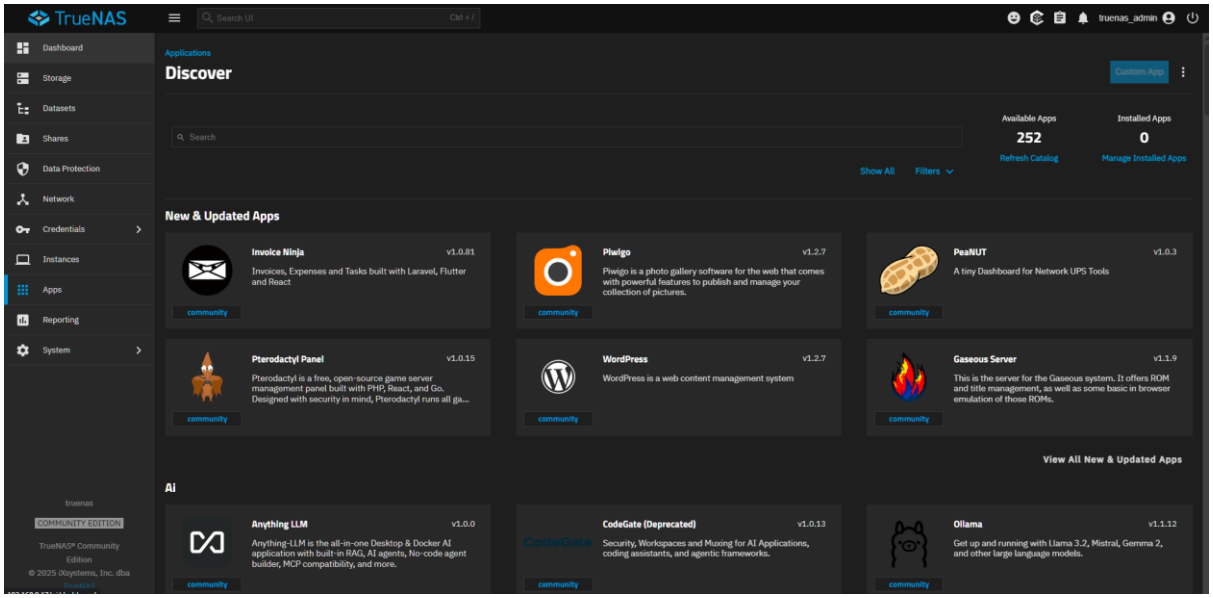
15 TrueNAS web-ui login page. Admin username = truenas_admin

The TrueNas web-ui login page can be configured to work with HTTPs and login with 2FA via OTP. To utilize the 2FA functionality it should be enabled globally in the settings menu. (www.truenas.com,2024)



16 *TrueNAS web-ui dashboard*

The dashboard is displayed each time that we log in to the system. This allows us to catch any relevant surface problems with a quick glance, in addition to the ability to check for updates with the press of a button.



17 *TrueNAS Apps*

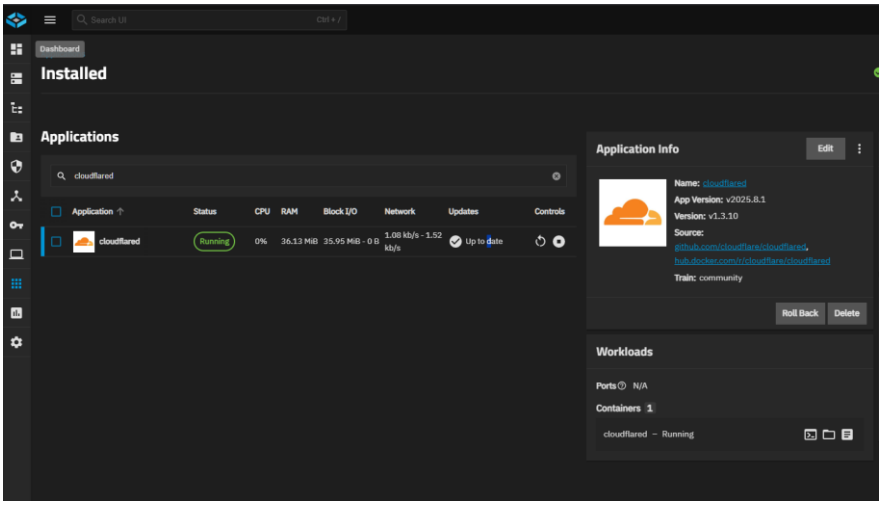
TrueNAS apps are essentially guided containerized deployments. The support for advanced deployment configurations would depend on the application developer. Some applications would allow us to specify a network for the container allowing it to be added to a vlan.

***18** TrueNas Reporting*

The TrueNas Reporting feature allows us to gain valuable insights into the server's resource usage. This is a must have to be able to identify potential system problems, usage trends & anomalies, and for resource capacity forecasting & planning.

Task 2: Installing Cloudflared and a proxy solution used for containerized applications hosted on TrueNAS.

Installing the Cloudflared application.



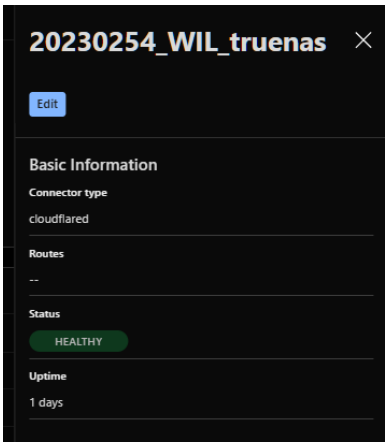
19 Installed TrueNAS Applications filtered with application name search.

Cloudflared App configuration:

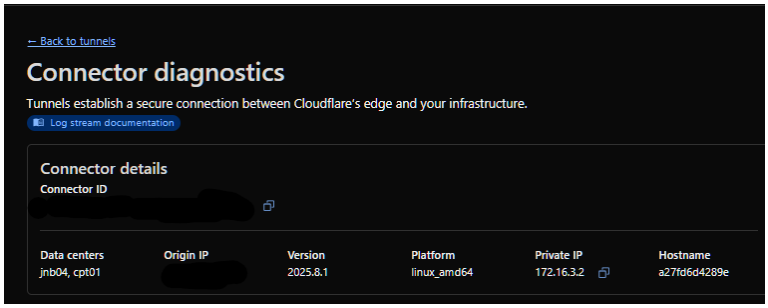
1. Application name
    a. cloudflared
2. Cloudflared Configuration
    a. The mode Tunnel or Proxy DNS. (Tunnel)
    b. Tunnel Token
3. User and Group Configuration
    a. User ID
    b. Group ID
4. Network Configuration
    a. Port Number
5. Resources Configuration
    a. CPUs
    b. Memory (in MB)

20 Cloudflared App configuration

(developers.cloudflare.com, 2025) (www.truenas.com,2025)



21 Viewing the tunnel information in cloudflare dashboard.

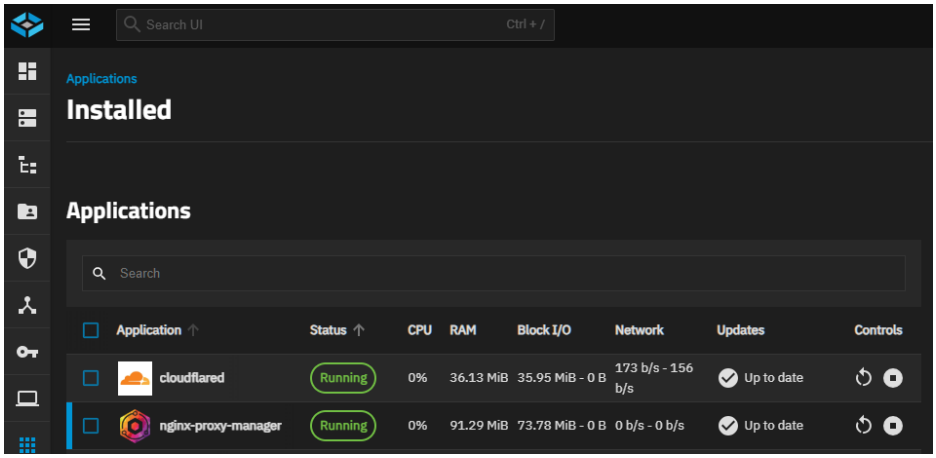


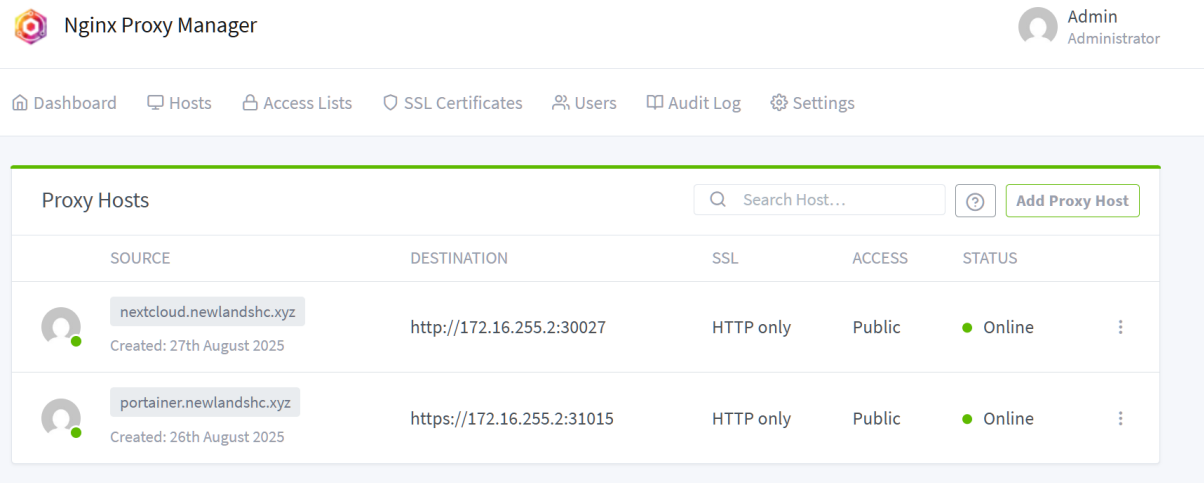
22 Viewing more details about the tunnel.

Installing nginx-proxy-manager

Nginx-proxy-manager App Configuration:

1. Application Name
    a. nginx-proxy-manager
2. Nginx Proxy Manager Configuration
    a. Time Zone ('Africa/Johannesburg')
3. User and Group Configuration
    a. User ID
    b. Group ID
4. Network Configuration
    a. Web UI Port number & Host IP binding (0.0.0.0/0:81)
    b. HTTP Traffic Port (80)
    c. HTTPS Traffic Port (443)
5. Storage Configuration
    a. Data storage (ixVolume)
    b. Certs storage (ixVolume)
6. Resources Configuration
    a. CPUs (1)
    b. Memory MB (512)





23 NGINX Proxy Manager Interface - Proxy hosts

24 Cloudflare Zero Trust Dashboard, viewing the public hostname configurations made with the cloudflared container on the server.

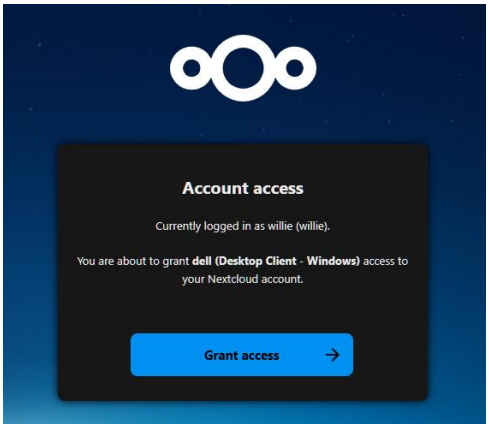
Task 3: Deployment of NextCloud

The NextCloud application allows us to host an open-source content and collaboration platform that can be used remotely in our business environments. At a high level the configuration included:

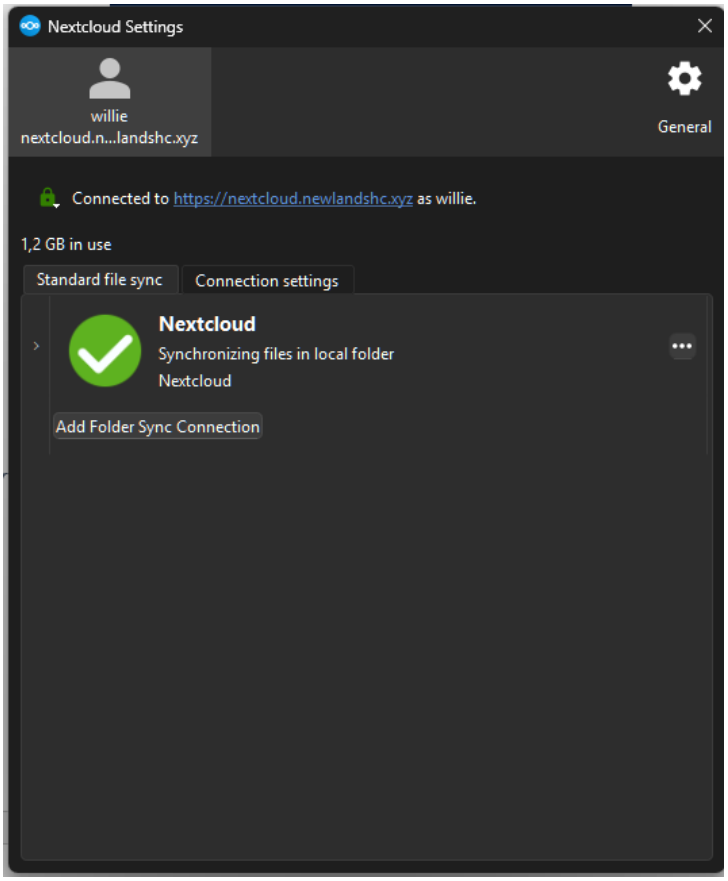
1. Application Name
    a. Nextcloudcontainer
2. Nextcloud Configuration
    a. Postgres Image (17)
    b. Admin username & Password
    c. Host (nextcloud.newlansdshc.xyz)
    d. Data Directory Path (/var/www/html/data)
    e. Redis Password
    f. Database Password
    g. PHP Upload Limit (3 GB)
    h. Max Execution Time (30 seconds)
    i. PHP Memory Limit (512)
    j. Enable Cron Jobs (schedule: */5 * * * *)
3. Network Configuration
    a. Web UI Port
        i. Port Bind Mode (Publish port on the host for external access)
        ii. Port Number (30027)
        iii. Host IPs (0.0.0.0)
4. Storage Configuration
    a. Nextcloud AppData Storage (ixVolume created automatically by system)
    b. Nextcloud User Data Storage (ixVolume created automatically by system)
    c. Nextcloud Postgres Data Storage (ixVolume created automatically by system)
5. Resources Configuration
    a. CPUs (1)
    b. Memory (1024MB)

25 Nextcloud App Configuration

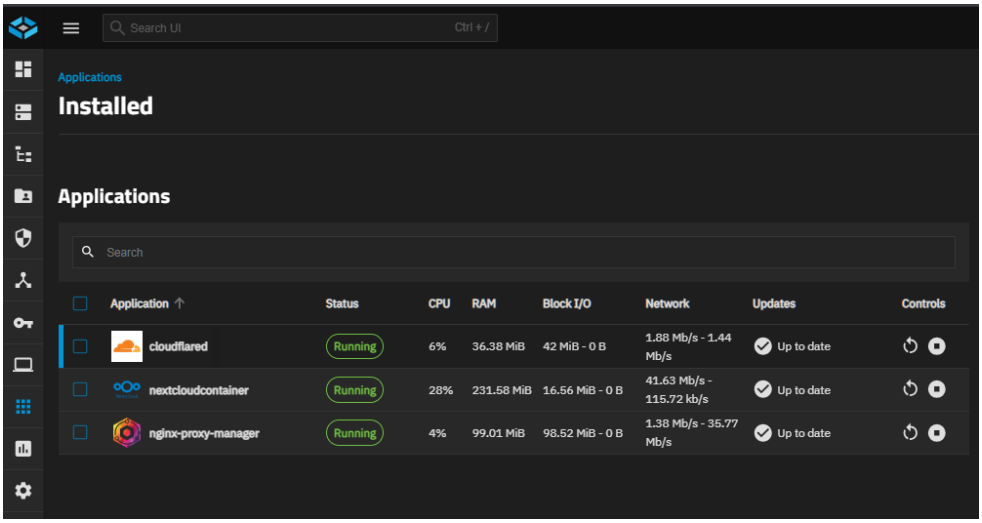
Installing the Nextcloud Files Desktop Application: [(nextcloud.com, 2025)]



26 Granting the Nextcloud desktop application access to my NextCloud Account.



27 Verifying Nextcloud connectivity in the Nextcloud Files desktop application

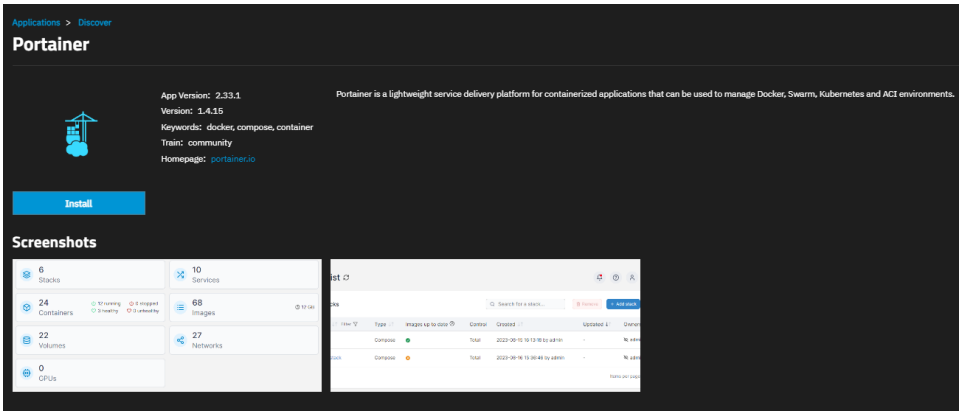


28 Viewing the installed applications in TrueNAS after installation of the Nextcloud app.

Task 4: Installing and utilizing the enterprise Edition of Portainer.

Task 4: Installing and utilizing the Community of Portainer.

Portainer is an advanced container management solution utilized by car manufacturers such as Volks Wagen and one of the leading banks in France.



29 TrueNAS Web UI App listing for portainer

Portainer CE App Configuration:

1. Application Name
    a. Name (Portainer)
    b. Version (1.4.15)
2. Portainer Configuration
    a. Image (Portainer Community Edition)
3. Network Configuration
    a. Web UI Port
        i. Port Bind Mode (Publish port on the host for external access)
        ii. Port Number (31015)
    b. HTTP Port
        i. Port Bind Mode (None)
        ii. Port Number (31017)
4. Storage Configuration
    a. Portainer Data Storage
        i. Type (ixVolume)
5. Resource Configuration
    a. Limits
        i. CPUs 1
        ii. Memory 512MB

30 Portainer CE App Configuration

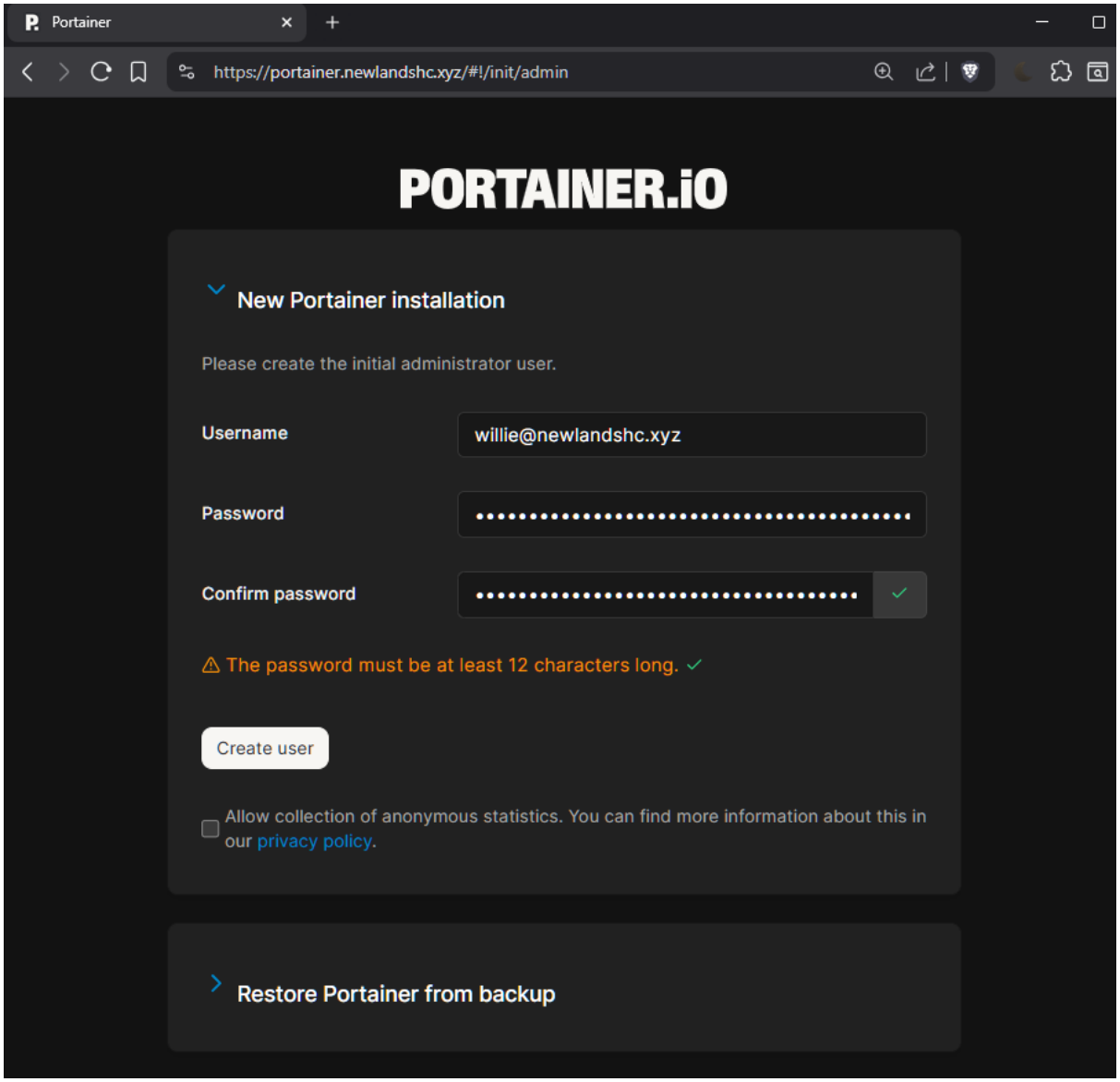


Figure 31 Creating the inital admin user.

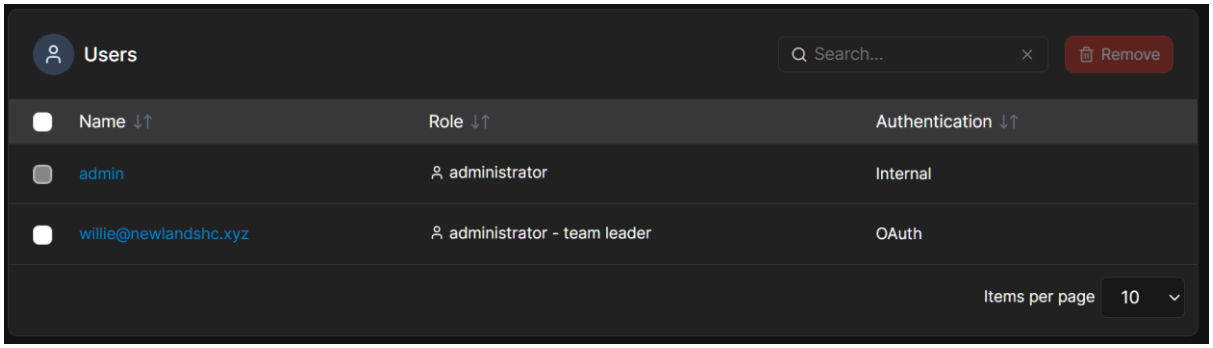
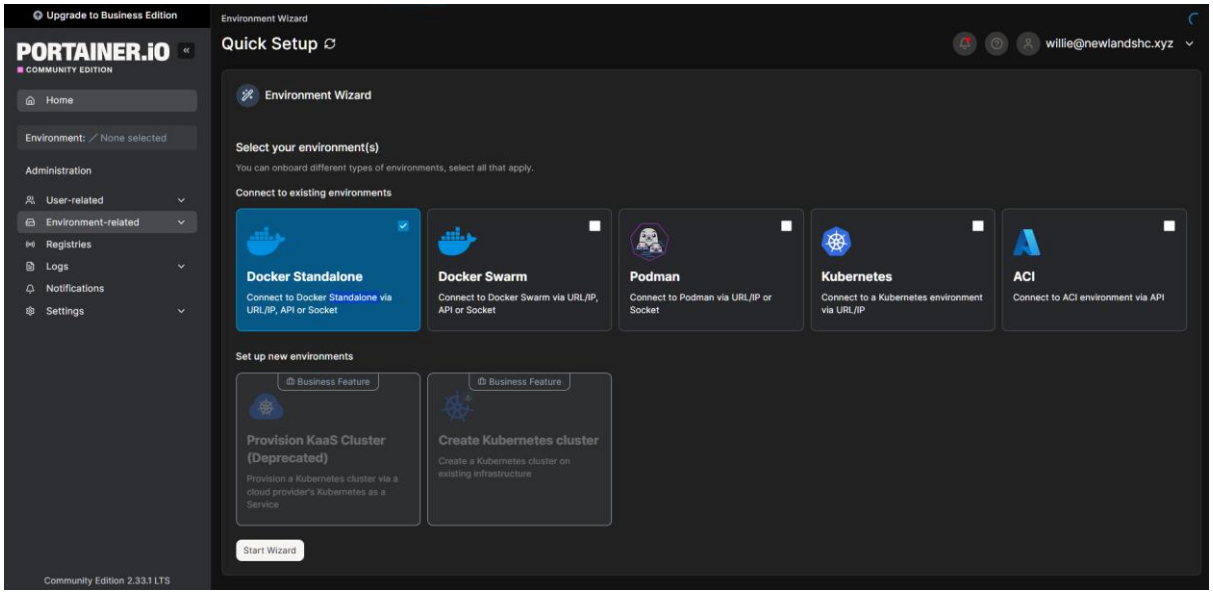
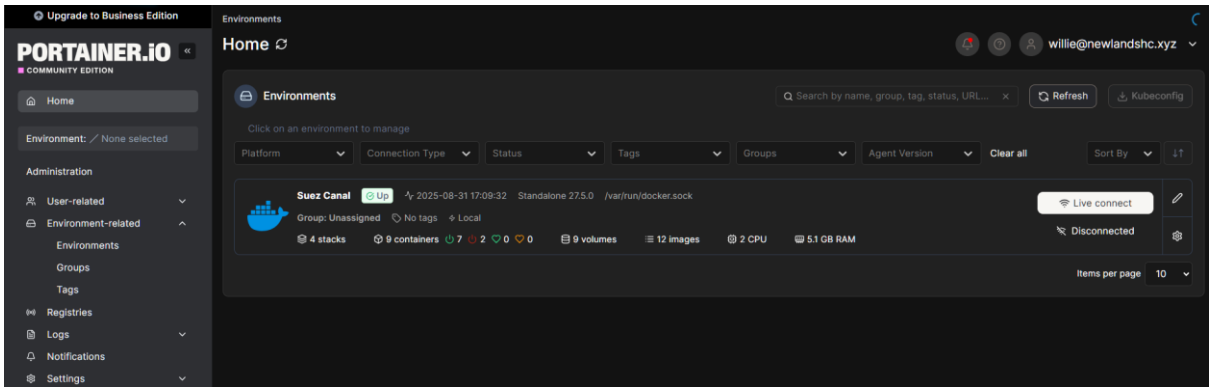


Figure 32. Note to prevent conflicts with OAuth I had to change the inital username to admin

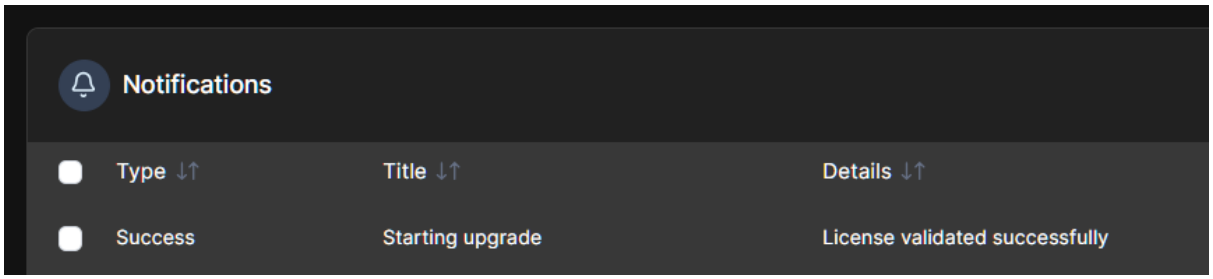


33 Docker environments that can be managed through portainer.



34 The local environment, renamed to Suez Canal

I performed a license upgrade to the enterprise edition of portainer.



Task 5: Setting up Authentication through OAuth with Microsoft Entra ID to enhance security on portainer.

```
PS C:\Users\willie\Documents\GitHub\wil730-portainer> az deployment group create --resource-group app-reg-rg --template-file azure/auth-app/auth-app.bicep
{
  "id": "/subscriptions/cc9b6eaf-f835-4ba4-9dfb-1551d87a9b34/resourceGroups/app-reg-rg/providers/Microsoft.Resources/deployments/auth-app",
  "location": null,
  "name": "auth-app",
  "properties": {
    "correlationId": "ba87b8ff-964b-4b5d-a1ba-1c974992595e",
    "debugSetting": null,
    "dependencies": [],
    "duration": "PT8.3575043S",
    "error": null,
    "mode": "Incremental",
    "onErrorDeployment": null,
    "outputResources": [],
    "outputs": {
      "appName": {
        "type": "String",
        "value": "PortainerAuth"
      },
      "logoUrl": {
        "type": "String",
        "value": "https://aadcdn.msftauthimages.net/c1c6b6c8-qtzpaoyljivr1bhdmqfxfyv-2ez0fsaghthspld5pa/appbranding/uj0nxuqwfhgyribrrttfdgzso1t-t9rvjgovrgjirw/1033/bannerlogo?ts=6389225216
      }
    }
```

Figure 35 To register the application, I made a bicep template.

(willie-de-klerk@Newlands-Health, 2025)

(microsoftgraph, 2025)

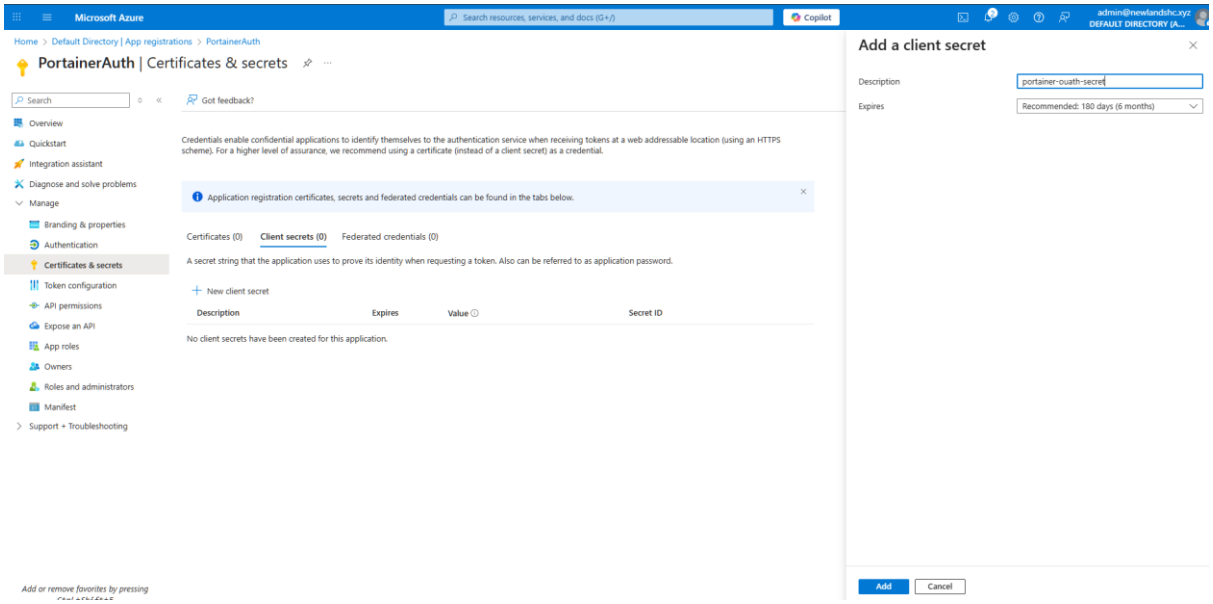


Figure 36 I manually registered a client secret

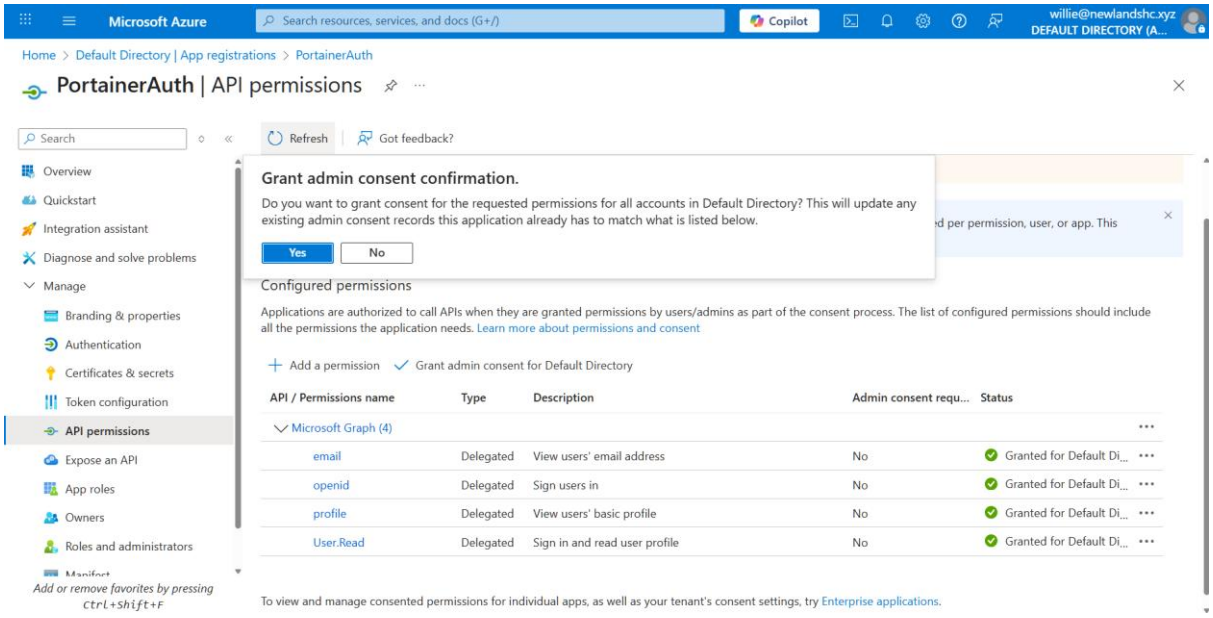


Figure 37 I granted the required Microsoft Graph API permissions.

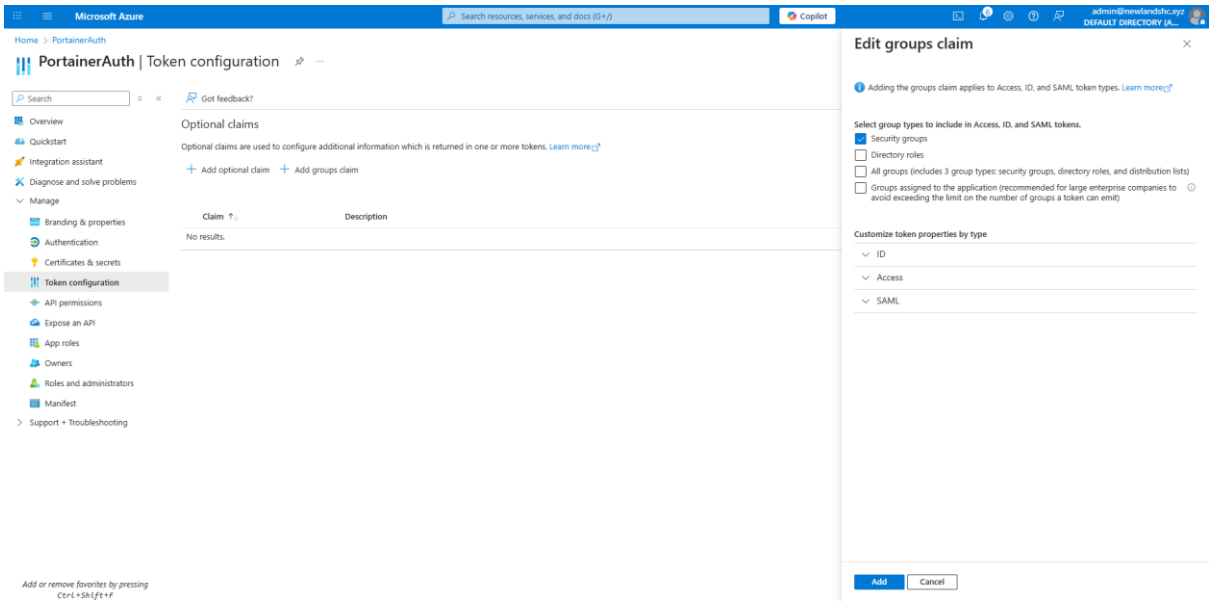


Figure 38 I created groups claim for security groups, as this is needed for automatic team membership in portainer.

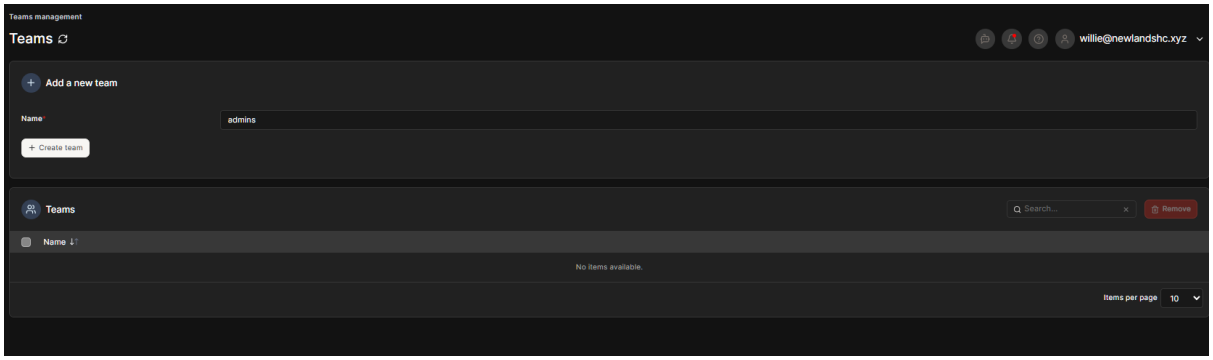


Figure 39 I created a team that matches my security group in my Entra id environment.

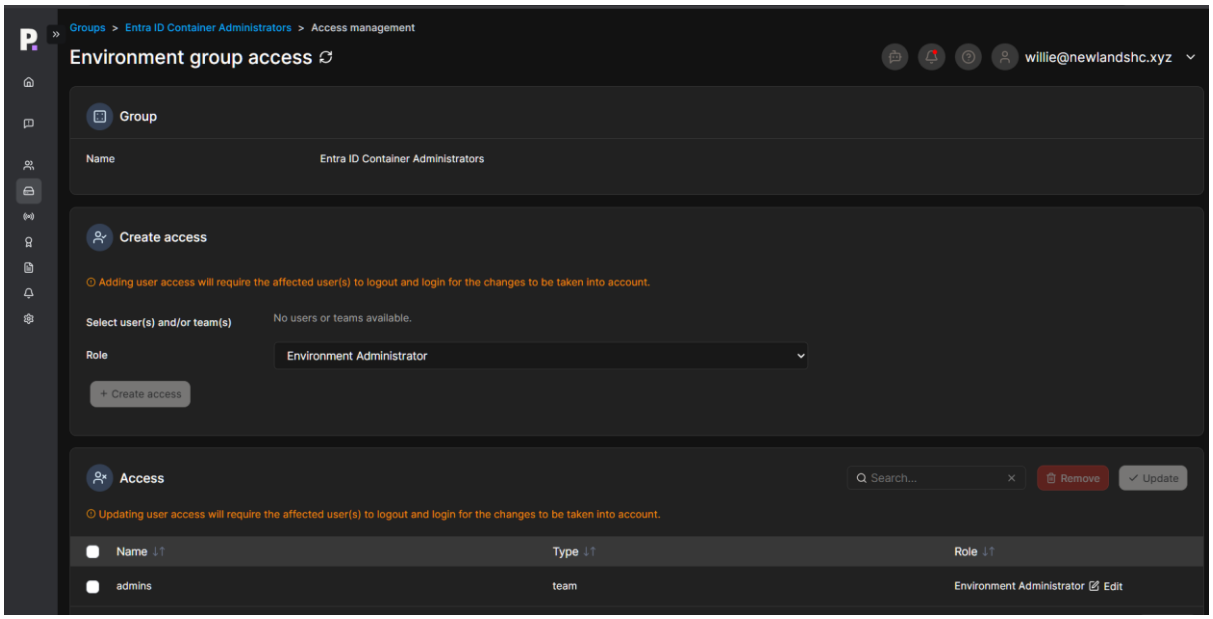


Figure 40 I also created an environment group that will allow access to resources within the environment group to be granted to specific teams.

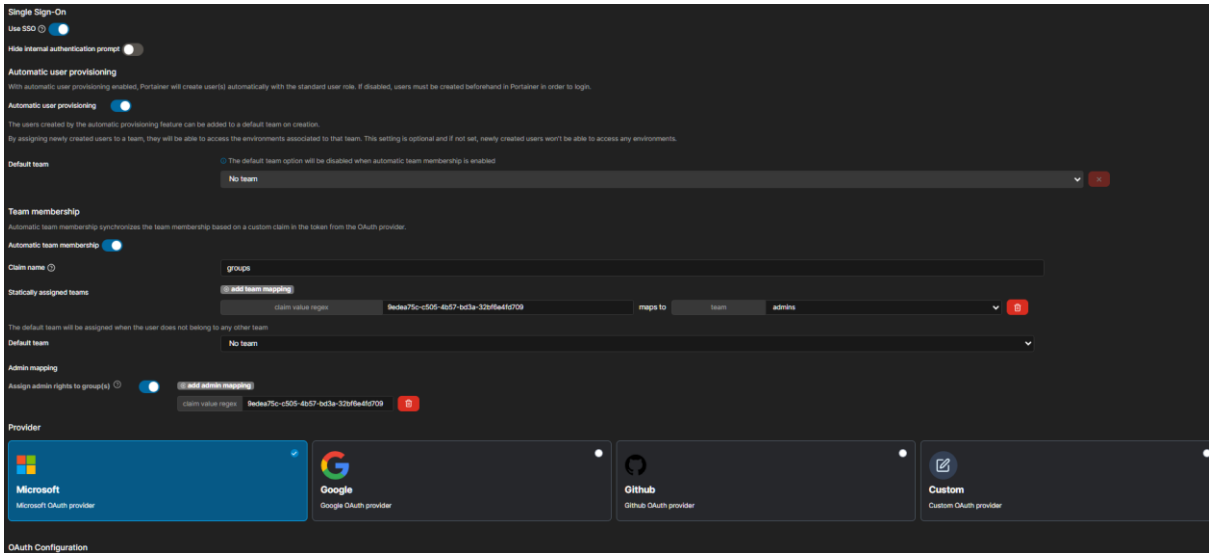


Figure 41 Enabling SSO, configuring Team membership, with the statically assigned team via regex (object id on az portal), mapped to team on portainer.

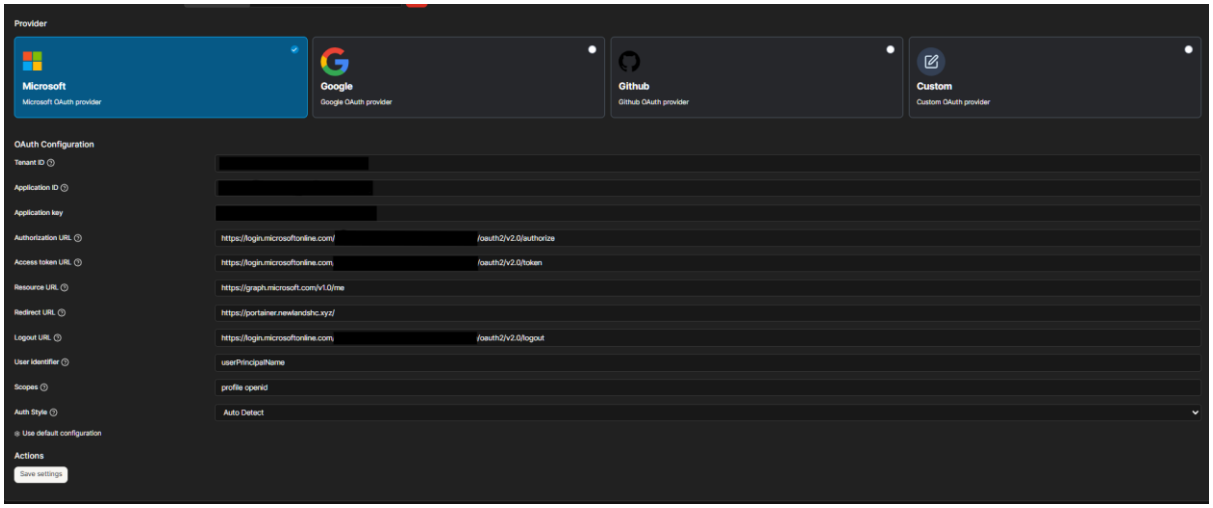


Figure 42 I configured the OAuth parameters as stated in portainer's documentation.

(docs.portainer.io, 2025)

Testing the login

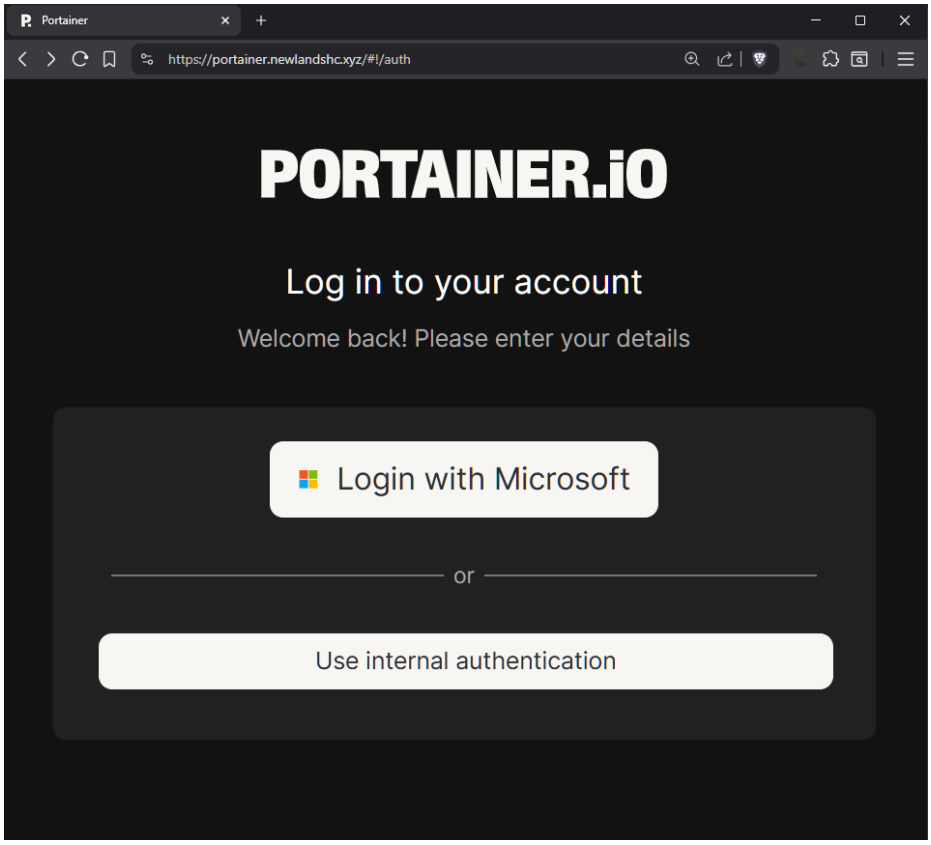


Figure 43 Portainer login screen

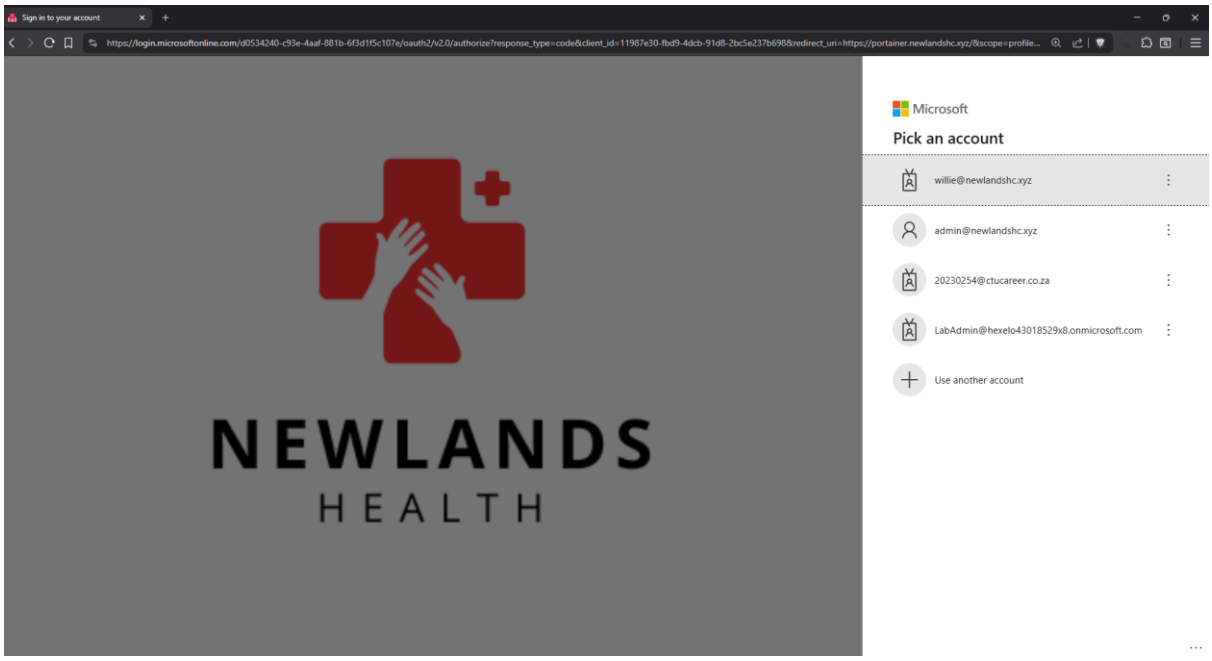


Figure 44 Microsoft Online login required to access portainer dashboard.

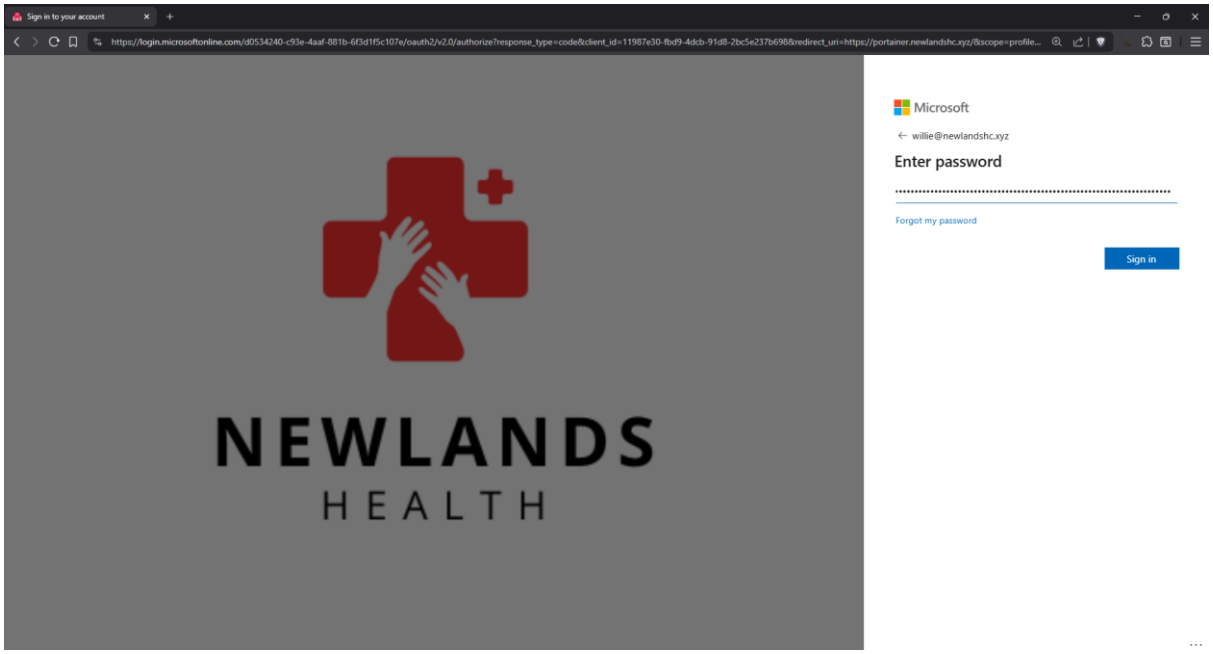


Figure 45 I paste my password from my vault.

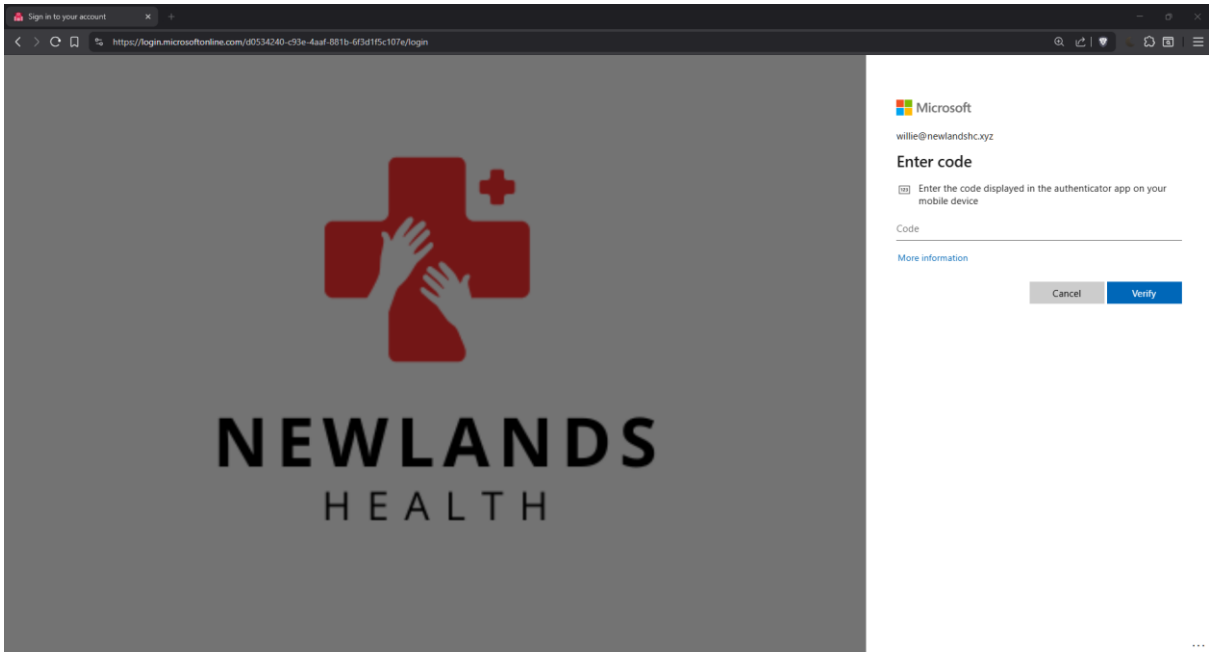


Figure 46 I entered a code from my Authenticator app on my phone.

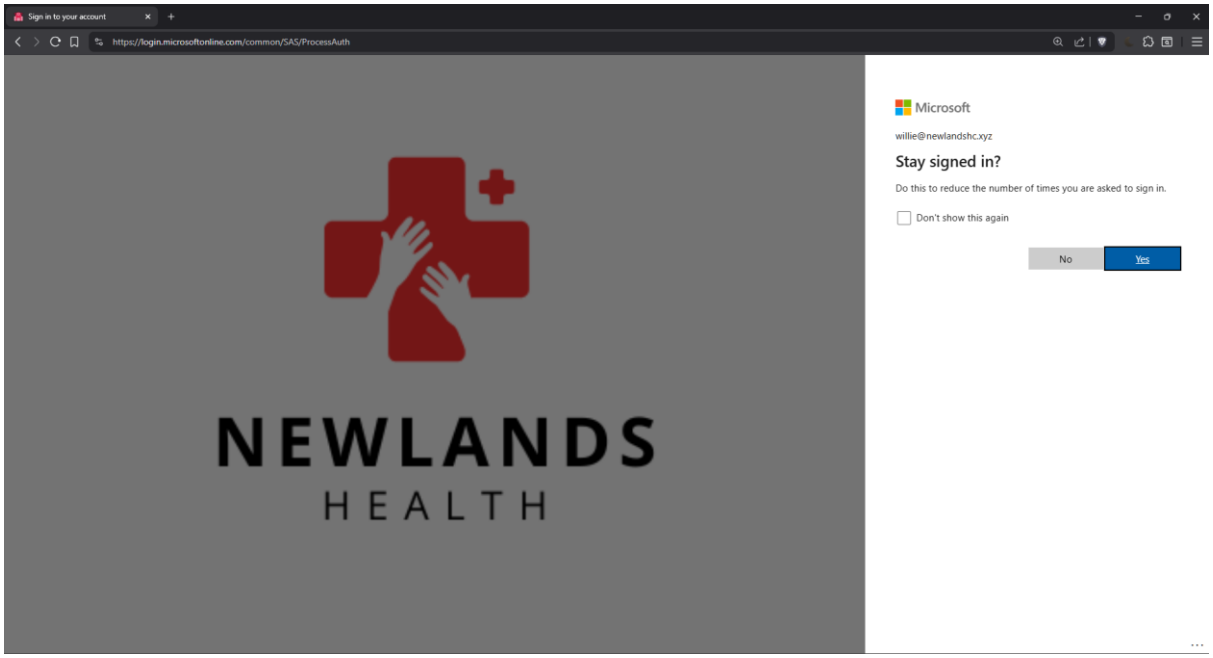


Figure 47 I stated that I want to stay signed in.

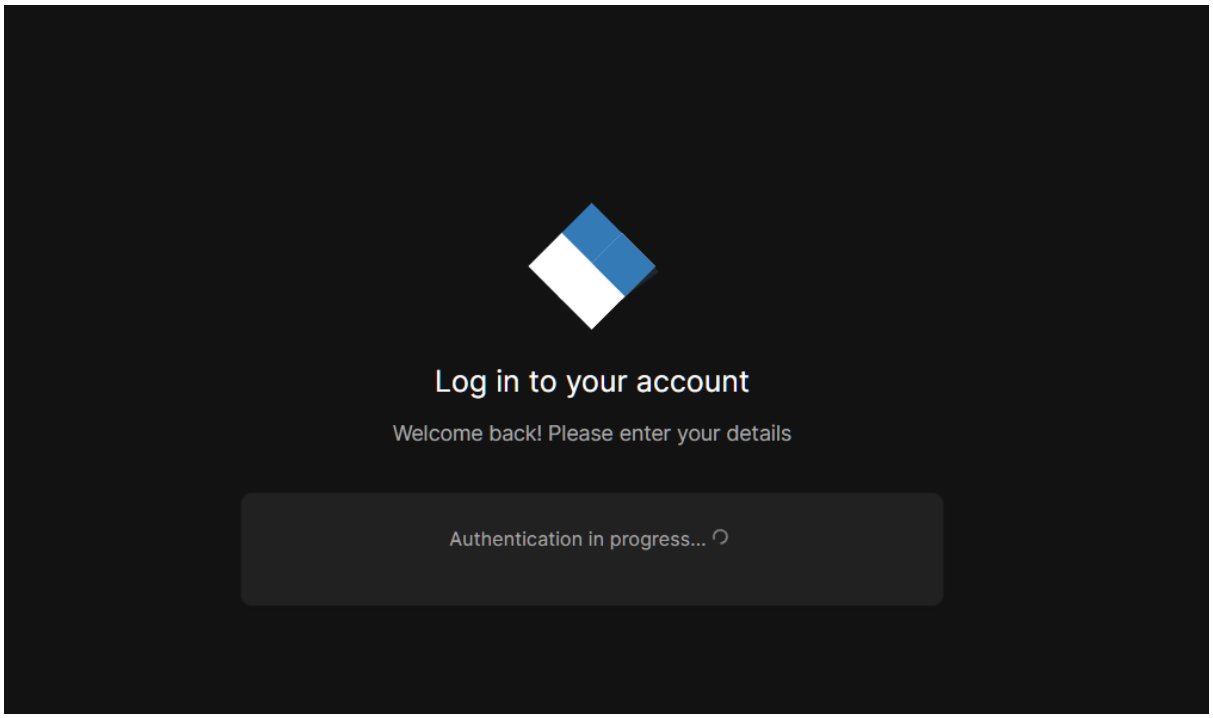


Figure 48 Loading Screen whilst authentication takes place.

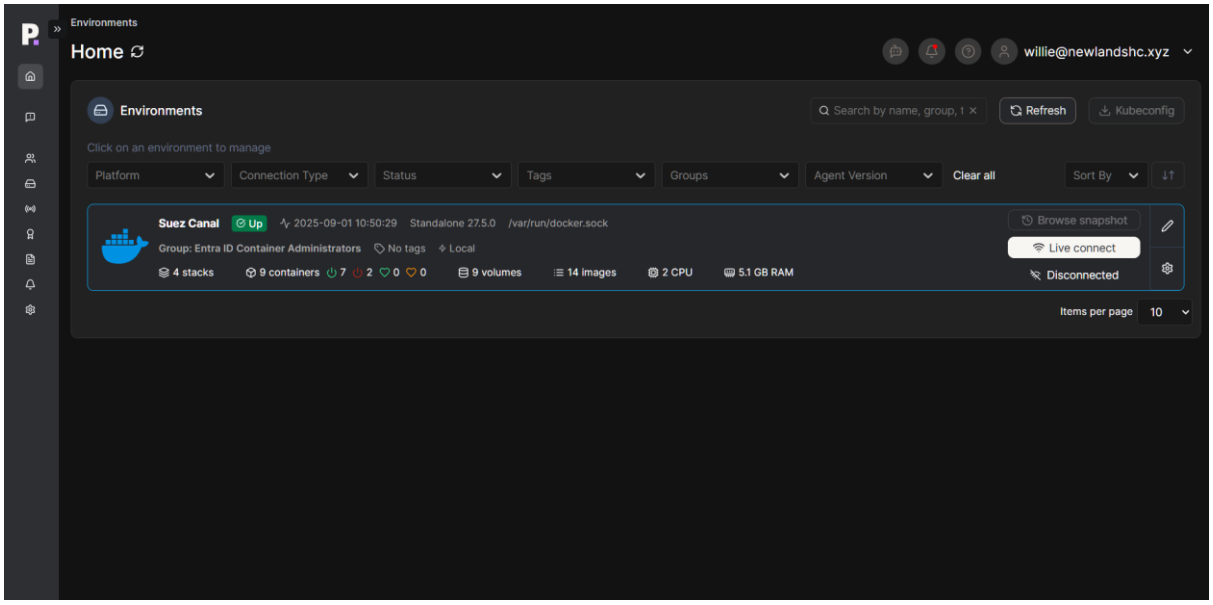


Figure 49 Dashboard access after successful authentication.

Task 5 conclusion

The implementation of OAuth using Microsoft Entra ID as the authentication provider will enhance security since Microsoft provides extensive logs related to all login attempts that can be used during an incident investigation.

It provides users with a familiar login process, with a professional log in screen. Additionally, it drastically reduces management overhead.

Examination of placement experience

This experience made me feel positively upon completion as I have had the opportunity to validate some of my firewalling skills, in addition to learning new skills. I succeeded since I had the opportunity to bring class board power point, and class lab ideas to life.

In class, I am taught to make use of arm templates and bicep files for azure deployments since it is idempotent. I was challenged with the creation of a bicep template to register an application. This was challenging because it's an area that Microsoft implemented a mechanism during development that is not being removed since it provides everyone else with convenience. If I created my app deployment using the azure cli and the application is deleted but still in the restore bin, the deployment would fail.

My perspective of business equipment procurement changed. Leveraging open-source software can help to drastically reduce costs.

Articulation of Learning

During my work integrated learning module, I gained knowledge and technical skills related to Microsoft Azure, domain verification via DNS records, Microsoft Entra ID, Azure CLI, Bicep Templates, Docker Containers, Cloudflare Zero Trust Tunnels, NGINX Proxy Configuration, DHCP,

Firewall configuration, Network Address Translation (NAT), ICMP, TrueNAS, Operating System Installation and Multi Factor Authentication.

I learned these skills through hands on configuration with mentor reviews. The skills above are vital to my development as a junior IT professional since the tasks delegated to me may be part of my daily work tasks.

In my future practice in view of this learning experience, I would make use of backups and snapshots, even in testing environments as anything can go wrong at any time.

Bibliography

developers.cloudflare.com, 2025. *Cloudflare Tunnel.* [Online]
Available at: https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/
[Accessed 31 08 2025].

docs.netgate.com, 2025. *Configuring Firewall Rules.* [Online]
Available at: https://docs.netgate.com/pfsense/en/latest/firewall/configure.html
[Accessed 31 08 2025].

docs.portainer.io, 2025. *Authenticate via OAuth.* [Online]
Available at: https://docs.portainer.io/admin/settings/authentication/oauth
[Accessed 01 09 2025].

Kevin Wallace Training, LLC, 2023. *Subnetting - Deep Dive.* [Online]
Available at: https://youtu.be/vY4cjGpRiIs?si=8Xh_8q8O6icMYKuf
[Accessed 31 08 2025].

microsoftgraph, 2025. *msgraph-bicep-types/quickstart-templates.* [Online]
Available at: https://github.com/microsoftgraph/msgraph-bicep-types/tree/main/quickstart-templates
[Accessed 01 09 2025].

nextcloud.com, 2025. *NextCloud Files Desktop Application.* [Online]
Available at: https://nextcloud.com/install/#desktop-files
[Accessed 31 08 2025].

willie-de-klerk@Newlands-Health, 2025. *wil730-portainer.* [Online]
Available at: https://github.com/Newlands-Health/wil730-portainer
[Accessed 01 09 2025].

www.iana.org, 2025. *Private-use IP addresses.* [Online]
Available at: https://www.iana.org/help/private-addresses
[Accessed 31 08 2025].

www.truenas.com, 2024. *2FA (Two-Factor Authentication).* [Online]
Available at: https://www.truenas.com/docs/core/13.0/uireference/system/2fa/
[Accessed 31 08 2025].

www.truenas.com, 2024. *TrueNAS Hardware Guide.* [Online]
Available at:
https://www.truenas.com/docs/scale/gettingstarted/scalehardwareguide/#:~:text=If%20a%20motherboard%20includes%20hardware%20RAID%20functionality%2C%20do%20not%20use%20or%20co

nfigure%20it%2C
[Accessed 13 08 2025].

www.truenas.com, 2025. *Cloudflare Tunnel.* [Online]
Available at:
https://www.truenas.com/docs/scale/24.04/scaletutorials/apps/appsecurity/cloudflaretunnel/
[Accessed 31 08 2025].