Technical Whitepaper

HPE OneView 9.0 Best Practices Guide for Deployment and Management

HPE OneView 9.0

Table of contents

Introduction 5

- HPE OneView 9.0 Features 6
- Supported Hypervisors and Versions 7
- Browser Requirements 7
- Supported HardwareOF 8
- HPE OneView User Interface Overview 10
- Deploying Your Appliance 11
- Microsoft Windows Server 2016 / 2019 / 2022 Hyper-V 11
- VMware vSphere 6.5 or Later 14
- KVM 17
- Guided Setup 20
- First Time Setup 21
- Installation Checklist 21
- HPE Synergy Composer First Time Setup 25
- Set Time and Language (Optional) 28
- HPE OneView Appliance based Firmware Repository 30
- External based Firmware Repository 32
- Adding HPE OneView Advanced Licenses to the HPE OneView Appliance 34
- Viewing HPE OneView Licenses 36
- Notification and Automated Download of Available Firmware / Driver Updates 38
- Network Configuration 42
- Network Configuration Checklist 42
- Creating Ethernet Networks 43
- Creating Fibre Channel Networks 47
- RDMA over Converged Ethernet (Synergy Virtual Connect only) 55
- Creating Network Sets 57
- Create Logical Interconnect Group 60
- Reviewing Logical Interconnect Group Configuration 74
- Create Enclosure Group 75
- Setting up Remote Support for supported devices 78
- Using Labels 80

Importing a ProLiant DL, ML or Apollo Managed Server 82
Importing a ProLiant DL, ML, Apollo or Superdome Flex / Superdome Flex 280 or Compute Scale-up Server 3200 as a Monitored Server 86
Importing a Range of Servers as Managed Devices 88
Importing a Range of Servers as Monitored Devices 90
Managing HPE Storage (3PAR StoreServ, Alletra, Primera or Nimble) 92
HPE OneView Import HPE 3PAR StoreServ, Alletra, Primera or Nimble Checklist 92
Importing Storage Systems - HPE 3PAR StoreServ / Alletra / Nimble systems 101
Examine Imported Storage System 107
Import Existing Storage Volumes 108
Create Storage Volume Templates to create Volumes 110
Creating StoreServ Storage Volumes 114
Enabling StoreServ Compression and using Large Volumes 119
Creating Nimble Storage Volumes 122
Creating Primera Storage Volumes 129
Upgrade Infrastructure Firmware 135
Managing Virtual Connect Firmware 136
Updating Firmware on a Server without a Server Profile 140
Creating Server Profiles 143
Create Server Profile Template 144
Creating Server Profiles from a Server Profile Template 161
Assign a Server Profile to a newly discovered / imported server 164
Add Hypervisor Manager 166
Import VMware Cluster Profile 168
Create One-Off Server Profile 171
Create a Server Profile for Gen10 or newer DL Servers 188
Create a Server Profile for Gen8 / Gen9 Servers 202
Environment Management 215
Physical data center configuration 215
HPE Superdome Flex 221
HPE Superdome Flex 280 231
HPE Compute Scale-up Server 3200 243
Configuring power delivery topology for the Data Center 255
Adding HPE iPDU's 255
Adding Unmanaged Devices 258
Securing the Appliance 259
(Optional) Integrating Active Directory / LDAP Security 259
Active Directory or OpenLDAP Checklist 259
(Optional) Integrating with Active Directory / OpenLDAP 259
(Optional) Integrating with Two-Factor Authentication 265
Creating a Scope 267
Maintaining Your Appliance 270
Changing the IP address of the HPE OneView Appliance 270

Upgrading the OneView Appliance / Synergy Composer 272
Changing the SNMP Read String of the HPE OneView Appliance 277
Configuring SNMP v3 279
Backing up the HPE OneView Appliance – One time method 282
Restoring an HPE OneView Appliance from Backup 283
Setting a remote Backup location and Schedule for Backups 286
Setting up Remote Support for supported devices 289
Viewing Reports 291
Exporting Reports 293
Printing Reports 295
Creating New Users 297
Deleting Existing Users 299
Creating Groups 300
Changing User Permissions 302
Adding a Dashboard Panel to the HPE OneView Dashboard 304
Removing a Dashboard Panel from the HPE OneView Dashboard 306
Alerts and Monitoring 307
Viewing Activity, Alerts and Tasks 310
Multi-use Commands 312
Changing the hardware for a Server Profile 313
Putting a Server in Maintenance Mode 317
Launch HTML5 Console 319
Set One-Time Boot Option on Server 320
Add New Networks to a Logical Interconnect Group 322
Create a Server Profile Template from existing server profile 328
Edit Server Profile 329
Assign a Server Profile to a newly discovered server 331
Perform rolling cluster update on ESX cluster 333
Configuring Boot from third party LUNs in a Server Profile 335
Adding an Ethernet Network 337
Adding a Fibre Channel Network 340
Adding an Ethernet Uplink to a Logical Interconnect 342
Adding a Fibre Channel Uplink 345
Create Additional Storage Volume Templates for StoreServ Volumes 348
Create Additional StoreServ Storage Volumes 353
Configuring 3PAR Thin Dedupe on Volumes 357
Create Storage Snapshots 359
Viewing Storage Snapshots 360
Deleting Storage Snapshots 362
Reverting to previous Storage Snapshots 364
Removing Networks from a Server Profile 366
Deleting a volume from HPE OneView 368
Adding New Racks Based on Location Discovery Services 370

Adding Servers to Racks without Location Discovery Services (LDS) 370
Adding a Service Pack for ProLiant (SPP) or Synergy Service Pack (SSP) Bundle 372
Adding an External SPP / SSP Repository 373
Updating the Firmware Baseline for Servers deployed with Server Profile Templates 375
Updating the Firmware Baseline for Single Servers with Profiles Assigned 379
Deleting a Service Pack for ProLiant (SPP) / Synergy Service Pack (SSP) Bundle 381
Modifying Virtual ID Pools 382
Synergy Static IP Address Assignment for Compute Modules and Interconnects 383
Creating a Support Dump 385
Appendix 386
Appendix A: Sample HPN 5900CP FCF Switch Configuration 386
Appendix B: REST API 393
Appendix C: Accessing the REST API with PowerShell 394
Appendix D: Configuring a Brocade SAN switch for HPE OneView REST API access 396
Additional Resources 398

Introduction

Welcome to the Best Practices Guide for Deployment and Management for the HPE OneView 9.0 release.

HPE OneView 6.6.x long term support (LTS) release offers extended support for HPE hardware platforms (server, network, storage device) until their software end-of-support-life (EOSL) date.

An LTS release can be patched, as required, to address security and other customer identified critical issues. The released LTS patch will not contain new features. An attempt to update from an LTS release to a newer release with end-of-life (EOL) hardware platforms or devices is blocked.

The EOSL (end of support life) date for HPE OneView 6.6.x was 31st December 2023.

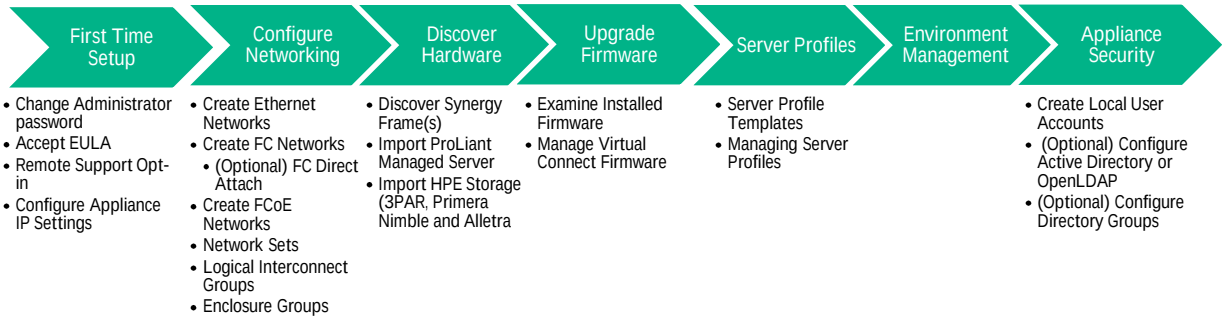
In order to upgrade to this release, you must remove the EOL hardware platforms or devices from the HPE OneView appliance for a successful update (once these are removed you can update to 7.0, 8.0, 8.3 and then 8.6 which are mandatory upgrade milestone releases and then this release). These can be migrated from HPE OneView 6.6.x LTS version to 8.0 (which is the last version that supports migration of supported hardware from an older version to new, newer versions of OneView support migration ONLY between the same OneView versions). If you continue to use these EOL hardware platforms or devices, you can choose to remain on the specified HPE OneView LTS release as needed. Hewlett Packard Enterprise determines the LTS life cycle support period and this information is available on the HPE OneView Software Lifecycle page.

Synergy environments that have Composer 1 are also unable to upgrade beyond an LTS release. They will need to upgrade their Composer to Composer 2 as this is the only Composer hardware that is supported for 7.0 or later.

This document is intended to be a quick start guide as well as a reference guide for operations and administrators of HPE OneView.

HPE OneView provides a simple, consumer-inspired user experience that dramatically accelerates the everyday tasks of a Composable Infrastructure. By changing the focus from 'how devices are managed' to 'how people work', HPE OneView delivers a software-defined management platform that is extensible and easy to use.

This first part of the document will guide administrators through the setup process, and how to manage the next generation of Composable Infrastructure with HPE OneView. The flow chart below outlines these steps.



This remainder of the document will serve as a reference guide to administrators for the various functions they will encounter day to day as they manage an environment with HPE OneView.

HPE OneView 9.0 Features

The following list outlines the new features in the HPE OneView 9.0 release:

Table 1. HPE OneView 9.0 Features	
Synergy Composer / HPE OneView	Manage HPE iLO Security Dashboard (Server Profiles / Server Profile Templates) Provide REST and UI options to enable/disable HPE iLO "Ignore" security status tracking option in iLO setting section in Server Profile and Template for all HPE iLO Security Dashboard items.
Synergy Composer / HPE OneView	HPE OneView Admin account password rotation (OneView Device Management Account) Automatic rotation of OneView service account on iLO password without user intervention
Synergy Composer	Support new alerts for Synergy Frame Link Module (FLM) 5.0 Firmware New alerts so that customers can be more aware of when communication issues were encountered between the Frame Link Module (FLM) and the CANmic infoblock interface on storage blades and interconnects.
HPE OneView	Inventory-based Firmware / Driver download for OneView Appliance (Server Profiles / Server Profile Templates) Automatically download updated binaries based on inventory at the time when updates become available
HPE OneView	Support for System Firmware management through Server Profiles and Server Profile Templates on HPE Superdome Flex and HPE Compute Scale-up Server 3200
HPE OneView	Support for management of partitions on HPE Compute Scale-p Server 3200
HPE OneView	OneView Remote Support (OVRS) for HPE ProLiant MicroServer Gen11 and HPE ProLiant Gen11 Nutanix (DX) Servers

Supported Hypervisors and Versions

Please note that the following hypervisors are the minimum requirement to host the OneView Virtual Appliance:

Table 2. Supported Hypervisors and Versions

VMware vSphere ESXi	6.5 Update 2, 6.5 Update 3 6.7 Update 2, 6.7 Update 3 7.0 Update 1, 7.0 Update 2, 7.0 Update 3 8.0, 8.0 Update 1, 8.0 Update 2 Note: *A Minimum VM hardware version of 11 and ESXi 6 or later is required to install HPE OneView 5.x or later. Upgrades to OneView 5.x on ESXi 5.5 will succeed as long as the hardware version is not changed.*
Microsoft Hyper-V	Hyper-V is supported on the following Microsoft Windows platforms with the Hyper-V role installed: Windows Server 2016 Windows Server 2019 Long-Term Servicing Channel (LTSC) Windows Server 2022
KVM	RHEL 7.8, 7.9 RHEL 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8 RHEL 9.0, 9.1, 9.2 Ubuntu 20.04 LTS KVM Ubuntu 22.04 LTS KVM

Recommended minimums for the OneView Virtual Appliance

- Eight 2-GHz or greater virtual CPUs
- Exactly 24 GB of memory
- 275 GB of thick-provisioned disk space

Browser Requirements

Please note that the following web browsers are a minimum requirement:

Table 3. Supported Browsers

Mozilla Firefox	64 or newer
Mozilla Firefox Extended Support Release	52 or newer
Google Chrome	71 or newer
Microsoft Edge	Current version
Safari	Unsupported
Opera	Unsupported

Supported Hardware[1]

Supported Enclosures

- All Synergy 12000 Frames

Supported Servers

- Advanced License Support
  - All HPE Synergy Gen9 / Gen10 / Gen10 Plus / Gen11 Compute Modules
  - MicroServer Gen10 Plus, MicroServer Gen10 Plus v2 & MicroServer Gen11
  - HPE ProLiant DL110 Gen10 Plus / Gen11
  - HPE ProLiant DL320 Gen11
  - HPE ProLiant DL 360, 380 Gen10 / Gen10 Plus / Gen11
  - HPE ProLiant DL 560 and 580 Gen10 / Gen11
  - All HPE ProLiant Gen9 DL-family of servers
  - All HPE ProLiant Gen8 DL-family of servers
  - All HPE ProLiant DX Servers
  - All HPE Apollo 2000, 4000 and 6000 Gen9 / 10
  - ProLiant ML350 Gen9 / Gen10 / Gen11
  - ProLiant ML30 Gen11
  - All HPE ProLiant AMD DL325/DL385 Gen10 / Gen10 Plus / Gen10 Plus v2 / Gen 11
  - All HPE ProLiant AMD DL345/DL365 Gen10 Plus / Gen11
  - HPE Superdome Flex & HPE Superdome Flex 280
  - HPE Compute Scale-up Server 3200

Supported HPE 3PAR StoreServ Storage

- HPE 3PAR StoreServ 7000 / 8000 / 9000 (3PAR OS 3.3.1 or later)
- HPE 3PAR StoreServ 10000 / 20000 / 20000 R2 (3PAR OS 3.3.1 or later)

Supported HPE Primera

- HPE Primera Support added with OneView 5.00.01 version Primera OS 4.0 or later

Supported HPE Nimble Storage

- Nimble OS 4.5, Nimble OS 5.0, Nimble OS 5.1 or later

  Note: *Legacy Nimble iSCSI storage systems updated to 5.1, will retain VST as the default. New Nimble 5.1 system will have GST enabled as the default.*

Supported HPE Alletra

- Alletra 4000 Series
- Alletra 5000 - 6.1
- Alletra 6000 - 6.0, 6.1
- Alletra 9000 – 9.3, 9.4, 9.5
- Alletra Storage MP

Support Fibre Channel Fabric Managers

- Brocade REST API (FOS) – 8.2.1b, 9.0, 9.0.1a, 9.0.1c, 9.0.1d, 9.1.0b, 9.1.1
- HPE 5700, 5900CP / AF, 5930, 5940, 5950, 7900, 12900 (FC & FCoE)
- Cisco Nexus 5500 / 5600/6000 (FC & FCoE) - NX-OS 6.0, 7.0, 7.1, 7.2, 7.3(8)N1(1), 8.3
- Cisco MDS (FC & FCoE)

[1] Please review the HPE OneView Support Matrix on https://www.hpe.com/support/OneView-SM

Hardware Firmware and Fibre Channel Fabric Manager Minimum Requirements

Table 4 shows the minimum firmware requirements needed to successfully import an enclosure. Firmware will be updated via the appliance to the required versions later in this document.

Table 4. Minimum Firmware / Software Requirements

iLO6	1.10 or newer
iLO5	2.10 or newer
iLO4	2.44 or newer
HPE 3PAR OS	3.3.1 or newer
HPE Primera	4.0 or newer
HPE Nimble Storage	4.5, 5.0, 5.10 or newer
Alletra 9000	9.3 or later
Alletra 6000	6.0 or later
Alletra 5000	6.1 or later
Superdome Flex Rack Management Controller (RMC)	2.4.98 or newer
Superdome Flex 280 eRMC	1.0 or newer
Compute Scale-up Server 3200	1.0 or newer

Table 5. Post Import Firmware Minimum Version

iLO6 for Gen11 Servers	1.10
iLO5 for Gen10 / Gen10 Plus Servers	2.10
iLO4 for Gen9 servers	2.44
iLO4 for Gen8 servers	2.44

Note:
The Appliance Virtual Machine should not be deployed on a hypervisor within the same enclosure it will manage. Please use an externally available hypervisor host.

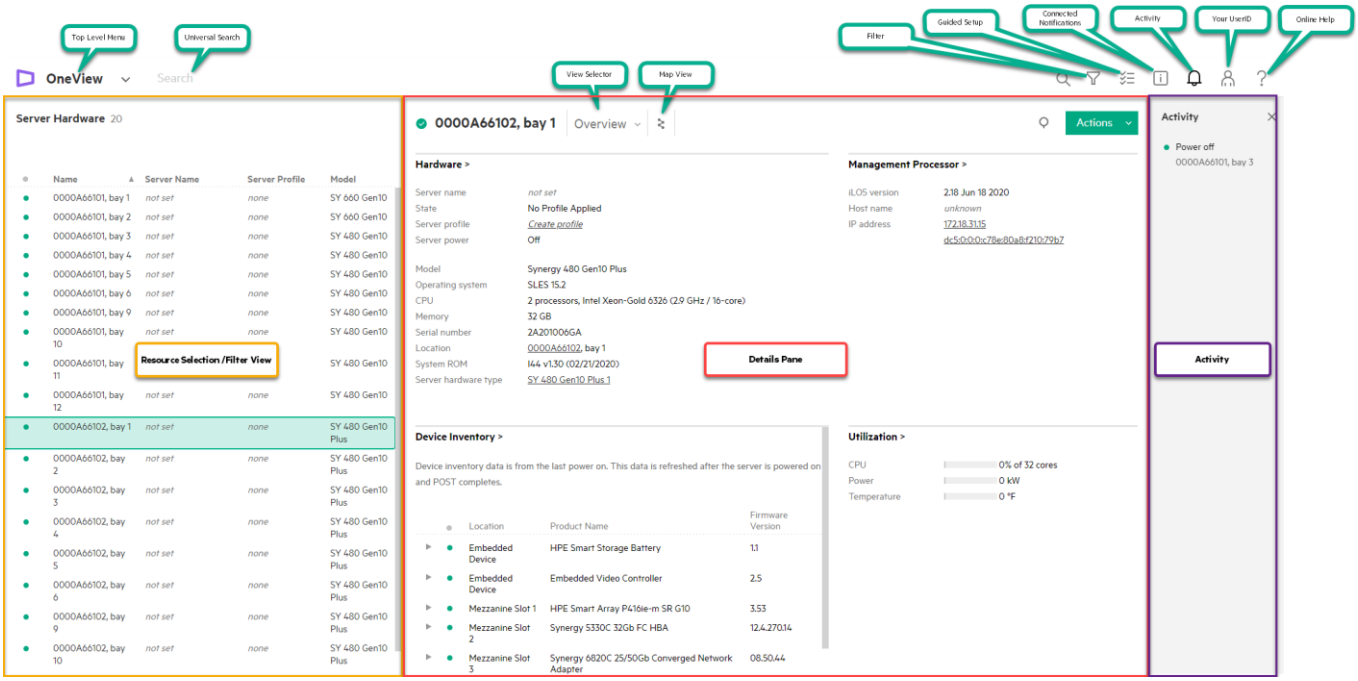
Table 6. Supported Maximums for standard HPE OneView Appliance

Total Servers	1024
Managed Servers	740
Monitored Servers	1024
Total number of unassigned Server Profiles	100
Total Number of volumes per Server Profile	512
Rack Managers	80
Total number of Superdome Flex / Superdome Flex 280 Rack Managers	80
Total number of Superdome Flex / Superdome Flex 280 nPartitions	640

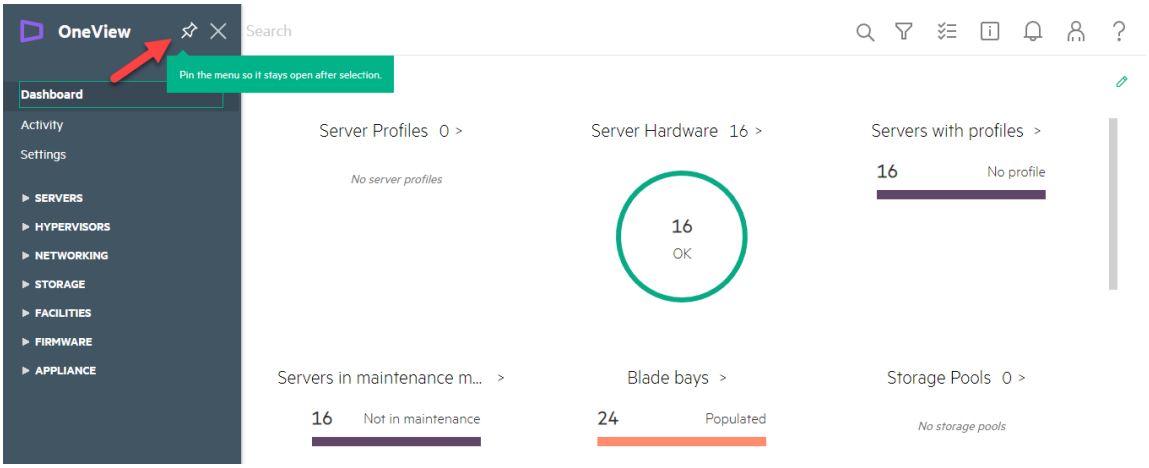
HPE OneView User Interface Overview

The HPE OneView user experience is significantly improved from previous generations of HPE Management software (e.g. HPE System Insight Manager). The HPE OneView user interface is built using modern web programming languages, HTML5 and CSS3. Below is an example of what the User Interface (UI) looks like.

Figure 1. HPE OneView User Interface



When you click on the Top Level Menu as shown above you, would see the following which is a feature released in HPE OneView 5.3 which is the "Pin Menu" feature that allows you to keep the menu flyout static. To pin the menu in place simply click on the *Pin*.



- The Top Level Menu is used for navigating the different sections of the UI. Each section is then categorized based on function and / or role (Servers, Hypervisors, Networking, Storage, Facilities and Appliance).
- The Universal Search bar defaults to local context searching but can also search the global index for resources the administrator is looking for.
- The Sub-Menu is where the current context view, or the Details Pane, can be changed for the select Resource.
- The Activity Details section within the Details Pane will display the most recent activity, whether it was an Administrator performing actions or an automated alert is generated. It can be expanded to view further details, and the administrator can then navigate to the activity item to clear, assign or provide notes regarding the event.
- The Actions menu is also context and resource specific and provide the administrator with specific actions to perform for a selected resource.
- The Activity Window displays the current activity of the administrator performing various actions within their session, which can be pinned out or collapsed to increase the viewing dimensions of the Details Pane. Individual activity items can be selected, and then directly navigated to in the case of Create and Update actions.

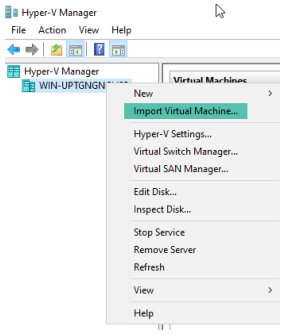
Deploying Your Appliance

This segment will guide you through deploying your HPE OneView appliance for ProLiant. It will cover the various steps within the First Time Setup experience.

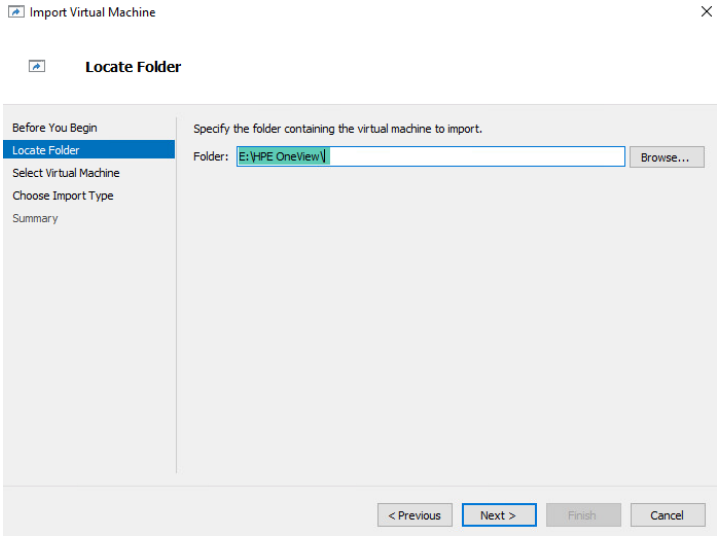
Microsoft Windows Server 2016 / 2019 / 2022 Hyper-V

HPE OneView supports Microsoft Windows Server Hyper-V as a hosting platform. The following steps outline the process to import the template.

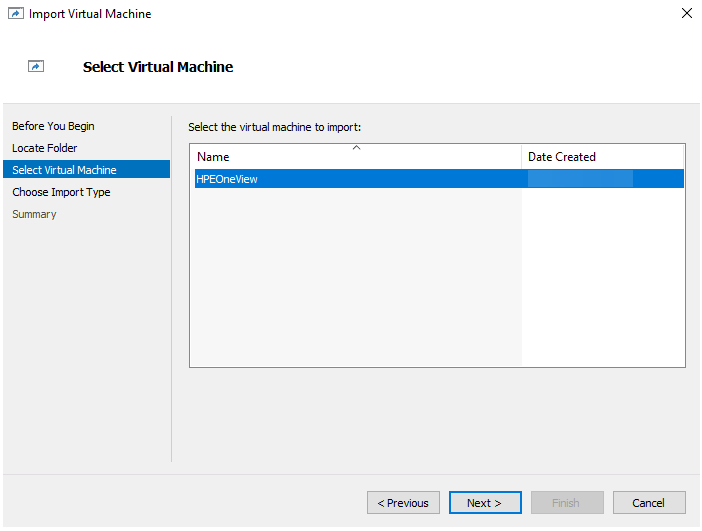
1. Within the Hyper-V Manager Console, select *Import Virtual Machine*.



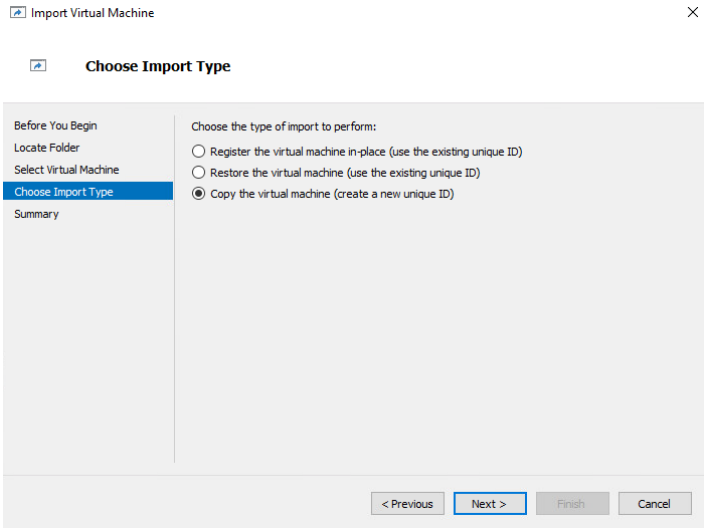
2. Specify the directory where the extracted appliance contents are located.



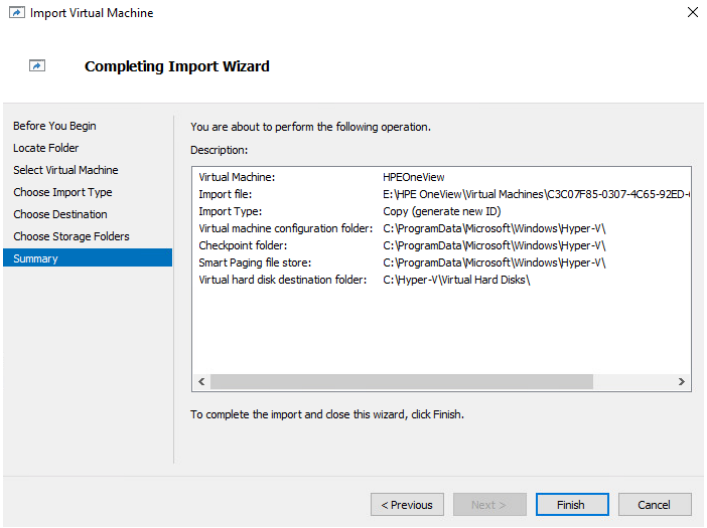
3. Click *Next*



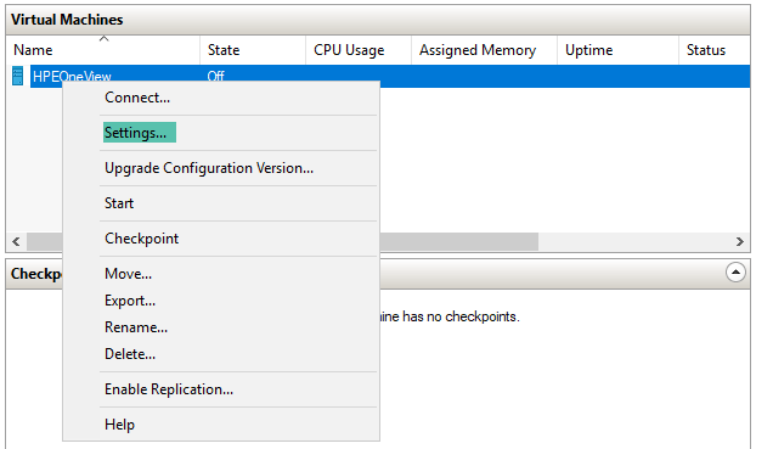
4. Choose “Copy the virtual machine” and then click *Next*



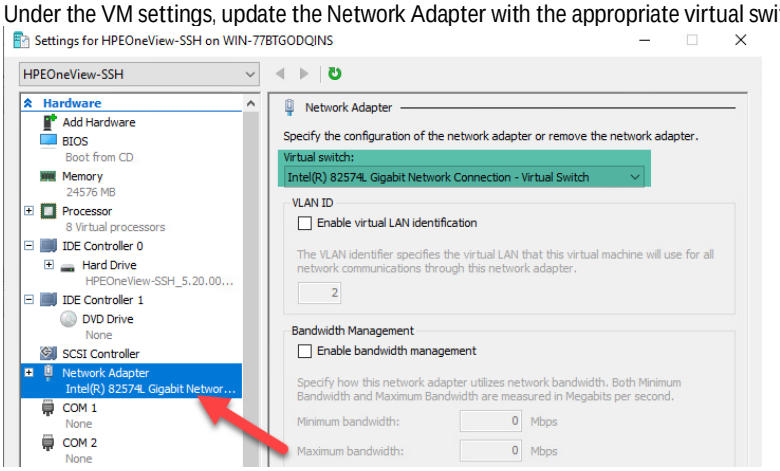
5. Enter the location of the HPE OneView Virtual Machine Hard Disks and click *Finish* on the Summary screen.



6. Once the VM has been deployed, edit the *Settings*.

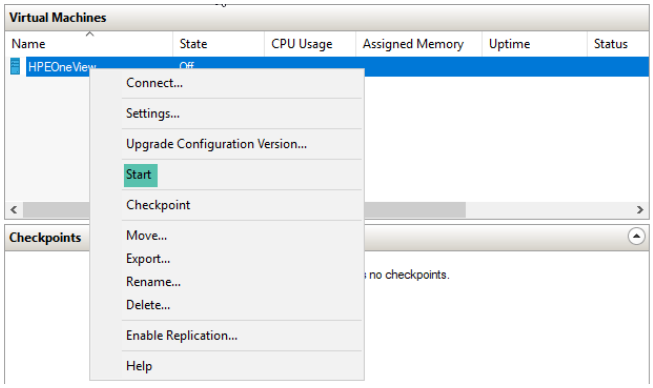


7. Under the VM settings, update the Network Adapter with the appropriate virtual switch.



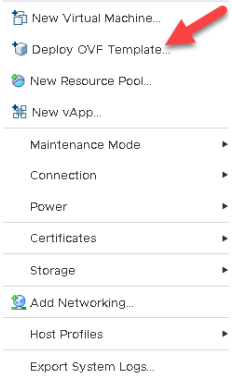
8. Click *OK* to save the settings

9. *Start* the virtual machine.

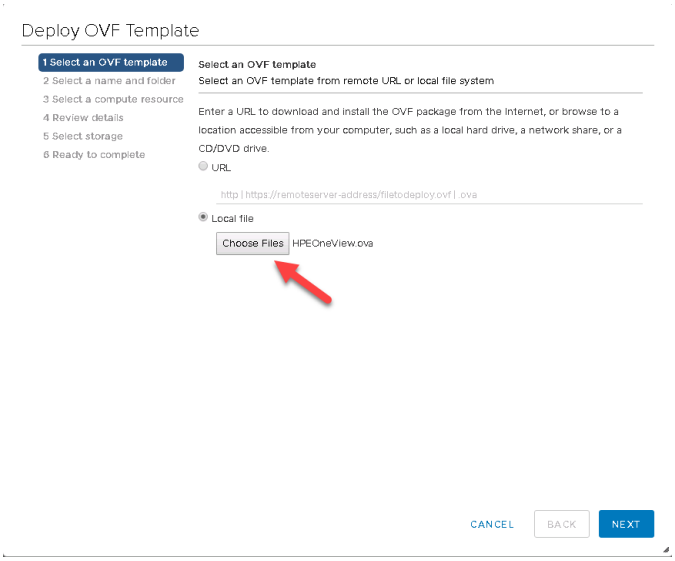


VMware vSphere 6.5 or Later

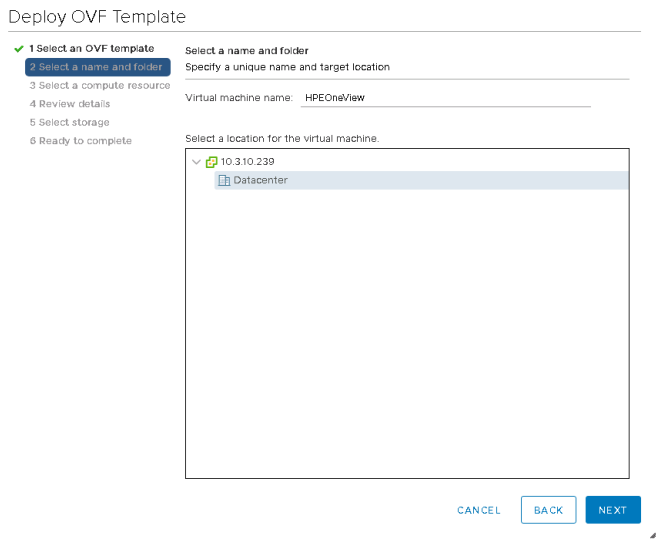
1. Select *Deploy OVF Template* from within vCenter



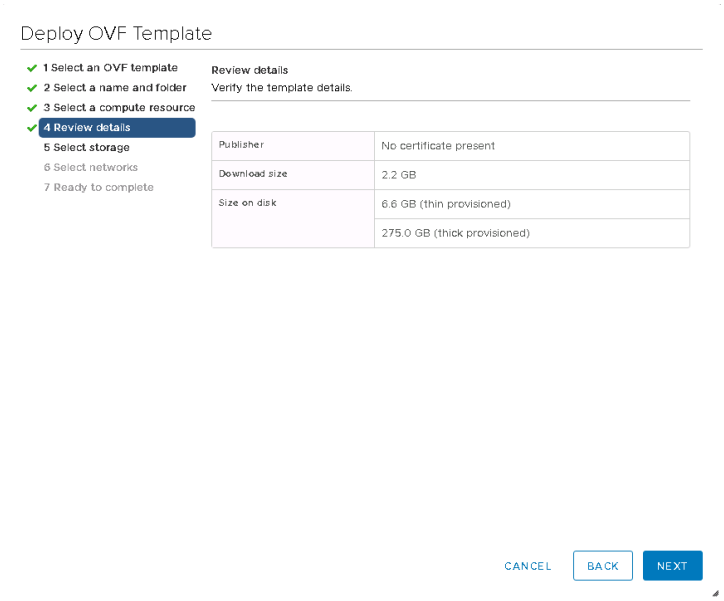
2. Select *Choose Files* then select the OVA file from the location where the file is stored and then click *Next*



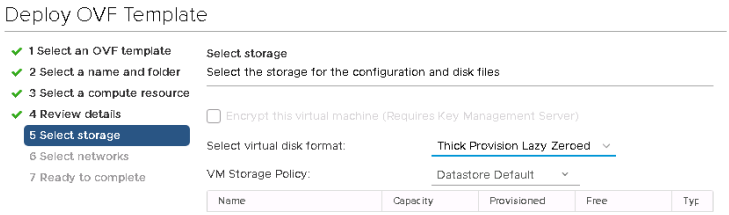
3. Enter the Virtual machine name and click *Next*.



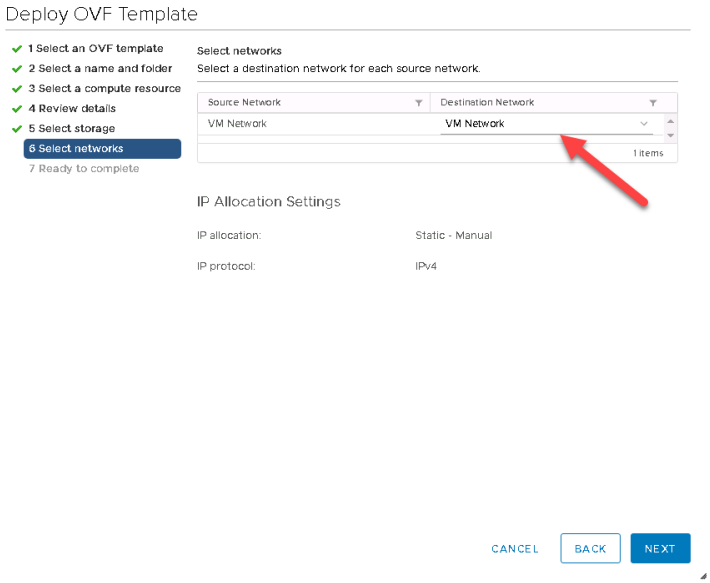
4. Select a Compute Resource to initially host the VM and after you click *Next* the following screen will be shown. Then click *Next*



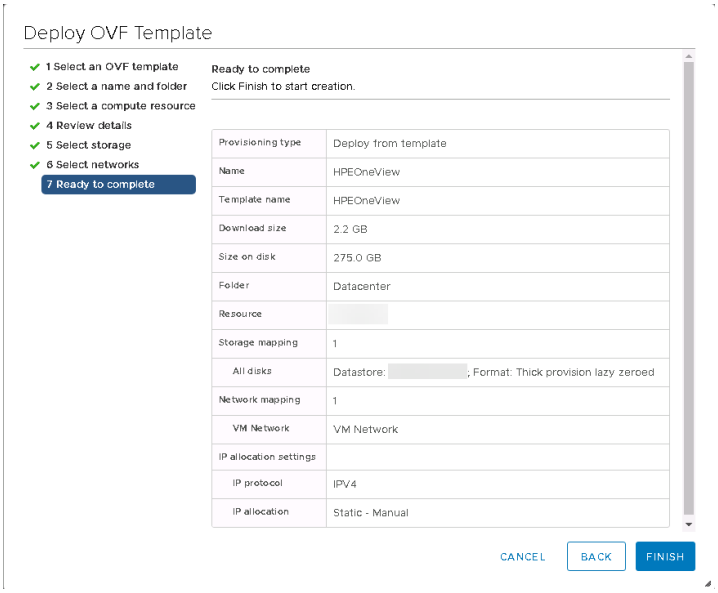
5. Choose the Storage to locate the VM on and then click *Next. HPE recommends that Thick Provision Lazy Zeroed be used for the HPE OneView appliance.*



6. Select the Destination Network for the HPE OneView appliance and click *Next*



7. You will now be shown a summary of your choices and if correct click *Finish*



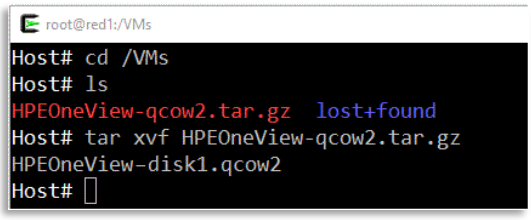
8. The progress window will show you the status of the deployment process.



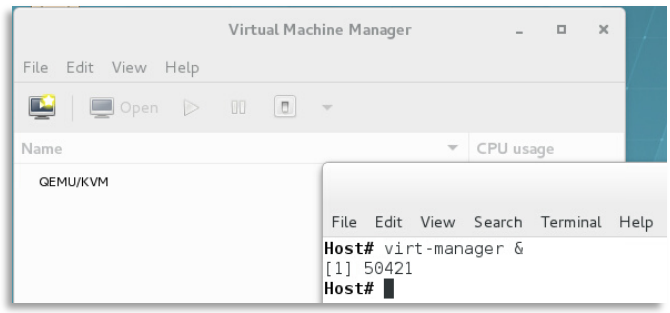
9. Proceed to the First Time Setup to begin to use your HPE OneView appliance

KVM

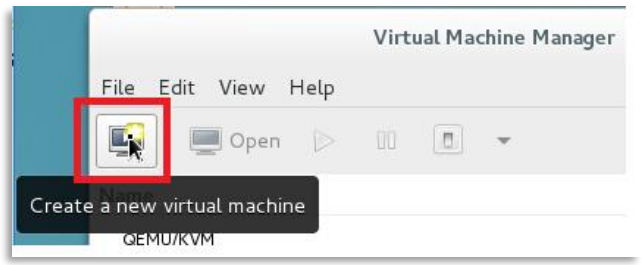
1. Extract the qcow2 image tar.gz file to a location accessible from the Linux host.



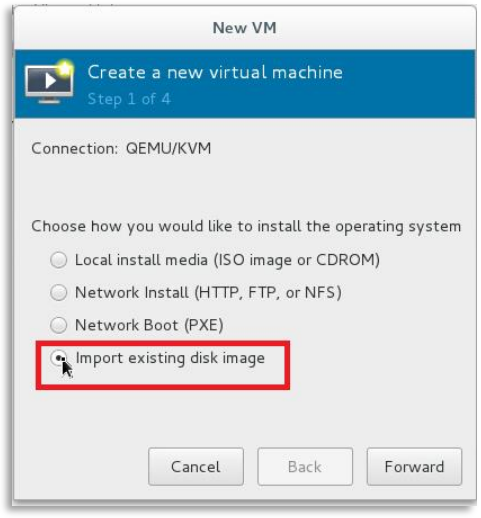
2. Open Virtual Machine Manager, or any other virtual machine management tool.



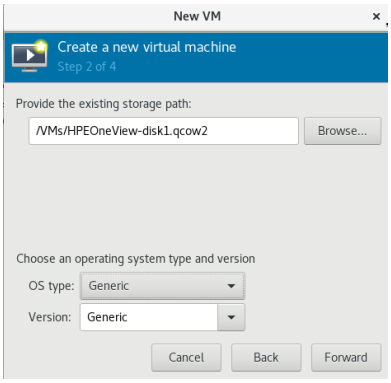
3. From the menu of Virtual Machine Manager, select File > New Virtual Machine to launch the New VM wizard.



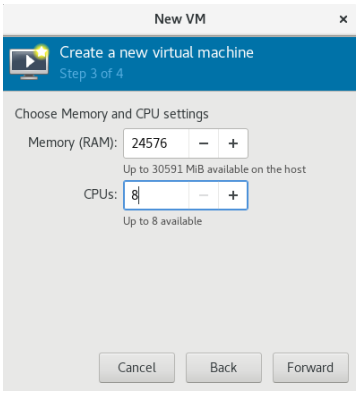
4. Select the Import existing disk image option for installing the operating system.



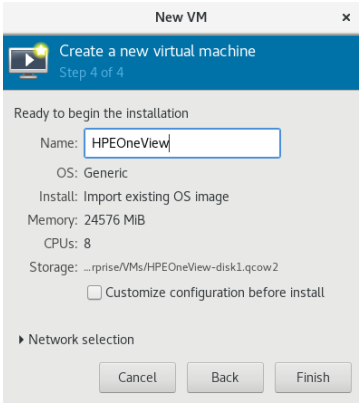
5. Browse to the location of the tar.gz file on your local machine. Select Generic for the OS type and then select Generic for the version.



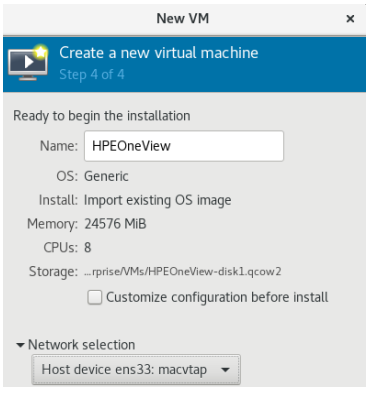
6. Set Memory (RAM) to 24,576 MiB, and CPUs to 8.



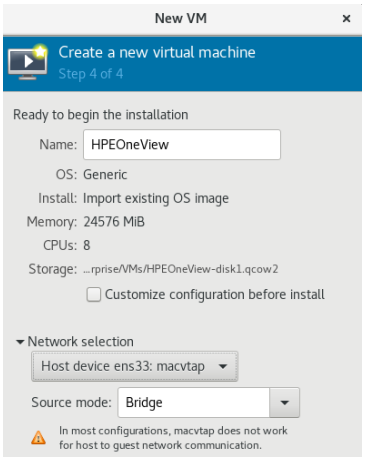
7. Specify the name of the VM.



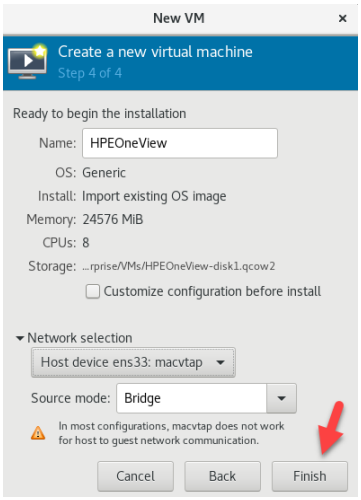
8. Expand the Network selection and select a network device that has connectivity to your management LAN.



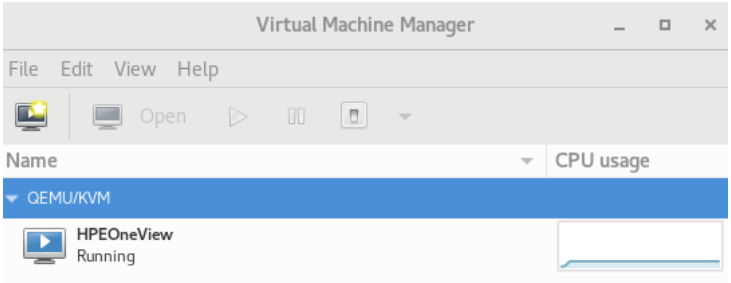
9. Select Bridge as the Source mode.



10. Click Finish.

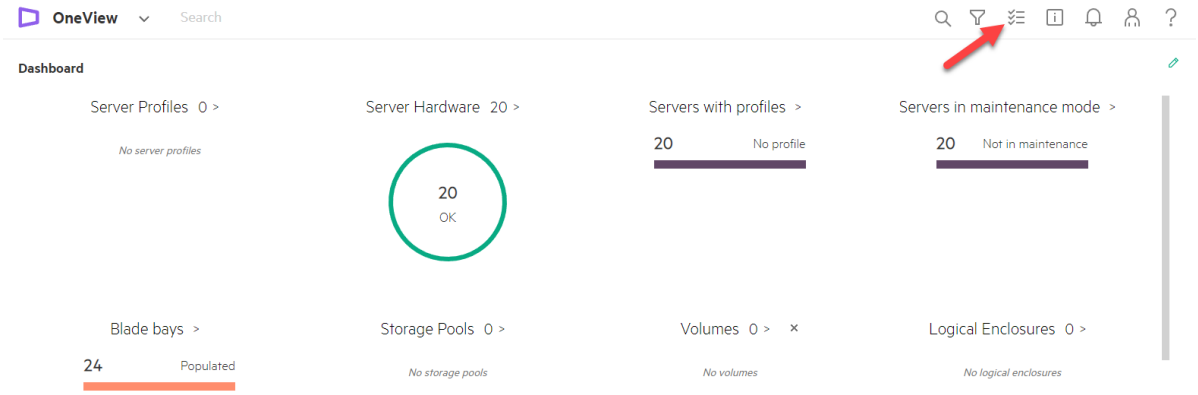


11. The appliance will now start from the virtual machine console

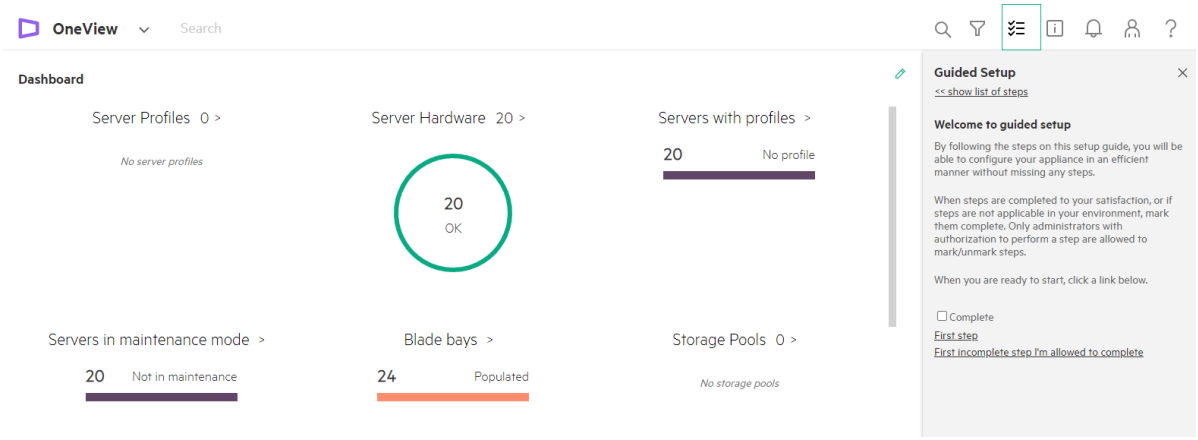


Guided Setup

HPE OneView has a guided setup feature. The guided setup gives step by step guidance for initial system setup along with product tour of key concepts and features. The guided setup can be easily accessed from the dashboard of the HPE OneView appliance.

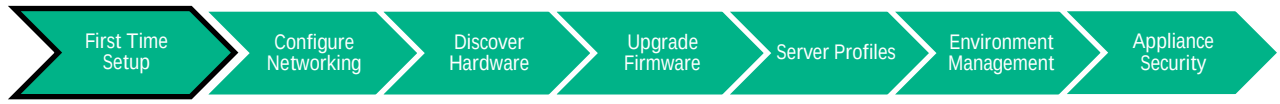


By following the steps on the guided setup, you will be able to configure your appliance in an efficient manner without missing any steps. When steps are completed to your satisfaction, or if steps are not applicable in your environment, mark them complete. Only administrators with authorization to perform a step are allowed to mark / unmark steps.



The remaining portion of the document will discuss, in detail, the sections covered in the guided setup process.

First Time Setup



- Change Administrator password
- Accept EULA
- Remote Support Opt-in
- Configure Appliance IP Settings

Completing the HPE OneView appliance First Time Setup is designed to be simple and straight forward. By default, the management interface is configured for IPv4 DHCP. If DHCP is not available on the management network, you can access the Kiosk Browser within the VM console to complete the initial setup. If DHCP is available, you can configure the appliance with a browser remotely to complete the First Time Setup. The First Time Setup consists of Accepting a License Agreement, HPE Remote Support Access for remote troubleshooting, changing the default Administrator account password and configuring IP information.

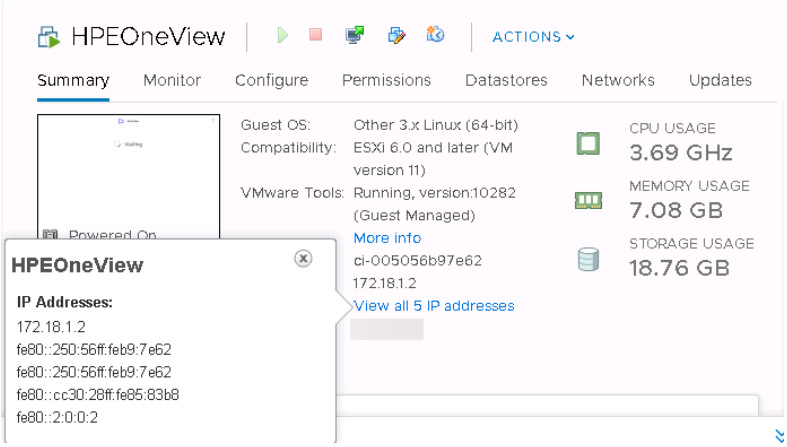
Installation Checklist

Prior to continuing with this document, please make sure you have completed the following:

Table 7. Installation Checklist

Task	Completed? (Y|N)
Have a supported KVM, Microsoft Hyper-V or vSphere 6.[2] or newer ESXi host for appliance	
Have Static IP Address, or DHCP Static Reservation	
Have DNS A and PTR Records created	
Have NTP Server FQDN or IP Address information	

1. Obtain the Virtual Machine IP Address from the VMware VIClient

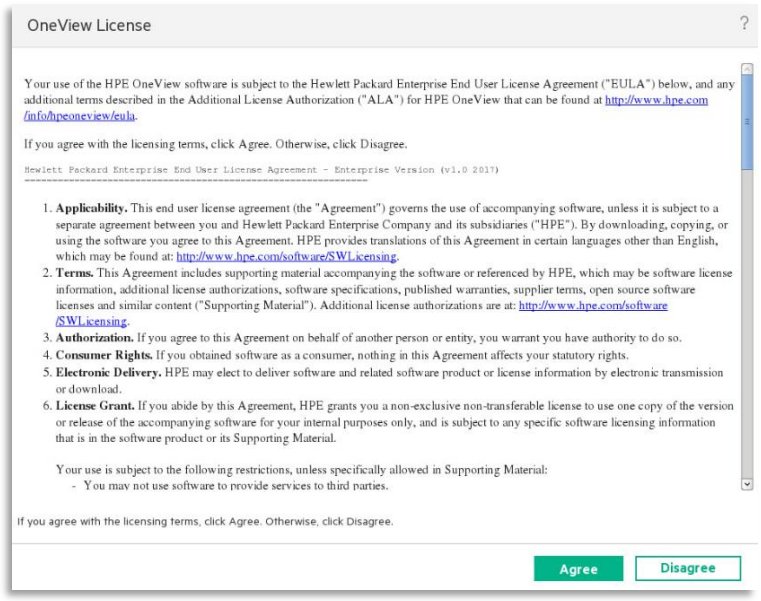


2. Open a supported Web Browser to the noted IP Address to complete the First Time Setup. If DHCP is not available, then you can continue the following steps using the embedded Kiosk Browser, by launching the VMware VM Remote Console or the Microsoft Hyper-V Remote Console.

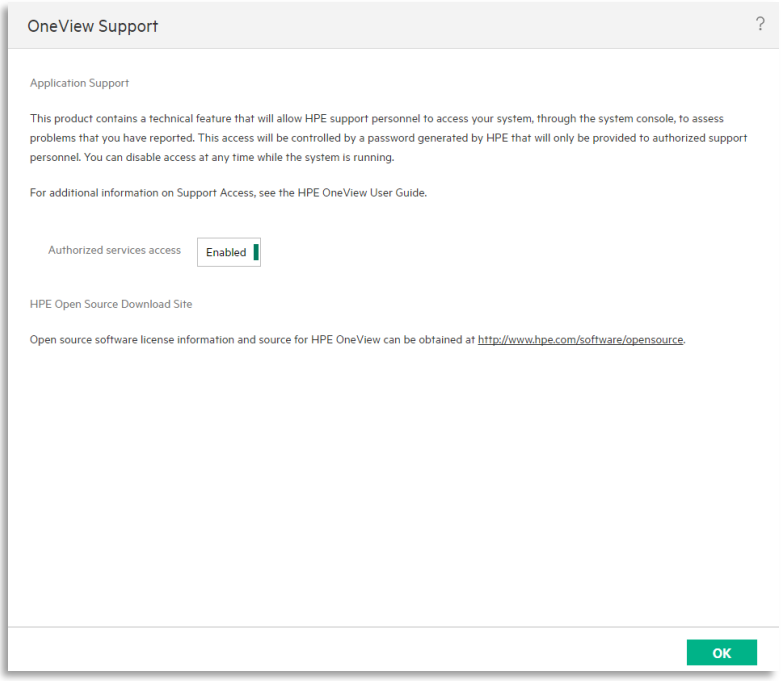
Note:
If the hypervisor host is Window Server Hyper-V, then the First Time Setup must be completed using the appliance console via the Hyper-V Remote Console.

[2] Please review the HPE OneView Support Matrix on http://www.hpe.com/info/oneview/docs for the officially supported hypervisors.

3. Read and if you accept the licence agreement, click on *Agree*



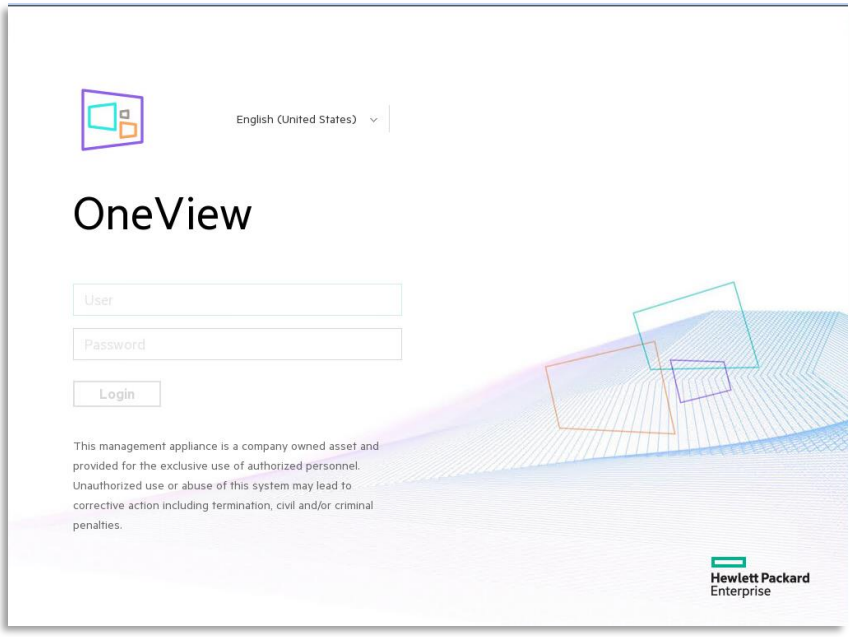
4. The HPE Support Access Opt-In is used for HPE Support Services remote access when the appliance is in an unhealthy state, and core services cannot start. By opting out, this also disables the ability to reset the appliance Administrator account password if ever lost.



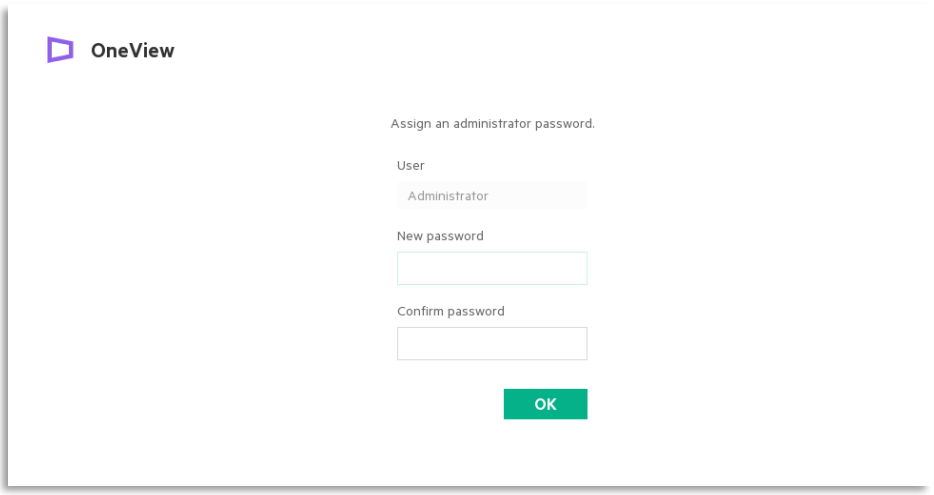
5. Login to the appliance using the default credentials

Table 8. Appliance Administrator Default Credentials

Username	Password
Administrator	admin

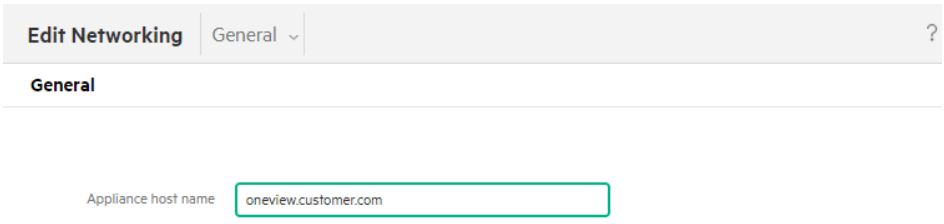


6. Change the default Administrator password.

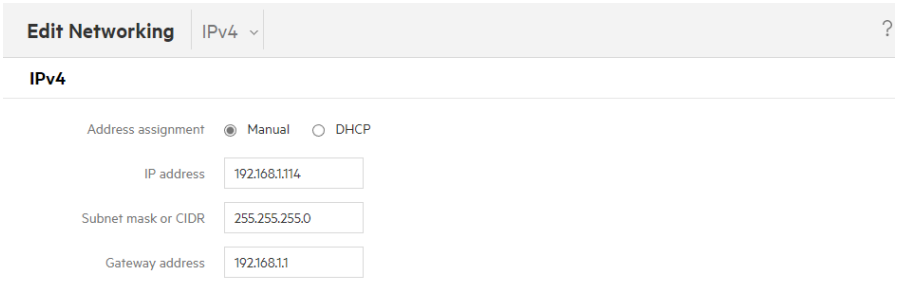


7. In the General section of the Appliance Networking window, enter a *hostname for the appliance* (e.g. oneview.customer.com)

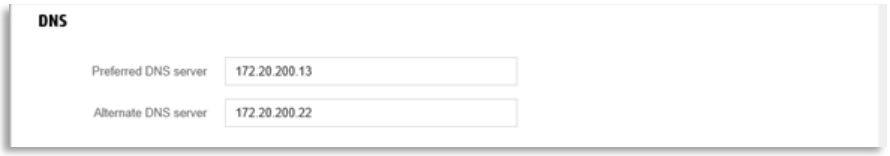
   a. If you specify an FQDN, verify valid A and PTR records exist. The appliance will perform a nslookup of the FQDN and IP address and report an appliance warning if neither are available / resolve.



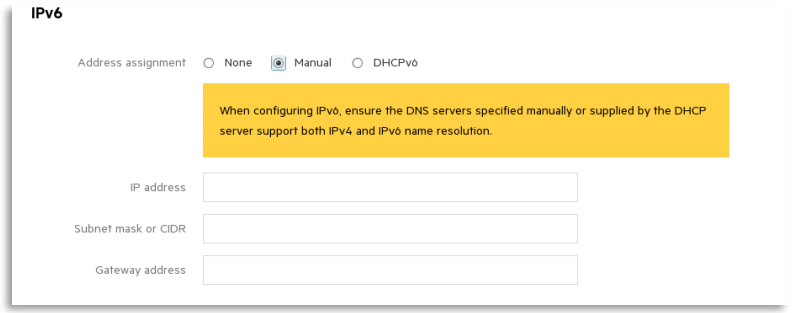
8. In the IPv4 section of the Appliance Networking window, enter *the IPv4 Address, Subnet Mask and Default Gateway for the appliance* (DHCP or Static can be used). If you are wanting to run the appliance in straight IPv6 mode select None for the IPv4 address assignment.
    a. DHCP is only supported when DHCP Static Reservations are used.



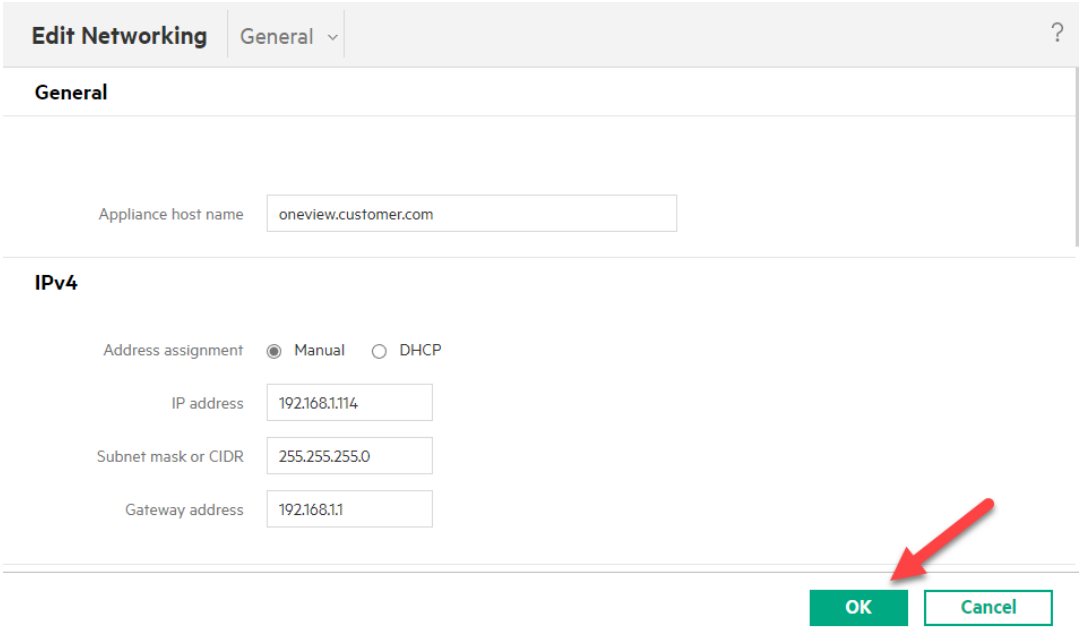
9. (Optional) In the DNS section of the Appliance Networking window, enter the *Preferred and Alternate DNS server addresses* for the appliance



10. (Optional) In the IPv6 section of the Appliance Networking window, configure the *IPv6 address* for the appliance



11. Click *OK* to apply the configuration.



12. After clicking OK, the appliance will configure those parameters. If you selected Static for the IP Address Assignment, you should be redirected to the new IP address. Please accept the certificate security warnings during the redirection, as a new SSL certificate is generated from the FQDN.

HPE Synergy Composer First Time Setup

1. Connect to the Composer

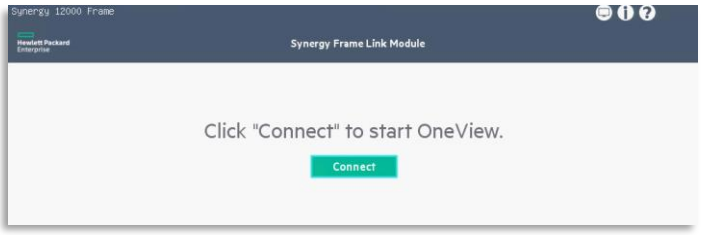
   Option 1: Connect to the Front Panel by connecting a monitor to the display port and the USB hub with a keyboard and mouse to the USB port.



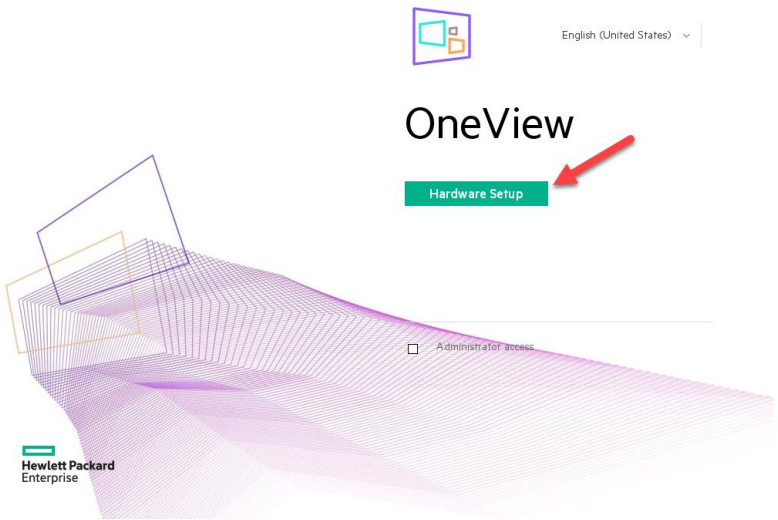
   Option 2: Connect to the Front Panel with a laptop.

   - Configure the notebook computer Ethernet adapter for DHCP and enable auto-negotiation.
   - Use a standard CAT5 or newer cable to connect the notebook computer Ethernet port to the notebook port on a front panel module. (A crossover cable is not required).
   - Wait for the notebook computer to obtain a DHCP address. The address the Frame issues should be 192.168.10.2
   - On the notebook computer, launch a VNC client application to connect to the Synergy console. If prompted by the VNC client, enter the Synergy frame IP address (including port 5900) to use for the connection: 192.168.10.1:5900

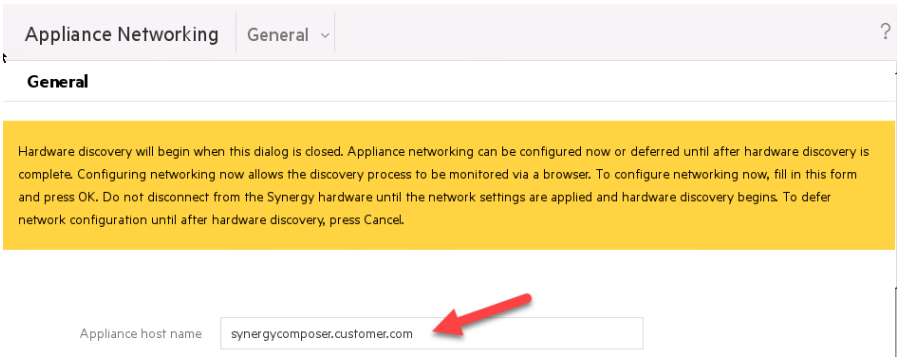
2. From the Synergy Frame Link Module screen, click the Connect button to launch HPE OneView



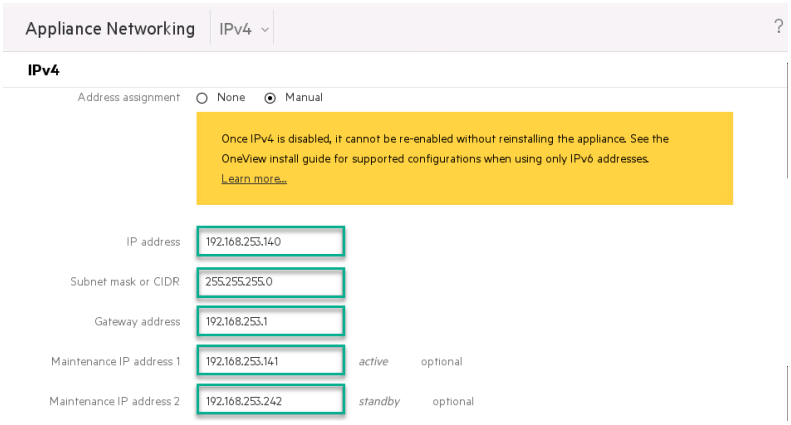
3. To connect with install technician user privileges, click Hardware Setup. This initiates the self-discovery of devices on the management ring using IPv6 link-local.



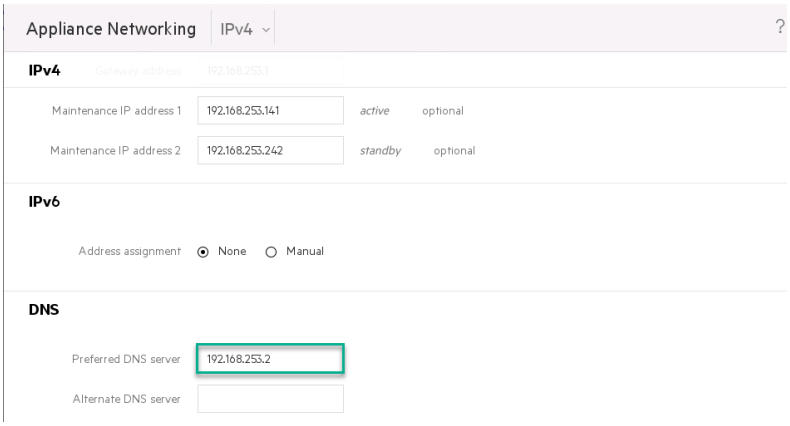
4. Enter the hostname for the Composer



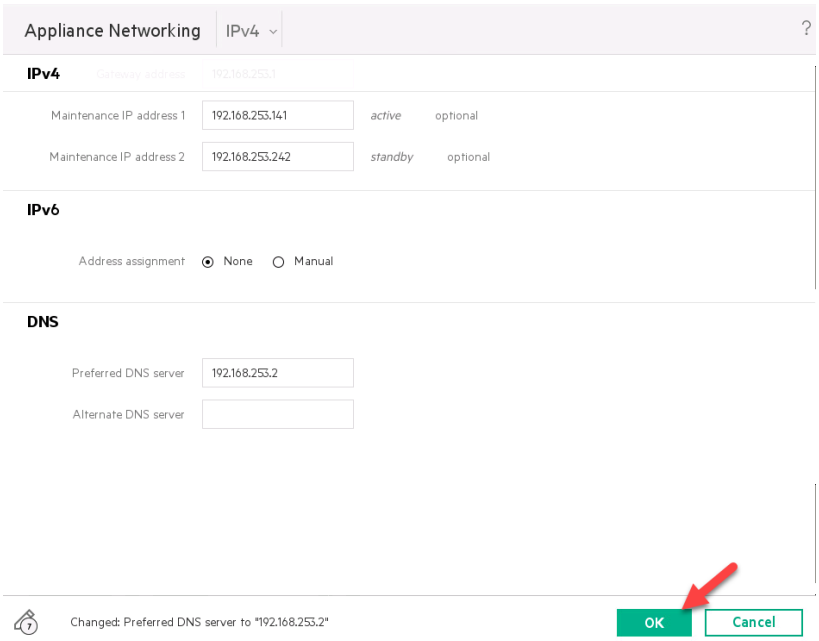
5. Enter the IPv4 information for the Composer, you need to enter information for ALL fields ie Gateway address, and the two Maintenance IP Addresses even though they are listed as “optional”.



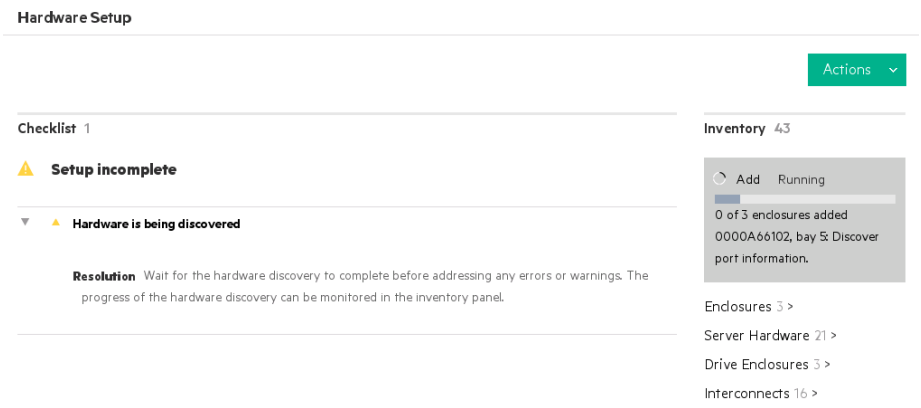
6. Enter the DNS information for the Composer



7. Click OK to begin hardware discovery

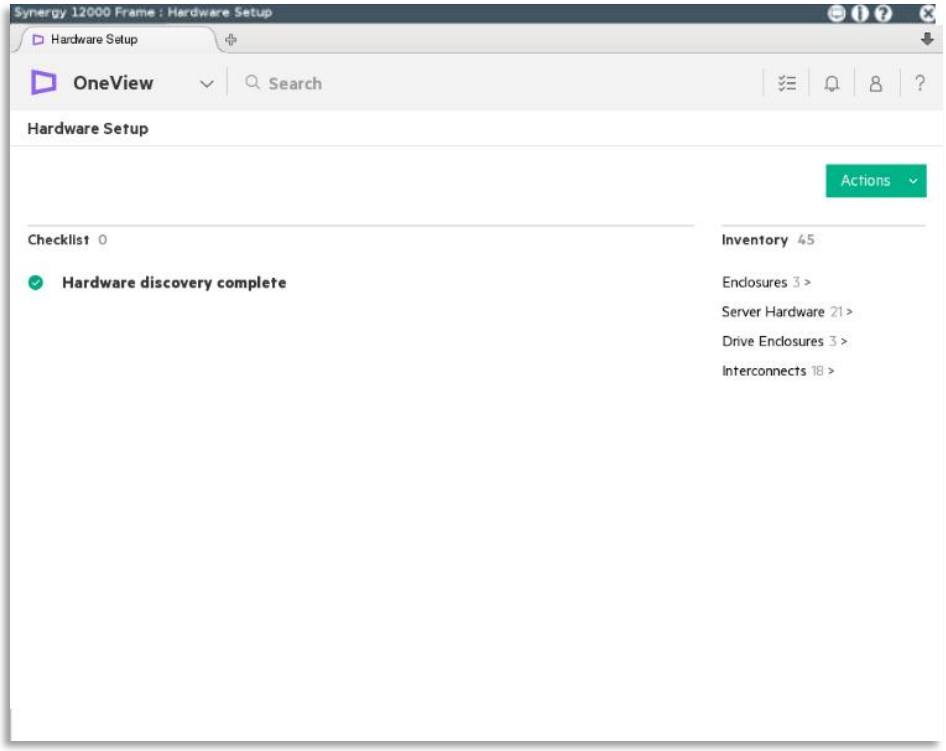


8. The composer will automatically discover all of the hardware within the Management Ring.



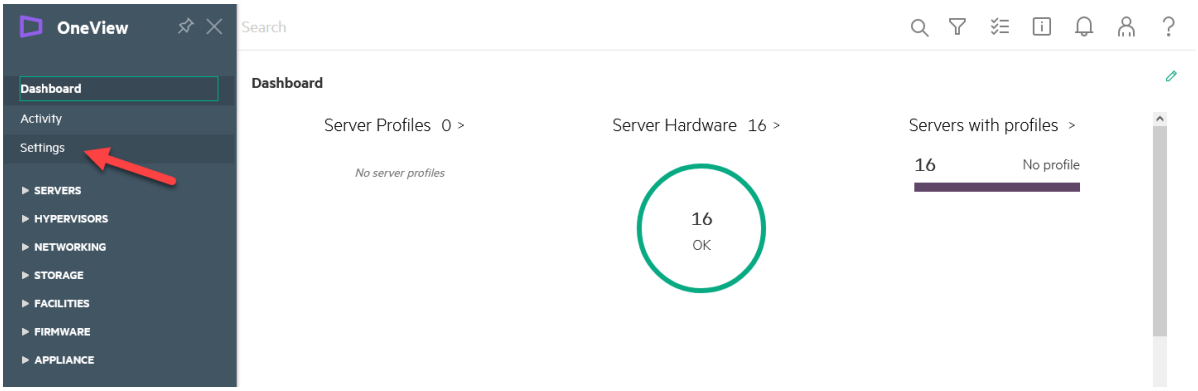
9. Review the hardware inventory after HPE OneView completes the add operation.
10. Confirm that the inventory includes all installed components.
11. For any hardware not discovered by Synergy Composer powered by HPE OneView, look for problems with frame link module cabling, hardware not fully inserted, or other hardware issues.

12. Review and correct any issues listed in the Hardware Setup Checklist. To troubleshoot all issues, follow the corrective actions in HPE OneView.

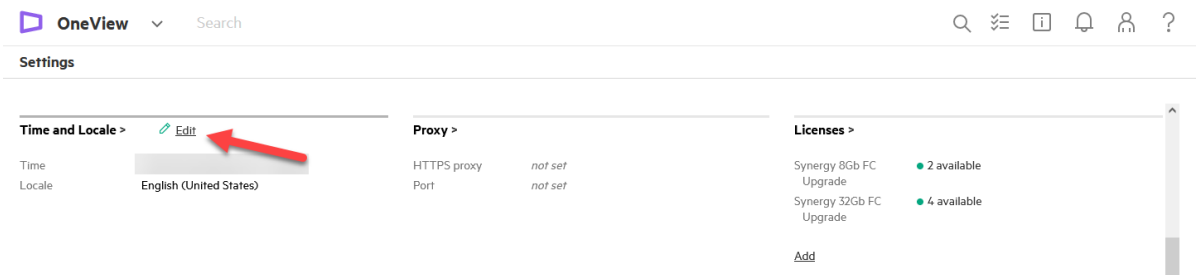


Set Time and Language (Optional)

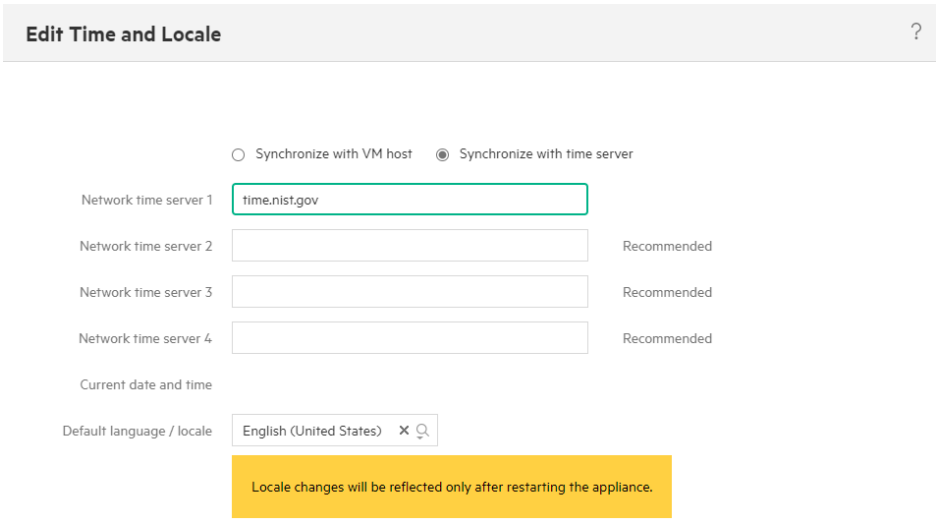
1. From the Top-Level menu, click *Settings*



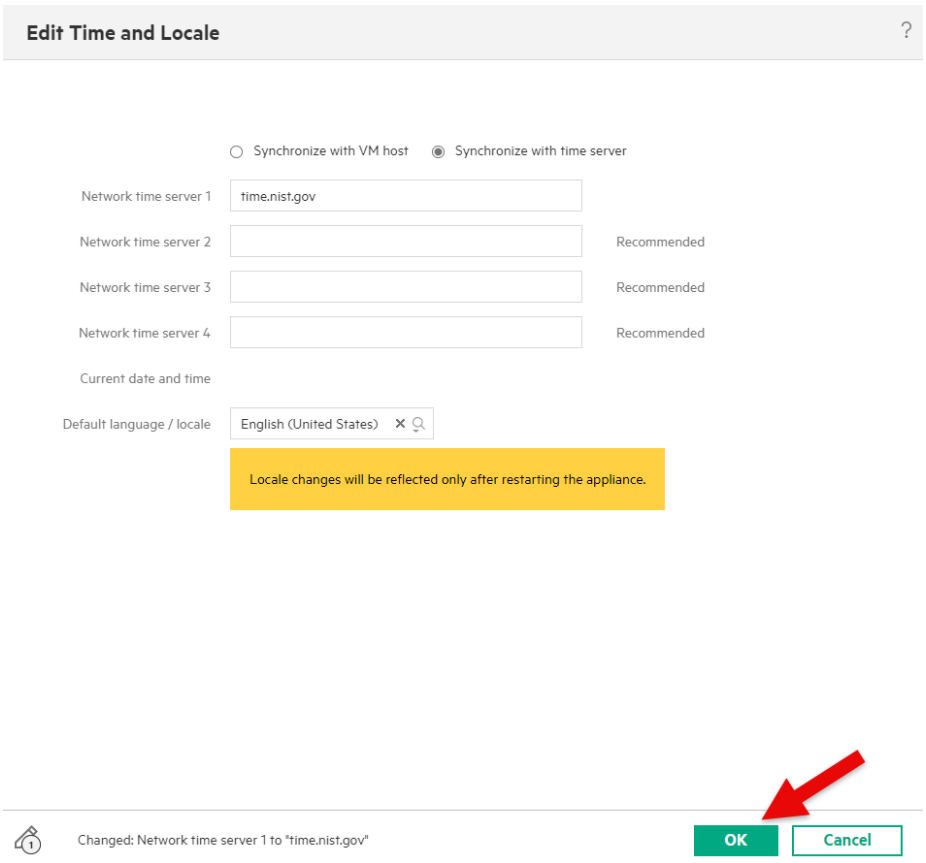
2. Click *Edit* in the *Time and Locale* section of the settings window



3. Configure the NTP and Locale information for the appliance



4. Click *OK* to apply the changes.

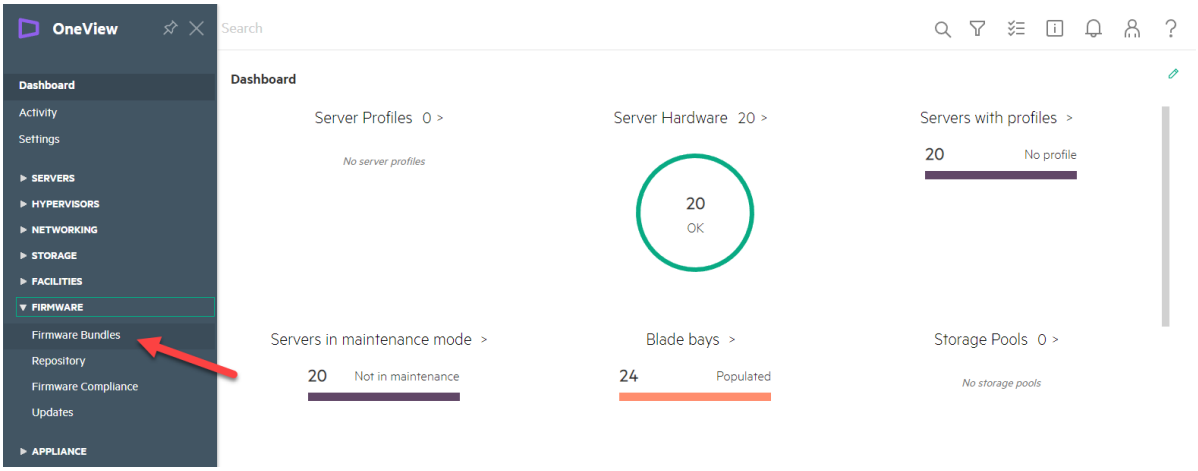


Note:
Any language / locale changes will require a restart of the HPE OneView appliance.

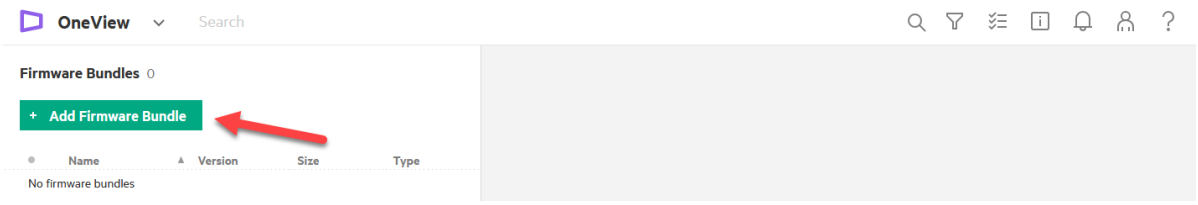
HPE OneView Appliance based Firmware Repository

The HPE OneView virtual appliance does not ship with a default SPP (Service Pack for ProLiant) or SSP (Synergy Service Pack) for the Synergy Composer. It is necessary to upload an SPP / SSP, unless a custom baseline (created by HPE SUM / HPE Custom SPP Portal) is required.

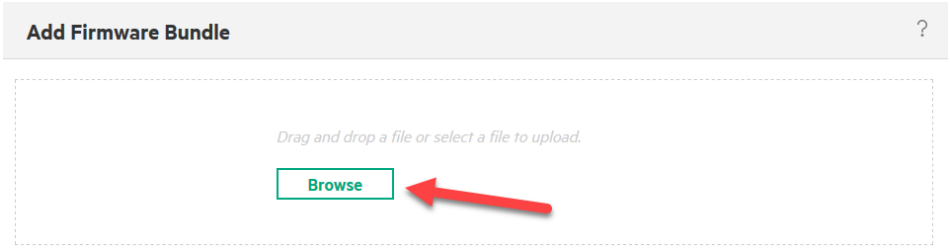
1. From the Top-Level Menu, expand the *FIRMWARE* option and then select *Firmware Bundles*



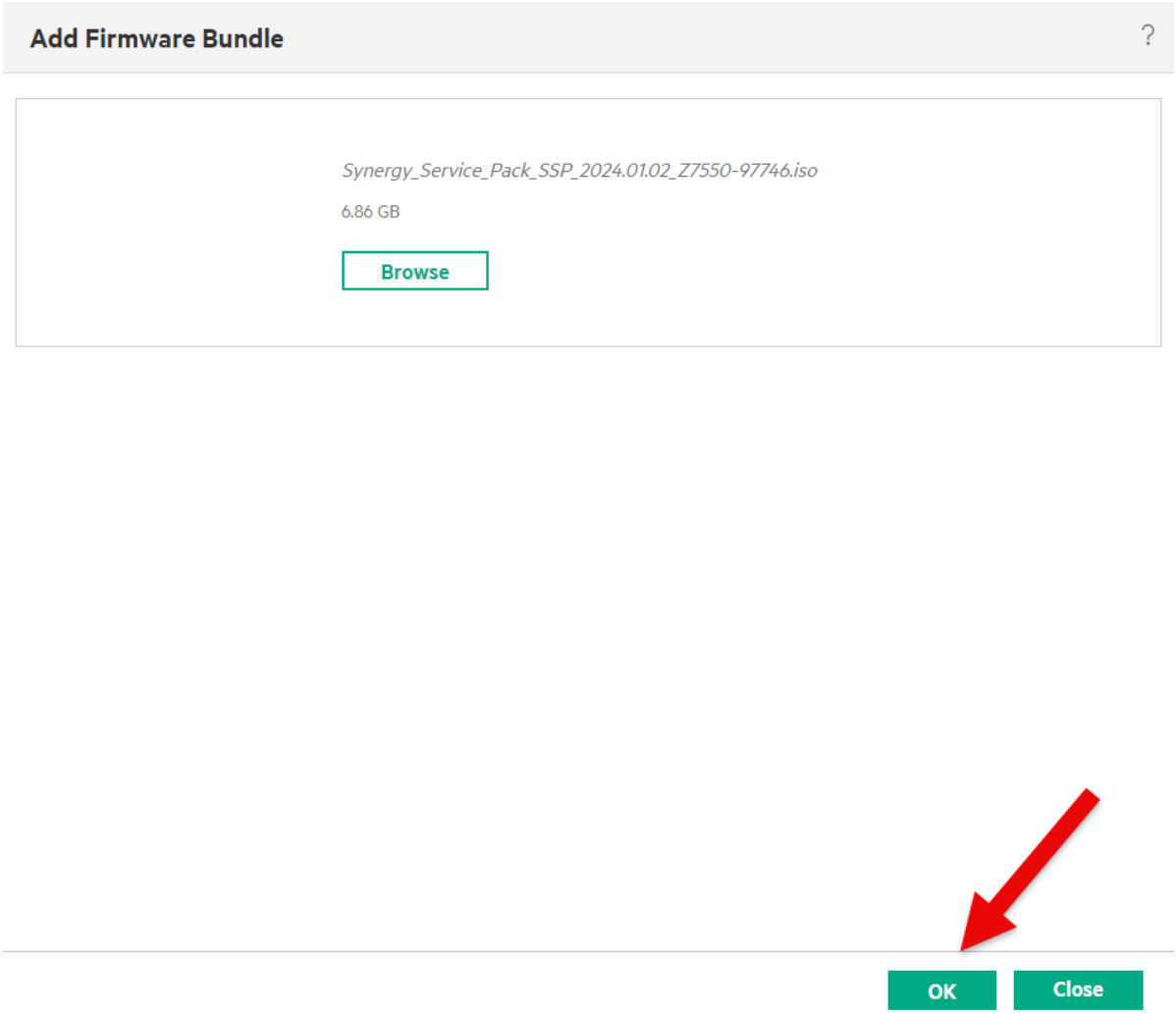
2. To upload an SPP / SSP Bundle, click the + *Add Firmware Bundle* button



3. On the Add Firmware Bundle window, click on the *Browse* button, and select the SPP / SSP ISO to upload.



4. Once selected, click the *OK* button. You can also drag-and drop firmware bundles (SPP / SSP) within Windows environments. You can navigate away from the Firmware Bundle screen to other areas within the UI, as the upload process is a background process within the browser.



5. The SPP / SSP upload will begin.

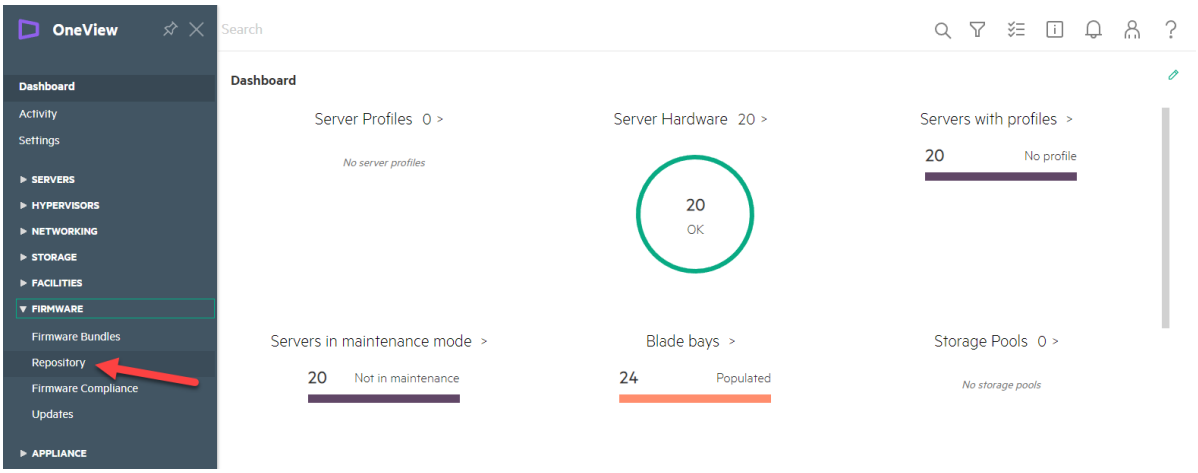
Note:
Do not close the browser window until the Firmware Upload task has completed.

External based Firmware Repository

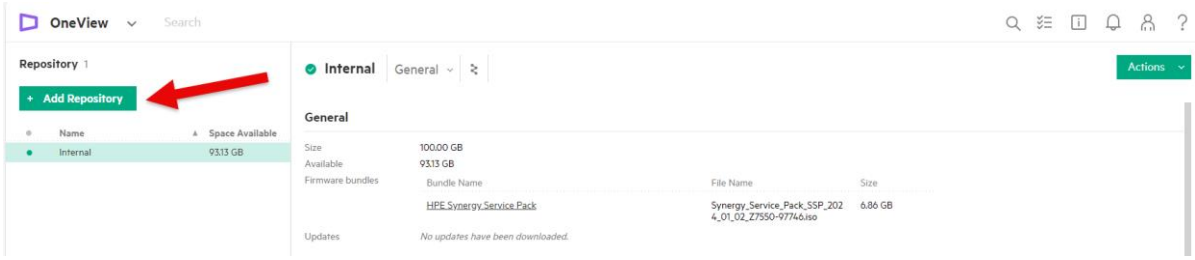
HPE OneView 3.1 or later supports external firmware repositories.

Note: *For details on how to configure a Windows or Linux Web Based external repository that OneView can use, please see the OneView Help by typing "External Repository"*

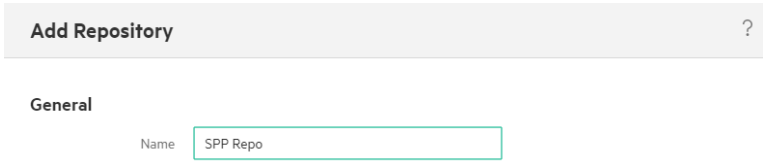
1. From the Top-Level Menu, select *Firmware* and then *Repository*



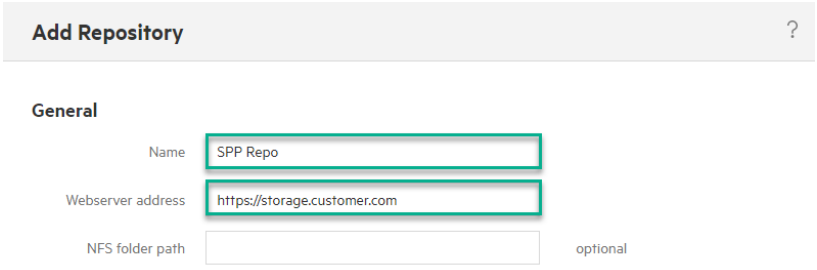
2. On the side of the page, click on the + *Add Repository* button



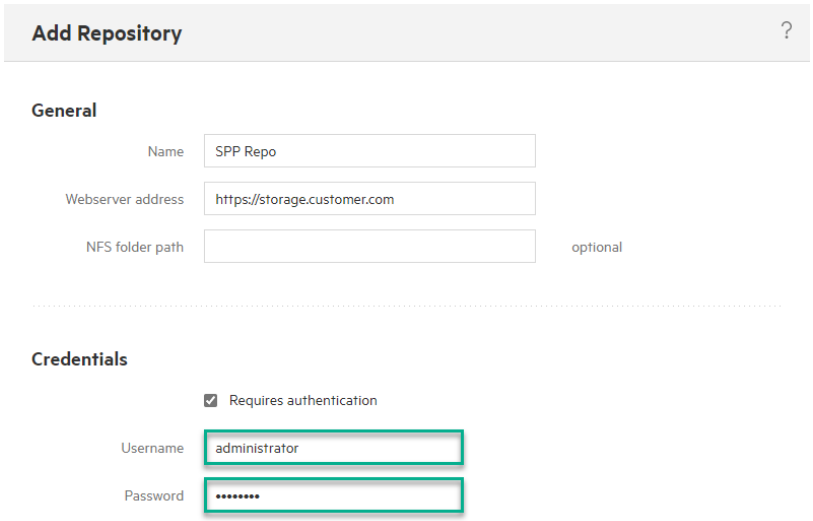
3. In the Add Repository menu, enter a name for the Repository.



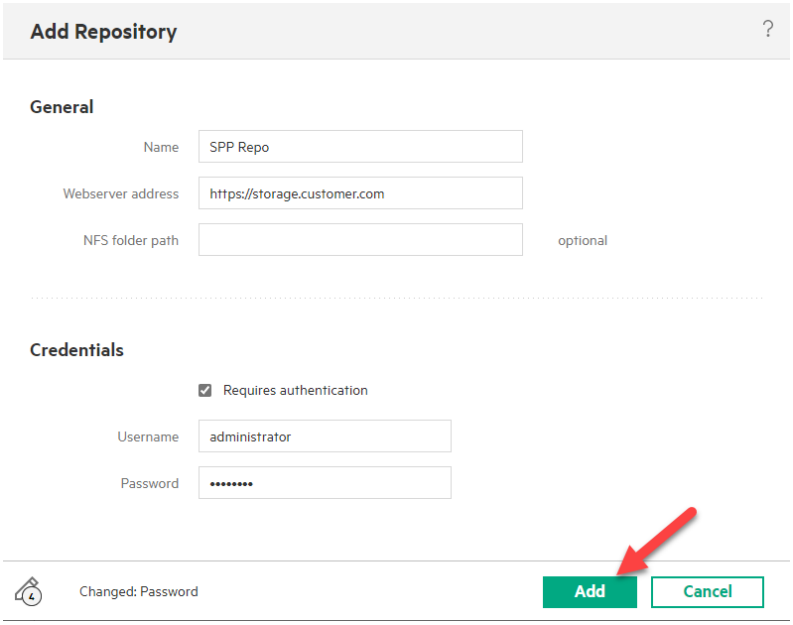
4. In the Add Repository menu, enter a webserver address for the Repository.



5. In the Add Repository menu, enter the credentials to access the Repository.



6. Click the *Add* button to finalize the repository.



Adding HPE OneView Advanced Licenses to the HPE OneView Appliance

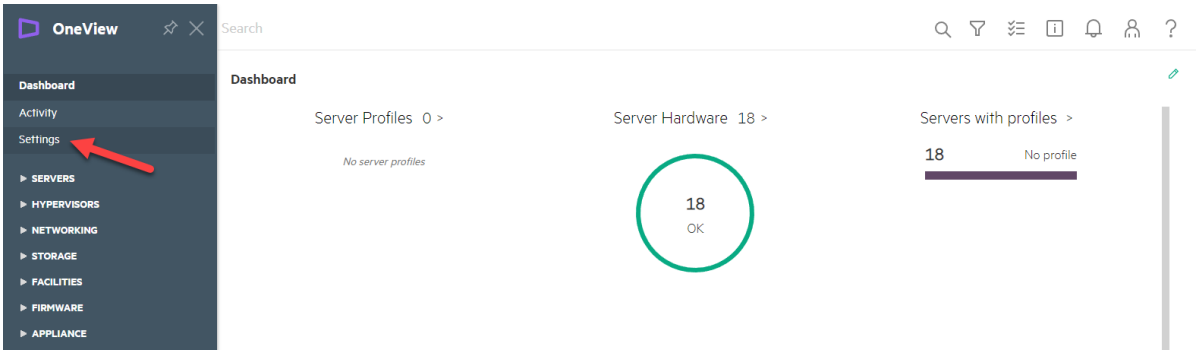
HPE OneView licensing is designed to be simplified, with the Advanced license may be embedded within the iLO. Please refer to the HPE OneView Quickspecs for all possible licensing options.

Note: *There are no OneView or iLO Advanced licenses required for the Synergy Compute Modules they are "included" with the HPE Synergy Composer Appliance. The only licenses you would add to the HPE Synergy Composer are for Virtual Connect to enable Fibre Channel (FC) Support.*

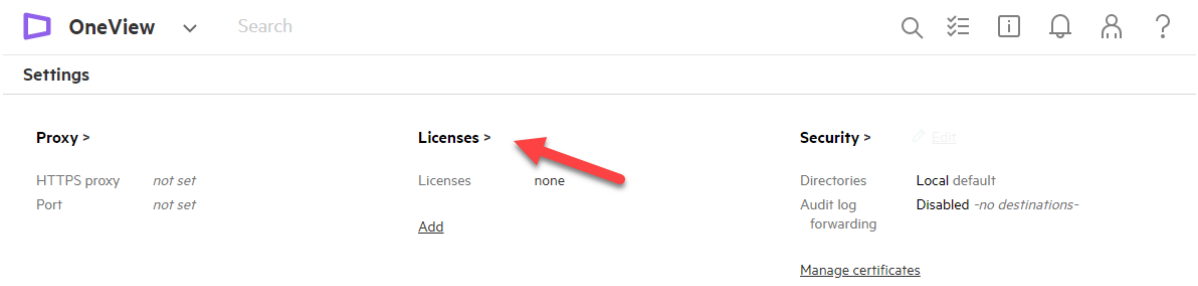
HPE OneView also has a built-in 60-day Advanced evaluation license. During this HPE OneView Advanced license evaluation period, HPE OneView will not enable iLO Advanced features or functionality. The ILO Advanced license (trial or retail) is also required for server and performance monitoring.

If you have received a license key, use the Appliance Settings menu to add licenses. The following steps outline that process.

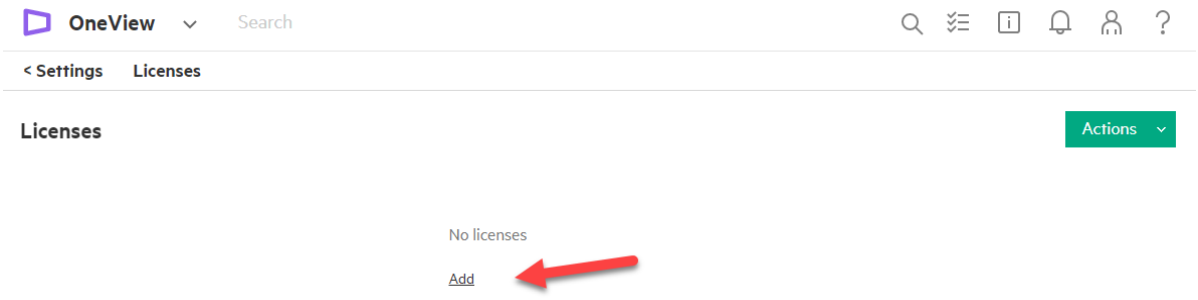
1. From the Top-Level Menu, select *Settings*



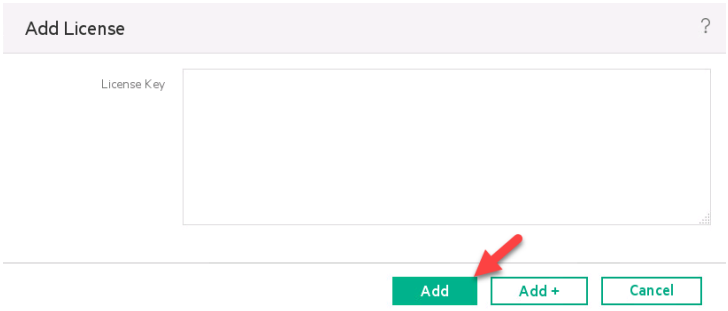
2. From the main settings menu, select *Licenses*



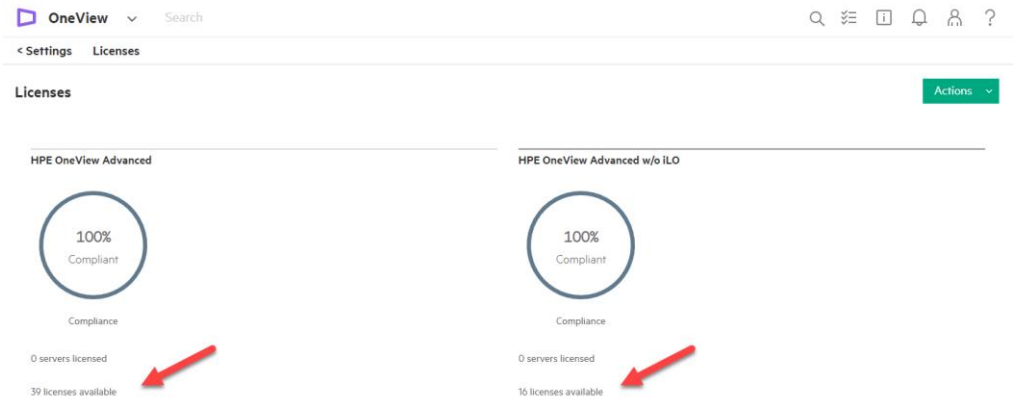
3. Select *Add License*.



4. In the Add License dialog box, paste in your license key in the dialog box and click *Add* to apply the license.



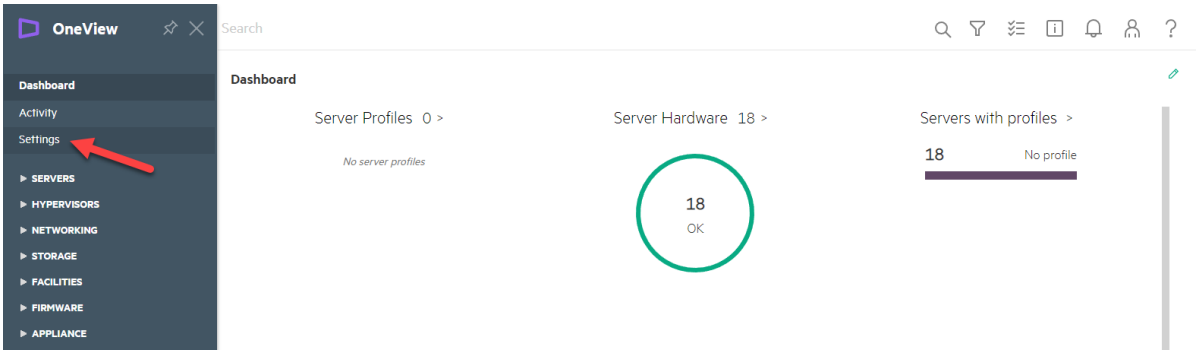
5. On the Licenses page, verify that your license count has increased.



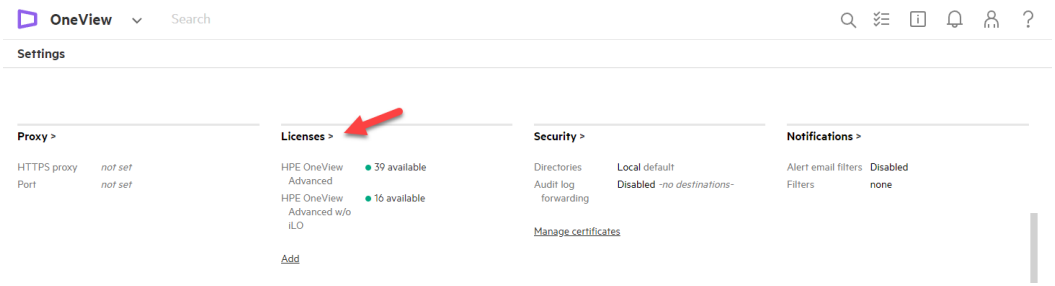
Viewing HPE OneView Licenses

With the release of HPE OneView / Synergy Composer Powered by OneView 6.6 there is a new option to view the licenses in the appliance. It will show the license keys, what it is available and if used what it is allocated to.

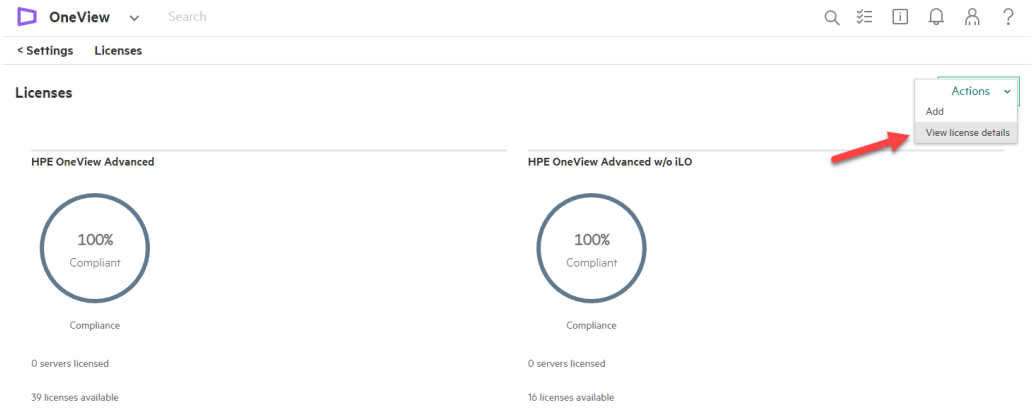
1. From the Top-Level Menu, select *Settings*



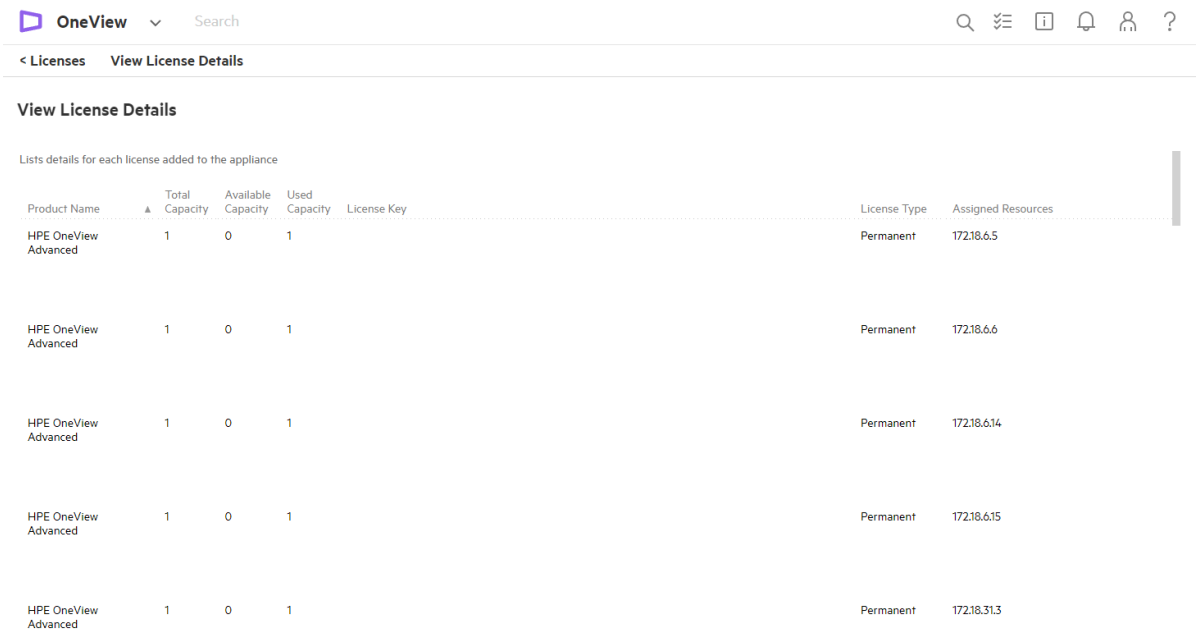
2. From the main settings menu, select *Licenses*



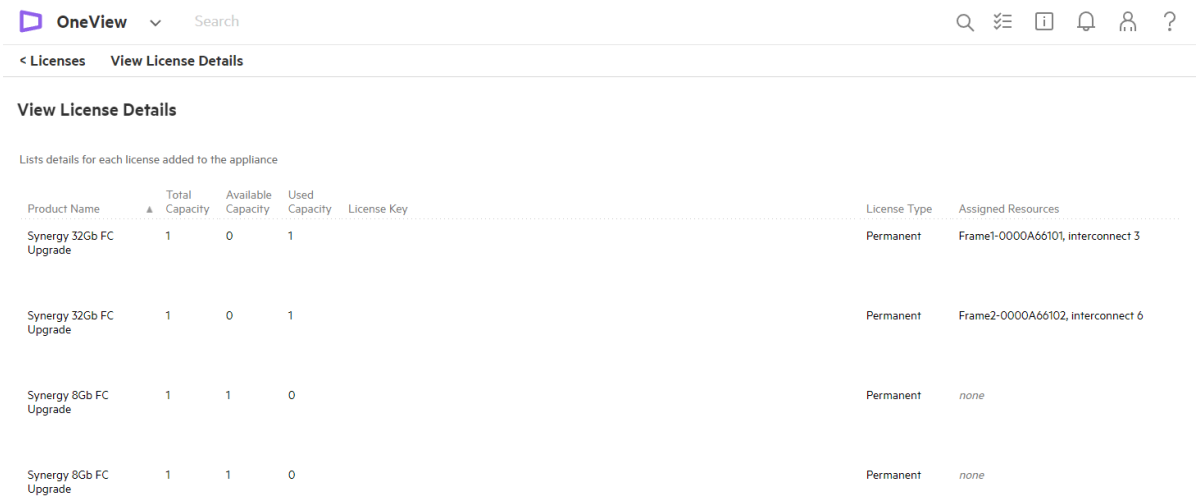
3. From the Action Menu you can select *View license details*



4. This then shows all the license details and what Servers / Devices they have been assigned to



Or for Synergy



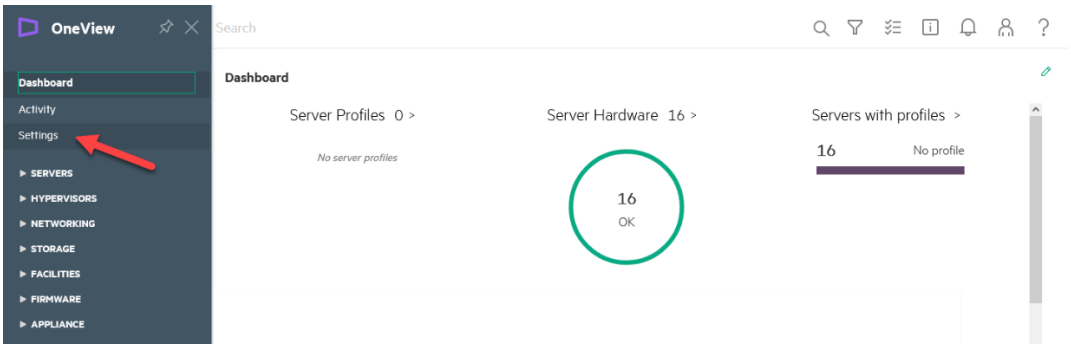
Notification and Automated Download of Available Firmware / Driver Updates

HPE OneView / Synergy Composer powered by OneView with the release of version 6.3 introduced new functionality which (if OneView has Internet access) allows HPE OneView to automatically check for new HPE Service Pack for ProLiant (SPP) or Synergy Service Pack (SSP). If an update is available you are notified via HPE OneView that there updated firmware which can be downloaded.

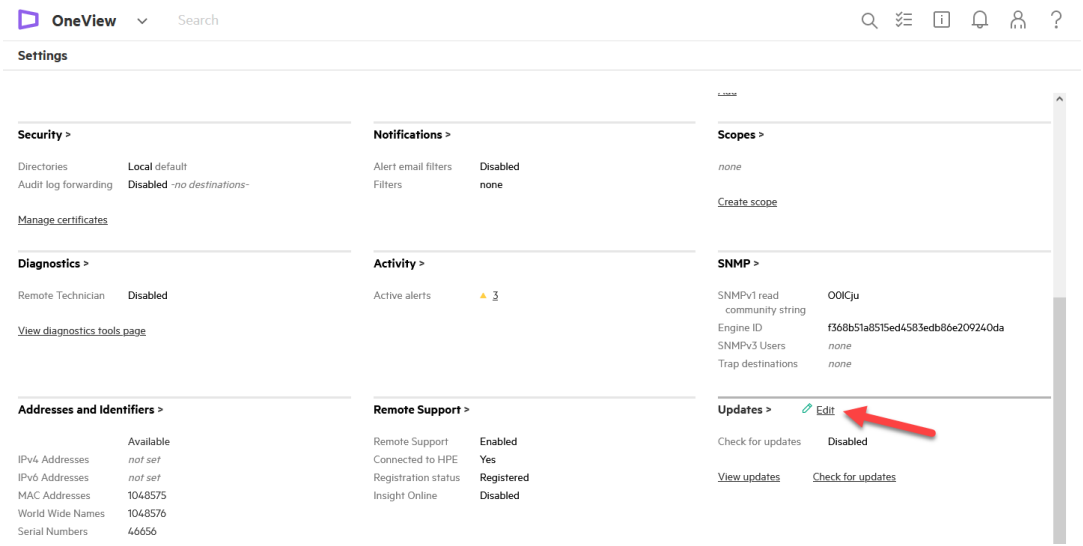
Once the Check for updates functionality is enabled you can use it to schedule periodic checks or perform a check manually. If you have enabled FIPS or CNSA mode then this functionality cannot be enabled.

With the release of HPE OneView / Synergy Composer 8.5 a new feature has been released that enables inventory-based firmware and software downloads. This requires a user token to be generated in the HPE Support Center and is also used to verify access to software and firmware components.

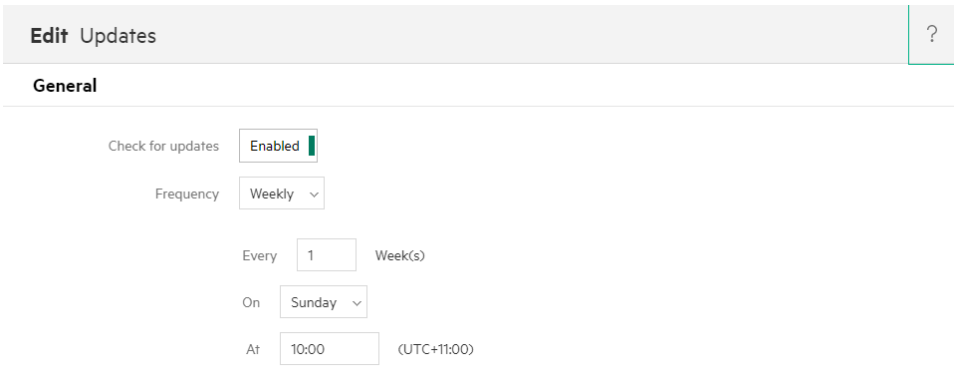
1. From the Top-Level Menu, select *Settings*



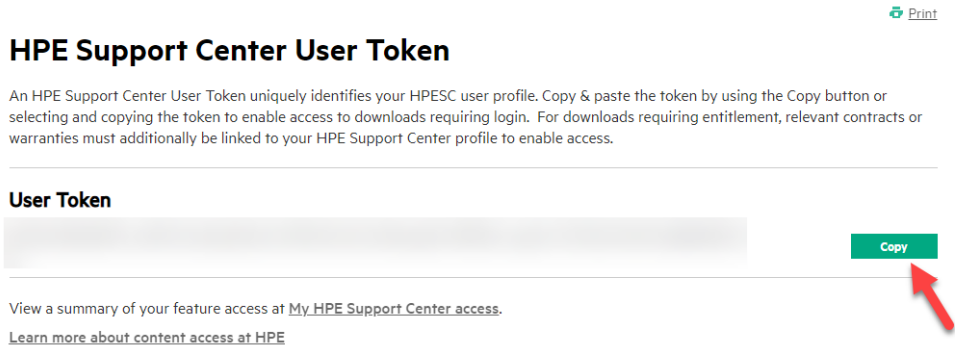
2. From the main settings menu select *Edit* in Updates (or click on *Updates*)



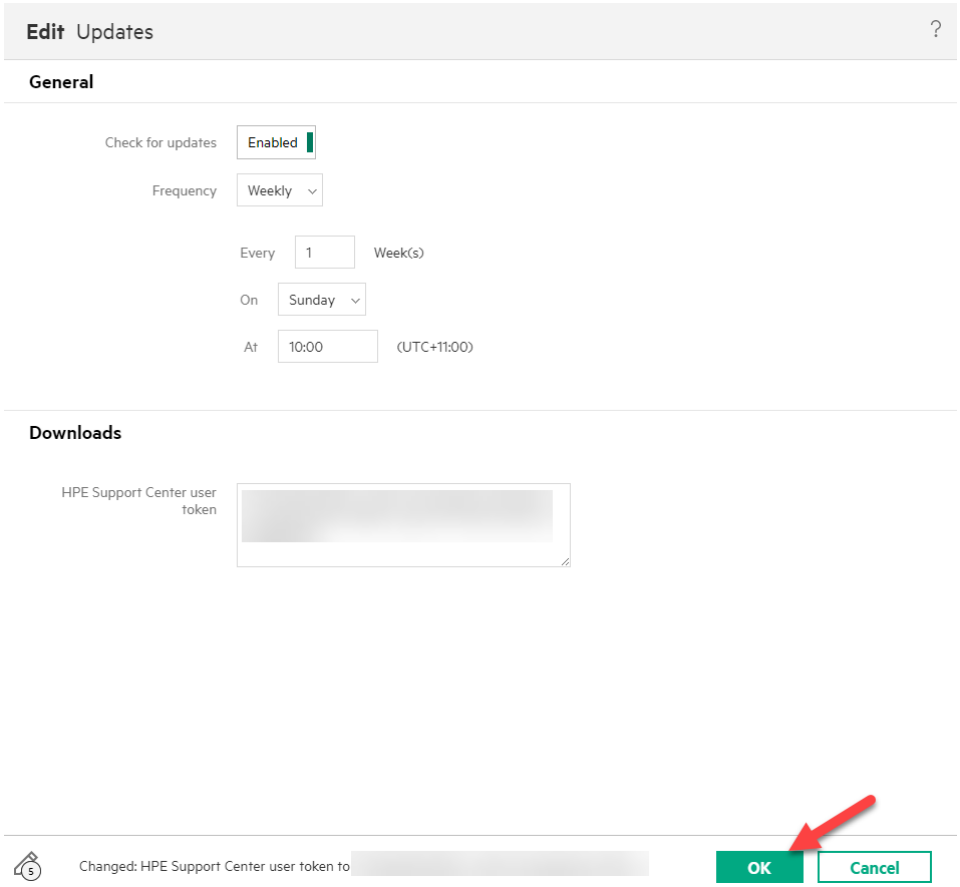
3. You now need to *Enable* the Check for updates functionality



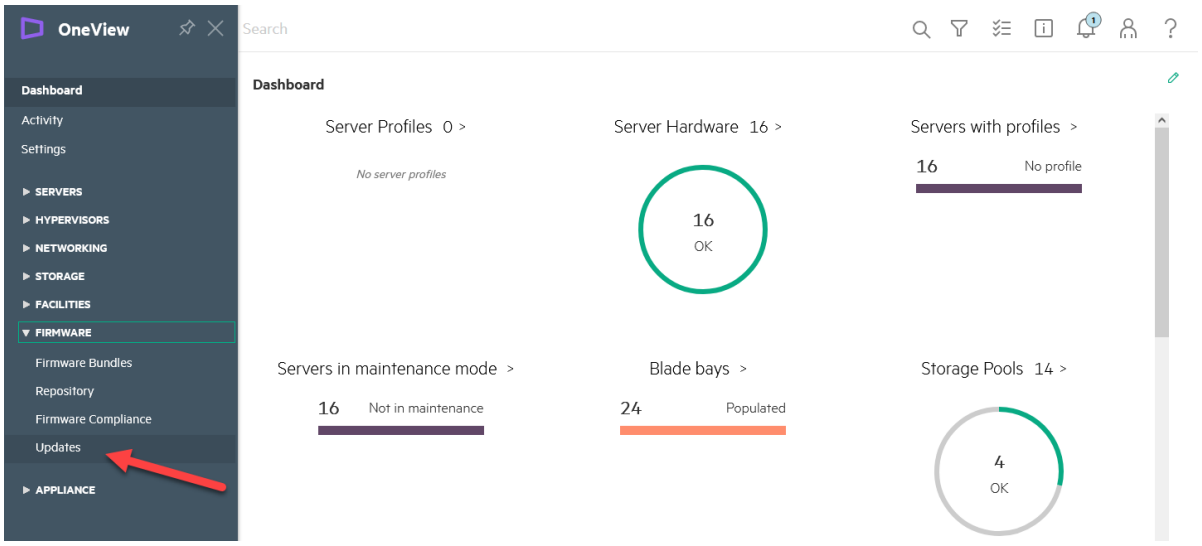
4. To enable the HPE Support Center you will need to *generate a user token* from the HPE Support Center (further step by step details available in OneView help by clicking on the **"?"** in the top right). Once you have logged in the you can *Copy* the token that has been generated to the clipboard



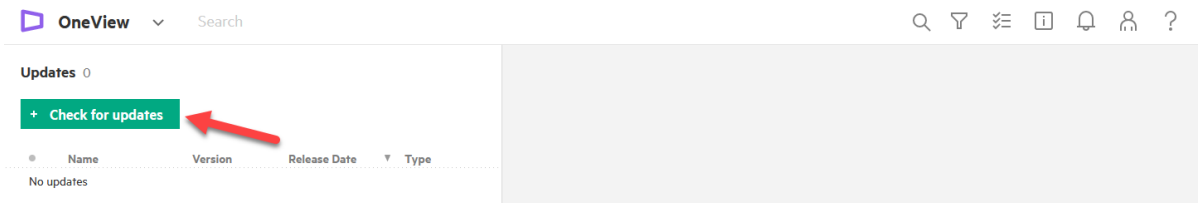
5. You can now paste the User Token into the provided field and click *OK* to continue.



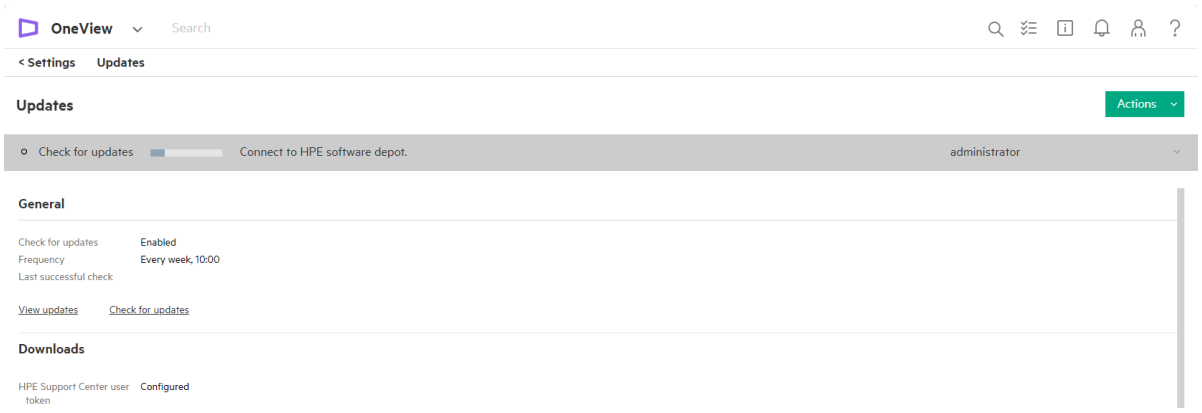
6. From the Top-Level menu expand *Firmware* and choose *Updates*.



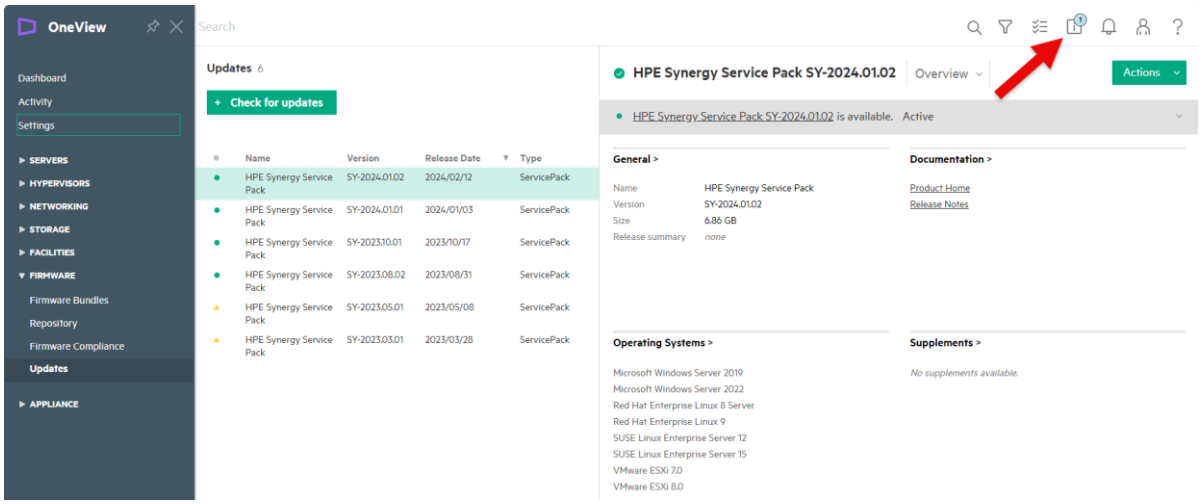
7. Click on + *Check for updates* to check and see if any updates are available



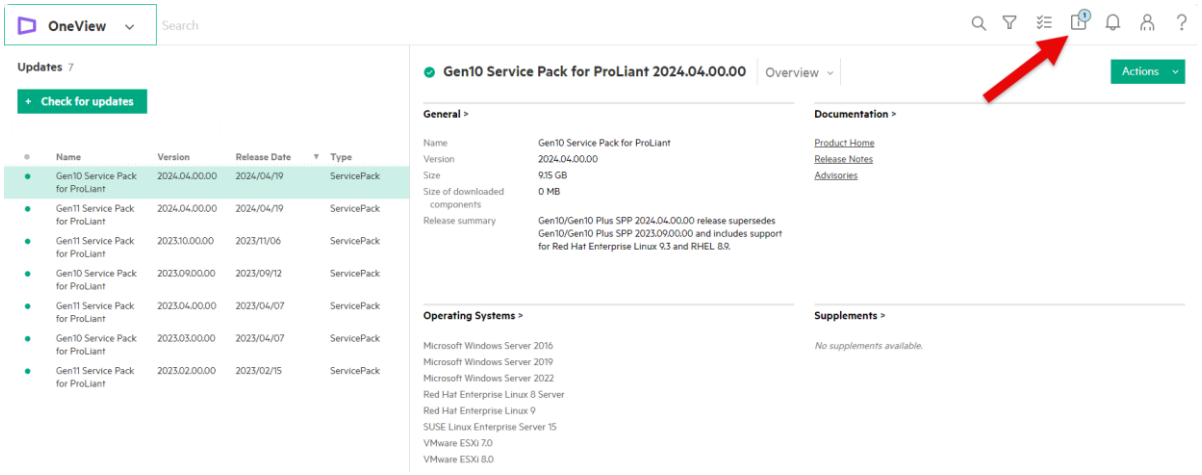
8. It will now connect to the HPE software depot to see if there are any updates.



9. There is now a notification about the available updates that are available in the HPE software depot which are able to be viewed

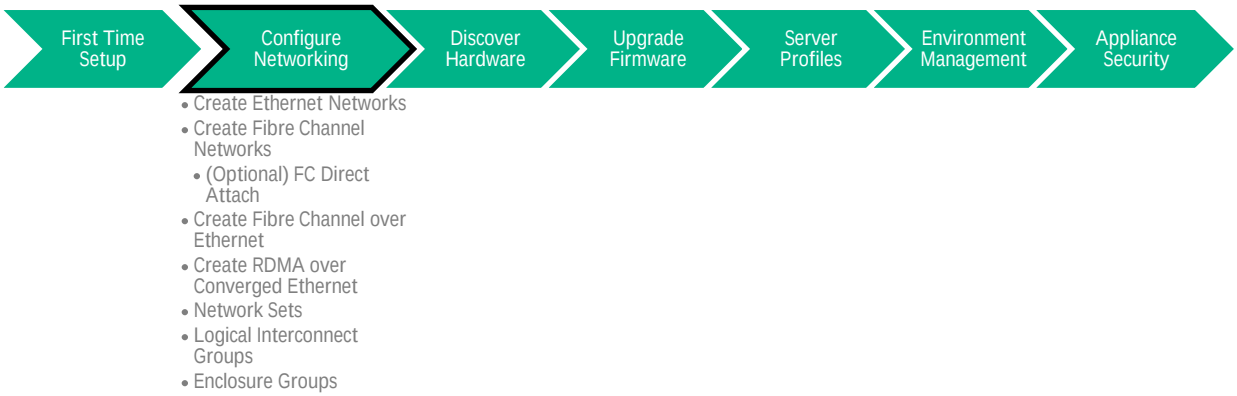


or



Note: You may still have to manually download the updated file (depending on your configured credentials that were used for the HPE Support Center User Token), HPE OneView will only notify you that a later version is available. However a link is provided in the Actions pull down menu for the software.

Network Configuration



In this section, you will create *Networks*, *Network Sets*, *Logical Interconnect Groups* and *Enclosure Groups (Synergy only)*.

Networks are constructs within the appliance that define a particular L2 network or FCoE / FC Fabric. A *Network* will be an object you can assign to *Server Profiles*, *Network Sets*, and *Logical Uplink Sets*.

Network Sets are aggregated networking objects that contain *Networks*. The *Network Set* will be an object you can assign to *Network Connections* within *Server Profiles* to greatly simplify multiple network management. For instance, if you have a number of standard *Networks* required for Virtual Machine connectivity, which is different for physical servers, you can create different *Network Sets* for each host connectivity model. *Network Sets* allow you to map multiple networks to a *Network Connection*.

Logical Interconnect Groups define what modules are located within a Synergy Frame and the module configurations like IGMP Snooping, Loop Protection, Multicast Filtering, etc. *Uplink Sets* define uplink connectivity for Ethernet, FCoE and FC *Networks*, and are members of *Logical Interconnect Groups*. The *Logical Interconnect Group* is then assigned to an *Enclosure Group* to complete the Enclosure configuration policy. A *Logical Interconnect is* patterned after the *Logical Interconnect Groups* and is defined automatically once an *Enclosure* is added to the HPE OneView console by associating it to an *Enclosure Group*.

Uplink Set can either be an Ethernet or Fibre Channel type, but not both. Any defined *Networks* not associated with an *Uplink Set* become *Internal Ethernet Networks* to the *Logical Interconnect* and are reported within the *Logical Interconnect*.

An *HPE OneView Domain* is a concept for the Composable Infrastructure management framework. While you cannot create additional *HPE OneView Domains*, the appliance itself is a single Domain construct. An *HPE OneView Domain* consists of one or more *Logical Interconnect Groups*, *Uplink Sets*, *Networks* and help to define how *Server Profiles* consume these resources. When defining a *Network*, it will be available within the *HPE OneView Domain* for consumption by either a *Logical Interconnect Groups*, *Logical Uplink Set*, *Logical Interconnect* (for one-off configuration requirements) or *Server Profiles* (for Internal Only networks.)

Network Configuration Checklist

Prior to continuing with this document, please make sure you have completed the following:

Table 9. HPE OneView Network Configuration Checklist

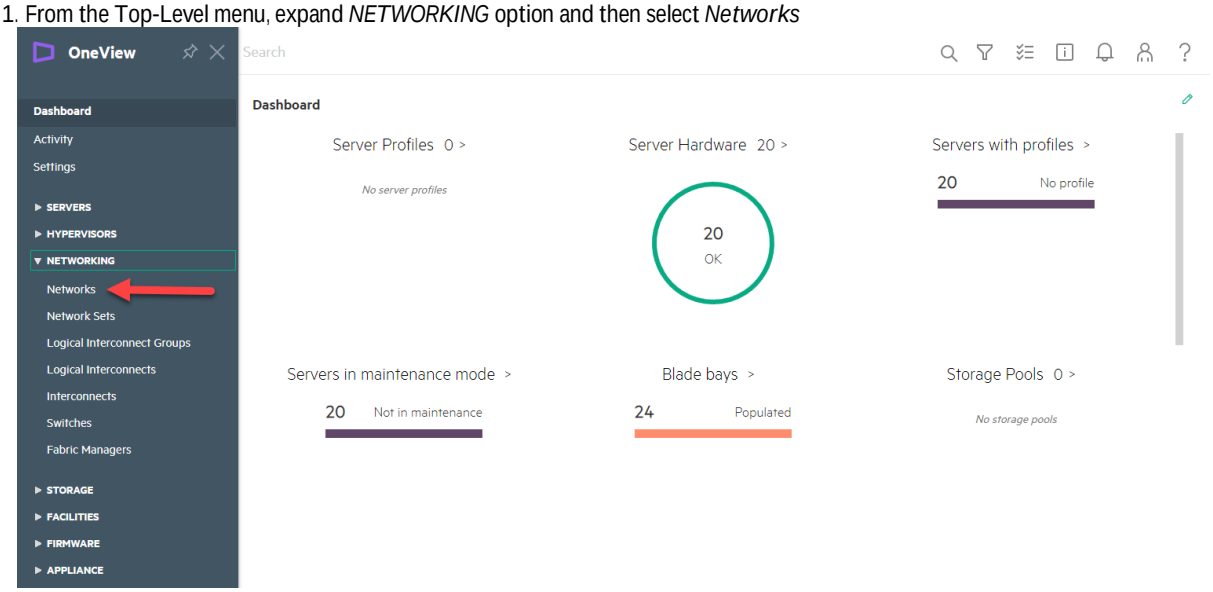
Task	Completed? (Y|N)
Collect the Virtual Connect Module Types	
Note the uplink ports connected to the upstream switches	
Document necessary VLAN IDs and names	
Document necessary Fibre Channel Fabrics	

Creating Ethernet Networks

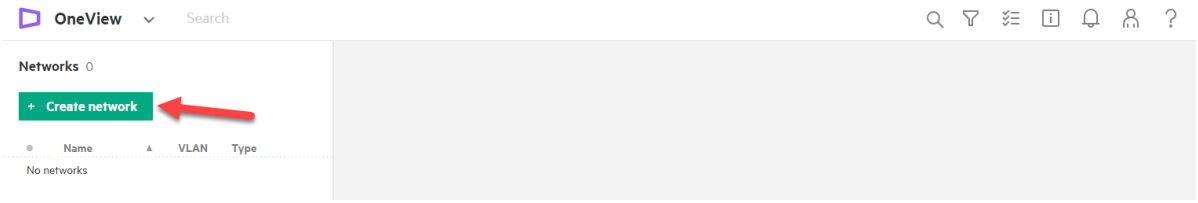


- Create Ethernet Networks
- Create Fibre Channel Networks
  - (Optional) FC Direct Attach
- Create Fibre Channel over Ethernet
- Create RDMA over Converged Ethernet
- Network Sets
- Logical Interconnect Groups
- Enclosure Groups

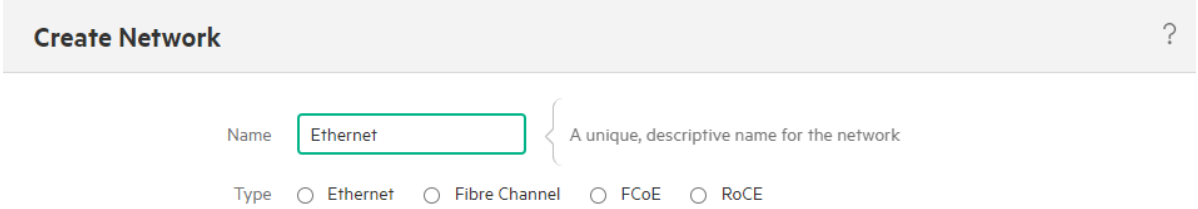
1. From the Top-Level menu, expand *NETWORKING* option and then select *Networks*



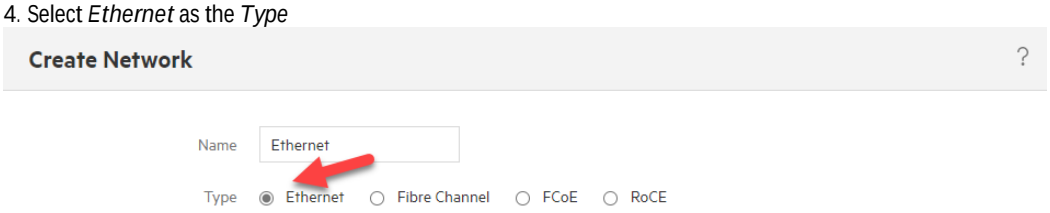
2. Once on the *Networks* screen, click the + *Create network* button on the far left.



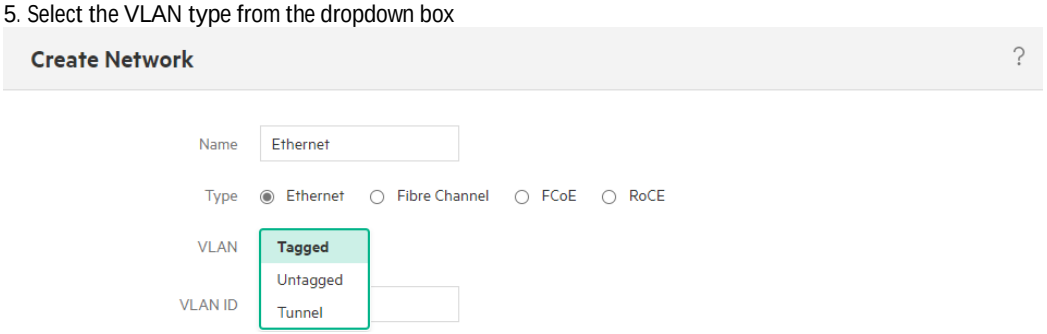
3. In the Create Network Dialog box enter the name of the network. The *Name* is not case-sensitive. The name can contain spaces and special characters.



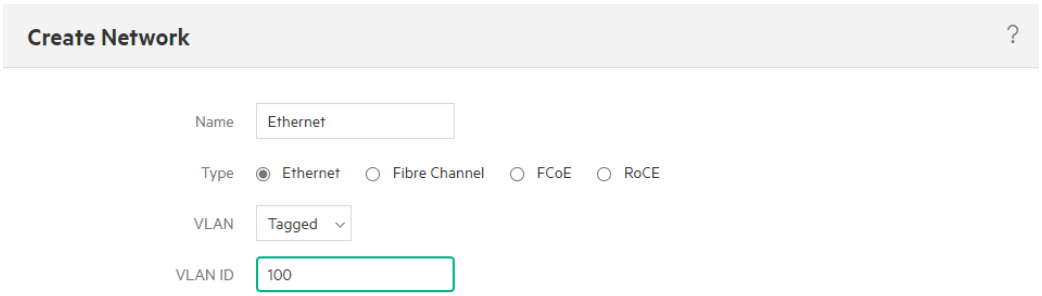
4. Select *Ethernet* as the *Type*



5. Select the VLAN type from the dropdown box



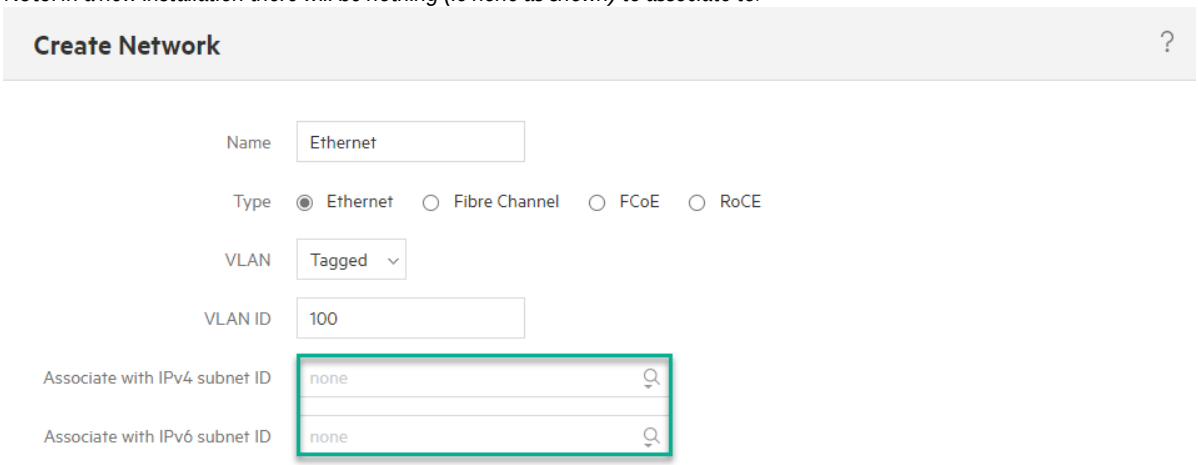
6. Enter the *VLAN ID*.



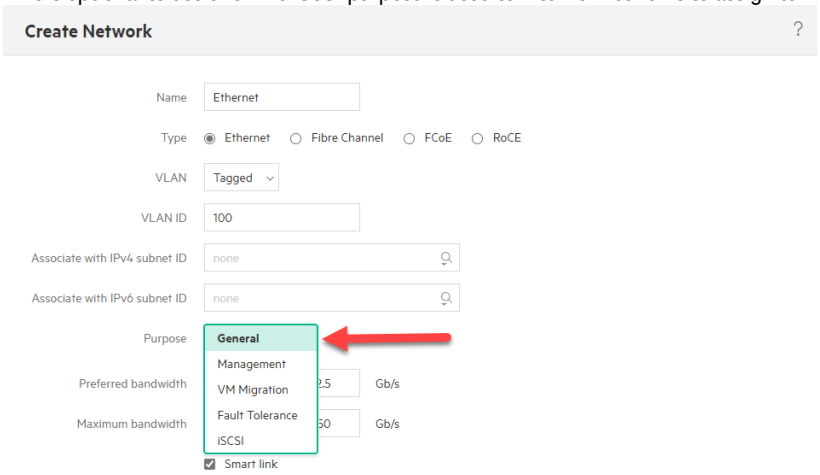
Note:
The VLAN ID field can accept ranges of VLANs (i.e. 10,15,20-50) and will append "_VLANID" to the end of the network name.

7. Choose to associate the VLAN ID with an existing IPv4 or IPv6 Subnet ID.

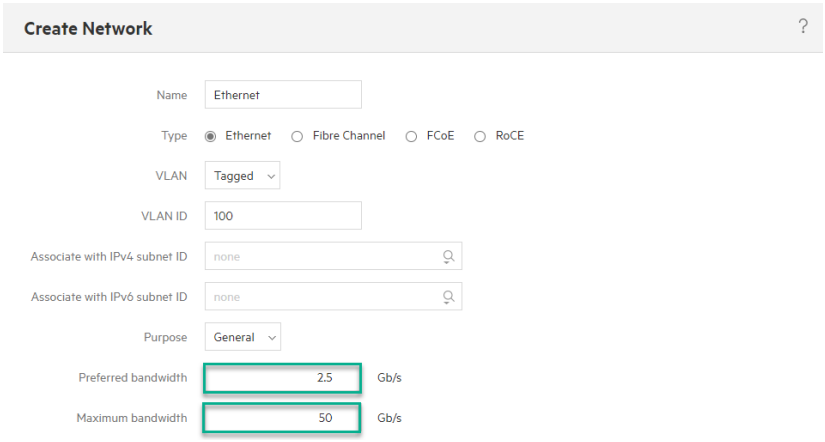
Note: *In a new installation there will be nothing (ie none as shown) to associate to.*



8. Select the Purpose of the network from the dropdown list. The *Purpose drop-down* selection is used by the HPE OneView for vCenter integration[3]. It is optional to use this. The *iSCSI* purpose is used to filter for networks to assign to Nimble Storage.

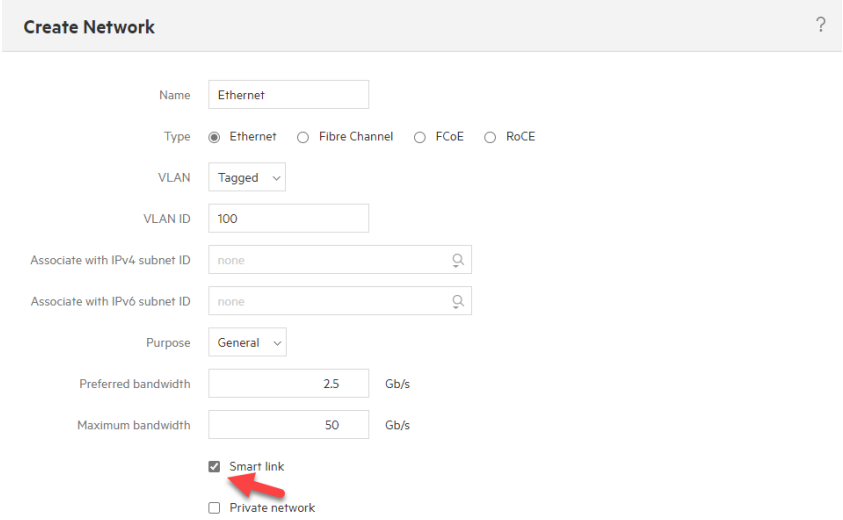


9. Assign the *Preferred* and *Maximum bandwidth* settings.



10. Enable any network options needed. Smart Link will automatically be selected by default. Selecting Private Network will mimic PVLAN behavior in that all assigned Network Connections will all be in an isolated network.

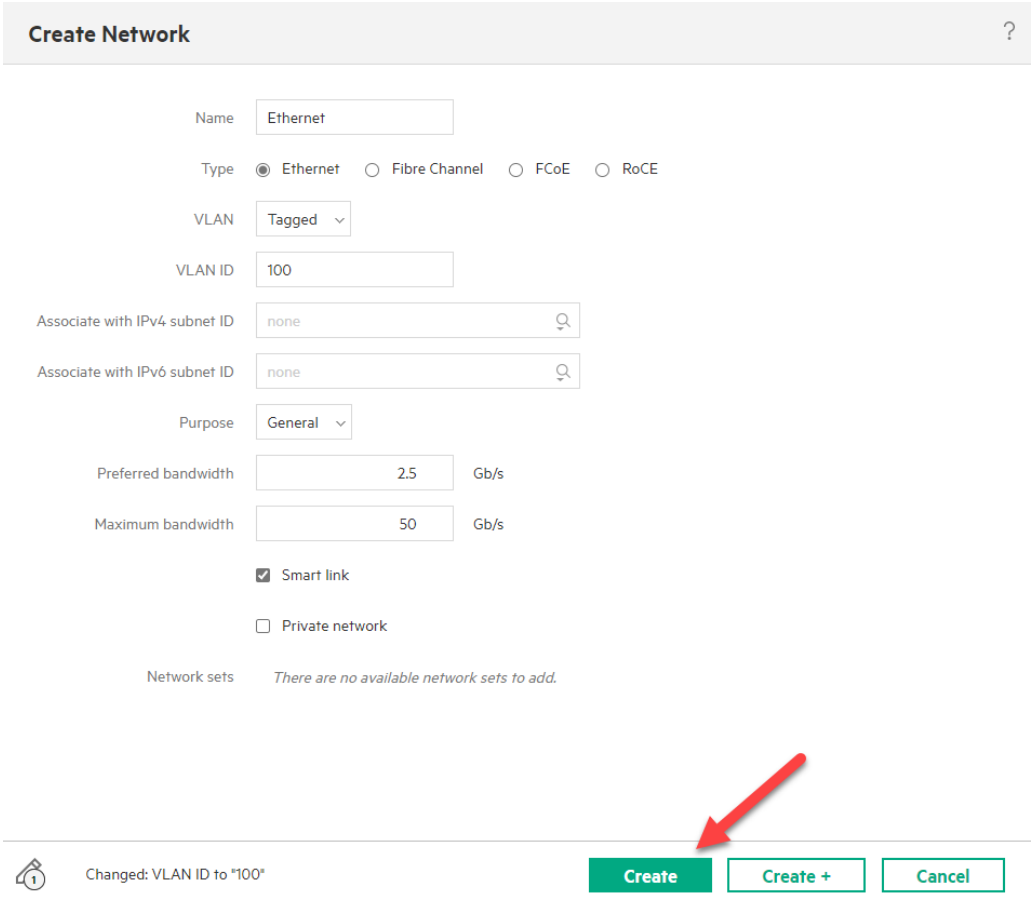
    Note: *Smart Link is a Virtual Connect feature that notifies the physical host that there is a no connectivity, when all uplink paths for the NIC are down.*



[3] HPE OneView for vCenter

11. Click the *Create* button to create the new Ethernet Network and close the Create Network dialog box. You can also select the *Create+* button to continue creating more Networks – e.g. Create the B-Side Ethernet Network.

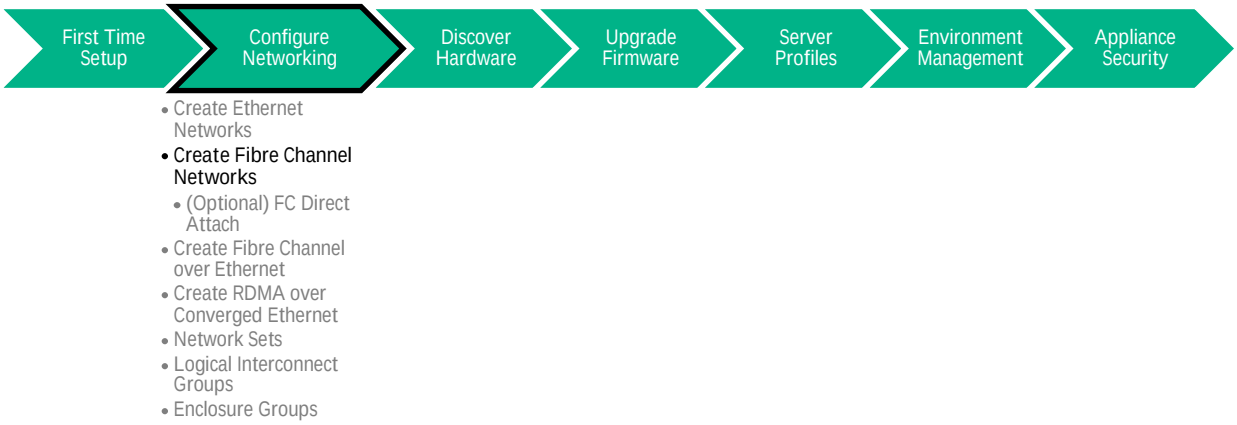
    Note: *As we have not yet created any Network Sets, none will be available*



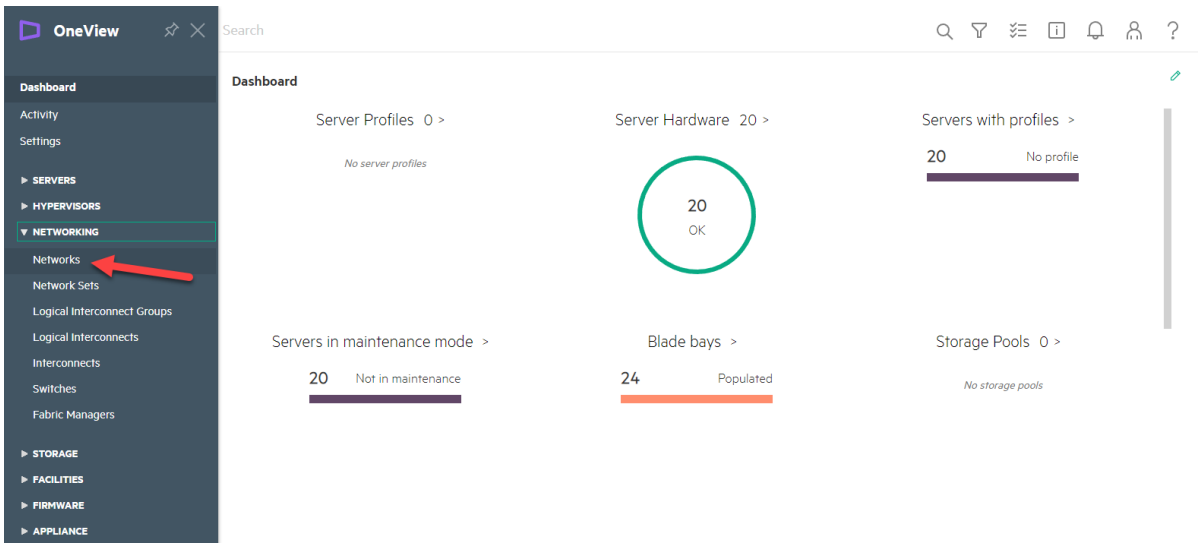
Creating Fibre Channel Networks

HPE OneView supports multi-hop FCoE Fabrics with either traditional Fibre Channel Fabric Attach, or Virtual Connect Direct Attach (Flat SAN) with HPE Alletra, HPE Primera, 3PAR StoreServ or Nimble Storage. Please choose the appropriate following scenario to create either a Fabric Attach or Direct Attach Fabric.

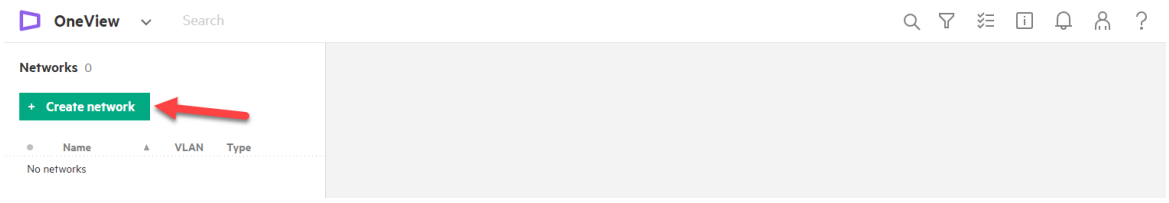
Fabric Attached Network



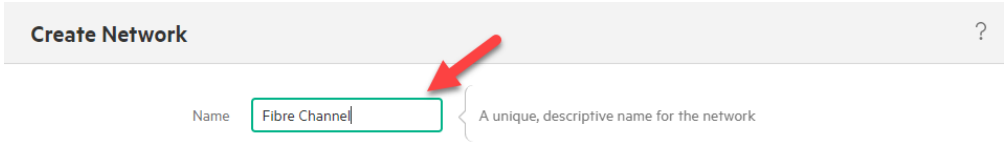
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Networks*.



2. Click the + *Create network* button on the far left.

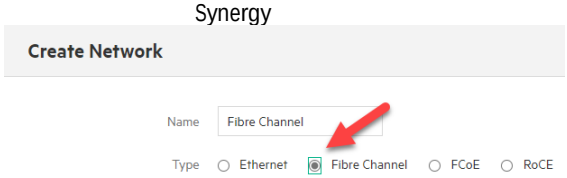


3. In the Create Network dialog box, enter the *Name* of the Fibre Channel network

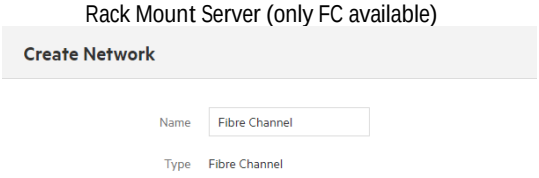


4. Select *Fibre Channel* as the *Network Type*

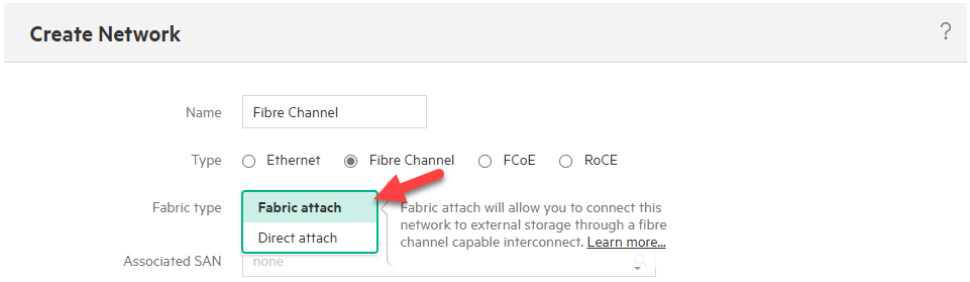
Synergy



Rack Mount Server (only FC available)

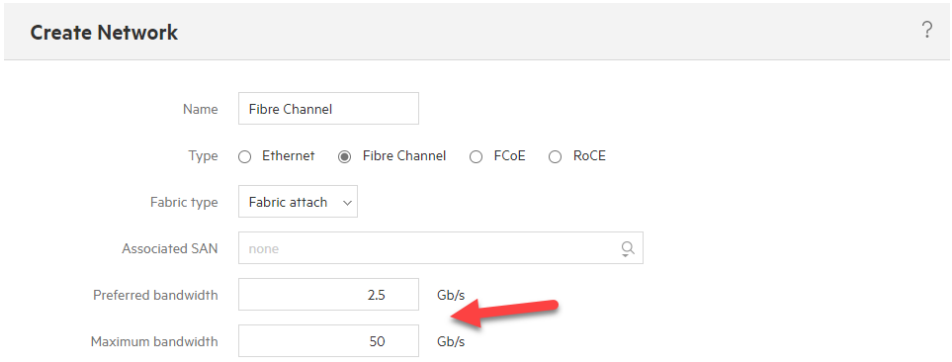


5. Select *Fabric attach* as the *Fabric type*



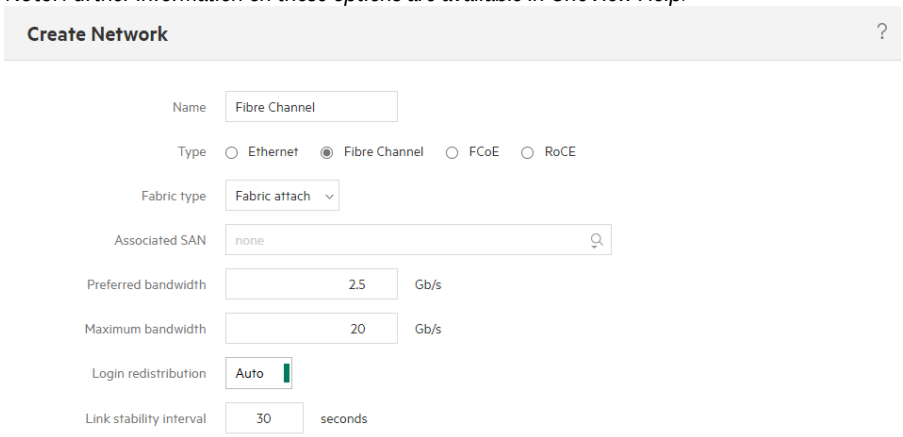
Note: *The Fabric Attach Fabric type is used for traditional Fibre Channel Fabric connectivity, which requires NPIV-capable upstream FC SAN Switches. By selecting the Fabric type, you determine whether the connection is via an FC SAN Switch or Directly Attached to Virtual Connect (Flat SAN).*

6. Set the *Preferred and Maximum Bandwidth*.

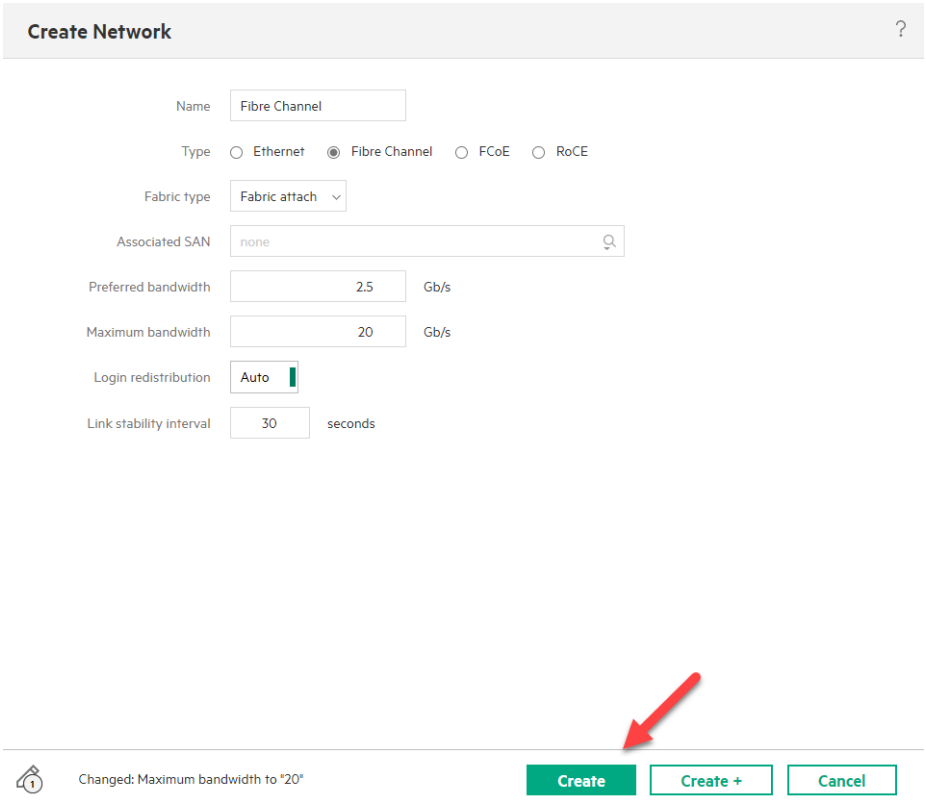


7. Set the desired *Login redistribution* and *Link stability interval* to be used.

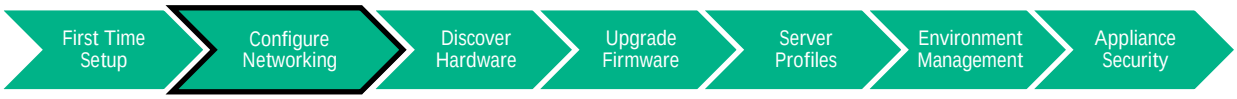
   Note: *Further information on these options are available in OneView Help.*



8. Click the *Create* button to create the new Ethernet Network and close the Create Network dialog box. You can also select the *Create +* button to continue creating more Networks.



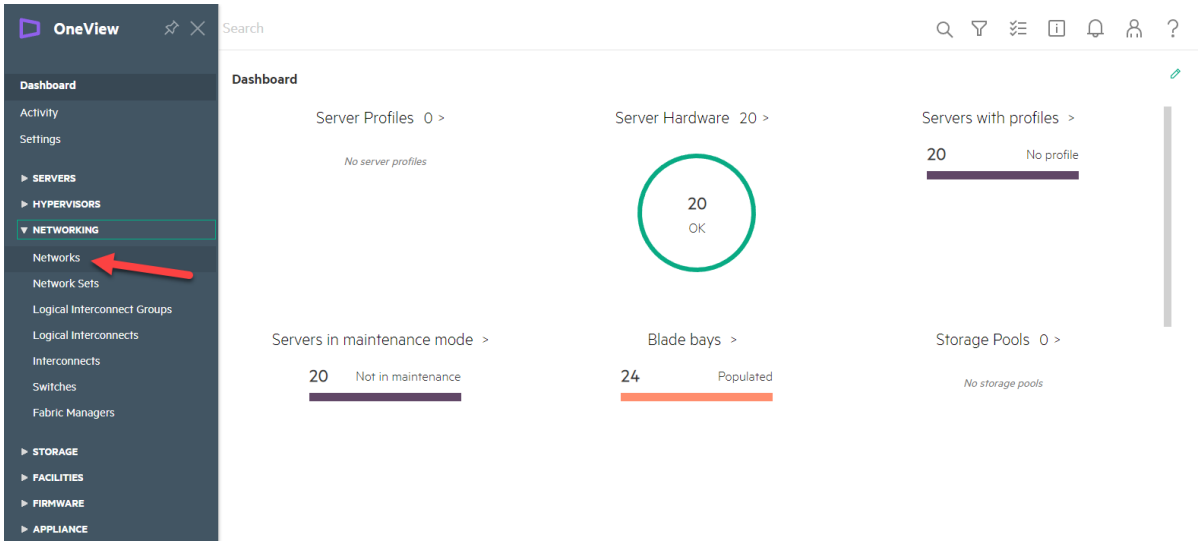
FC Direct Attach (Synergy Virtual Connect Only)



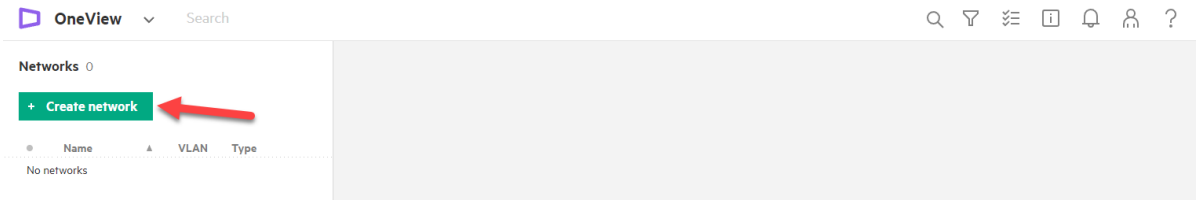
- Create Ethernet Networks
- Create Fibre Channel Networks
  - (Optional) FC Direct Attach
- Create Fibre Channel over Ethernet
- Create RDMA over Converged Ethernet
- Network Sets
- Logical Interconnect Groups
- Enclosure Groups

The FC Direct Attach (Flat SAN) feature extends Virtual Connects "Wire-Once" management to the FC fabric by reducing the complexity, and cost of expensive FC switches. This feature is only supported with HPE Alletra, Primera, 3PAR StoreServ and Nimble storage systems, not with other HPE or 3rd party storage arrays. This feature is only available with Synergy Virtual Connect modules. Details are available here *https://h20272.www2.hpe.com/SPOCK/Pages/spock2Html.aspx?htmlFile=hw_virtual_connect.html*

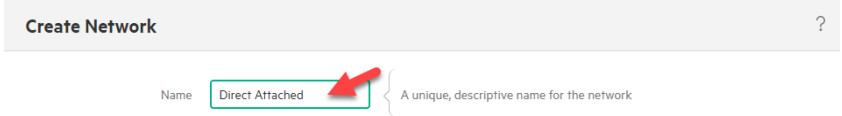
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Networks.*



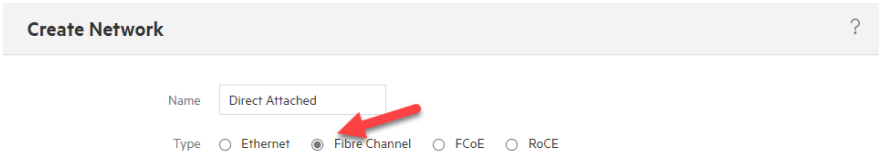
2. Once on the *Networks* screen, click the + *Create network* button



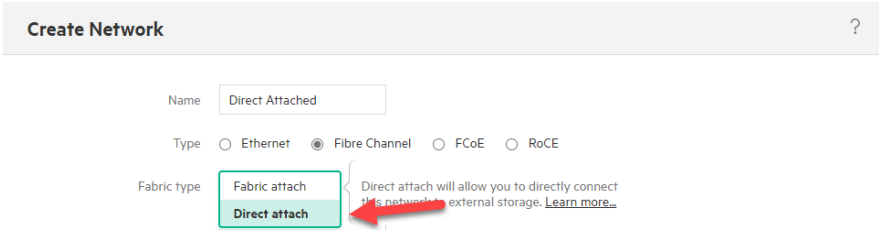
3. In the Create Network dialog box, enter the *Name* of the Fibre Channel network



4. Select *Fibre Channel* as the Network Type.

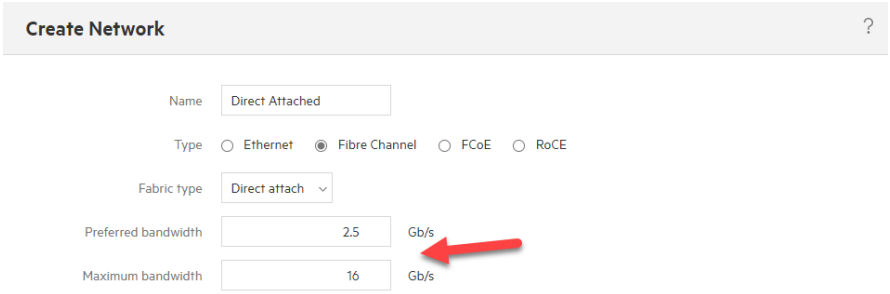


5. Select *Direct attach* as the Fabric Type

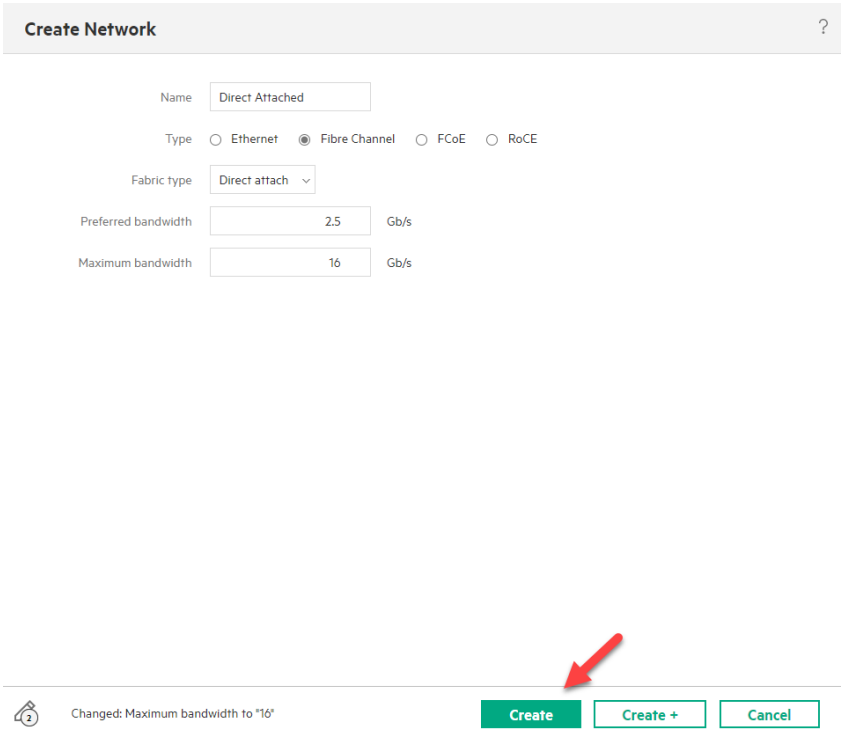


Note:
By selecting the Direct Attach Fabric Type, you can cable the chosen Fibre Channel capable port on the Virtual Connect module directly to an HPE Alletra, HPE Primera, 3PAR StoreServ or Nimble storage system's Fibre Channel port. Configure multiple Virtual Connect module ports for the direct attach network and cable them to different controllers on the storage system for resiliency.

6. Set the Preferred and Maximum Bandwidth.



7. Click the *Create* button to create the new Direct Attach Network and close the Create Network dialog box. You can also select the *Create +* button to continue creating more Networks.

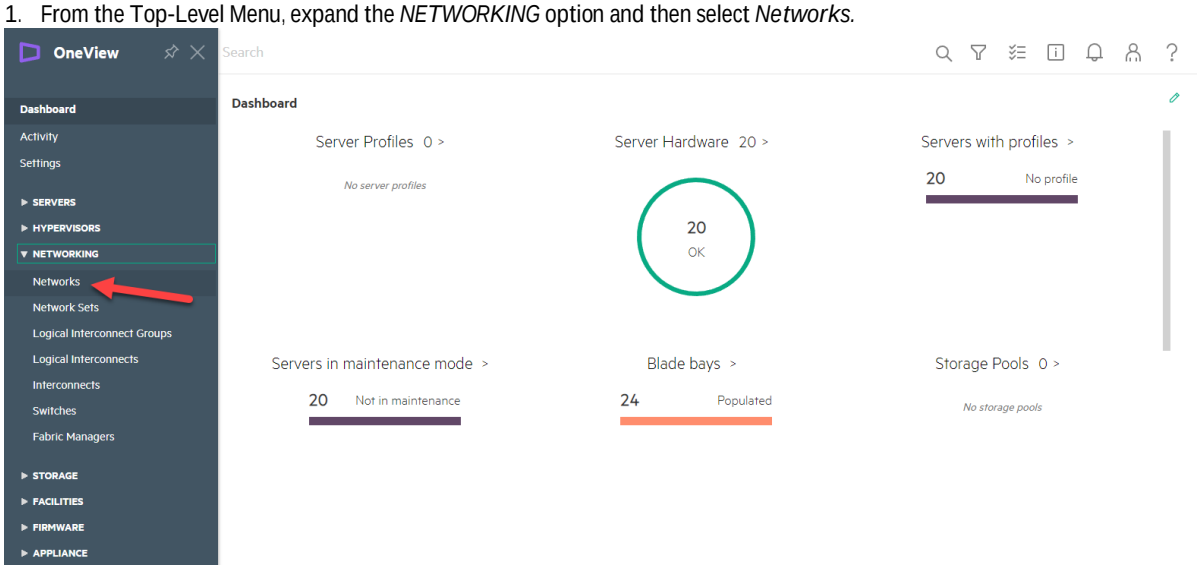


Fibre Channel over Ethernet Network (Synergy Virtual Connect Only)

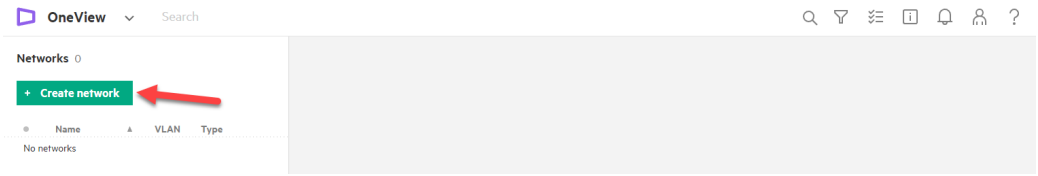
First Time Setup | **Configure Networking** | Discover Hardware | Upgrade Firmware | Server Profiles | Environment Management | Appliance Security

- Create Ethernet Networks
- Create Fibre Channel Networks
  - (Optional) FC Direct Attach
- **Create Fibre Channel over Ethernet**
- Create RDMA over Converged Ethernet
- Network Sets
- Logical Interconnect Groups
- Enclosure Groups

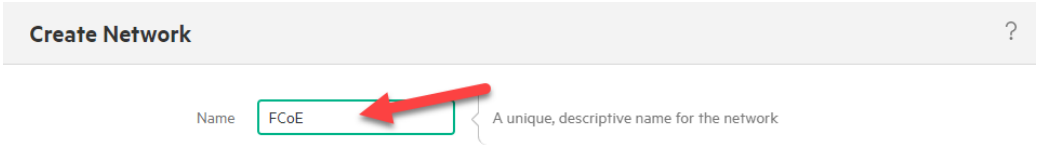
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Networks.*



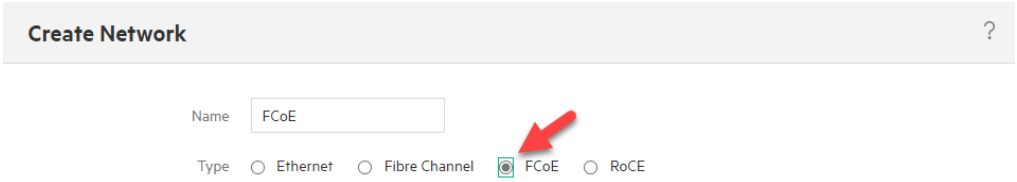
2. Click the + *Create network* button



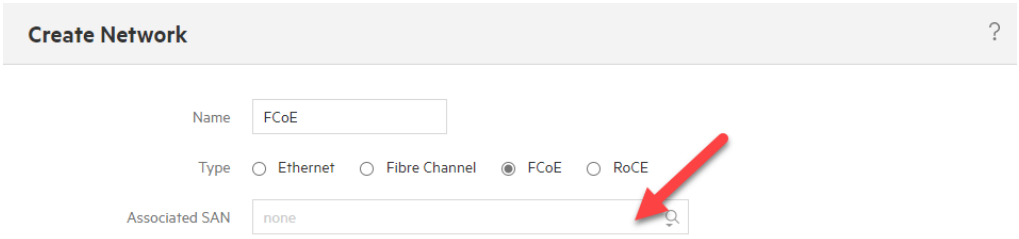
3. In the Create Network dialog box, enter the *Name* of the Fibre Channel over Ethernet network



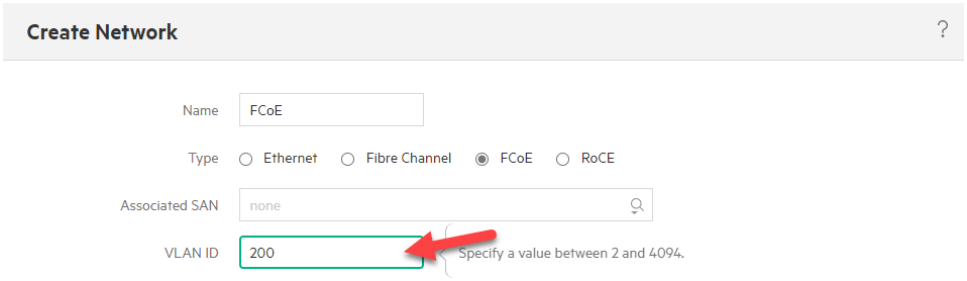
4. Select *FCoE* as the Network Type.



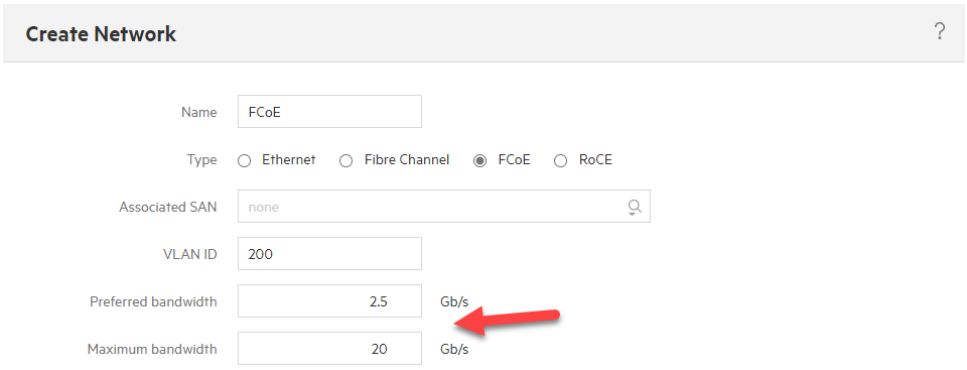
5. Enter the *SAN* that the FCoE network will be associated with



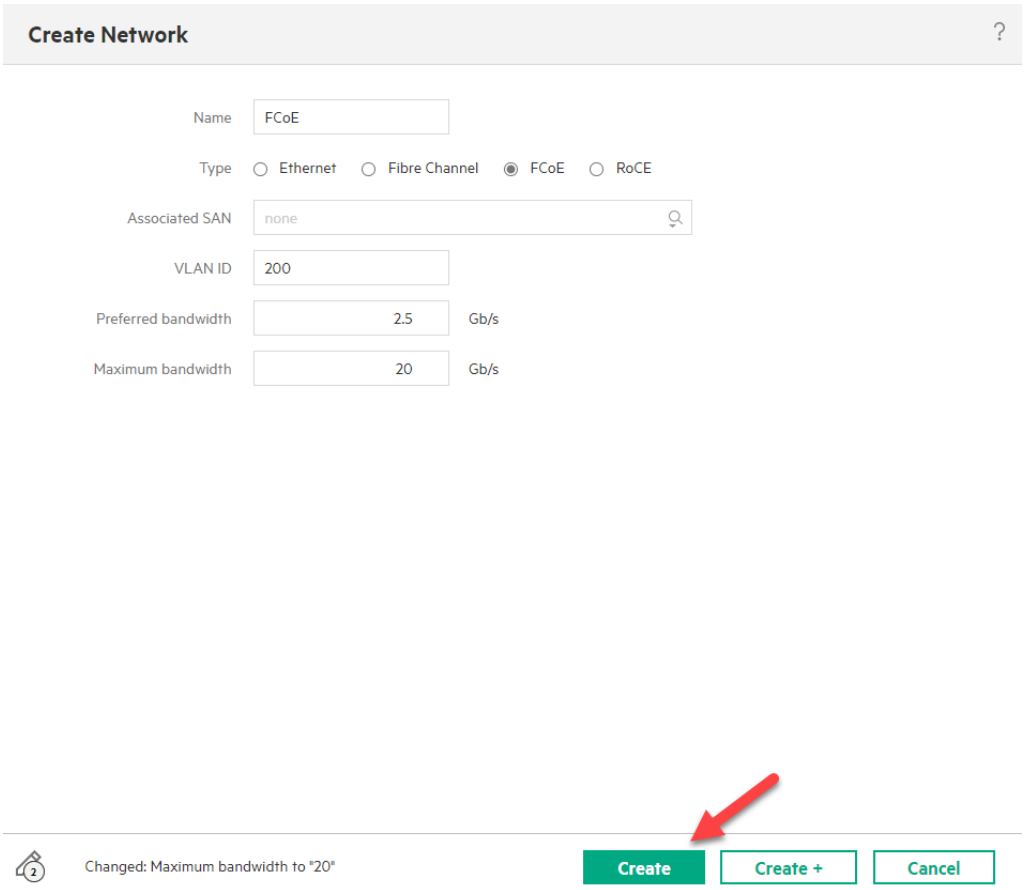
6. Enter a *VLAN ID*



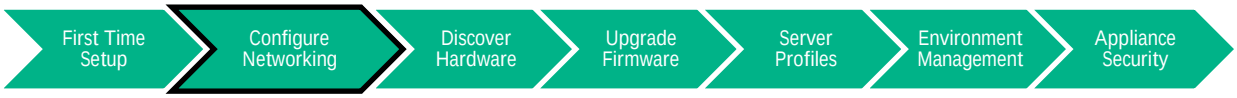
7. Set the *Preferred* and *Maximum Bandwidth*



8. Click the *Create* button to create the new Ethernet Network and close the Create Network dialog box. You can also select the *Create+* button to continue creating more Networks

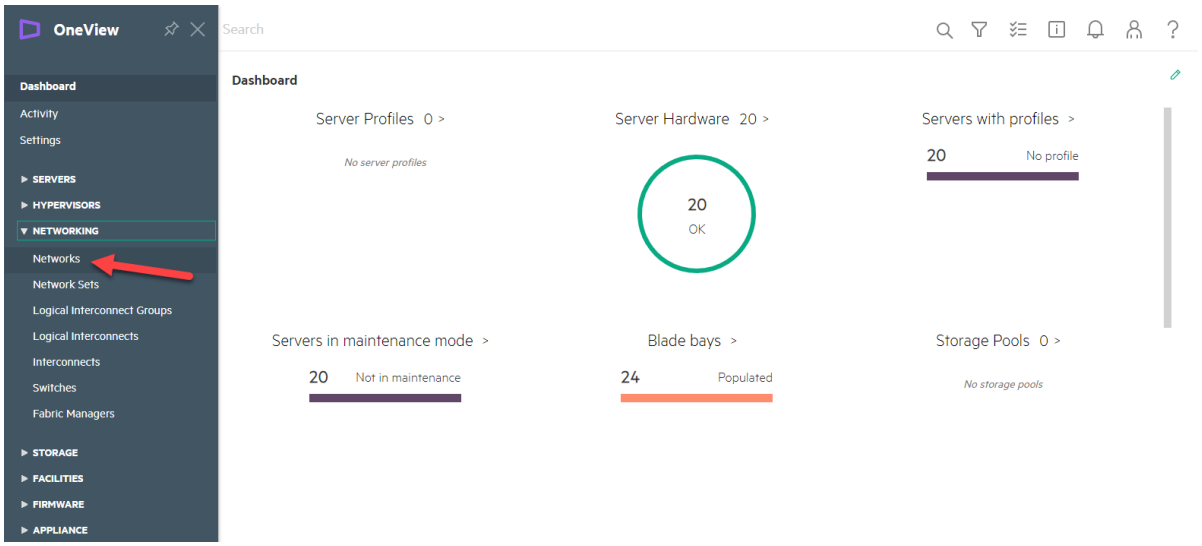


RDMA over Converged Ethernet (Synergy Virtual Connect only)

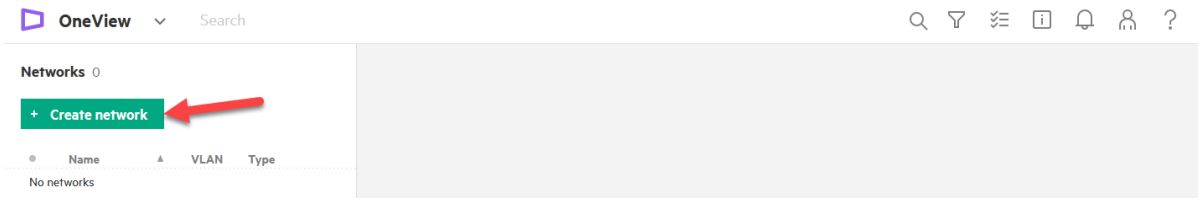


- Create Ethernet Networks
- Create Fibre Channel Networks
  - (Optional) FC Direct Attach
- Create Fibre Channel over Ethernet
- **Create RDMA over Converged Ethernet**
- Network Sets
- Logical Interconnect Groups
- Enclosure Groups

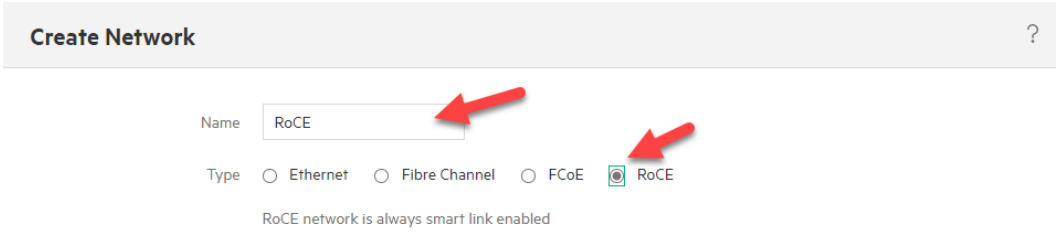
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Networks*.



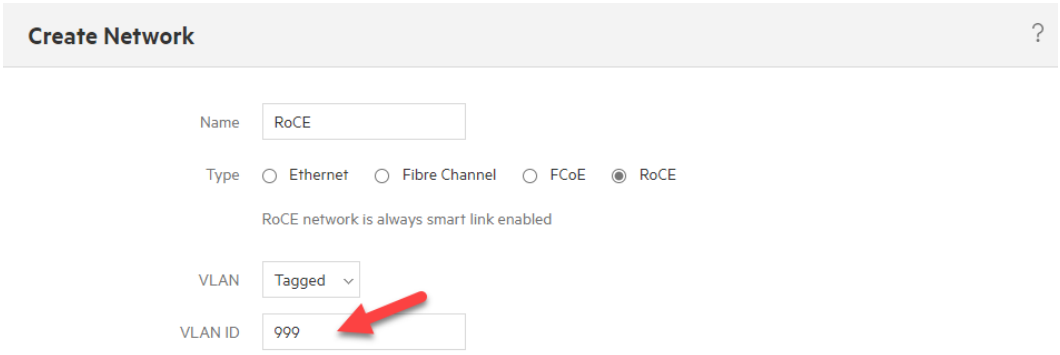
2. Click the + *Create network* button



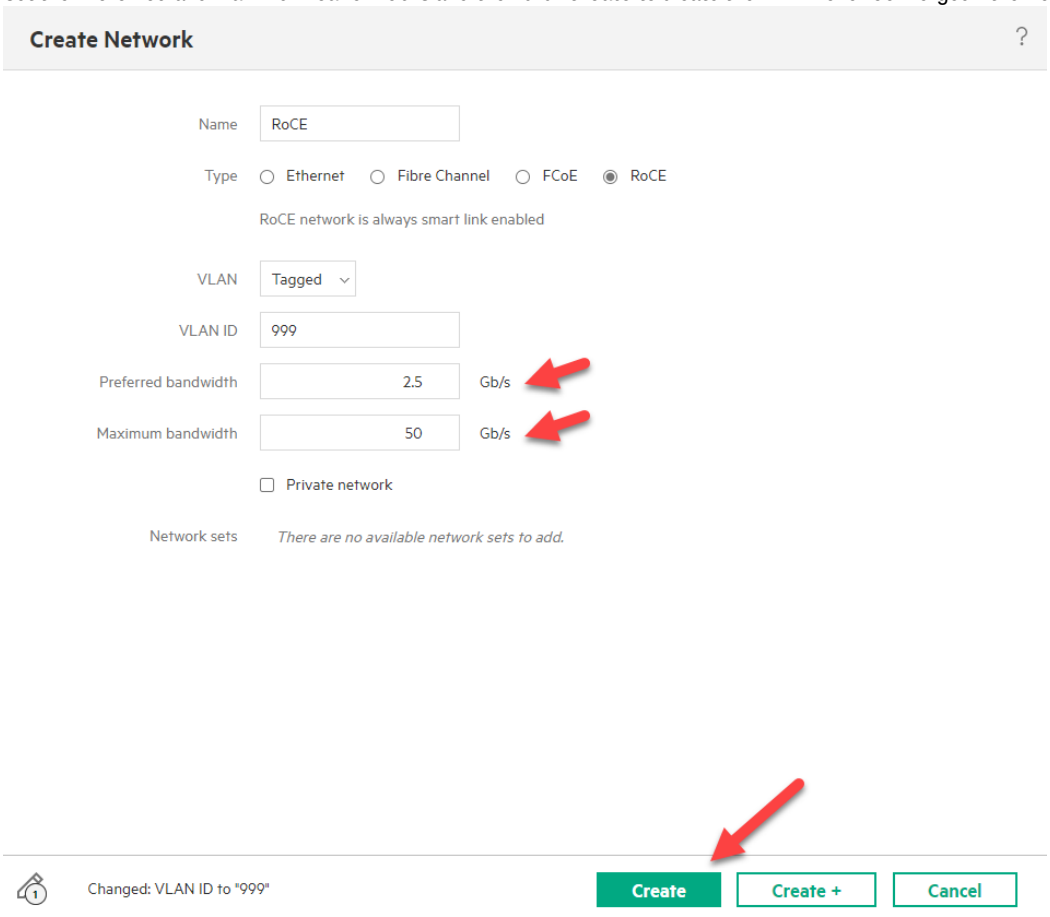
3. In the Create Network dialog box, enter the *Name* of the RDMA over Converged Ethernet network and select *RoCE*



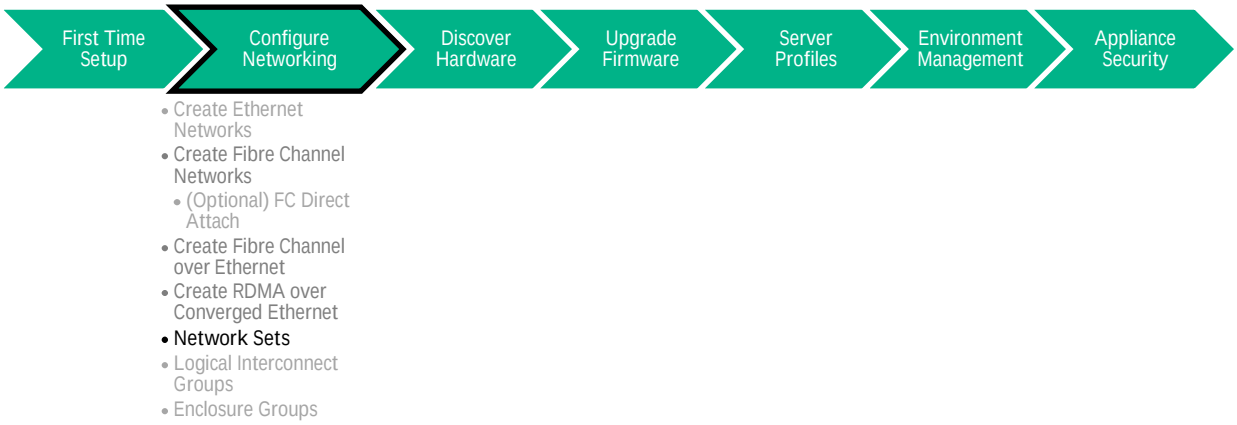
4. Set the VLAN ID for the RoCE Network



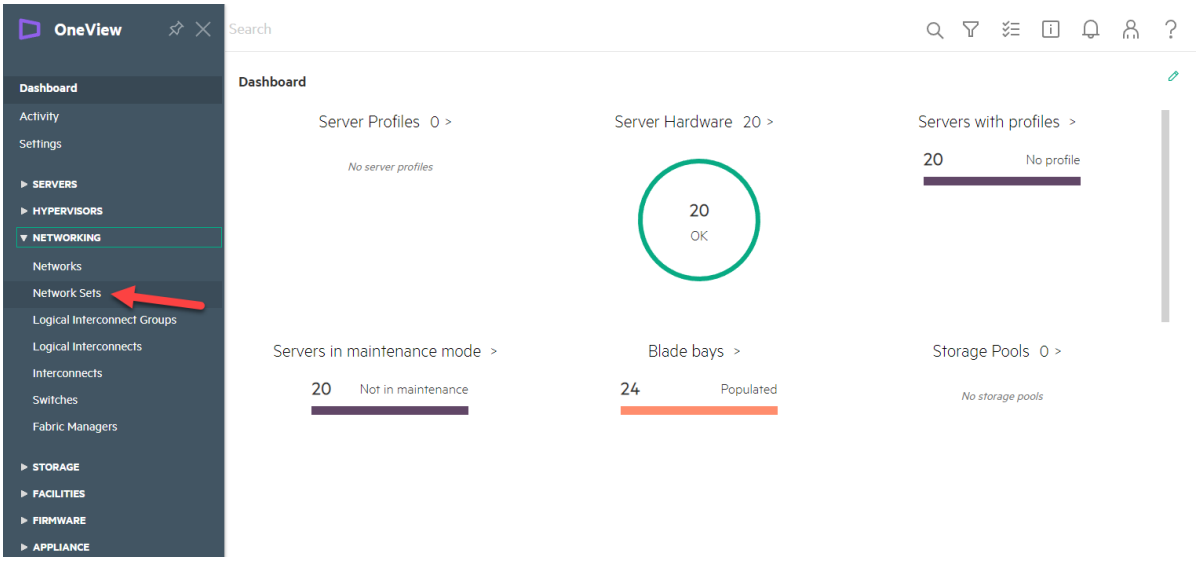
5. Set the *Preferred* and *Maximum bandwidths* and then click *Create* to create the RDMA over Converged Ethernet network.



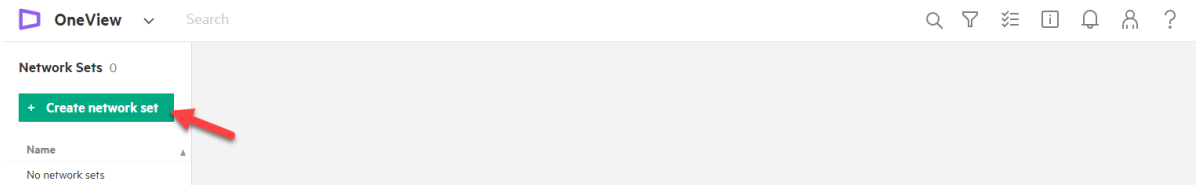
Creating Network Sets



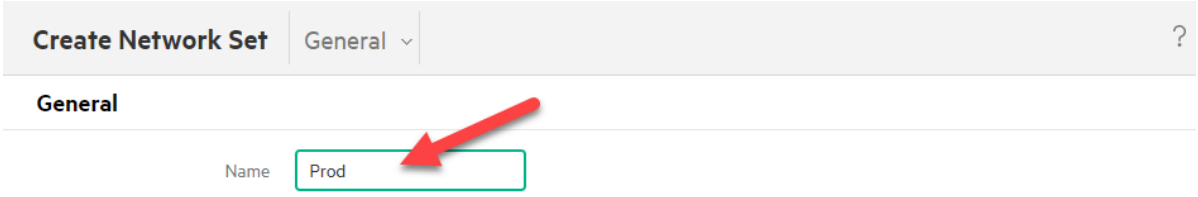
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Network Sets*.



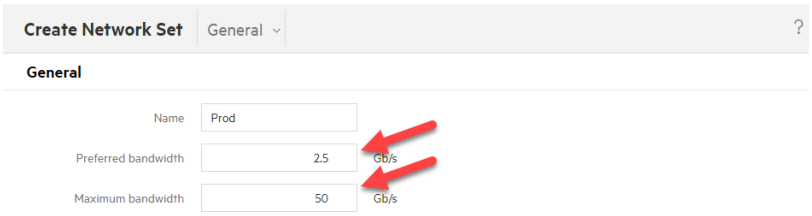
2. Click the + *Create network set* button.



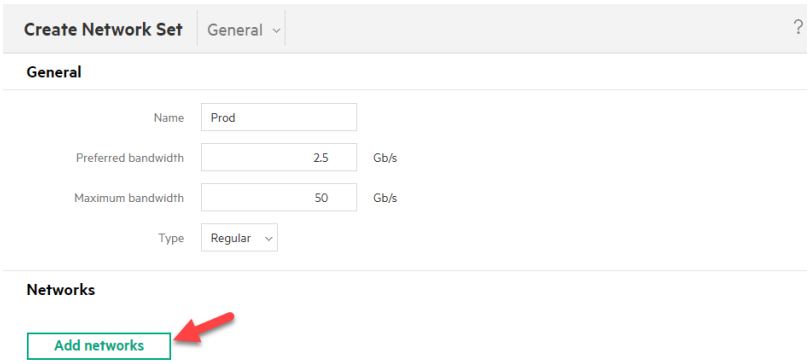
3. From the Create Network Sets dialog menu, enter a *Name* for the Network Set.



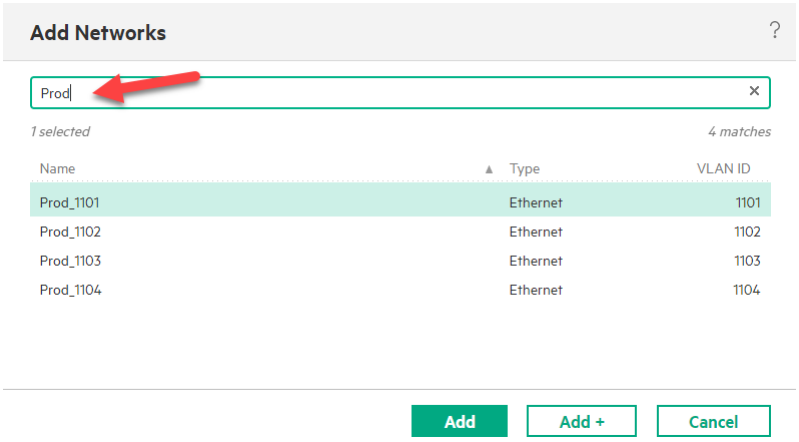
4. Set the *Preferred* and *Maximum Bandwidth*



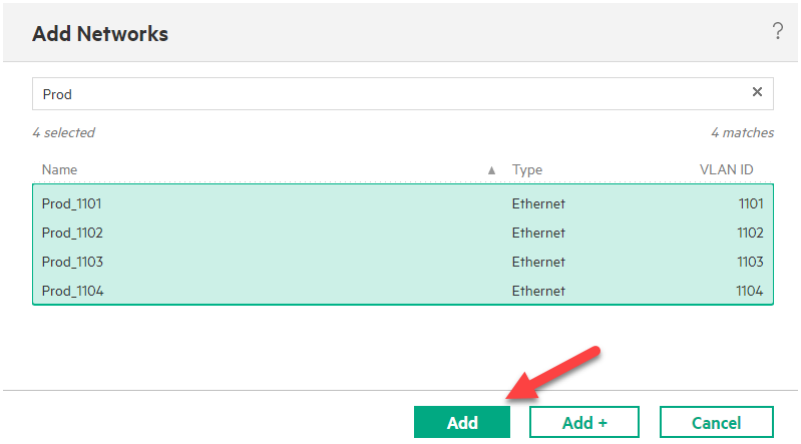
5. Select *Add networks*.



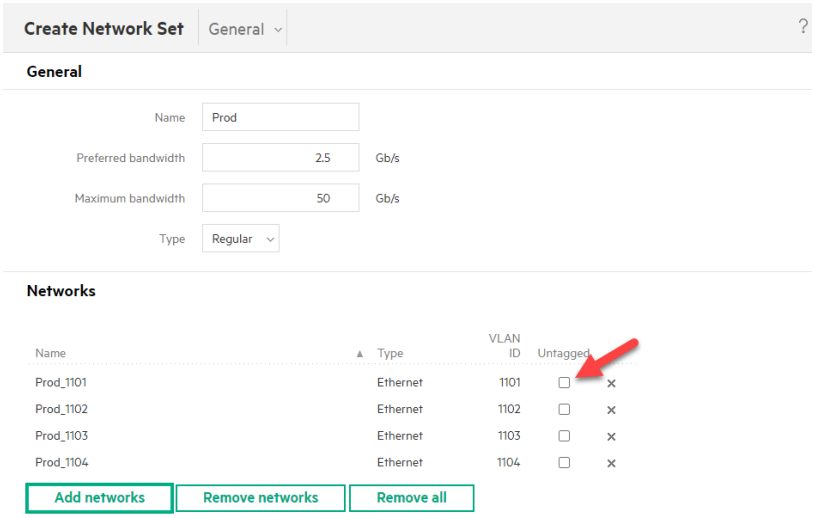
6. From the Add networks Dialog Box, you can search for a Network or multiple Networks, or either click SHIFT / CTRL+Left Mouse Click to select which will either select all in section, or multi-select the networks to add. The following example shows how to find the "Prod" Ethernet Networks, by putting *Prod* in the Search box. From there you can highlight all the networks for for the Network Set.



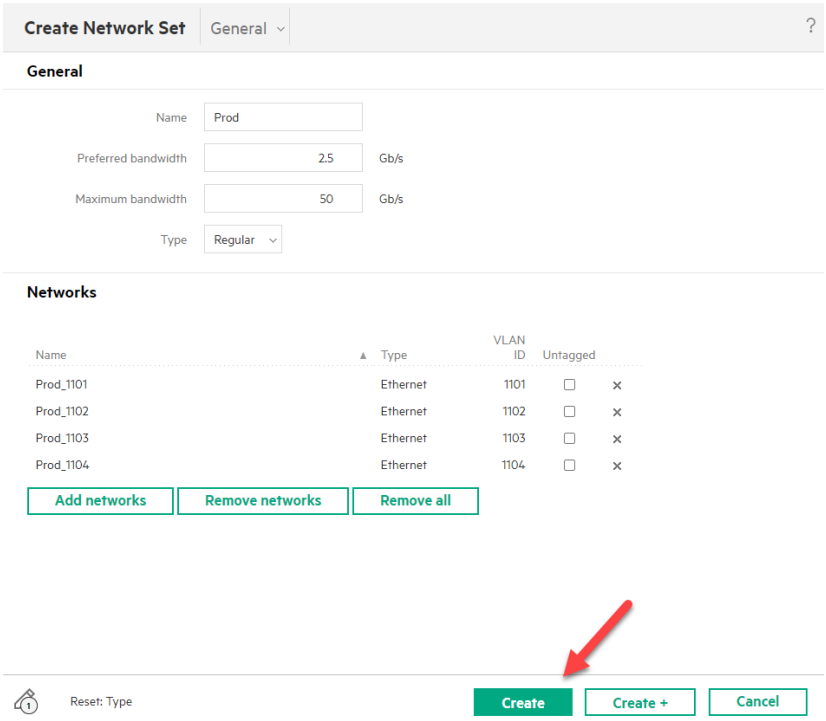
7. Click *Add* once the desired networks are selected.



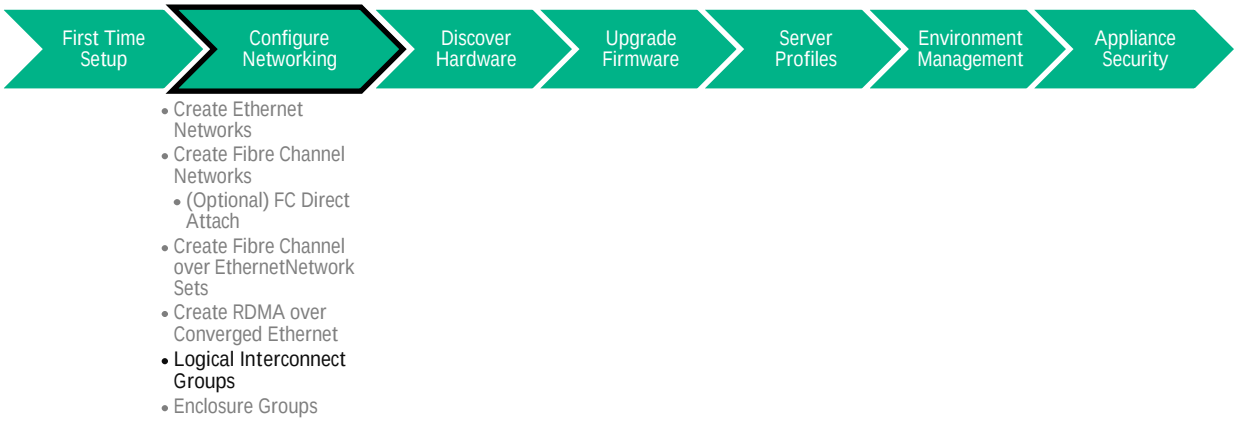
8. After clicking *Add*, you can select the specific network that will be the *Native VLAN*, or the default untagged network for the Servers Network Connection. This is typically used for PXE traffic.



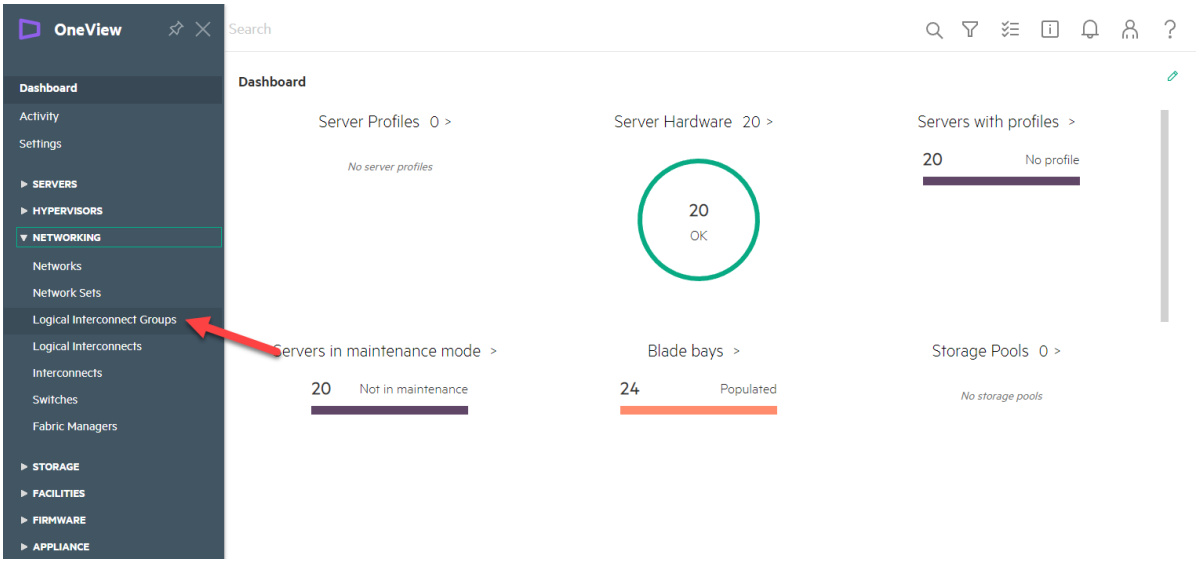
9. Click *Create* to create the Network Set



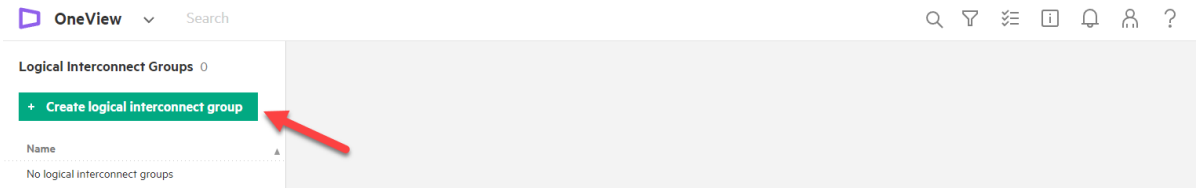
Create Logical Interconnect Group



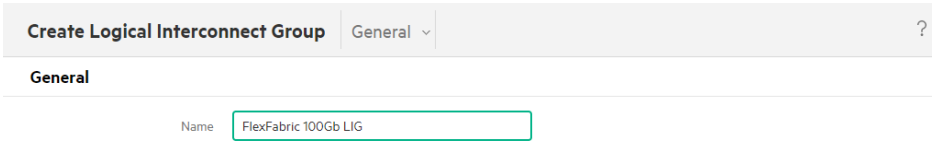
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Logical Interconnect Groups.*



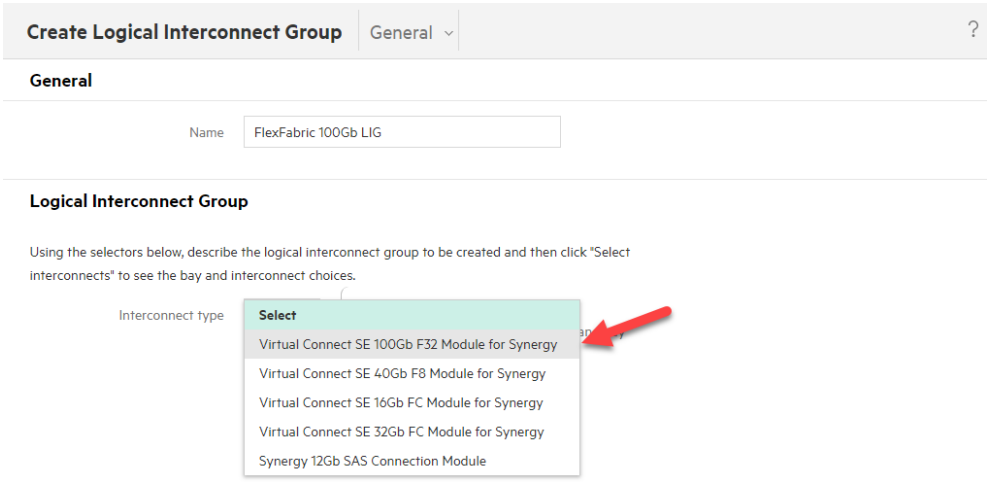
2. Select + *Create logical interconnect group* button.



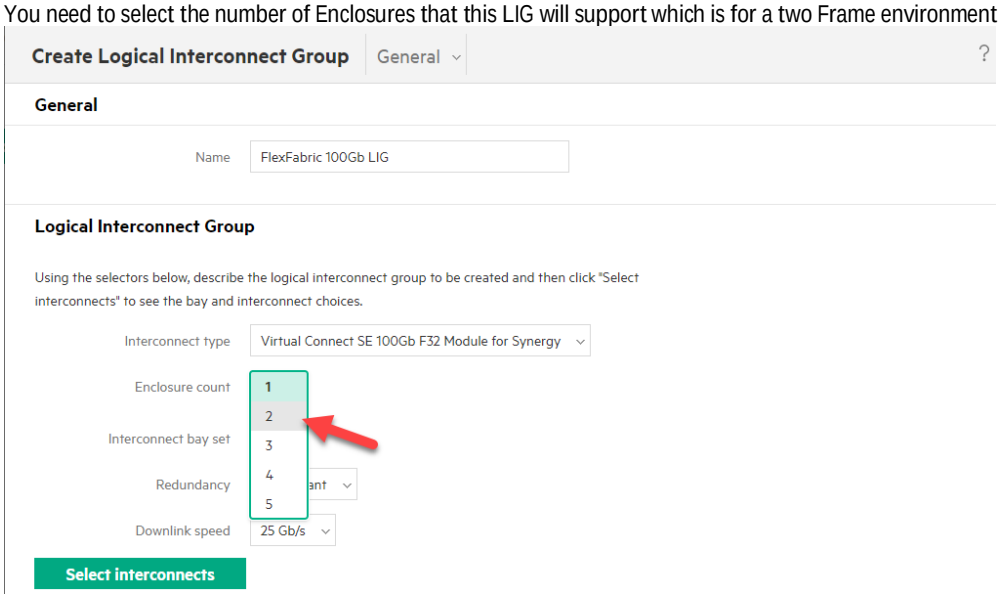
3. Enter a *Name* for the Logical Interconnect Group (LIG).



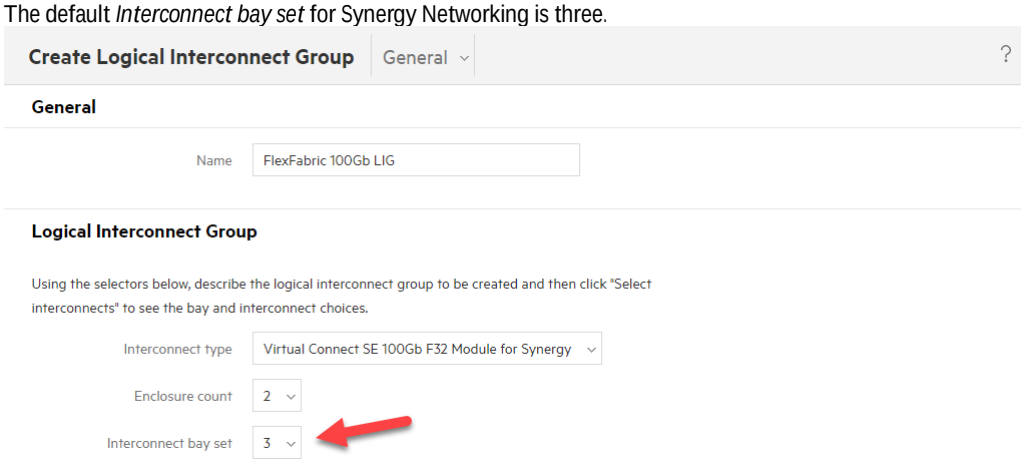
4. Use the dropdown list to select the type of LIG you want to configure, for the following example we will use the *Virtual Connect SE 100Gb F32 Module*.



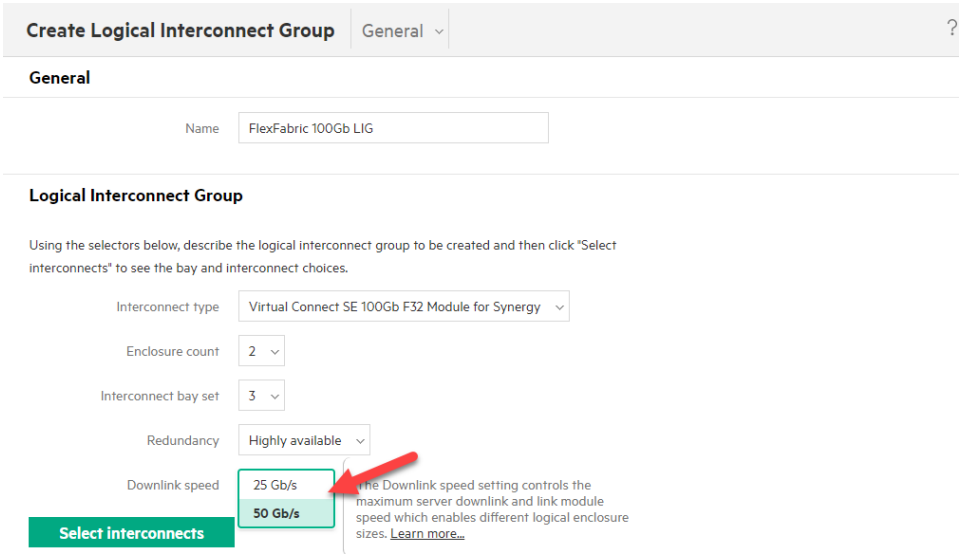
5. You need to select the number of Enclosures that this LIG will support which is for a two Frame environment for this example



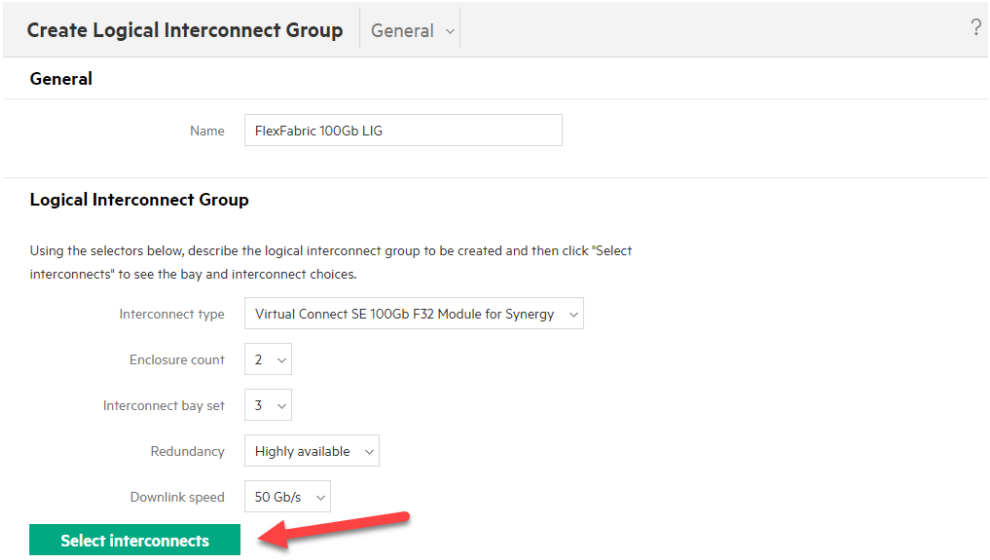
6. The default *Interconnect bay set* for Synergy Networking is three.



7. Select the *Downlink speed* this will need to be 25Gb/s or 50Gb/s based on the NIC / Number of Enclosures *50Gb/s* is what we will use for this example (for up to 3 Frames 50Gb/s is possible, 4 or more Frames would require 25Gb/s)

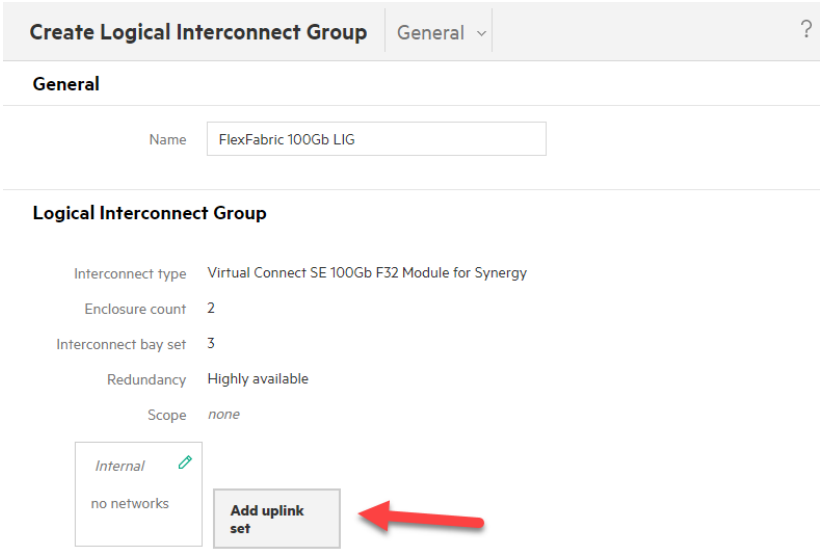


8. Click the *Select interconnects* button

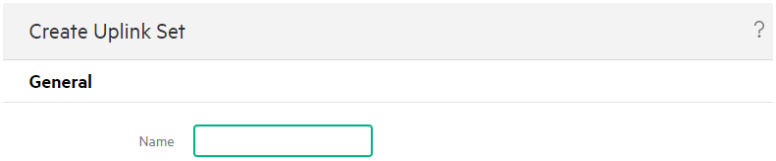


Creating Uplink Sets

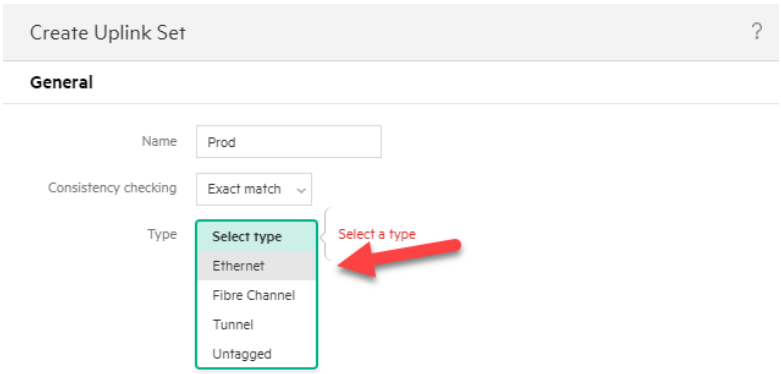
1. Click the *Add uplink set* button.



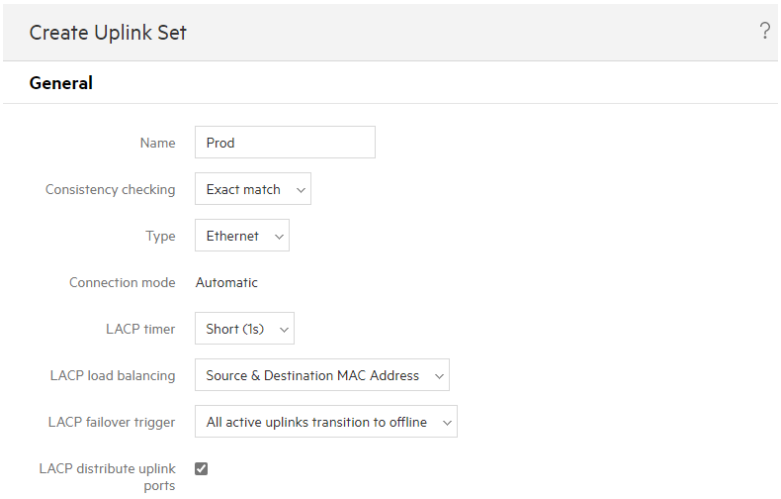
2. In the Create Uplink Set dialog window, select a *Name* for the uplink.



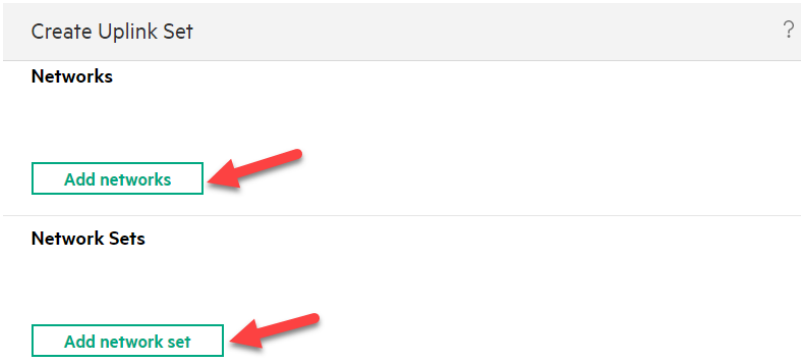
3. Select *Ethernet* as the *Type* from the drop-down box.



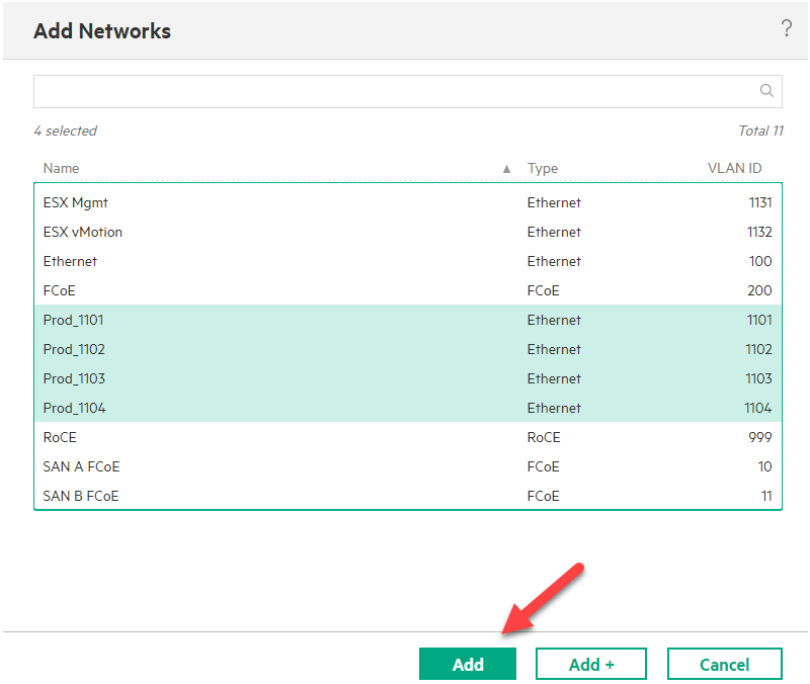
4. Adjust the *LACP* settings to be used by this uplink set.



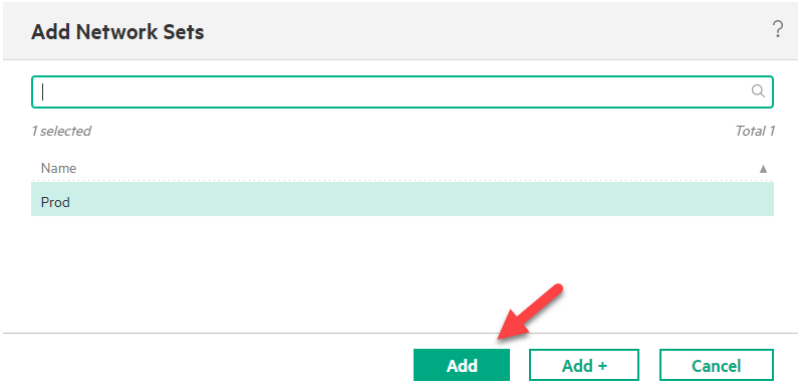
5. Click the *Add networks* (or *Add network set* if you have created a network set previously) button to select the networks to add. By not selecting a Network or multiple Networks, they will be *Internal Ethernet Networks* within the Logical Interconnect that is applied to each enclosure from the Logical Interconnect Group.



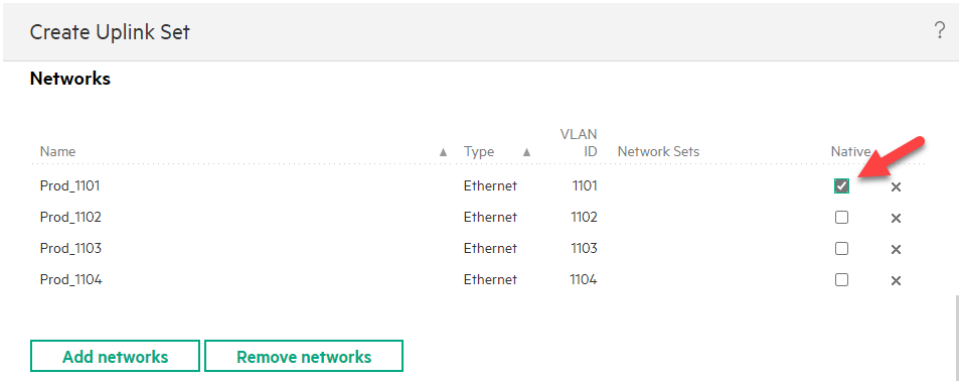
6. In the Add Networks to Uplink dialog window, add the desired networks for this uplink. A search field is provided to quickly locate a specific Network or multiple Networks. After searching you can either Left Click to select a single network or SHIFT/CTRL+Left Mouse Click to multi-select networks. Once all of your networks are selected, click the *Add* button, or click the *Add+* button to continue to add more networks by searching.



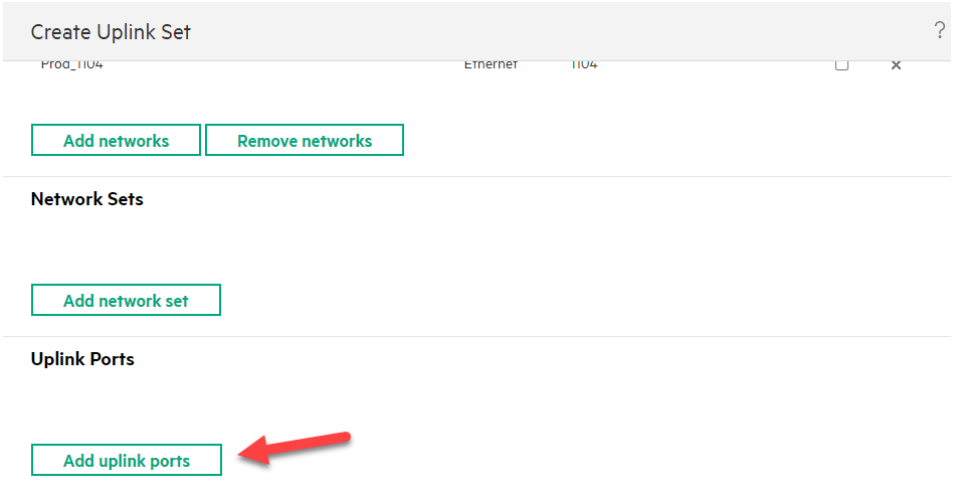
or Network Set



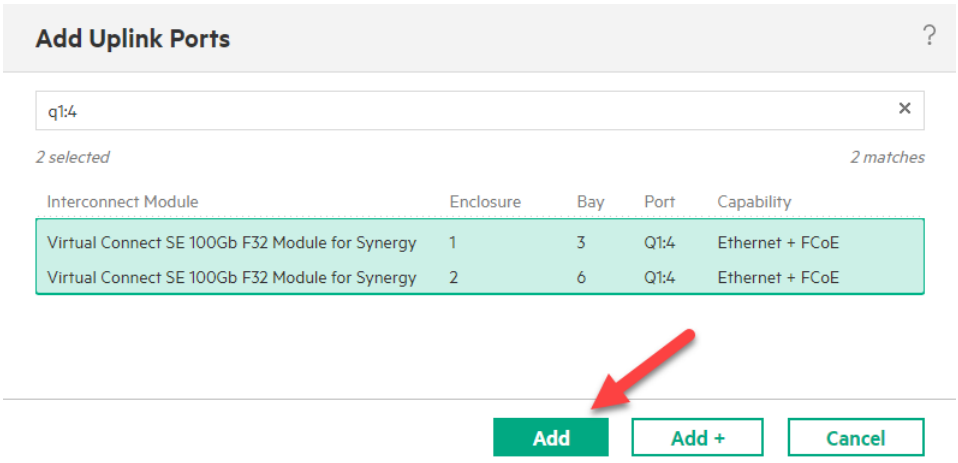
7. Make sure to mark the appropriate network as *Native* if the VLAN on the upstream switch is also the Native or Default VLAN.



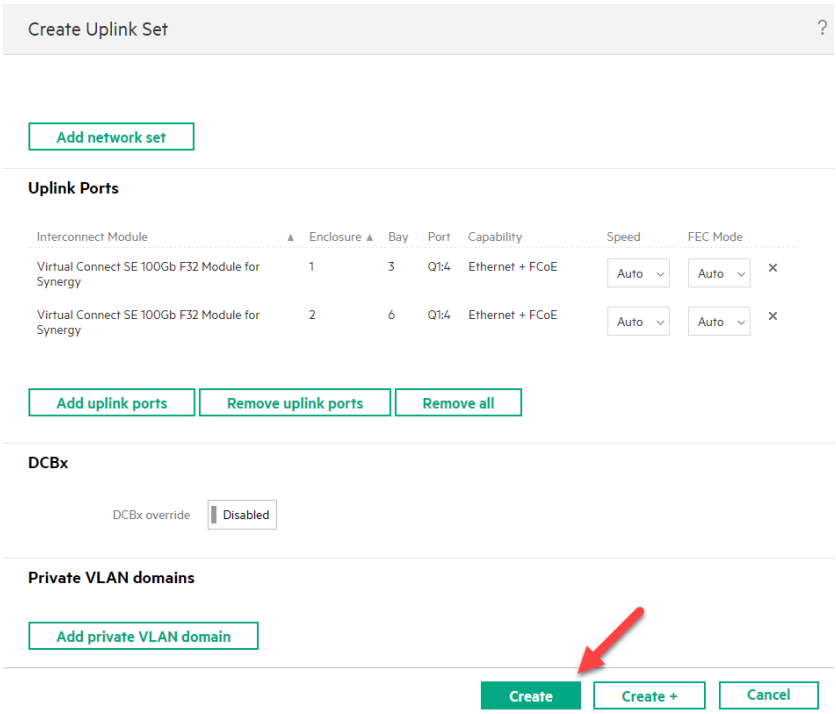
8. Click the *Add uplink ports* button to add uplink ports.



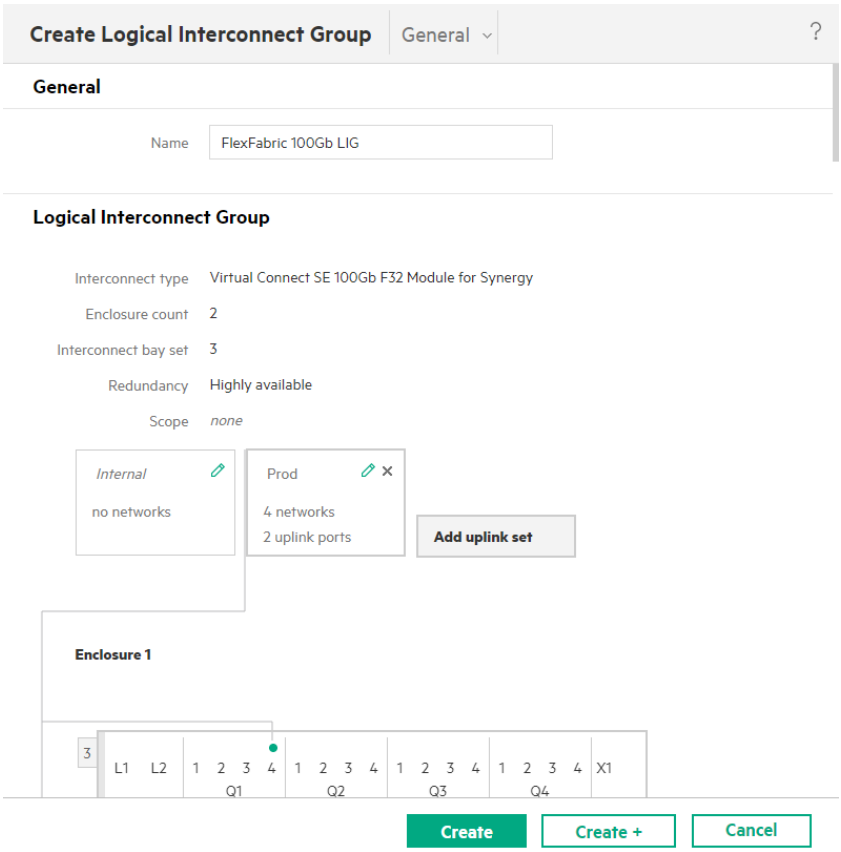
9. In the *Add uplink ports* to Uplink dialog, select at least one port from each Synergy SE 100Gb F32 Module. To quickly add multiple Uplink Ports, first search for a common port (e.g. *Q1:4*), select them (by using CTRL-Click), click the *Add* button.



10. After you have added the Uplink Ports to your Uplink Set, click the *Create* button. Select the *Create +* button if you wish to define an additional *Uplink Set(s)*.



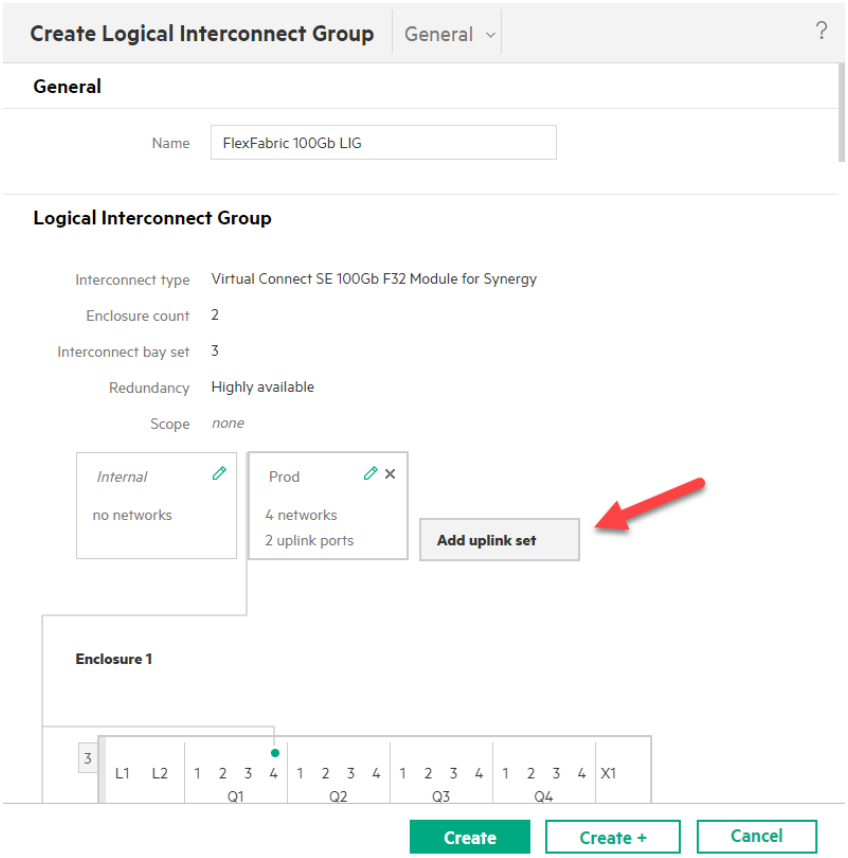
11. Verify that the uplinks are shown in the Create Logical Interconnect Group Dialog Window.



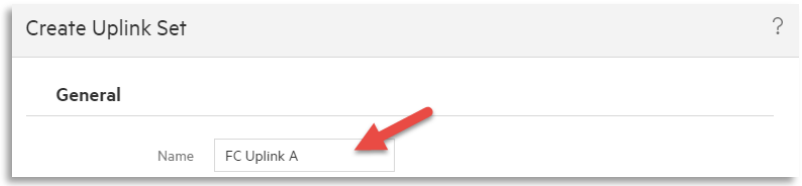
12. Continue to the next section to create *Fibre Channel Uplink Sets*.

Creating Fibre Channel Uplink Sets (Optional)

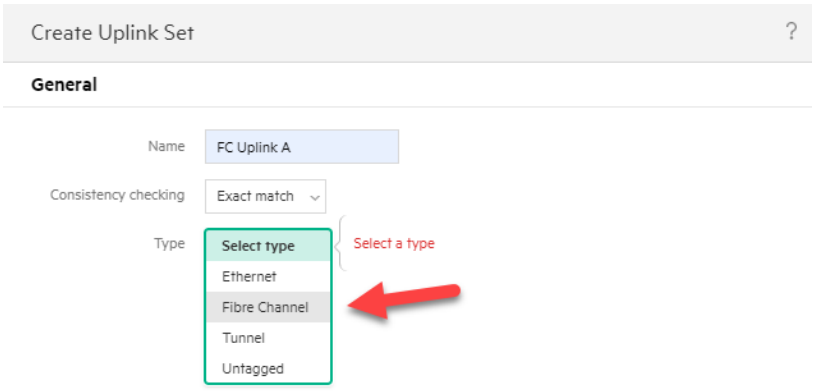
1. Click the *Add uplink set* button to add SAN Fabrics.



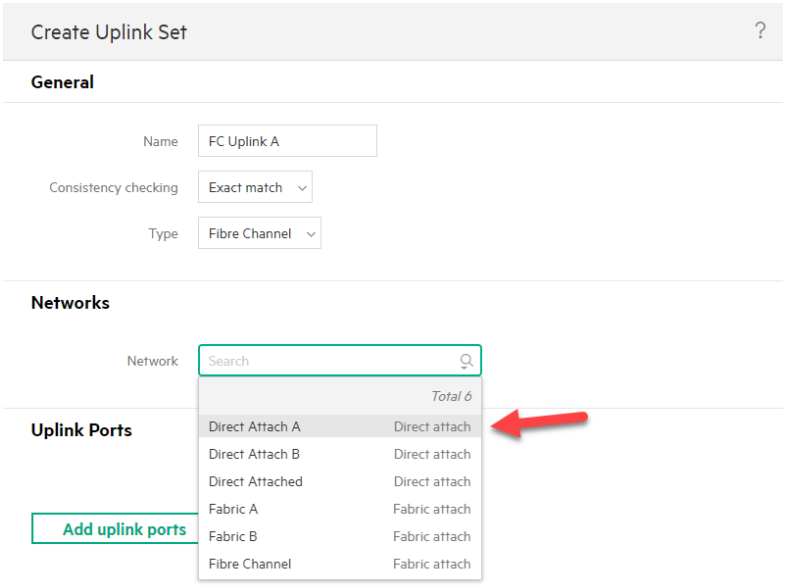
2. In the Create Uplink Set dialog window, enter a *Name* for the uplink



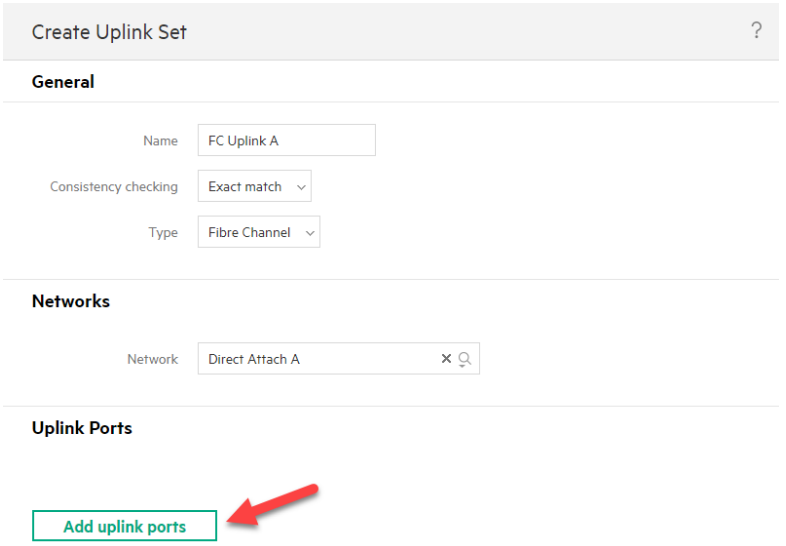
3. From the Type drop down list select *Fibre Channel*.



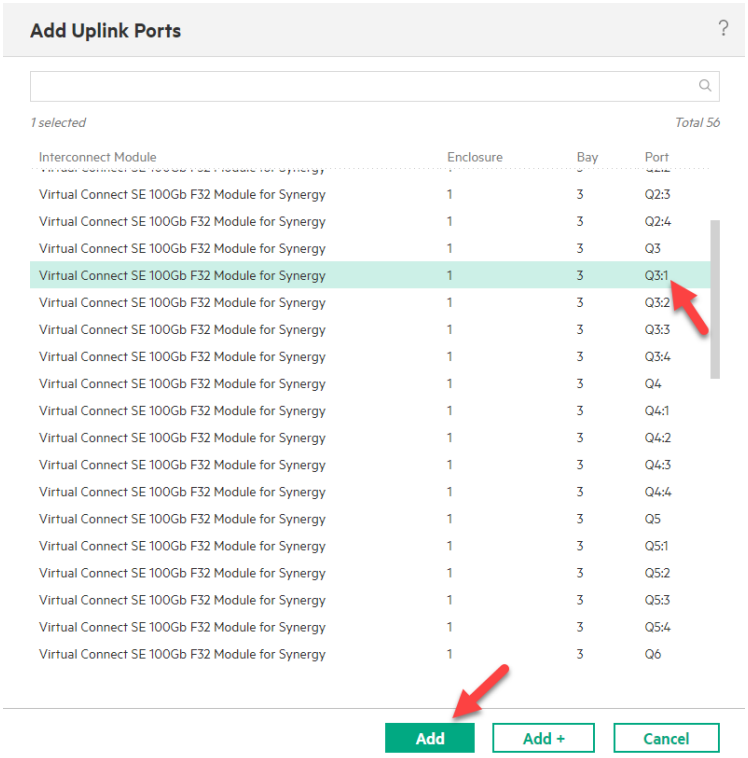
4. In the Networks section, select the desired SAN Fabric *Network* name from the drop-down list.



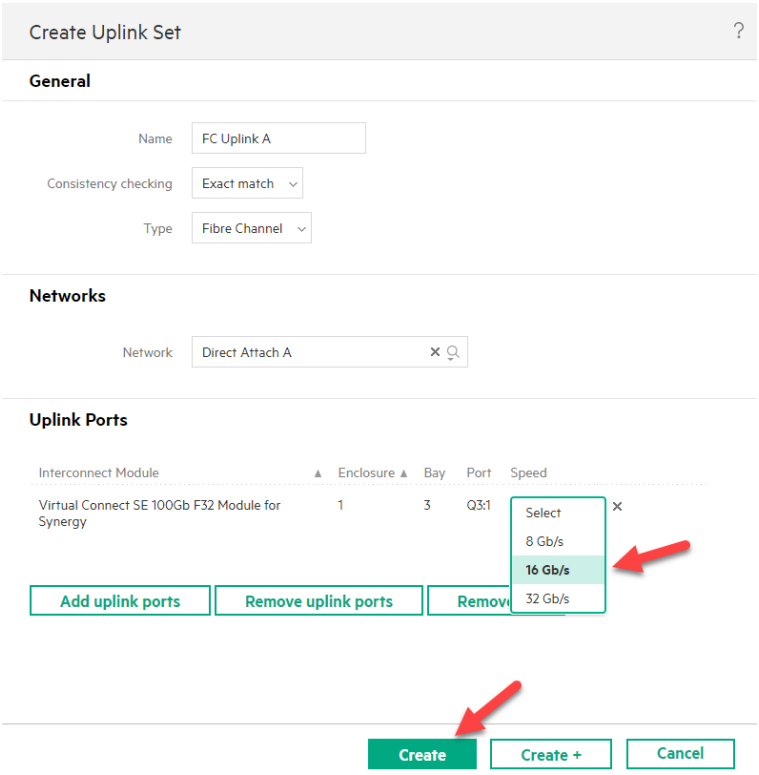
5. Under the Uplink Ports heading, click *Add uplink ports*



6. In the *Add uplink ports* to Uplink dialog, select at least one port for the uplink then click *Add*.



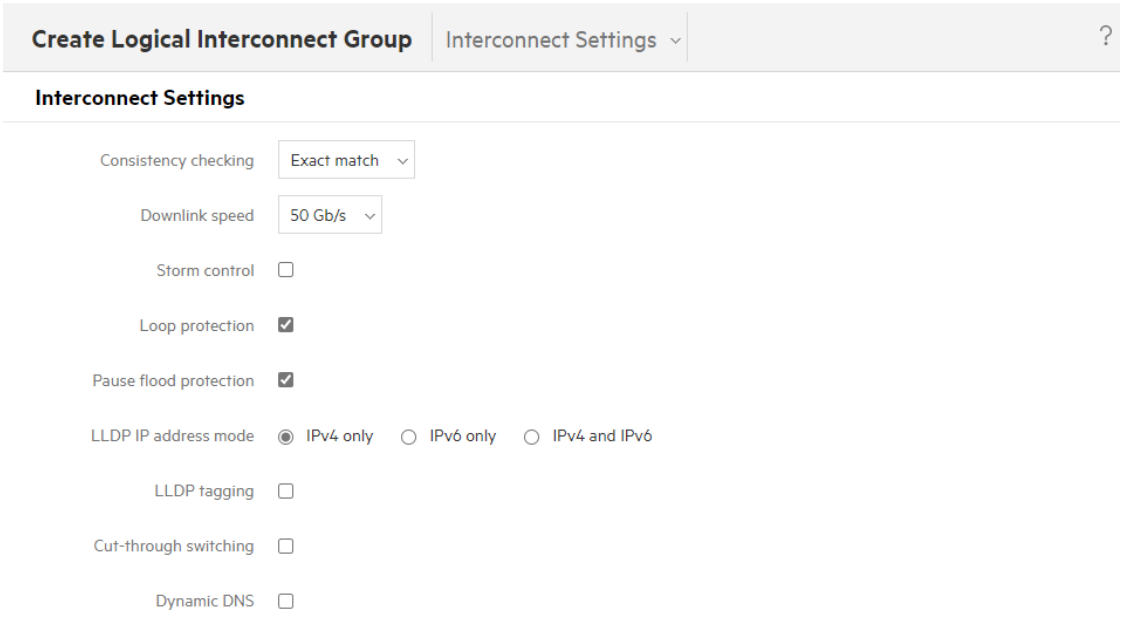
7. As this is a Direct Attach FC uplink (used for Flat SAN) a *Speed* needs to be selected for the connection. Click the *Create* button to finalize the Fibre Channel Uplink.



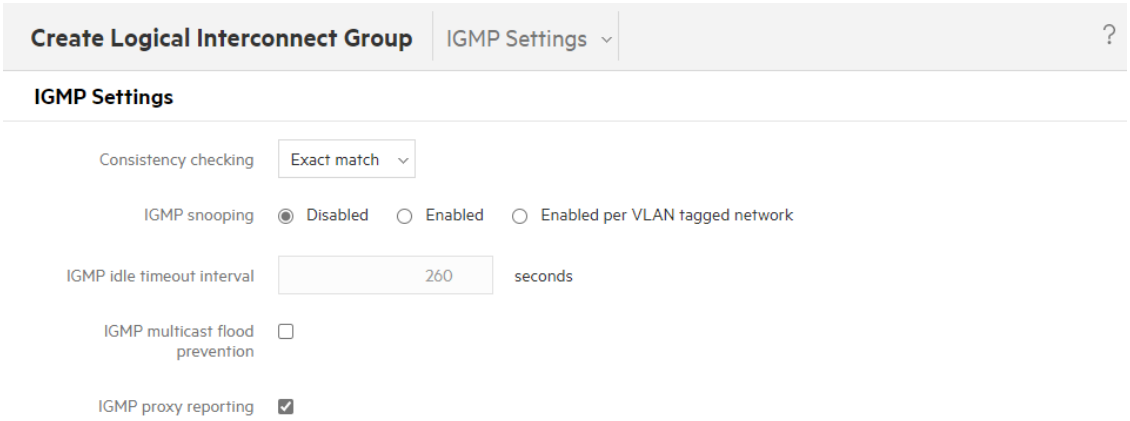
Note:
You can now follow the same procedure to create the connectivity to the "B" FC Fabric.

Finalizing the Logical Interconnect Group Settings

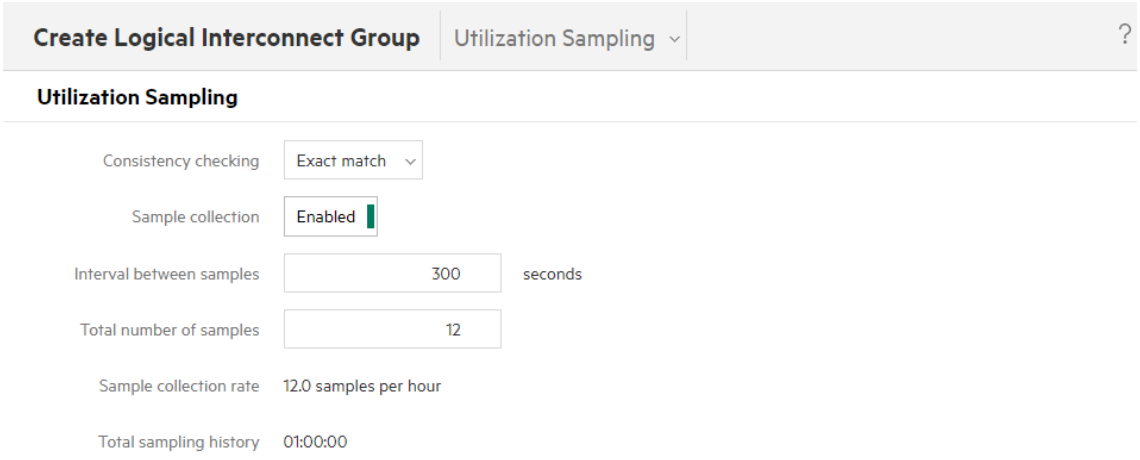
1. From the Create Logical Interconnect Group window, scroll down to the Interconnect settings section. Configure any of the settings that are needed.



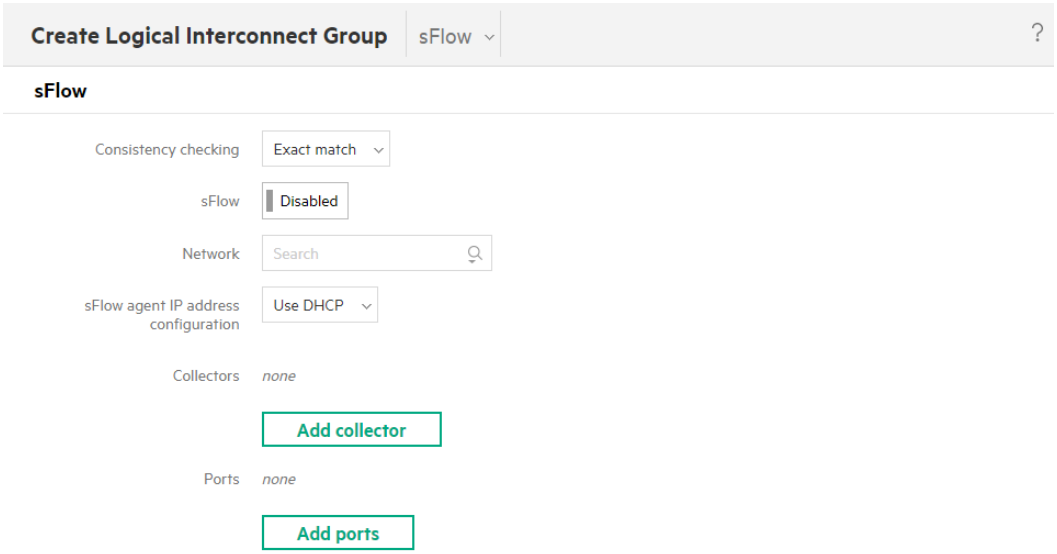
2. From the Create Logical Interconnect Group window, scroll down to the IGMP Settings section. Configure any of the settings that are needed.



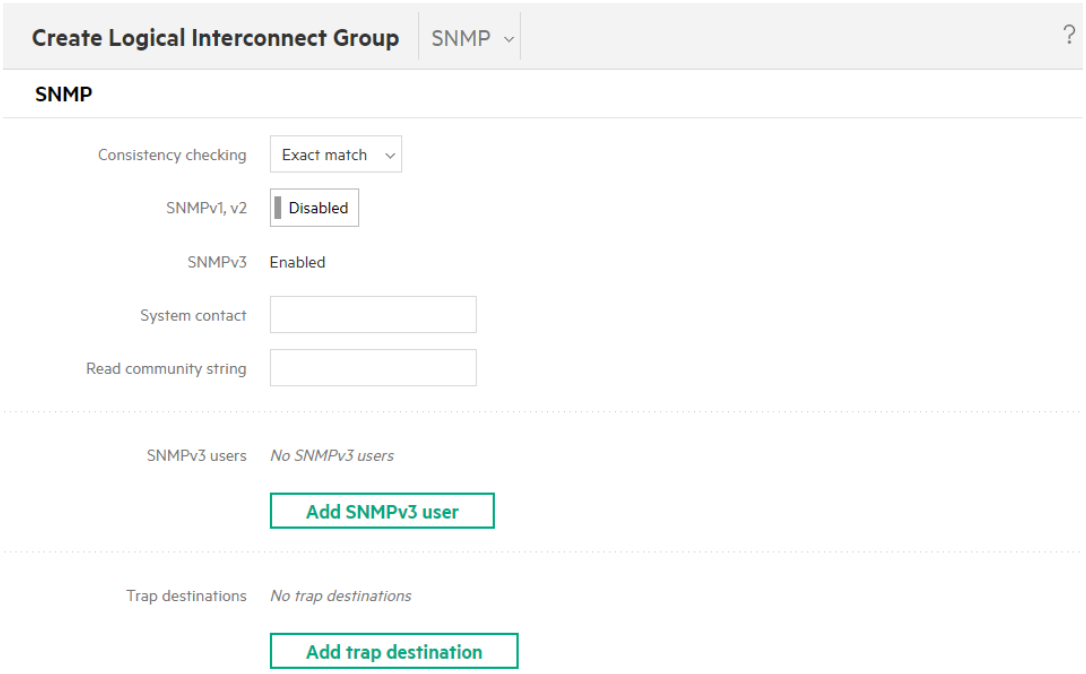
3. From the Create Logical Interconnect Group window, scroll down to the Utilization Sampling section. Configure any of the settings that are needed.



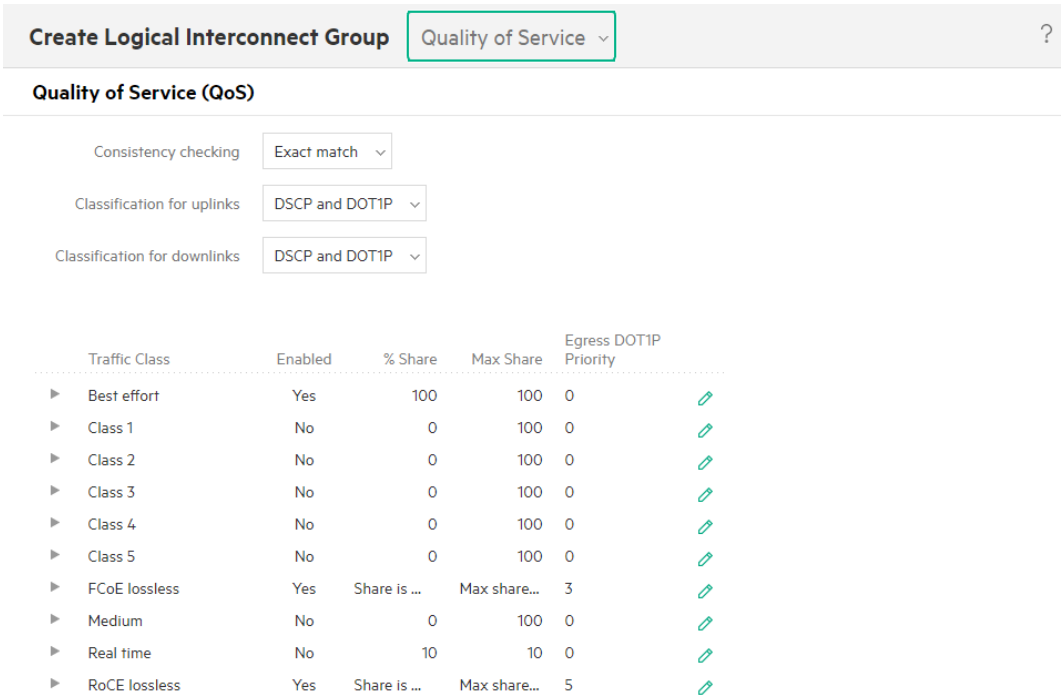
4. From the Create Logical Interconnect Group window, scroll down to the sFlow section. Configure any of the settings that are needed.



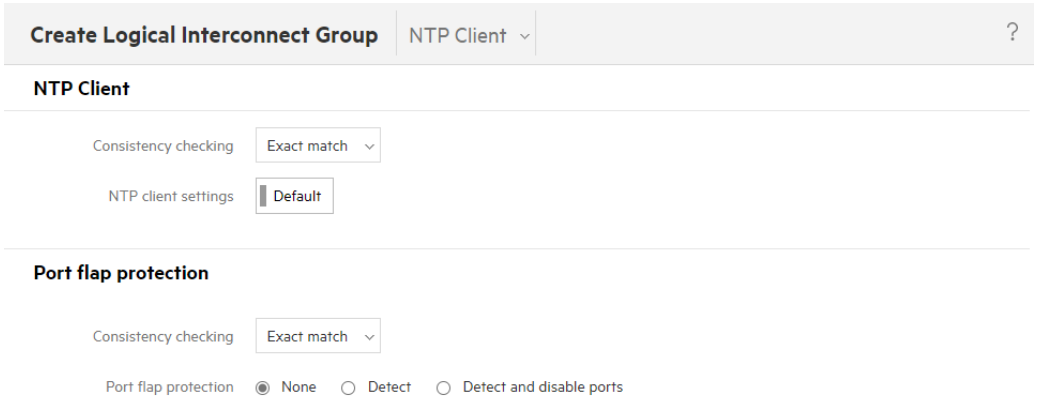
5. From the Create Logical Interconnect Group window, scroll down to the SNMP section. Configure any of the settings that are needed.



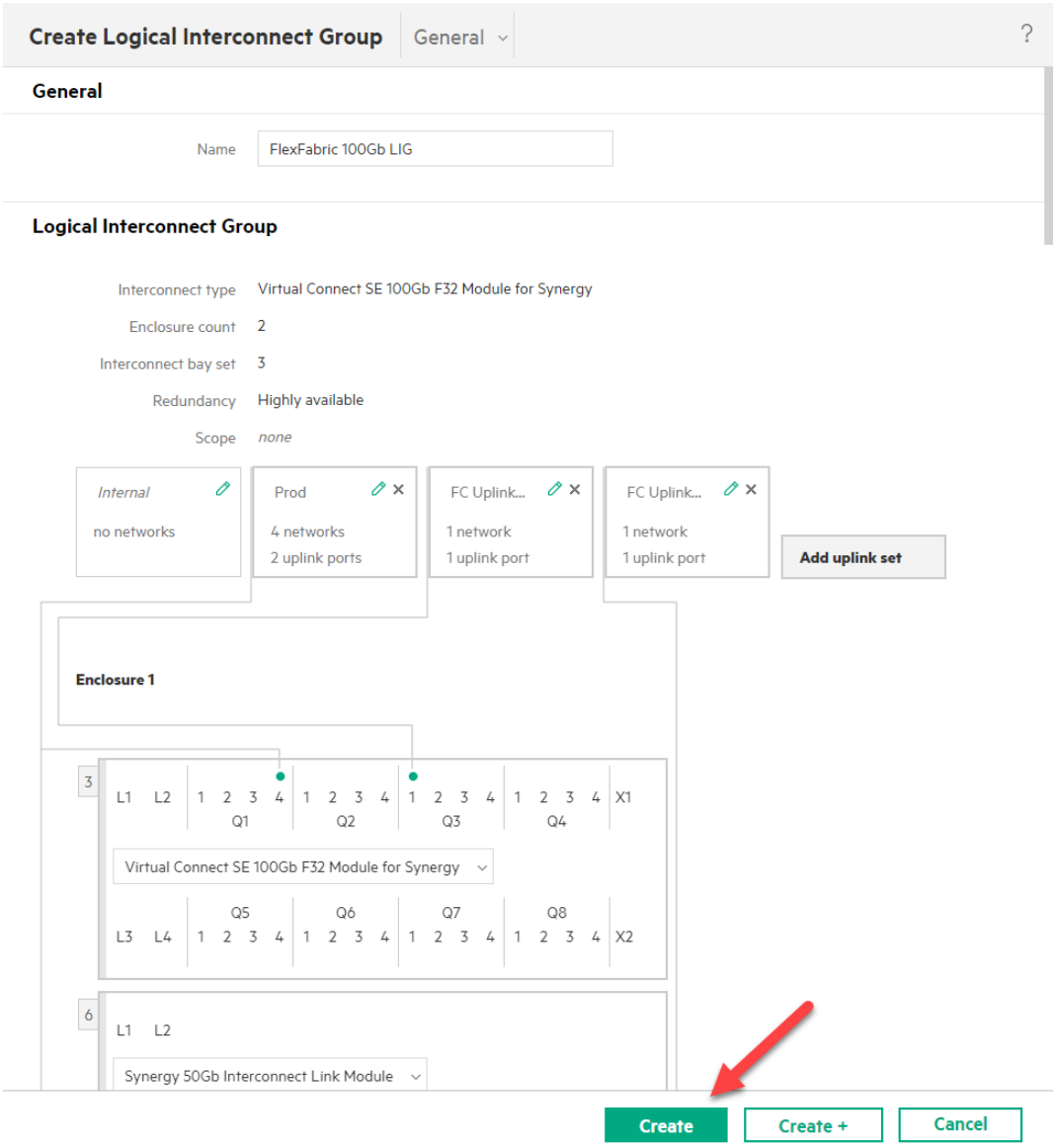
6. From the Create Logical Interconnect Group window, scroll down to the QoS section. Configure any of the settings that are needed.



7. From the Create Logical Interconnect Group window, scroll down to the NTP Client and Port flap protection section. Configure any of the settings that are needed.

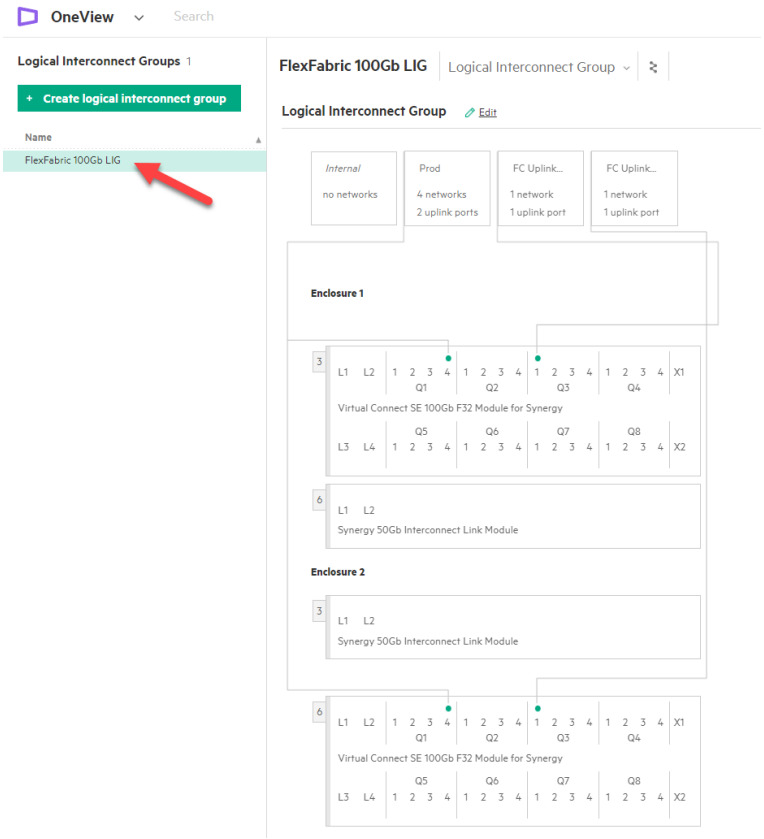


8. Click *Create* to create the Logical Interconnect Group

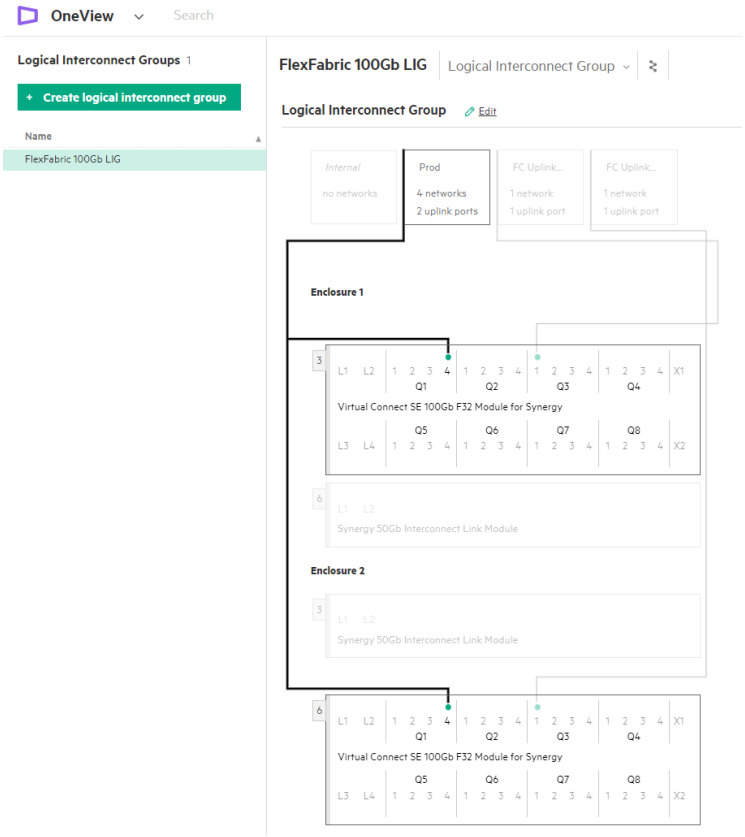


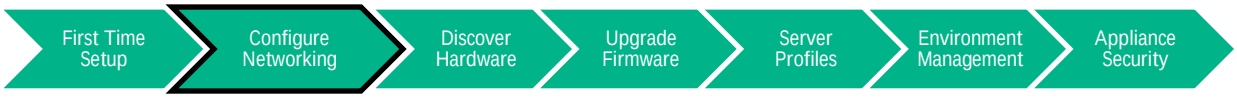
Reviewing Logical Interconnect Group Configuration

1. Select the Logical Interconnect Group by expanding the *NETWORKING* option and then select *Logical Interconnect Groups*. Now review the Logical Interconnect Group that you just created.



2. Hover over of the *Uplink sets*. Examine the relationship of the Uplink set to the physical modules and their uplink ports.





- Create Ethernet Networks
- Create Fibre Channel Networks
  - (Optional) FC Direct Attach
- Create Fibre Channel over Ethernet
- Create RDMA over Converged Ethernet
- Network Sets
- Logical Interconnect Groups
- Enclosure Groups

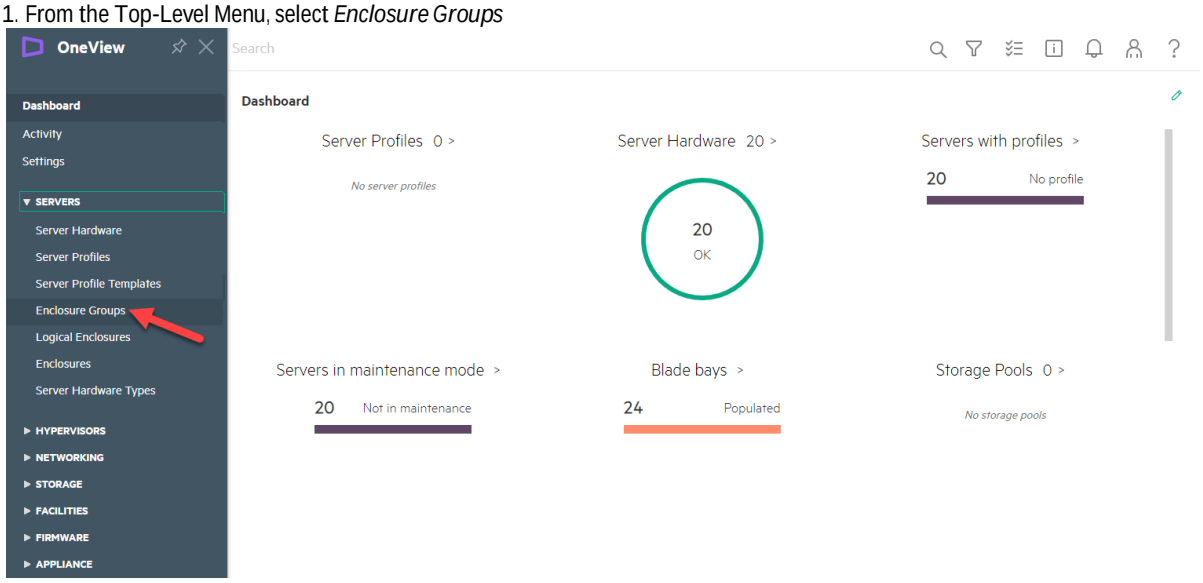
Create Enclosure Group

An Enclosure Group is a centralized configuration policy, similar to that of the Logical Interconnect Group, in which all associated Enclosures retrieve their configuration from. The Enclosure Group will define the Logical Interconnect Group association in relation to the Interconnect Bays in the rear of the Synergy Frame(s).

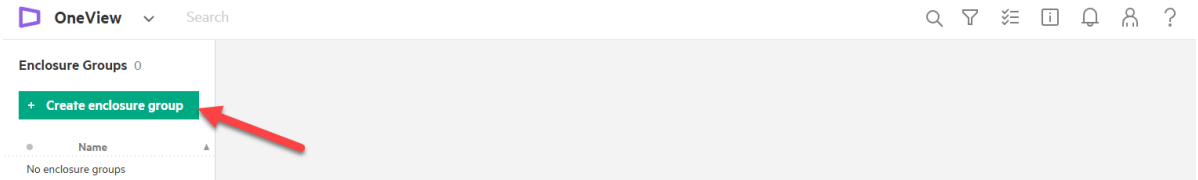
The following example is for two Synergy Frames. Remember that Synergy Virtual Connect can be spanned over a maximum of five Synergy Frames in the "Data Plane" while HPE Synergy Composer's can manage up to 21 x Synergy Frames in the "Management / Control Plane". This means that a single pair of HPE Synergy Composers can manage multiple Frame "Data Plane" environments.

Note: *For the following example it assumes that the required Logical Interconnect Groups have been configured.*

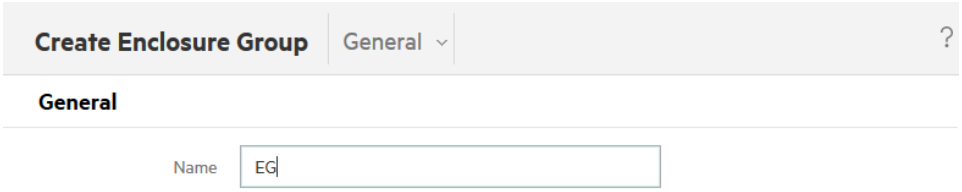
1. From the Top-Level Menu, select *Enclosure Groups*



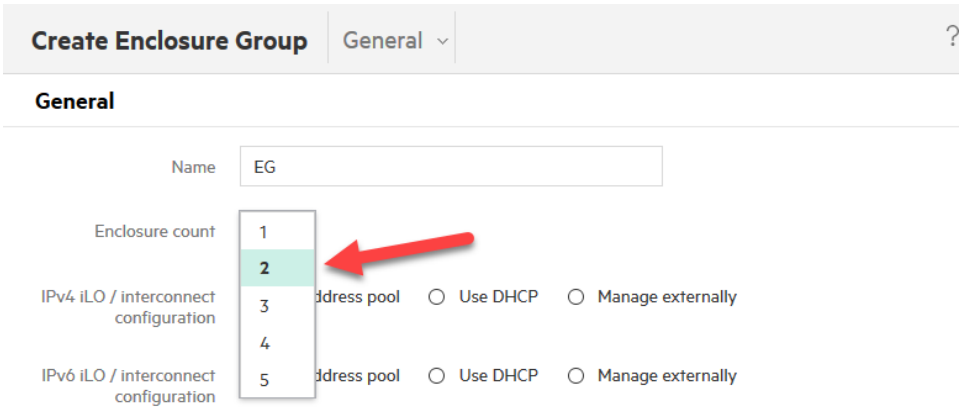
2. Click on the *Create enclosure group* button.



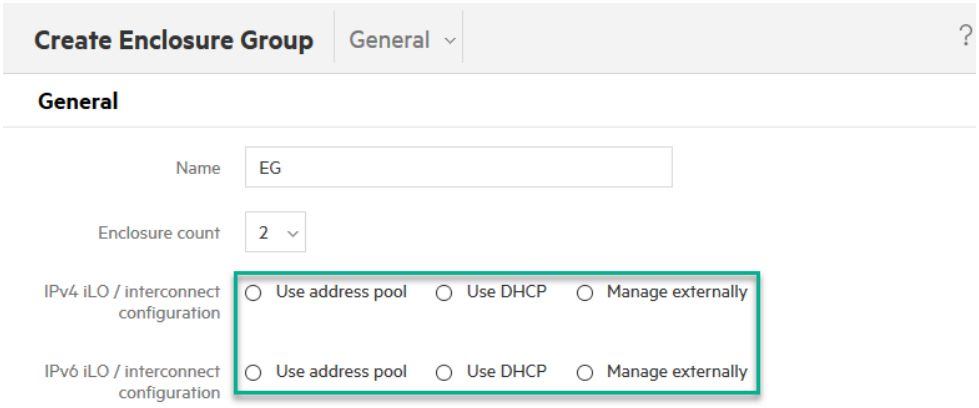
3. In the Create Enclosure Group screen, enter a *Name* for the enclosure group



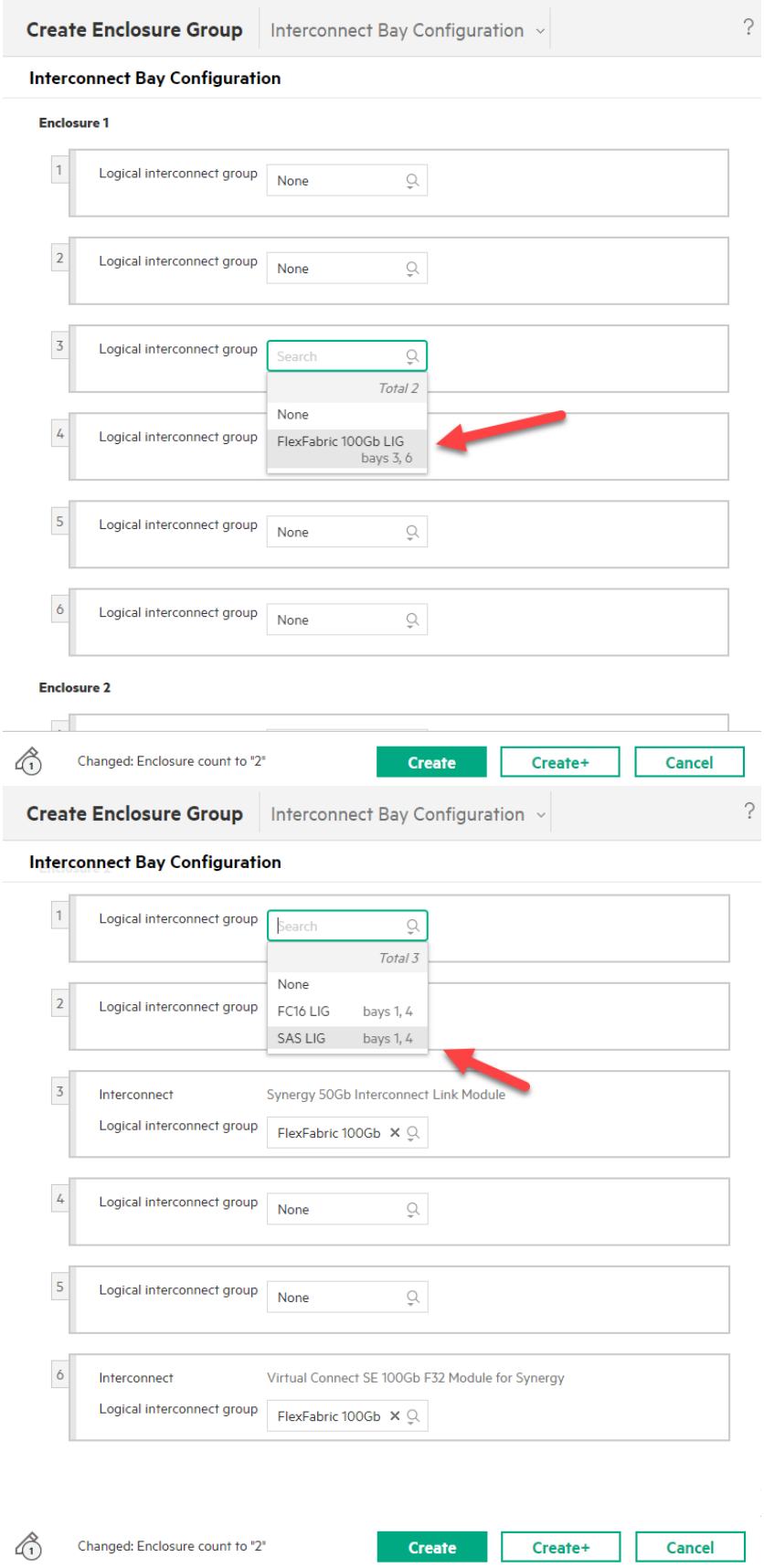
4. Choose your Enclosure count for this example we have two Frames



5. There are several options when creating the Enclosure Group for assigning IP Addressing to the iLO for the Compute Modules and Interconnects. Previously you could use the HPE Synergy Composer Address Pool or DHCP if available in the Management Network. A new option in HPE Synergy Composer to allow you to manually configure these IP Addresses, this can be done after the Logical Enclosure has been created, see the later section titled *"Synergy Static IP Address Assignment for Compute Modules and Interconnects"*. Choose the option that you require for your environment.



6. Select the Logical Interconnect Group for each of the Interconnect Bays that you created previously.

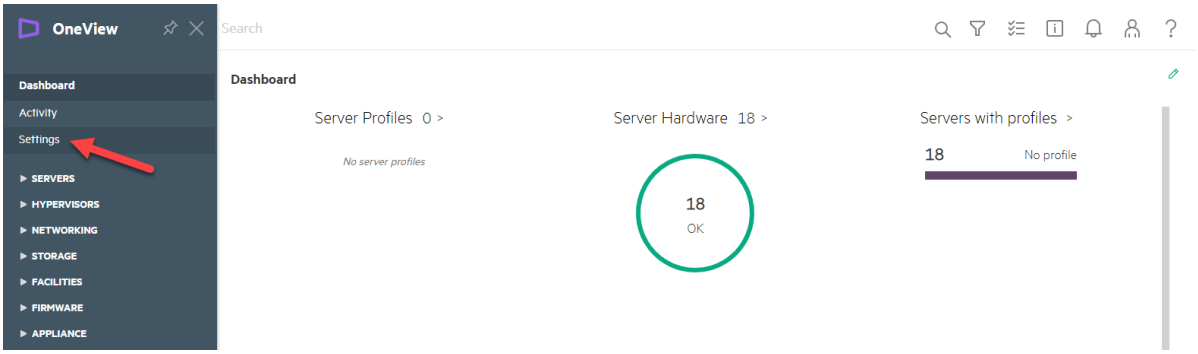


7. Click *Create* when you have completed your configuration requirements to create the Enclosure Group.

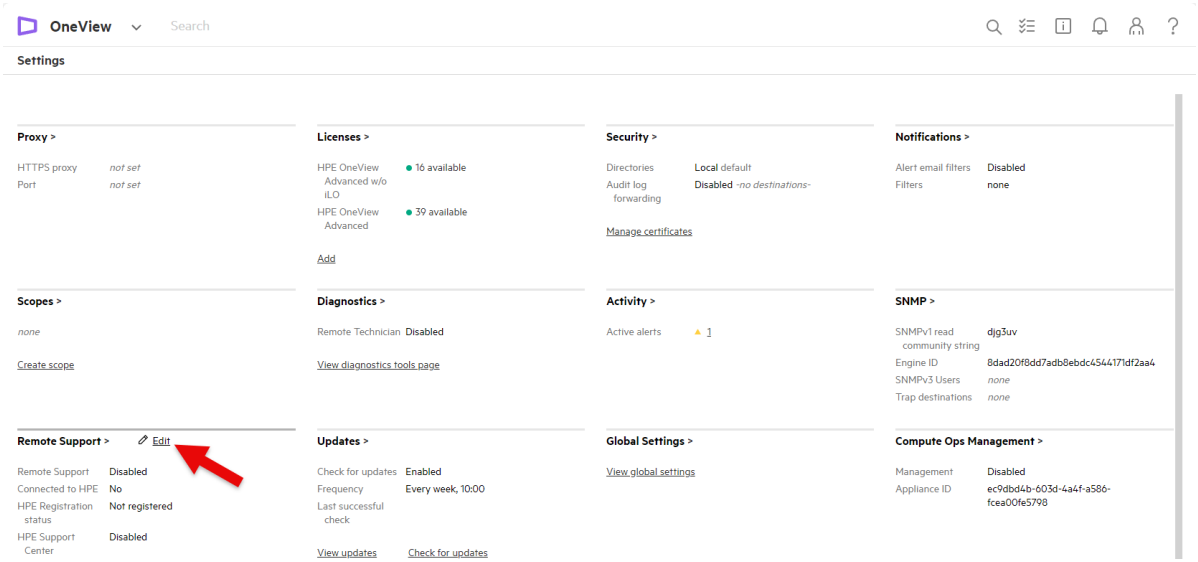
Setting up Remote Support for supported devices

HPE OneView contains support automation functionality for Gen8 and newer devices. These devices will have cases for them created automatically through the remote support functionality.

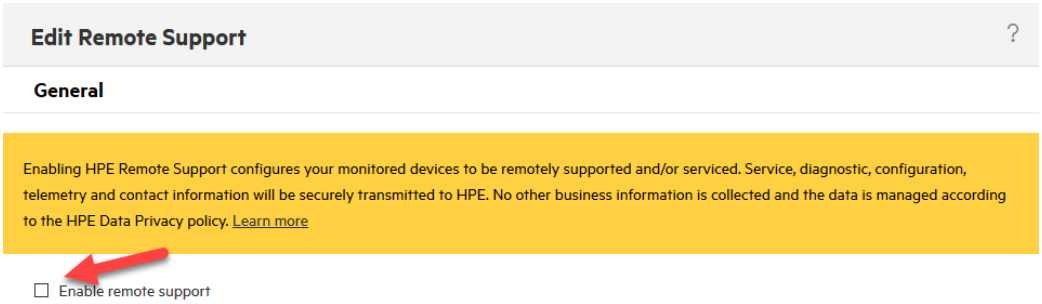
1. From the Top-Level Menu, select *Settings*



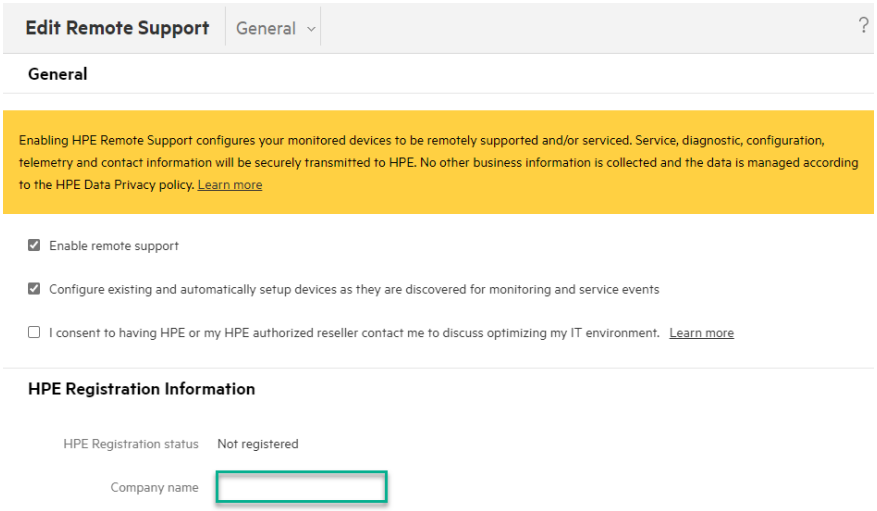
2. From the Settings page, find the Remote Support Section and select *Remote Support*



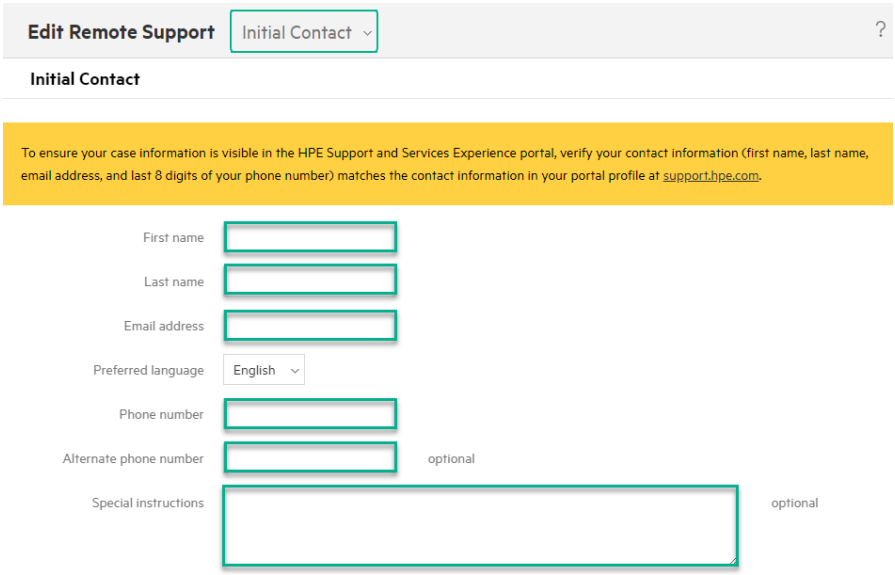
3. To enable Remote Support, check the box *Enable remote support*



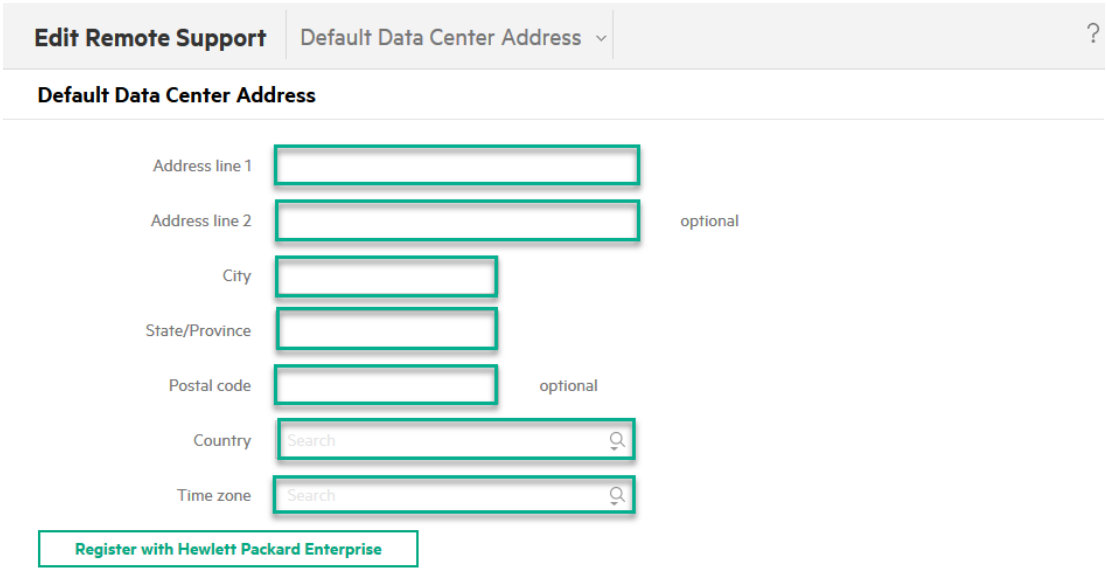
4. In the Registration Information section of the Edit Remote Support dialog window, enter the *Company Name*



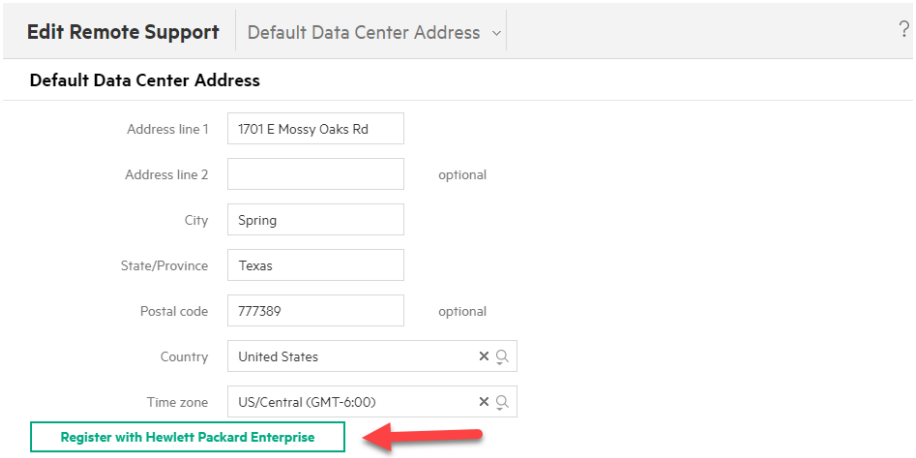
5. Enter the *Initial Contact Information*



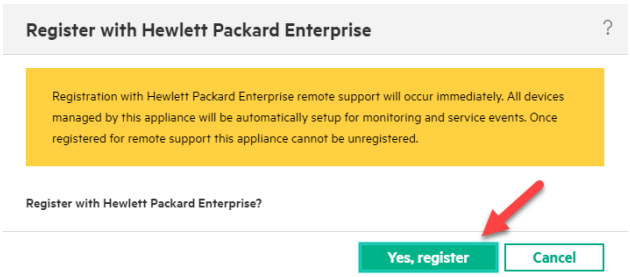
6. Enter the *Default Data Center Address*. This needs to be where the servers are physically located because this is where the parts will be sent.



7. Click *Register with Hewlett Packard Enterprise*



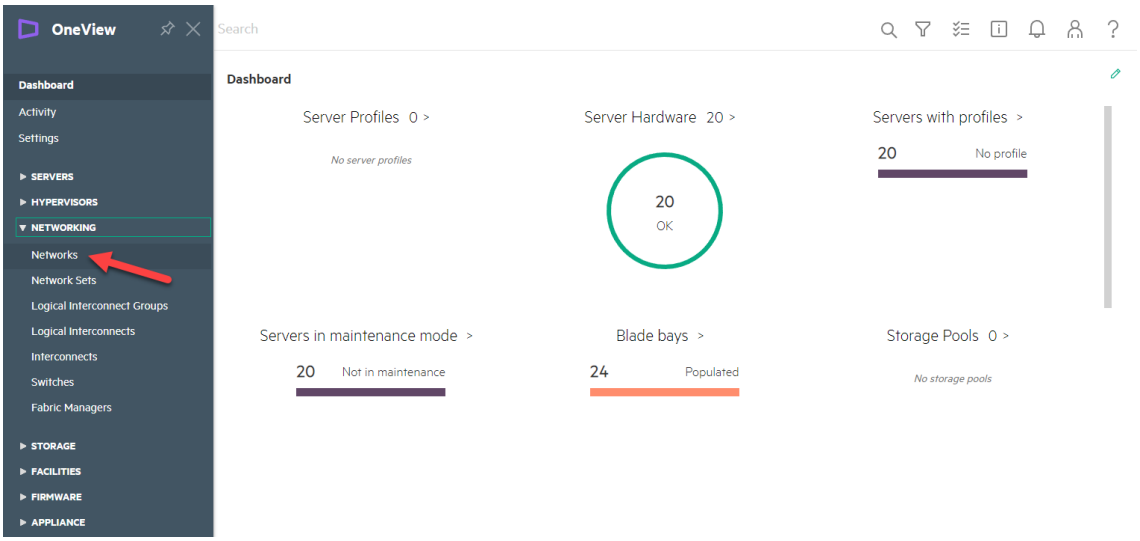
8. Click *Yes, register* to initiate the registration with Hewlett Packard Enterprise.



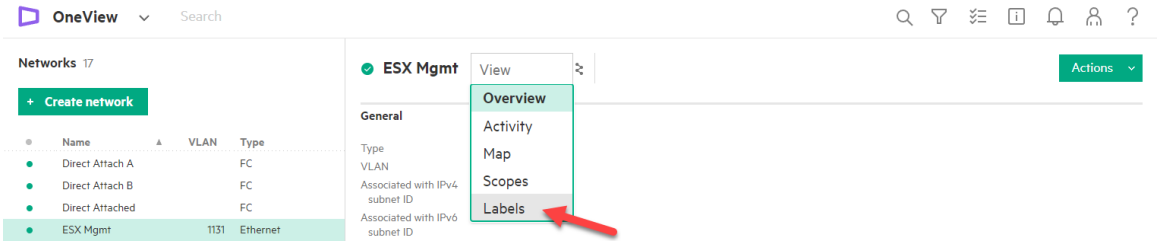
Using Labels

Labels provide a way to classify, or group common resources for filtering or locating. Any resource can be assigned to one or more labels.

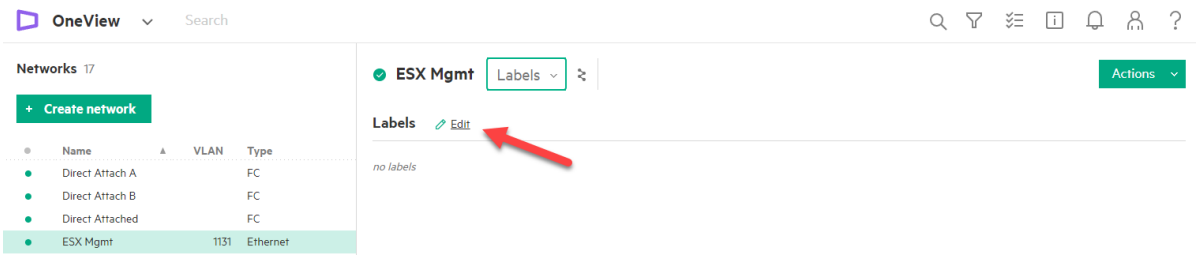
1. Select a resource, for our example we will use the Networks category, so expand the *NETWORKING* option and choose *Networks*.



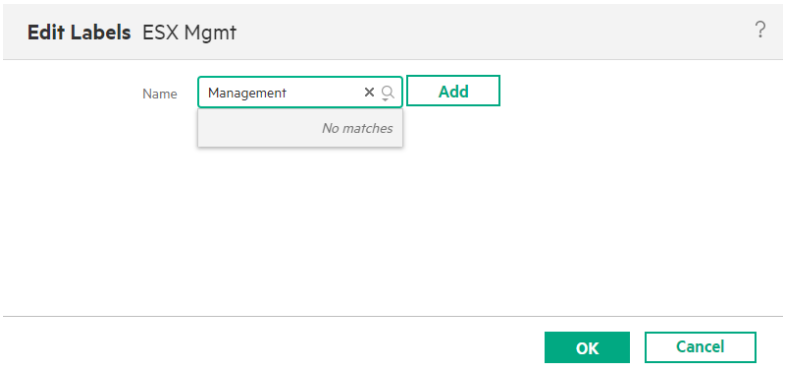
2. Select an item from the menu, then select *Labels* from the view selector menu.



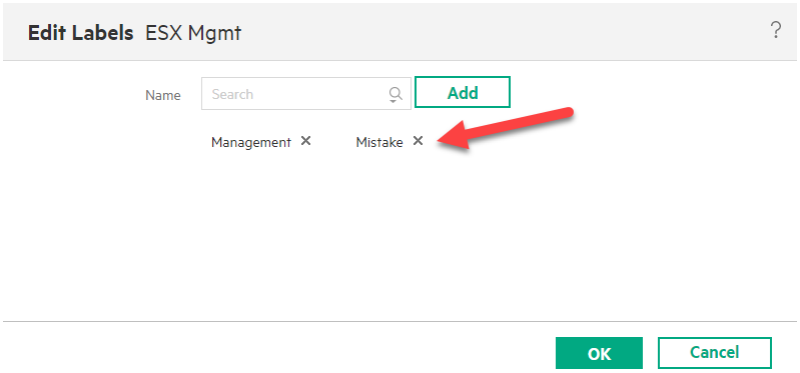
3. Select *Edit*



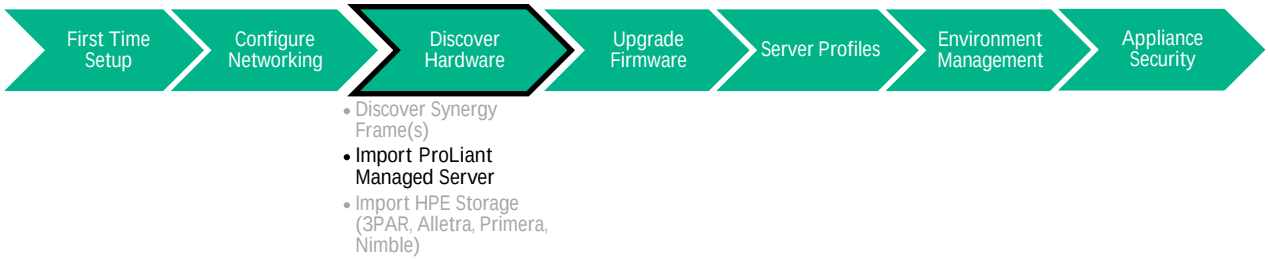
4. Specify the Label you wish to add. You can add one or more labels. Click the *OK* button to save your changes.



If you wish to delete a Label, click the *X* next to the label.

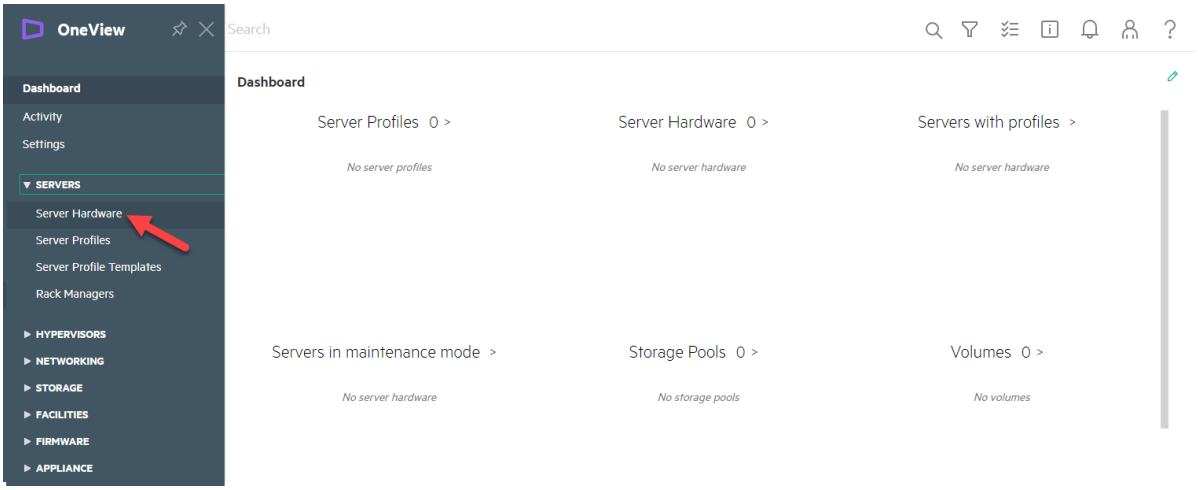


Importing a ProLiant DL, ML or Apollo Managed Server

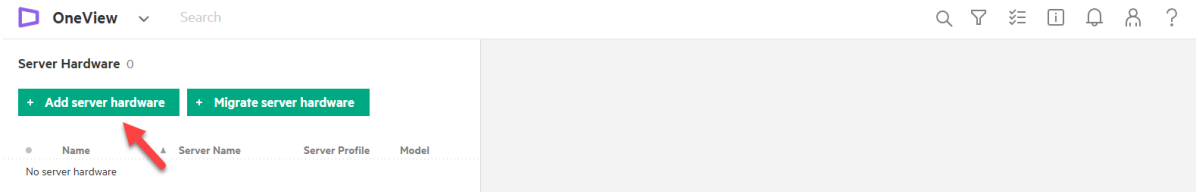


HPE OneView supports adding ProLiant DL Gen8 or newer, ML350 Gen9 or newer and Apollo Gen9 or newer servers for health, alert management and basic server profiles. In this section the example will show how to add a ProLiant DL Gen9 server by adding the iLO IP Address or FQDN.

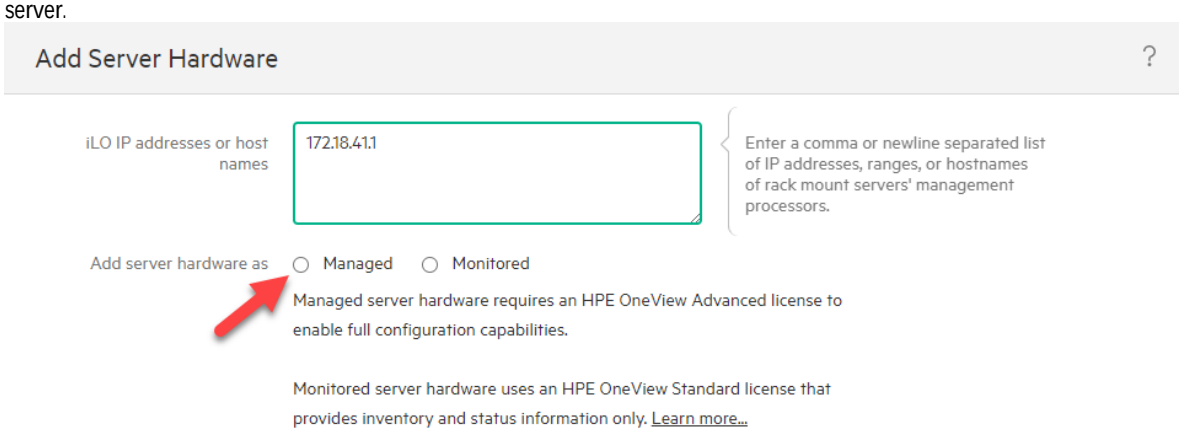
1. From the Top-Level Menu, expand the *SERVERS* option and select *Server Hardware*.



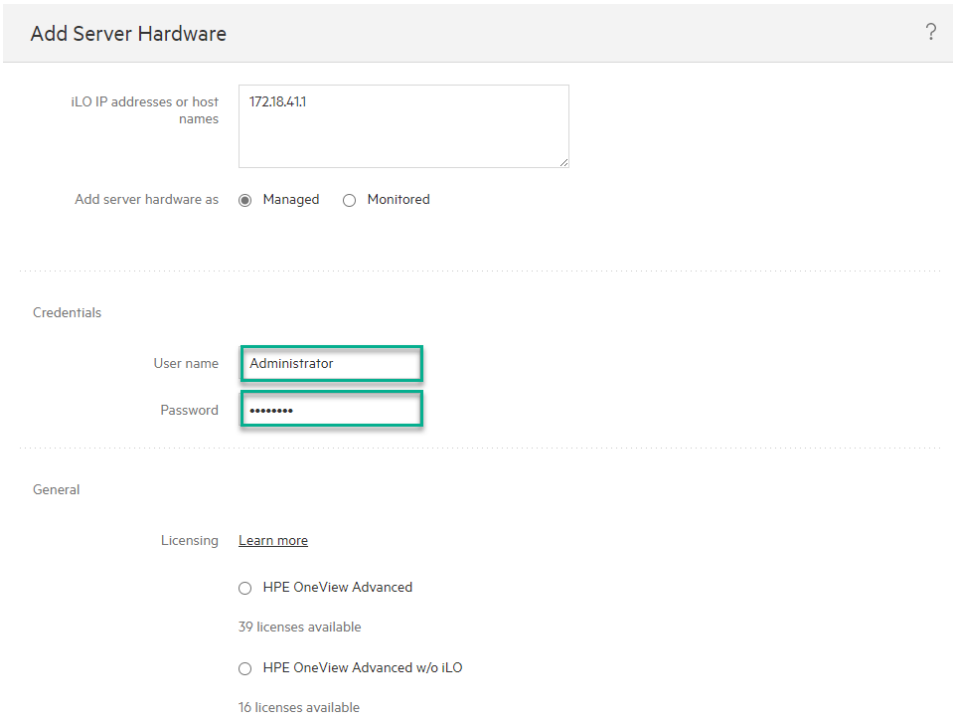
2. In the Server Hardware screen, click the *+Add server hardware* button.



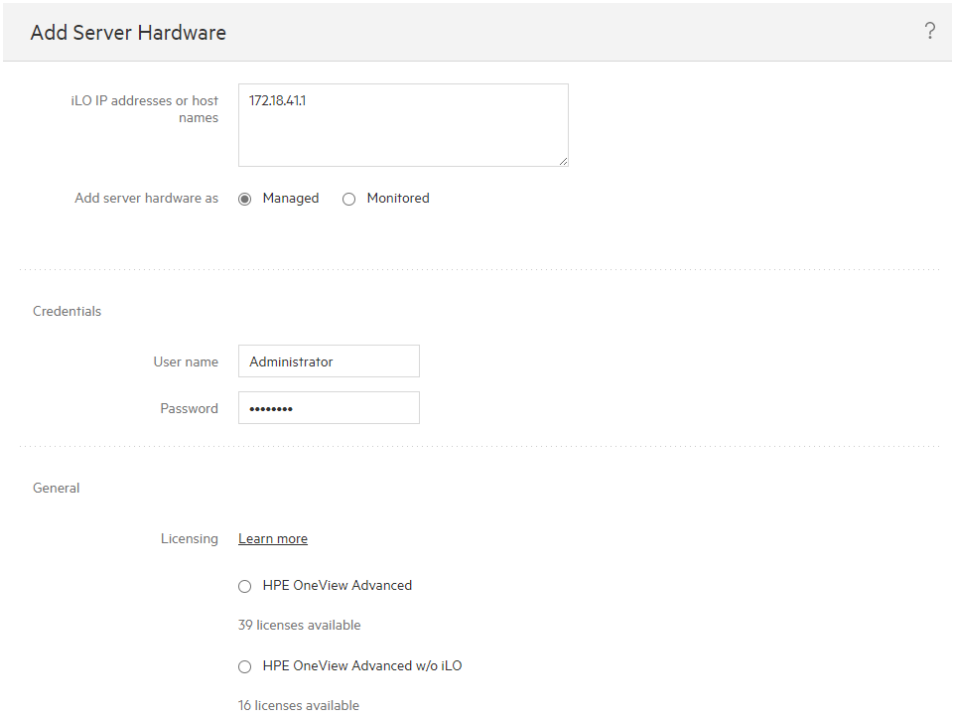
3. In the Add Server Hardware screen, add the *iLO FQDN or IP Address* of the DL server to be added and select the radial button for a *Managed* server.



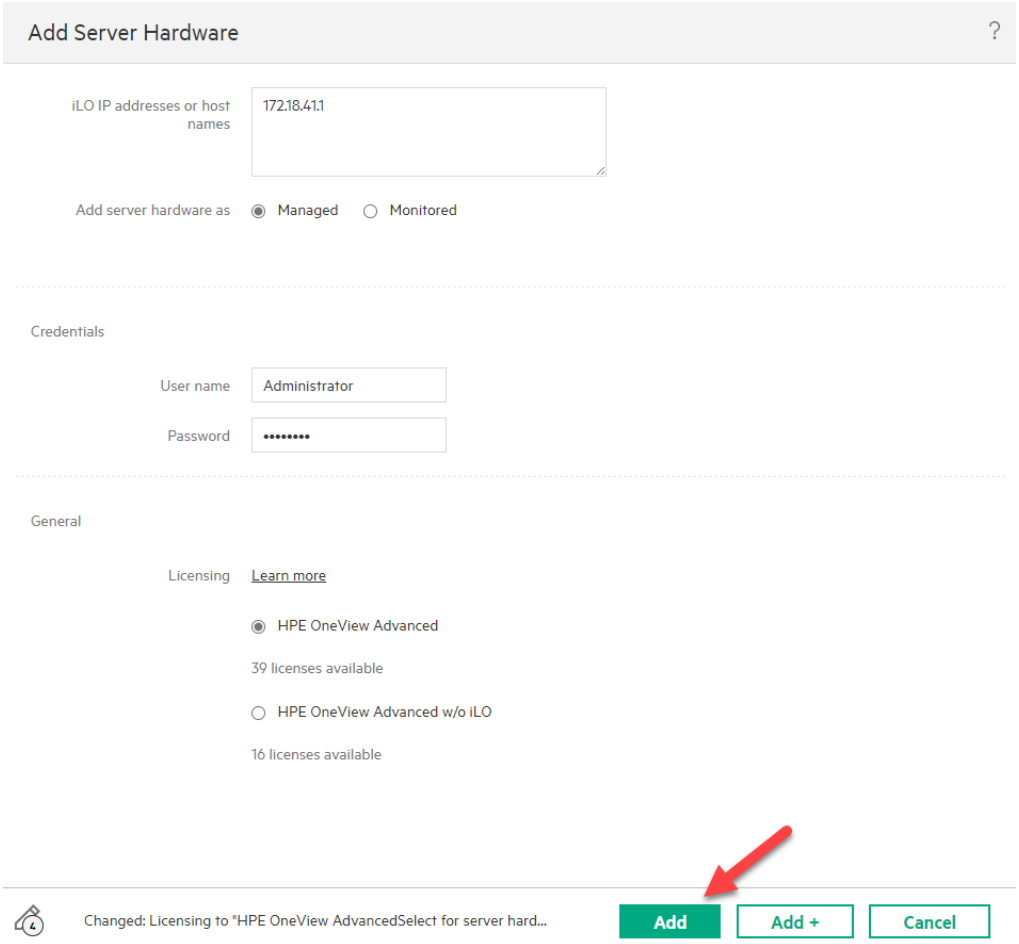
4. Enter the iLO Administrator credentials



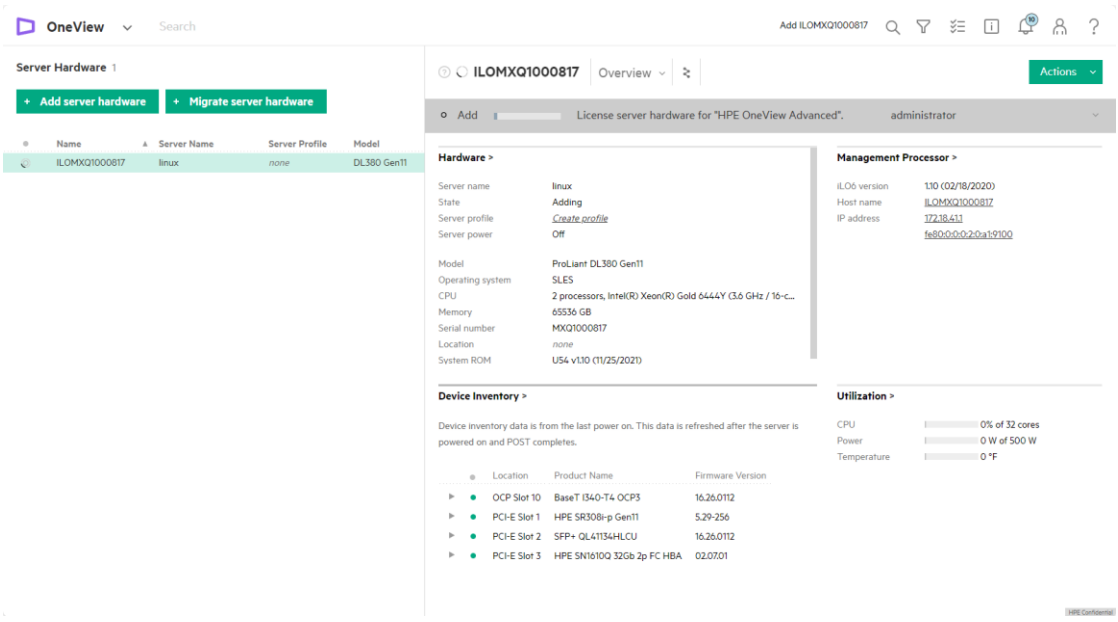
5. Select the license type to be applied to the server – *HPE OneView Advanced* or *HPE OneView Advanced w/o iLO*.



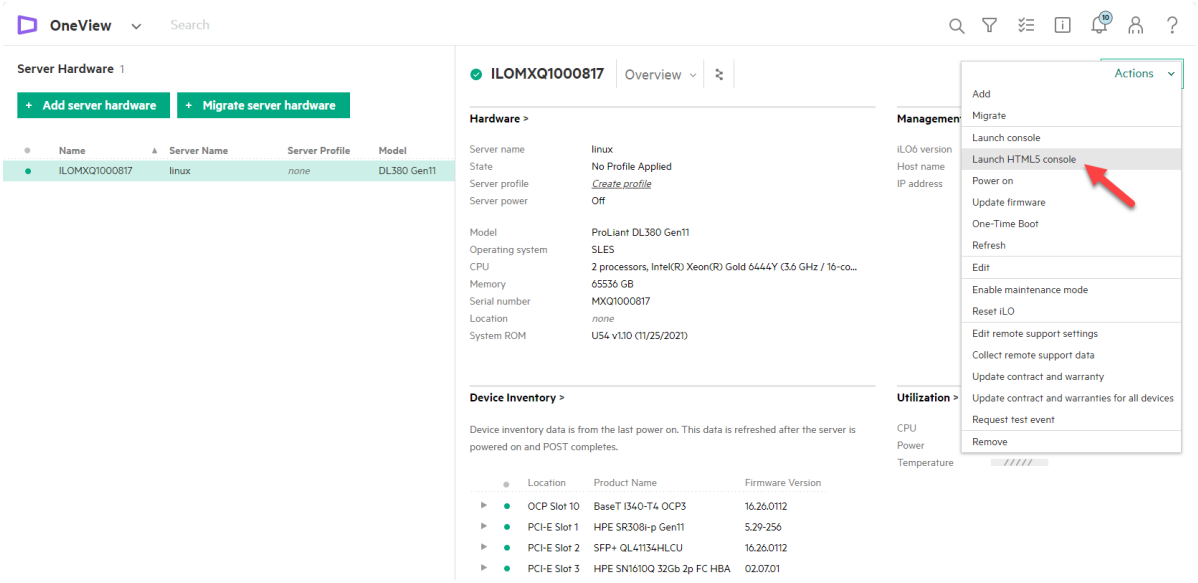
6. Click the *Add* button to add the DL server or select the *Add* + button to add other Managed DL servers.



7. After clicking the *Add* button, HPE OneView will begin to discover the server, and configure the iLO for management.



8. Once the server is added, the administrator has the capability of powering the server on, applying a server profile, or launch the *Remote Console* from the Actions menu.

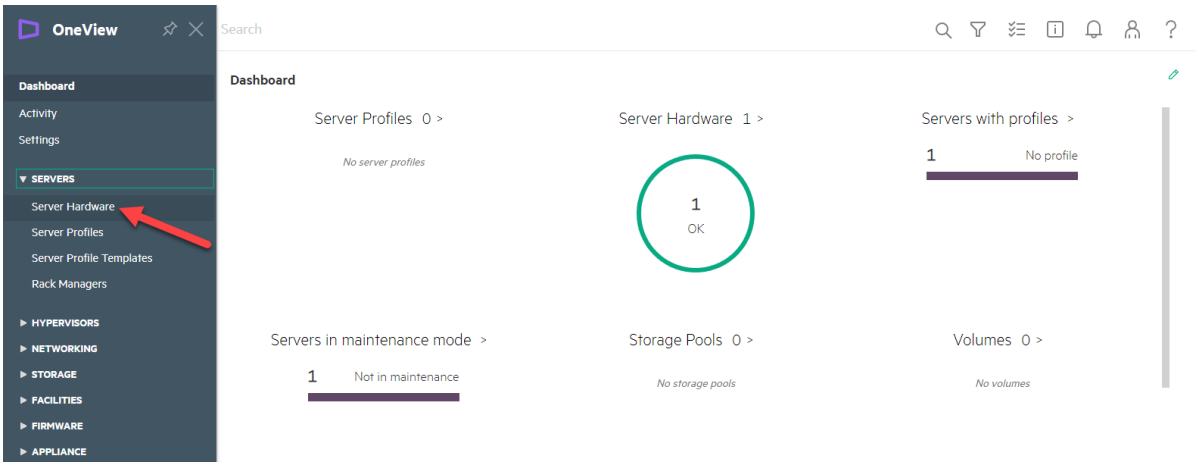


The server is now configured for element management by HPE OneView.

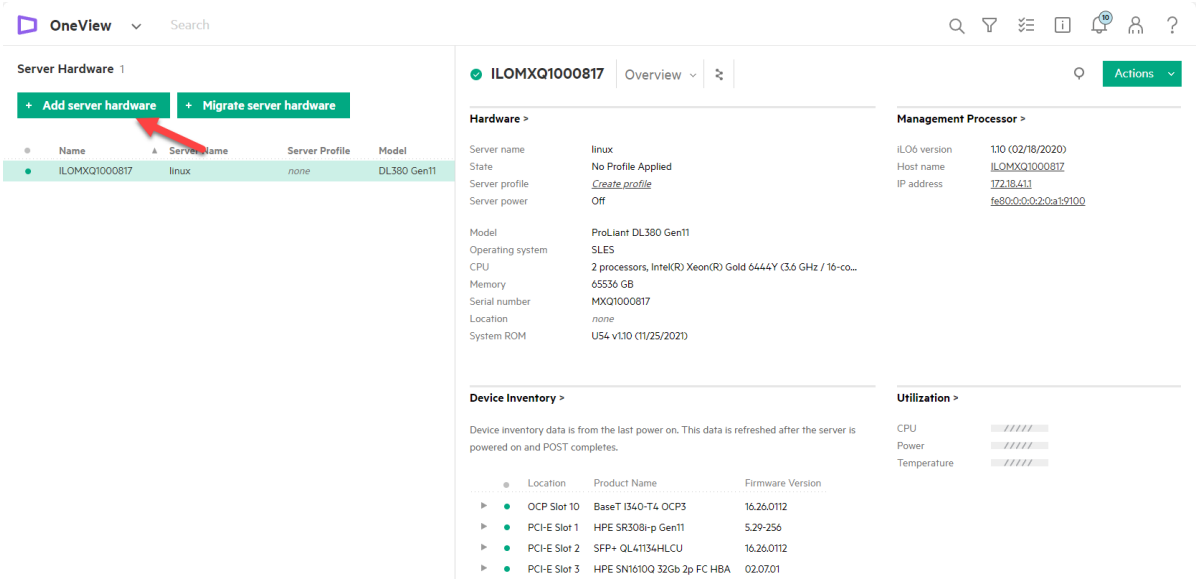
Importing a ProLiant DL, ML, Apollo or Superdome Flex / Superdome Flex 280 or Compute Scale-up Server 3200 as a Monitored Server

HPE OneView supports adding a ProLiant DL Gen8 or newer, ML Gen9 and Apollo 2000, 4000 and 6000 and Superdome Flex / Superdome Flex 280 or Compute Scale-up Server servers for hardware monitoring. In this section you will add a server for monitoring by adding the iLO IP Address or FQDN / Rack Manager.

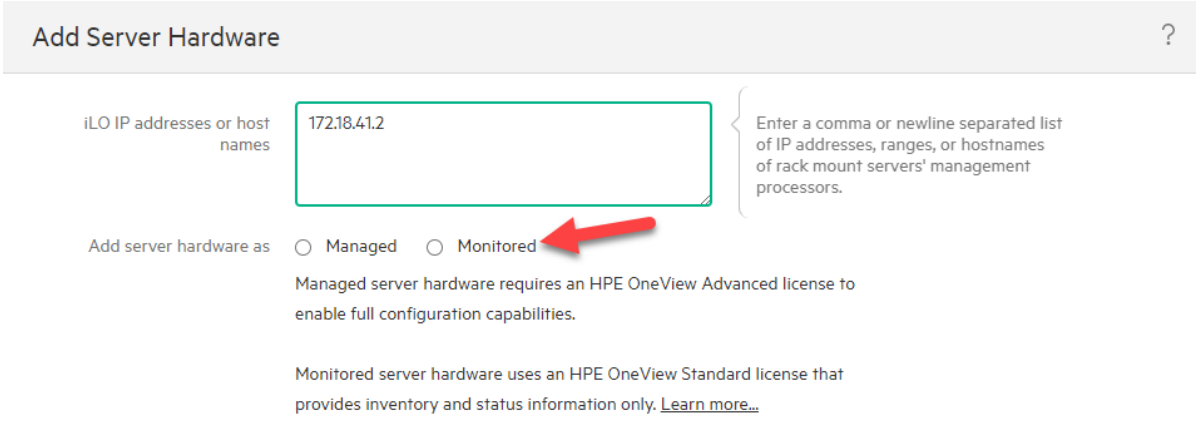
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Hardware.*



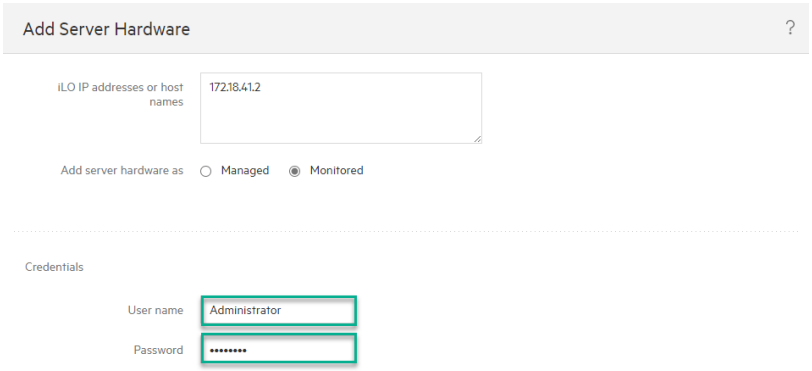
2. In the Server Hardware screen, click the + *Add server hardware* button.



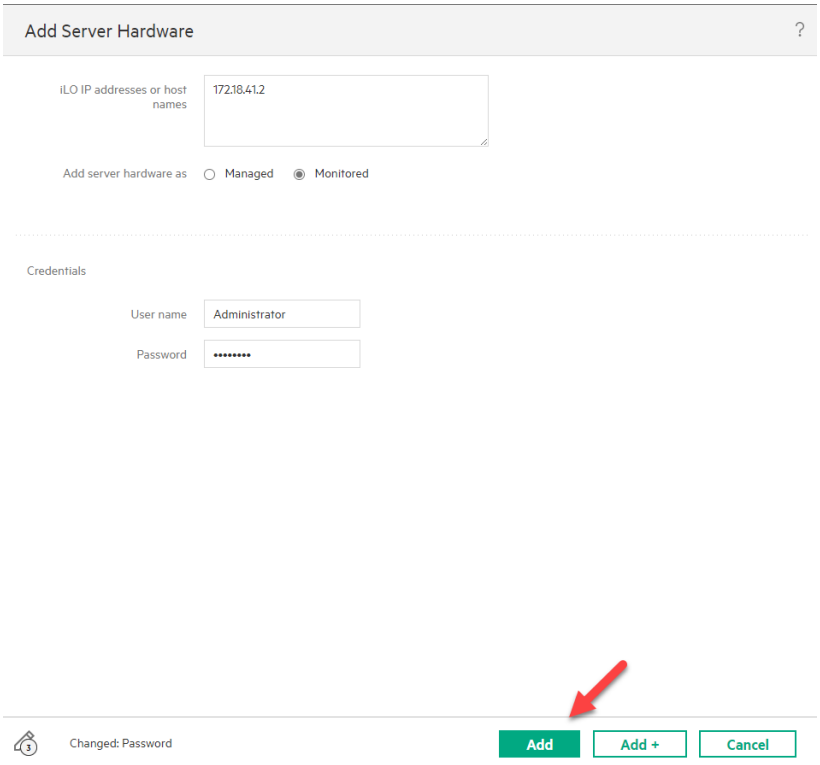
3. In the Add Server Hardware screen, add the iLO FQDN or IP Address of the DL server to be added and select *Monitored* for the license model.



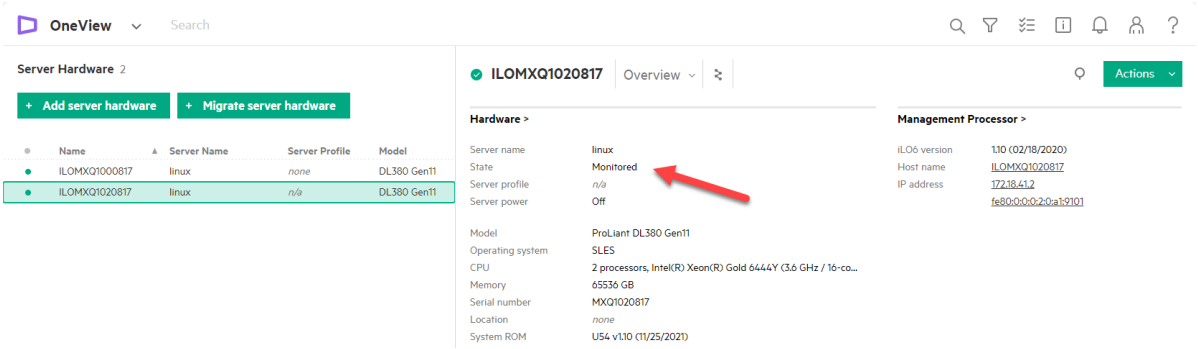
4. Enter the iLO Administrator credentials.



5. Click the *Add* button to add the DL server or select the *Add+* button to add other servers.



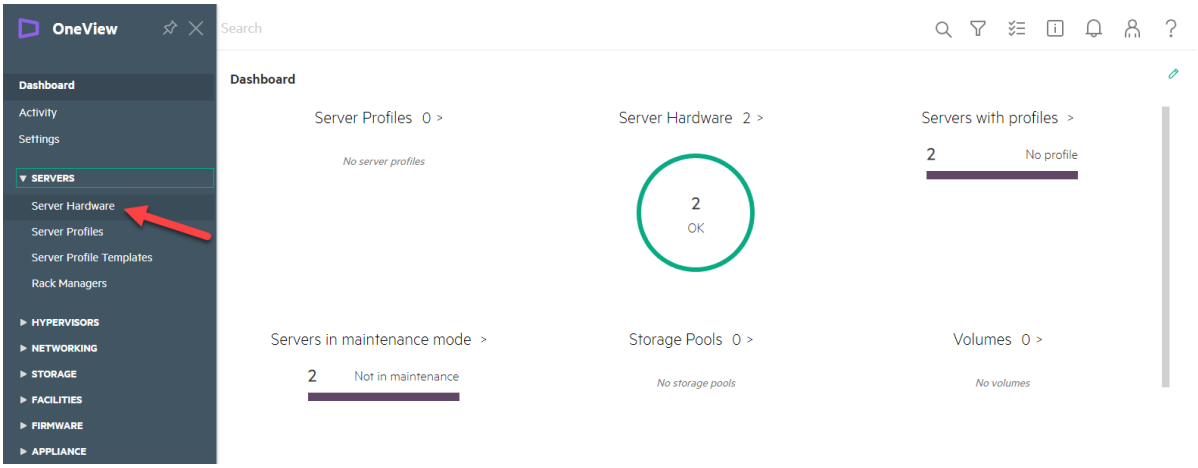
6. The server is now ready for hardware monitoring via HPE OneView



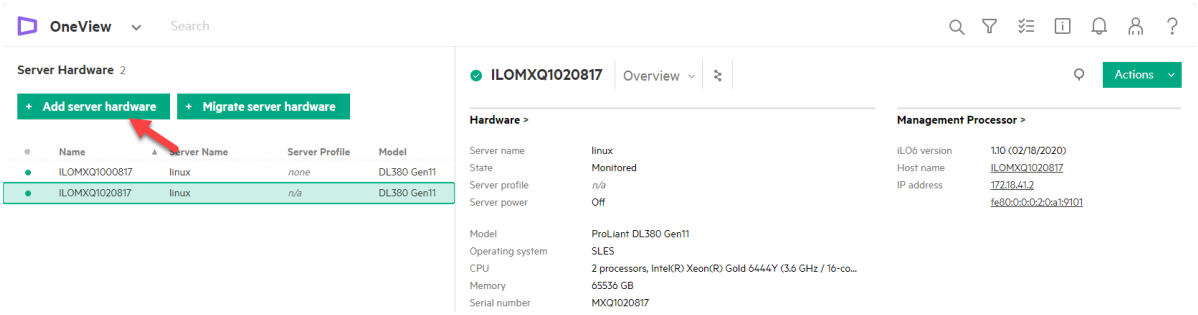
Importing a Range of Servers as Managed Devices

HPE OneView supports adding a range of iLO addresses to import large numbers of servers simultaneously.

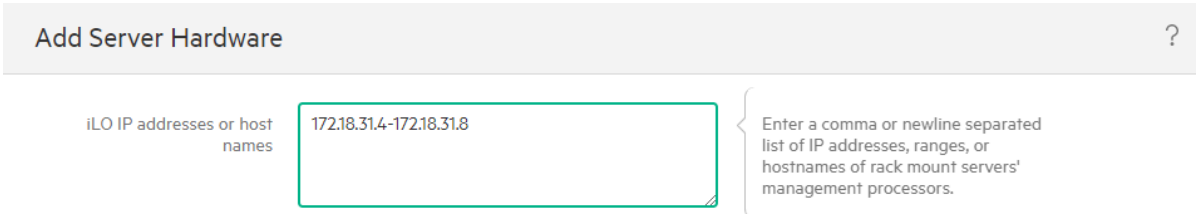
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Hardware*.



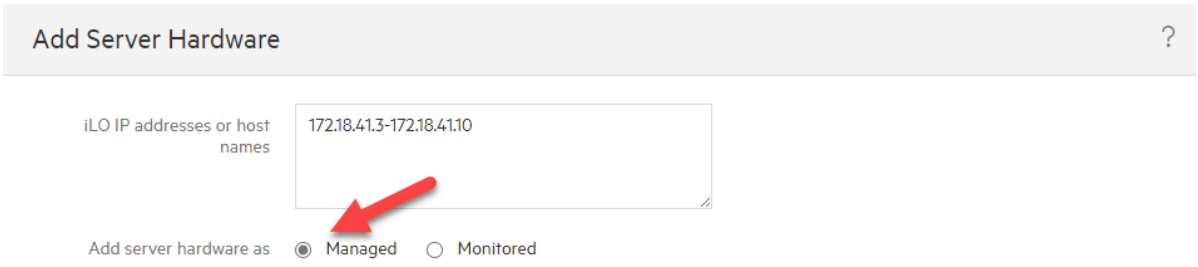
2. In the Server Hardware screen, click the + *Add server hardware* button.



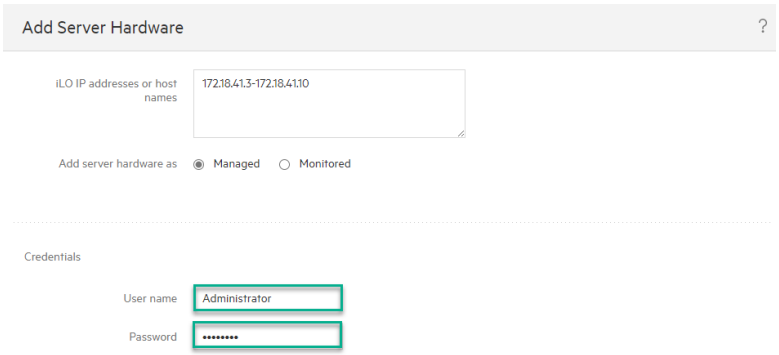
3. Enter the range of iLO IP addresses for the servers to be imported



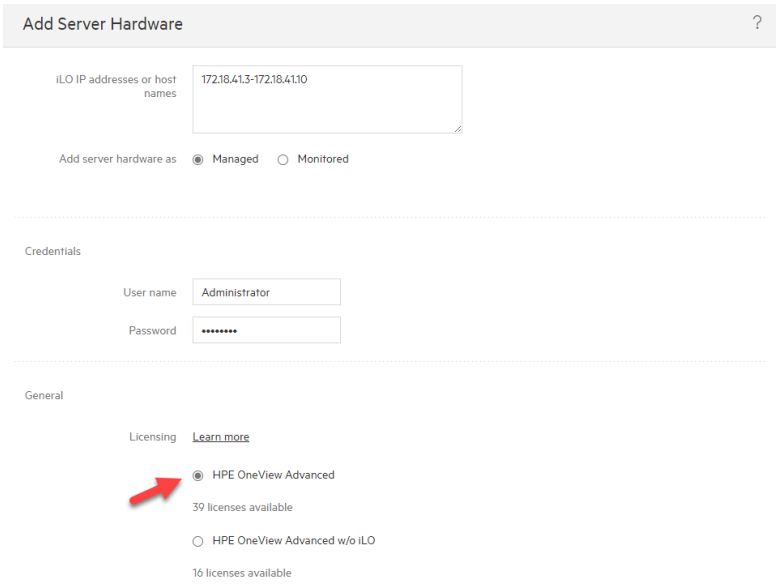
4. Select the *Managed* radial button to import the above referenced servers with an OneView Advanced license.



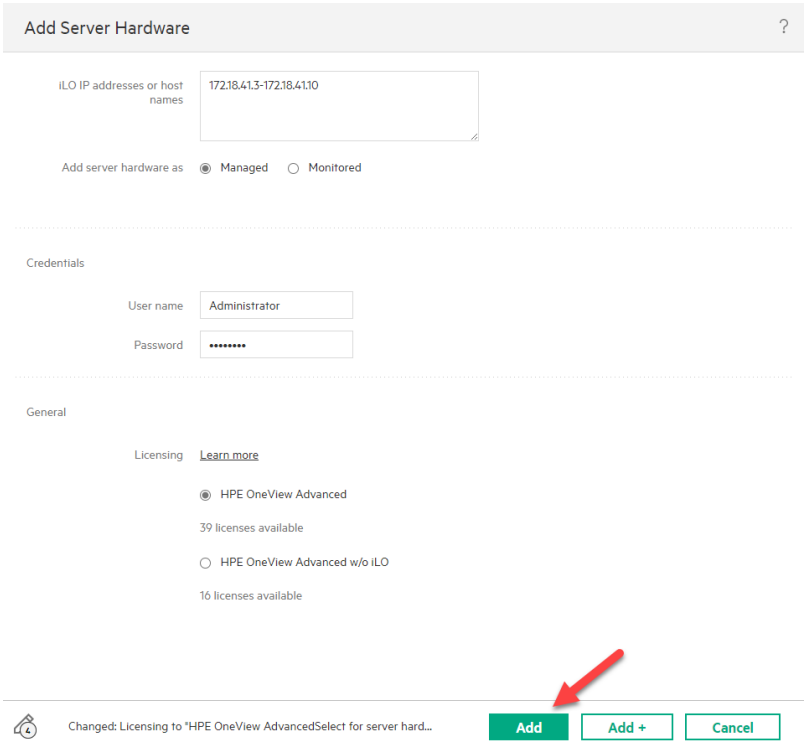
5. Enter the iLO credentials for the servers to be imported



6. Select the appropriate license type using the radial buttons for the servers to be imported.



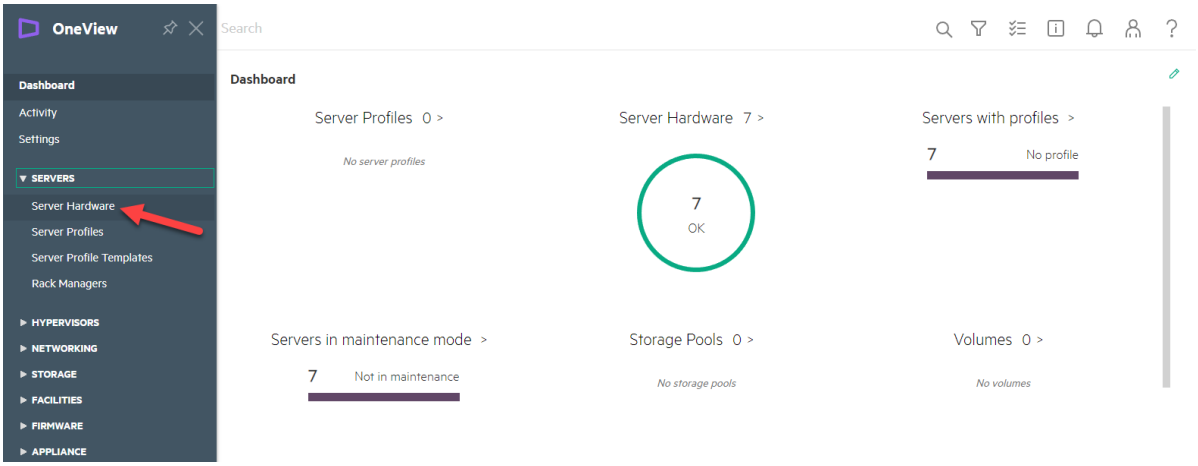
7. Click Add to begin importing the servers



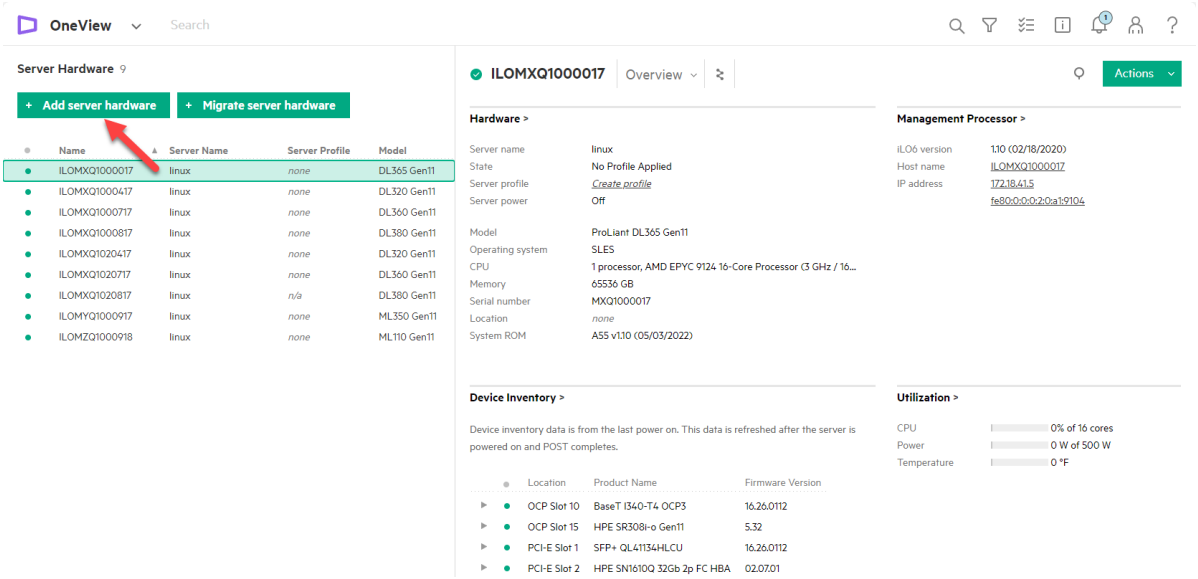
Importing a Range of Servers as Monitored Devices

HPE OneView supports adding a range of iLO addresses to import large numbers of servers simultaneously.

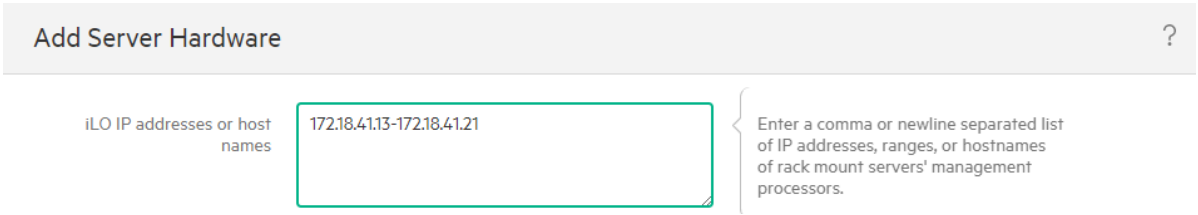
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Hardware*.



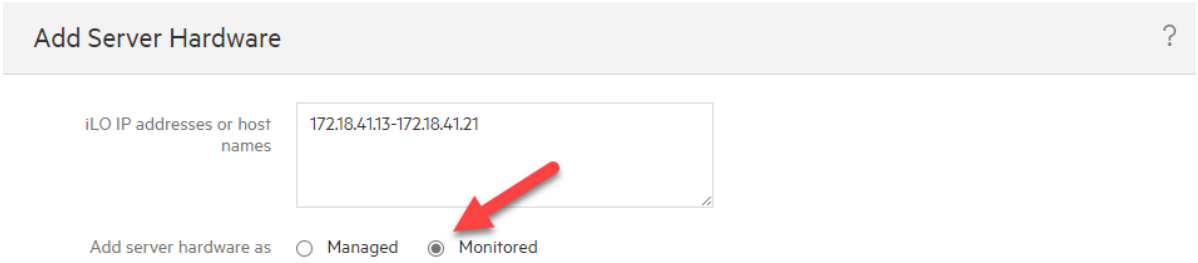
2. In the Server Hardware screen, click the + *Add server hardware* button.



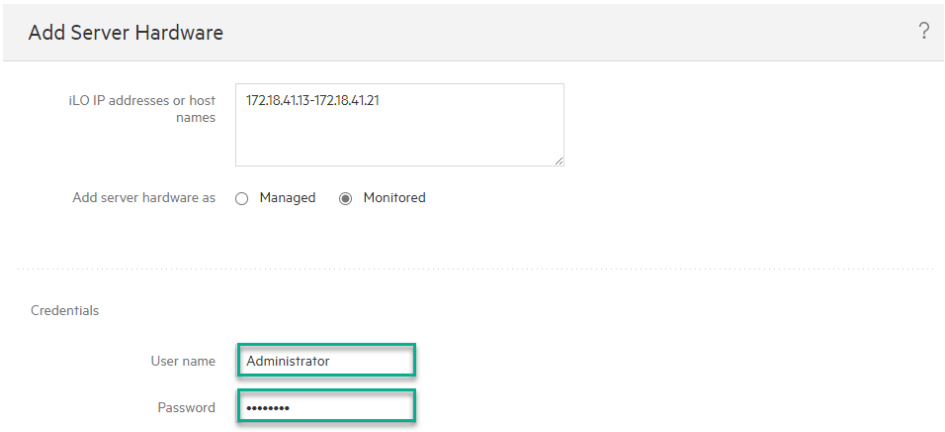
3. Enter the range of iLO IP addresses for the servers to be imported



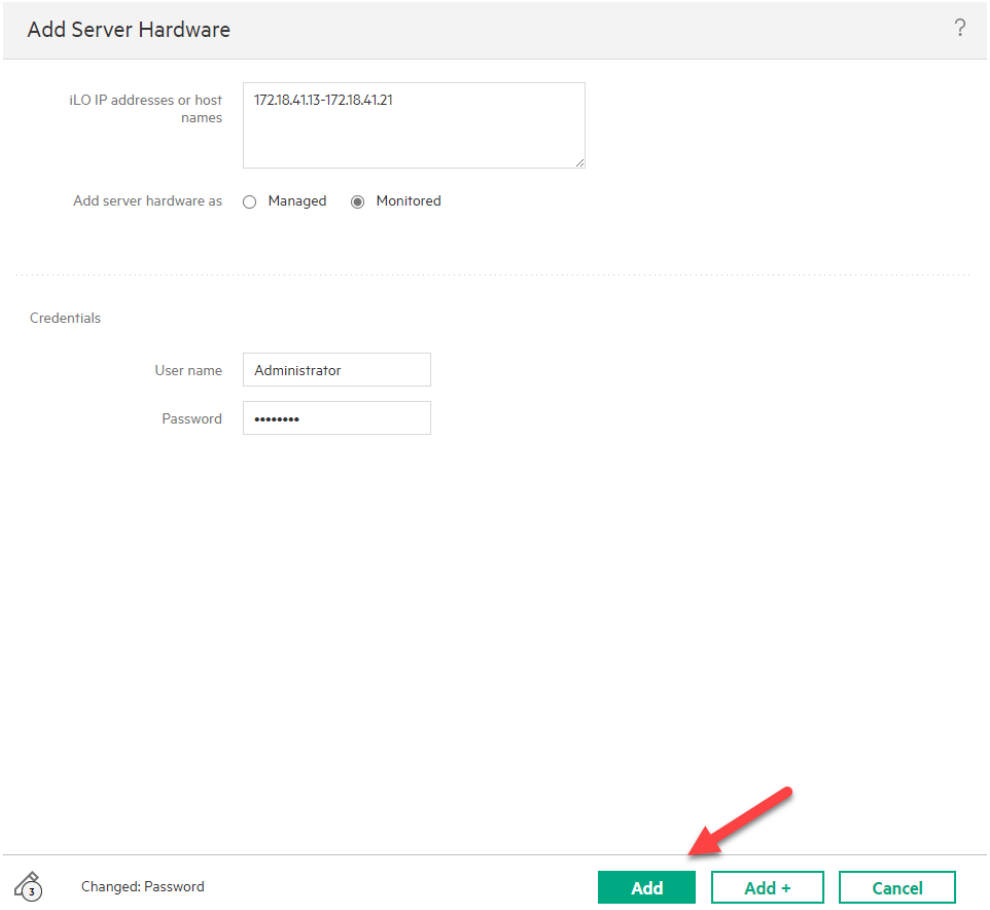
4. Select the *Monitored* radial button to import the above referenced servers with an OneView Advanced license.



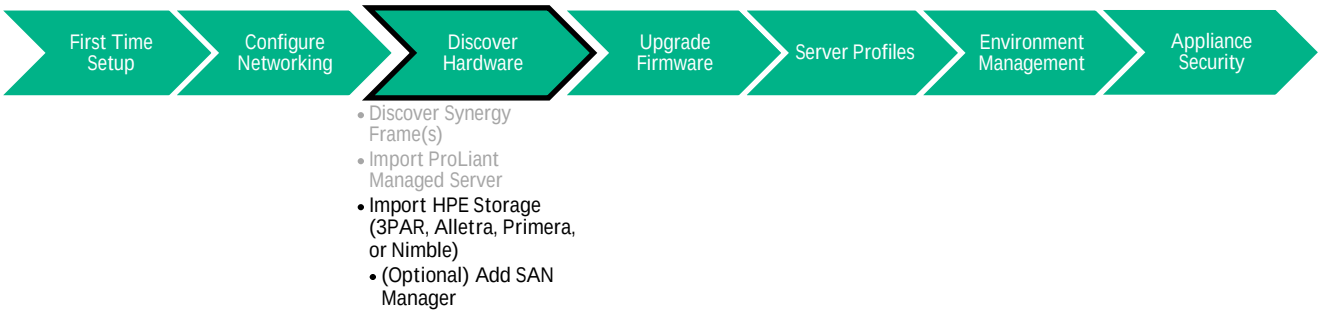
5. Enter the iLO credentials for the servers to be imported



6. Click *Add* to begin importing the servers



Managing HPE Storage (3PAR StoreServ, Alletra, Primera or Nimble)



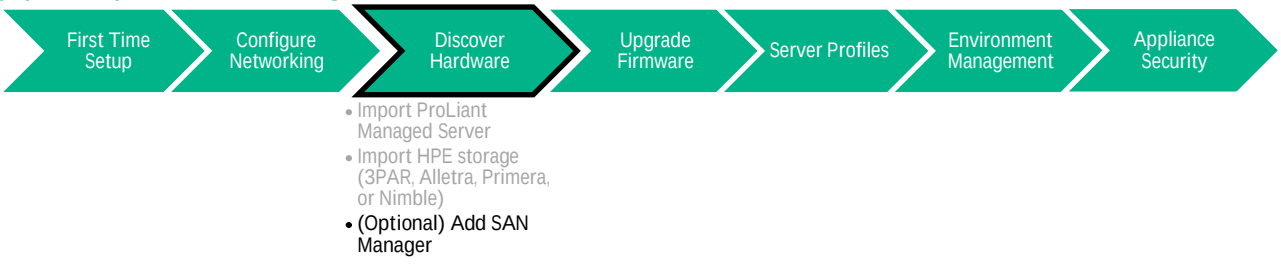
HPE OneView supports server profile driven volume provisioning and access configuration using 3PAR StoreServ, Alletra, Primera or Nimble storage systems with direct attach or Brocade, HPE or Cisco FC fabric attach SANs. Nimble (Volume Scoped Targets – VST) are supported with iSCSI. In this section you will import 1 or more storage systems that are already initialized, have existing storage pools, and any Virtual Domains[4] configured. Additionally, 1 or more SAN Managers are required to discover, monitor, view and perform automated zoning of SANs. SAN Managers for Brocade, HPE or Cisco SAN fabrics must be created explicitly, while SAN Managers to direct attach SANs are created automatically when Logical Interconnects are configured containing direct attach networks. For Brocade SANs, Brocade FOS Switch REST API (requires switch firmware level FOS 8.2.0b or later) must be installed and available to be configured as a *SAN Manager*. For HPE and Cisco SANs, the SAN Manager communicates directly with one of the physical switches in the SAN.

HPE OneView Import HPE 3PAR StoreServ, Alletra, Primera or Nimble Checklist

Table 12. HPE OneView Import HPE 3PAR StoreServ, Alletra, Primera, Nimble Checklist

Task	Completed? (Y|N)
Supported HPE 3PAR StoreServ, Alletra, Primera or Nimble storage system with the minimum firmware requirements.[5]	
HPE 3PAR StoreServ, Alletra, Primera or Nimble Management FQDN / IP Address and administrator account. 3PAR StoreServ and Primera administrator account requires at least Create role in root domain.	
(Optional) Brocade FOS Switch, HPE or Cisco switch Address and credentials.	

(Optional) Add SAN Manager



Fibre Channel or iSCSI Storage Area Networks (SANs) between servers and storage systems can be configured in different ways depending on the desired level of automation to be performed by OneView. Follow the configuration steps in the table below to configure an unmanaged, monitored or managed SAN in your environment. Choosing among these SAN management alternatives does not alter the storage system automated volume provisioning and presentation configuration or server storage initiator / boot configuration performed by OneView.

[4] HPE 3PAR Virtual Domains are a licensed feature.
[5] Review Supported Hardware section for more details.

SAN	Unmanaged		Monitored		Managed	
	Capabilities	Configuration	Capabilities	Configuration	Capabilities	Configuration
FC	• SAN Zoning configured outside of OneView • SAN Zoning unmonitored by OneView	• Create FC network • Set storage system ports' 'Expected SAN / Network' to created FC Network	• SAN Zoning configured outside of OneView • SAN Zoning monitored by OneView • SAN logins monitored	• Create FC network • Add SAN Manager to discover SAN • Associate FC network to discovered SAN • Set SAN's Auto Zoning Policy – "Automate Zoning" to "No". • Set storage system ports' 'Expected SAN / Network' to the SAN	• SAN Zoning configured by OneView • SAN Zoning monitored by OneView • SAN logins monitored	• Create FC network • Add SAN Manager to discover SAN • Associate FC network to discovered SAN • Set SAN's Auto Zoning Policy – "Automate Zoning" to "Yes". • Set storage system ports' 'Expected SAN / Network' to the SAN
FCoE	• SAN Zoning configured outside of OneView • SAN Zoning unmonitored by OneView	• Create FCoE network • Set storage system ports' 'Expected SAN / Network' to created FCoE Network	• SAN Zoning configured outside of OneView • SAN Zoning monitored by OneView • SAN logins monitored	• Create FCoE network • Add SAN Manager to discover SAN • Associate FCoE network to discovered SAN • Set SAN's Auto Zoning Policy – "Automate Zoning" to "No". • Set storage system ports' 'Expected SAN / Network' to the SAN	• SAN Zoning configured by OneView • SAN Zoning monitored by OneView • SAN logins monitored	• Create FCoE network • Add SAN Manager to discover SAN • Associate FCoE network to discovered SAN • Set SAN's Auto Zoning Policy – "Automate Zoning" to "Yes". • Set storage system ports' 'Expected SAN / Network' to the SAN
iSCSI	• Connectivity established from server and interconnect to Storage System	• Create Ethernet network • Set storage system ports' 'Network' to the created Ethernet Network	N/A			

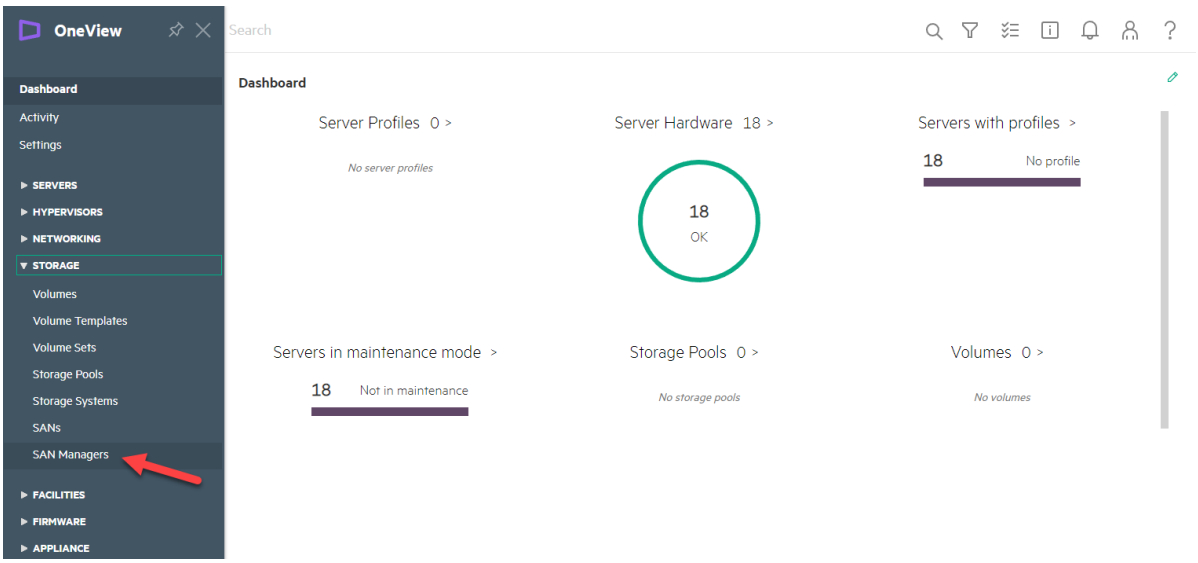
After configuring SANs as above and adding network connections to FC / FCoE / iSCSI SAN networks to your Server Profiles, OneView will manage volumes and configure data paths from servers to the managed volumes on the Storage Systems.

When creating a SAN Manager to a Brocade, HPN 5900 family or Cisco Nexus / MDS switch, only switches configured in FCF / Native mode can be added. Any switch in NPV / Access Gateway mode cannot be added as a SAN Manager. For more information regarding how to configure or setup a HPN 5900CP for FCF, please either review the sample switch configuration in Appendix A, or review *Scenario 7* in the *FCoE Cookbook for HPE Virtual Connect* whitepaper[6].

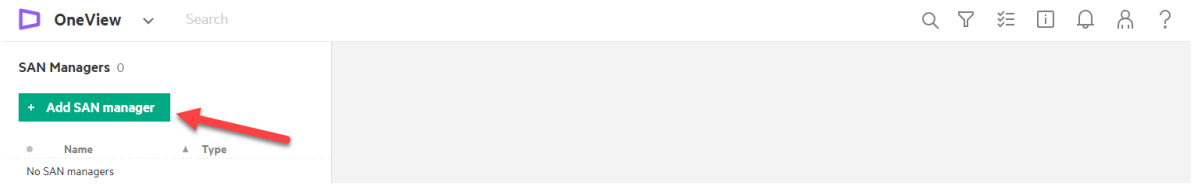
Brocade SAN fabrics can be auto-zoned by OneView using the switch's FOS REST API. Add the type of SAN manager that matches how you want OneView to manage zoning on the SAN. With Brocade ending Brocade Network Advisor (BNA) support (HPE OneView 7.0 or later no longer supports BNA), environments must use the Brocade FOS switch SAN manager type (see Appendix D: Configuring a Brocade SAN switch for HPE OneView REST API access for more information on configuring Brocade SAN switches for use with this SAN Manager type).

[6] https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c03808925

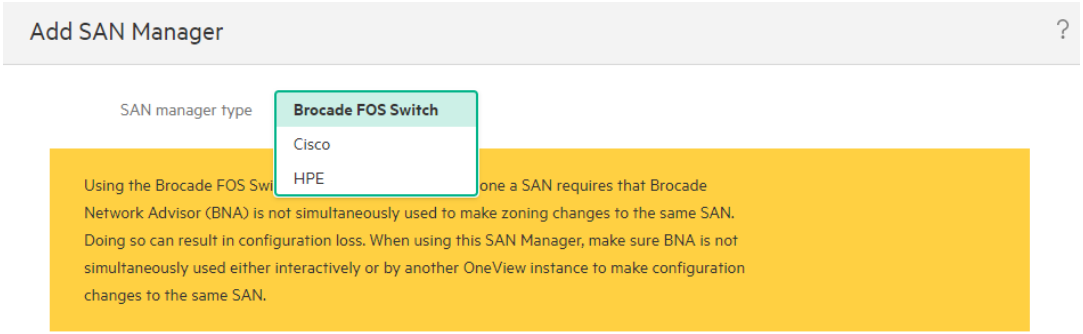
1. From the Top-Level Menu, expand the *STORAGE* option and then select *SAN Managers*.



2. Select *Add SAN manager* button.

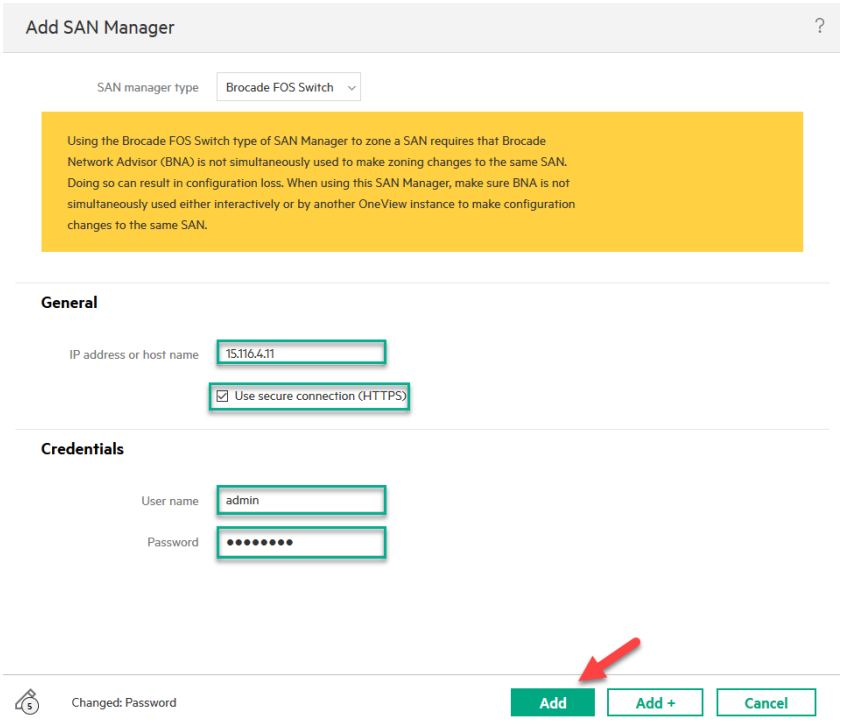


3. In the Add SAN Manager screen, select the SAN type of SAN manager to add from the drop-down list.



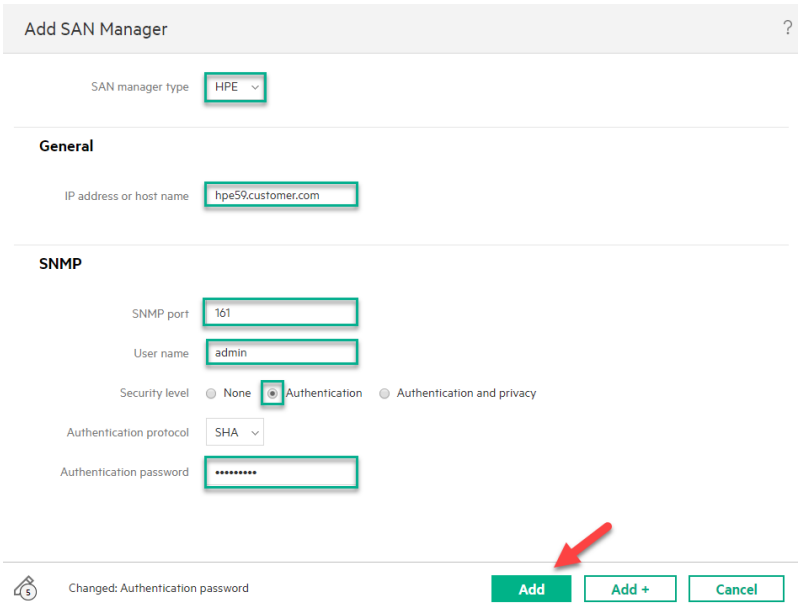
Add Brocade FOS switch SAN Manager

1. In the Add SAN Manager screen, select *Brocade FOS Switch* as the SAN Manager Type drop down list, provide the FQDN / IP Address of an Native mode switch in the SAN, and REST API login credentials to authenticate. Then click the *Add* button, or *Add +* button to add another SAN Manager



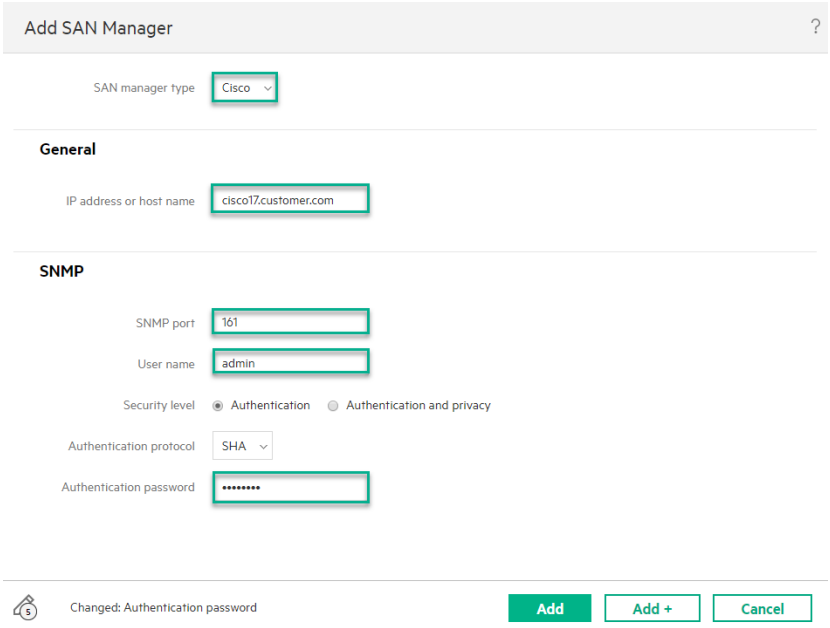
Add HPN 5900 family SAN Manager

1. In the Add SAN Manager screen, select *HPE* as the SAN Manager Type drop down list, provide the FQDN / IP Address of an FCF mode switch in the SAN, TCP Port (SNMP Port), SSH credentials and SNMPv3 password to authenticate. Then click the *Add* button, or *Add* + button to add another SAN Manager



Add Cisco Nexus / MDS SAN Manager

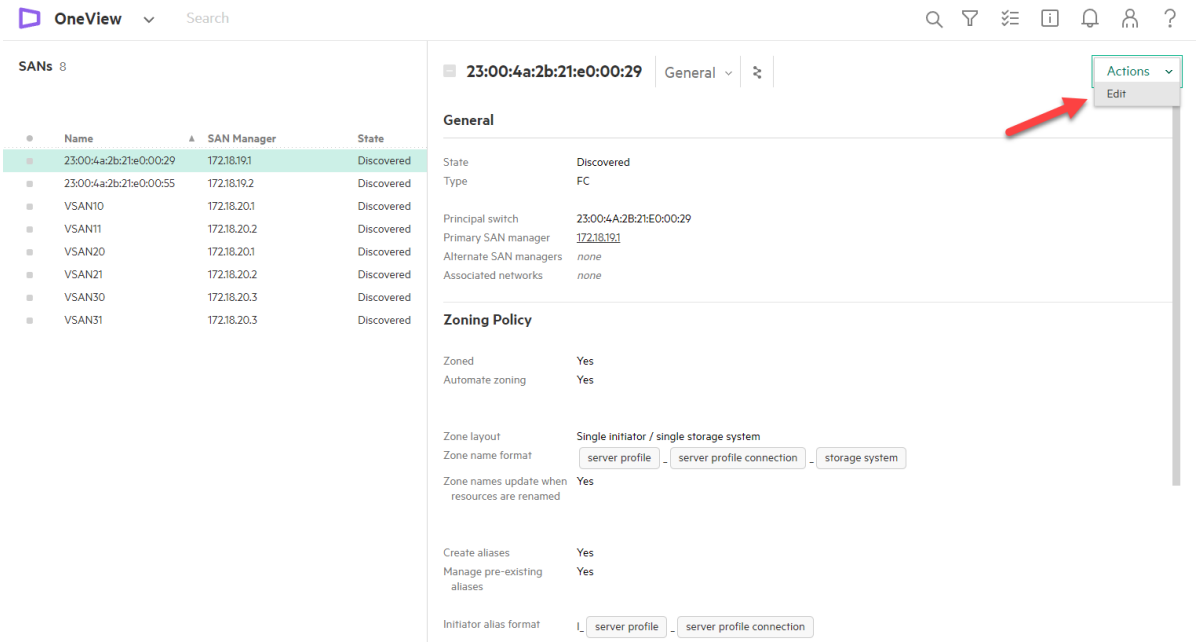
1. In the Add SAN Manager screen, select *Cisco* as the SAN Manager Type in the drop-down list, provide the FQDN/IP Address of an FCF mode switch in the SAN, TCP Port (SNMP Port), SSH credentials and SNMPv3 to authenticate. Then click the *Add* button, or *Add* + button to add another SAN Manager



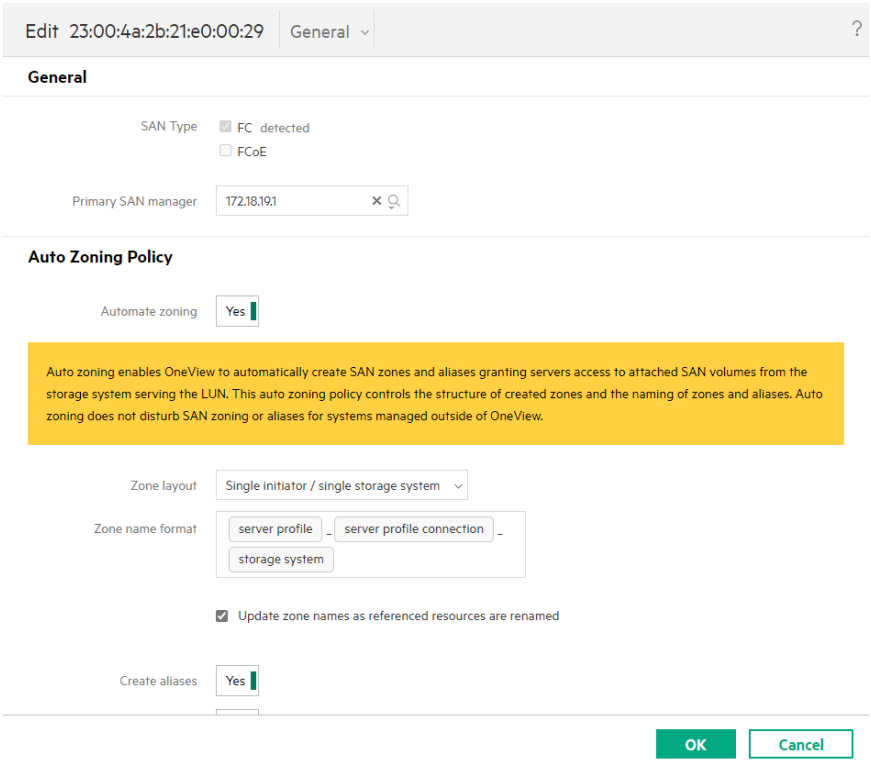
Modify **a SAN's** Primary SAN manager, SAN Protocols and Zoning Policy

After SANs are discovered by one or more SAN Manager, the storage administrator can change the SAN's primary SAN manager, the storage protocols supported on the SAN (only required when they could not be detected) and how HPE OneView will perform auto-zoning on the SAN.

1. From the *SANs* menu in *Storage* select the *SAN* and from the Actions menu, select *Edit*



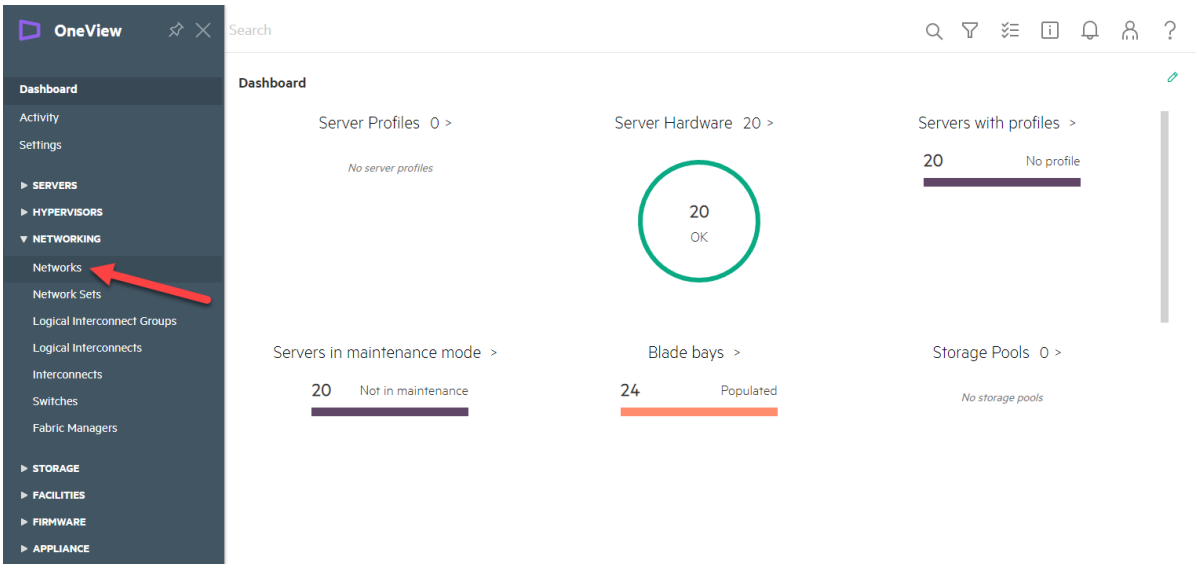
2. Modify the Primary SAN manager if you want to change which SAN manager OneView uses to configure zoning on the SAN, protocols in use on the SAN (that could not be detected at the switch the SAN Manager is communicating with). Modify the Auto Zoning Policy that will be used on each SAN. You can edit each field and replace tokens (ex. {server_profile}) with other pre-defined tokens or add other static text that will be used to name the respective zones and aliases configured onto the SAN.



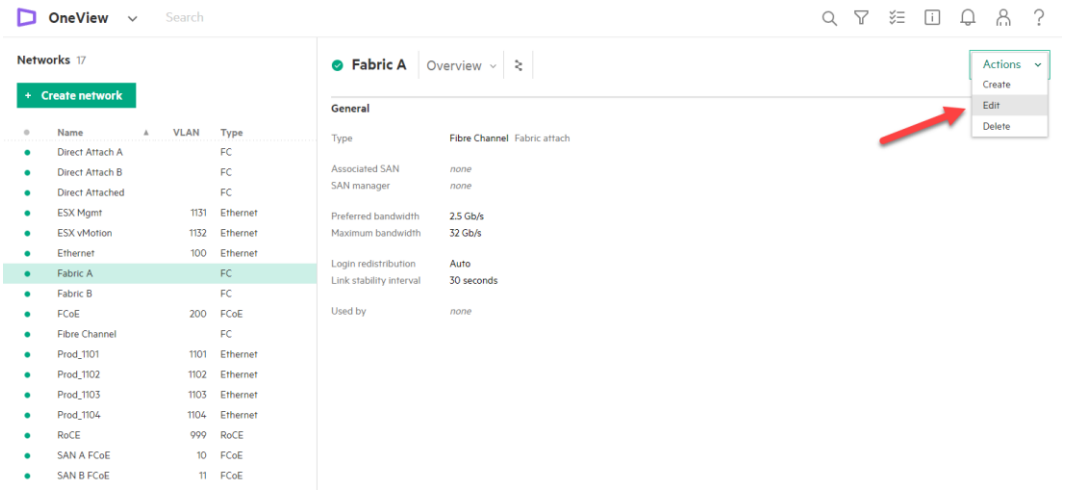
Update Fibre Channel Networks

After adding a supported SAN Manager, the Fibre Channel Networks will need to be updated, so they are associated with the correct discovered SAN Fabrics.

1. From the Top-Level Menu, expand *NETWORKING* option and then select *Networks*.

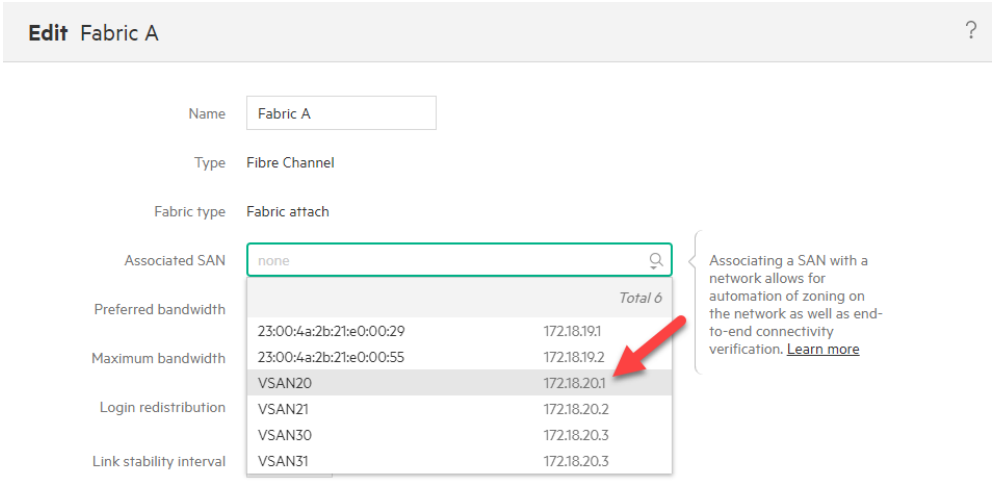


2. Select the FC Network to be updated, then select *Edit* from the Actions Menu.

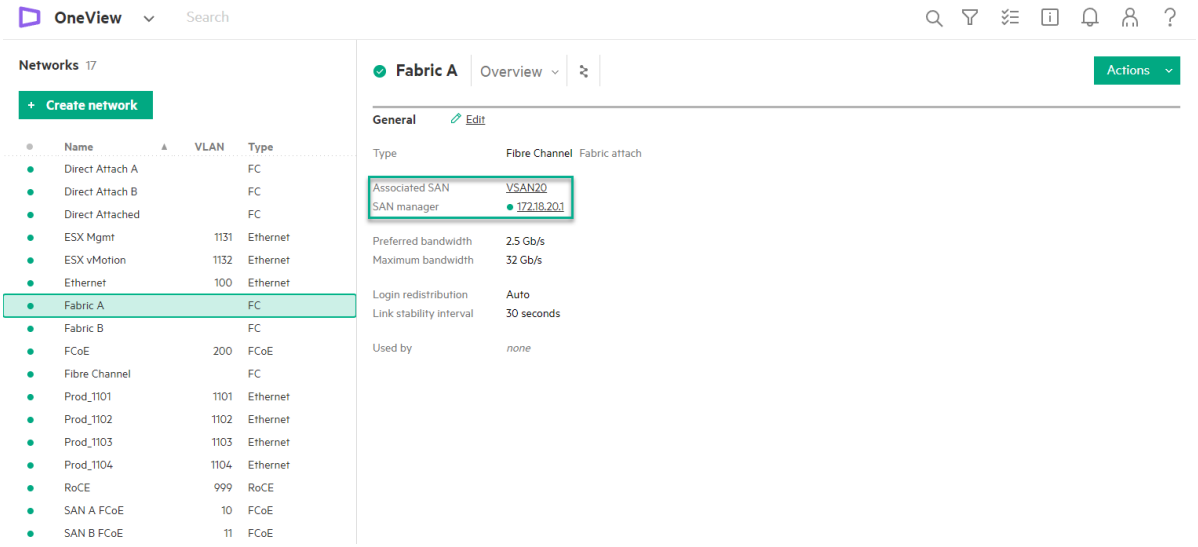


3. In the *Associated SAN* drop down list, select the SAN discovered by your SAN Manager earlier, then select *OK* to save.

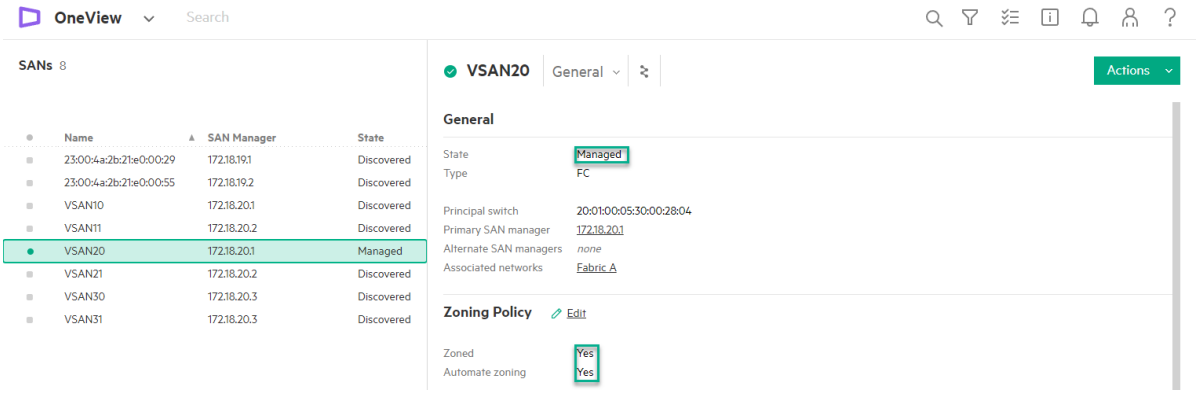
Note: *A network can only be associated to a single SAN, however a SAN can be associated to multiple networks.*



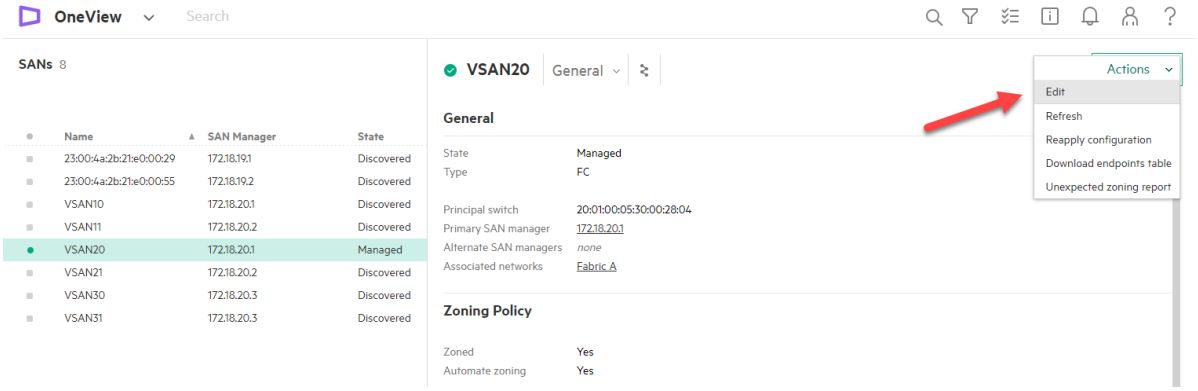
4. After updating the FC Network, examine the *Associated SAN* and *SAN Manager* Properties in the *General* view.



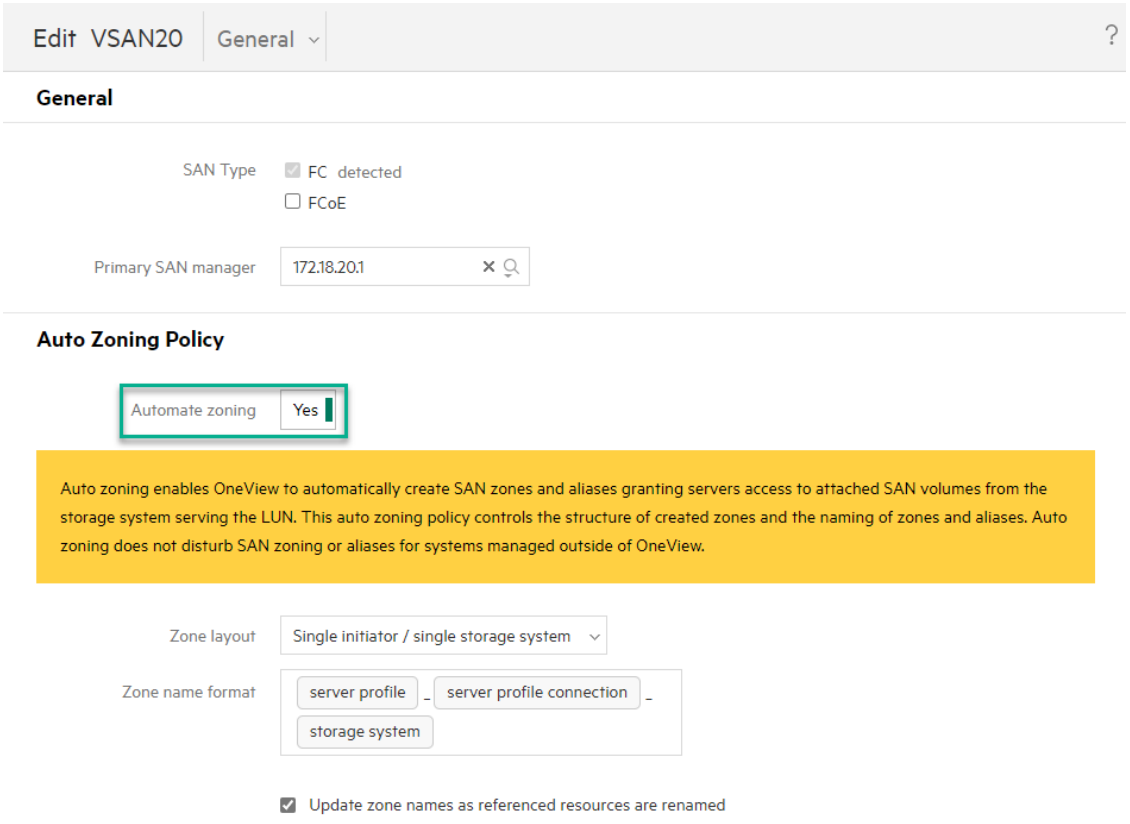
5. Clicking the Associated SAN, view that the SAN is now *Managed*, that the SAN is a *zoned* SAN, and that automated *zoning* will be performed.



6. If desired, Automated Zoning can be disabled on a per SAN basis. If automated Zoning is not desired, select and *Edit* the SAN

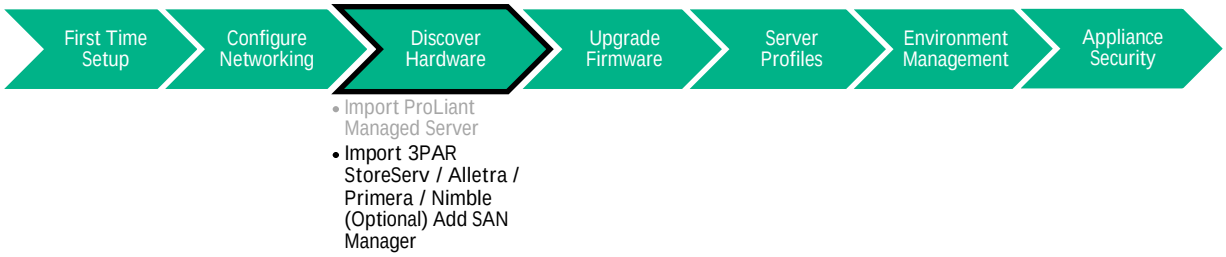


7. Then click the option to disable *Automated zoning*

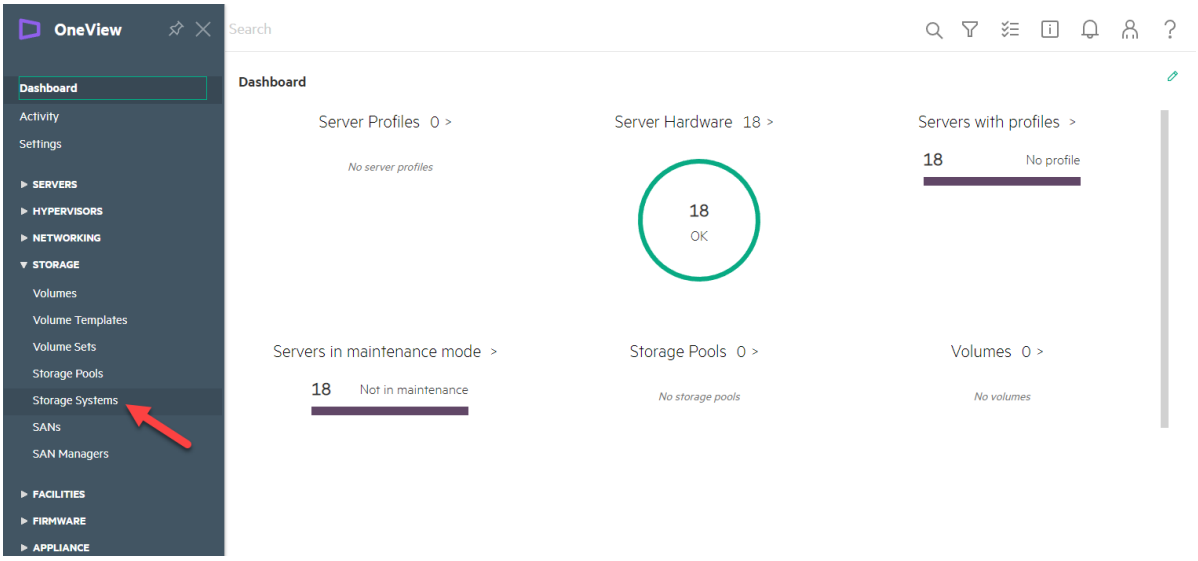


8. Repeat the same steps to update any additional FC Networks.

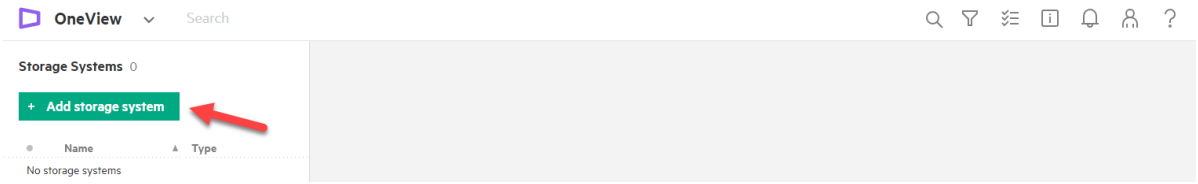
Importing Storage Systems - HPE 3PAR StoreServ / Alletra / Nimble systems



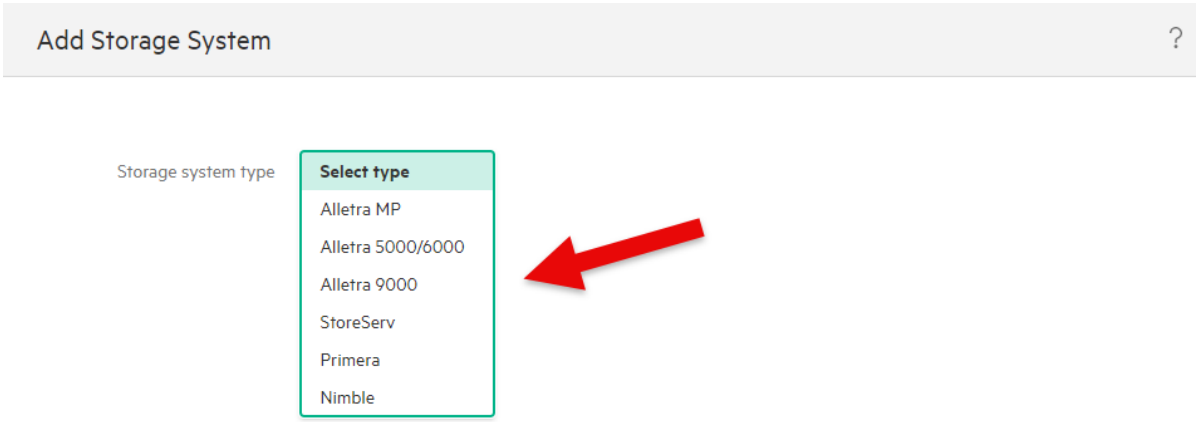
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Storage Systems*.



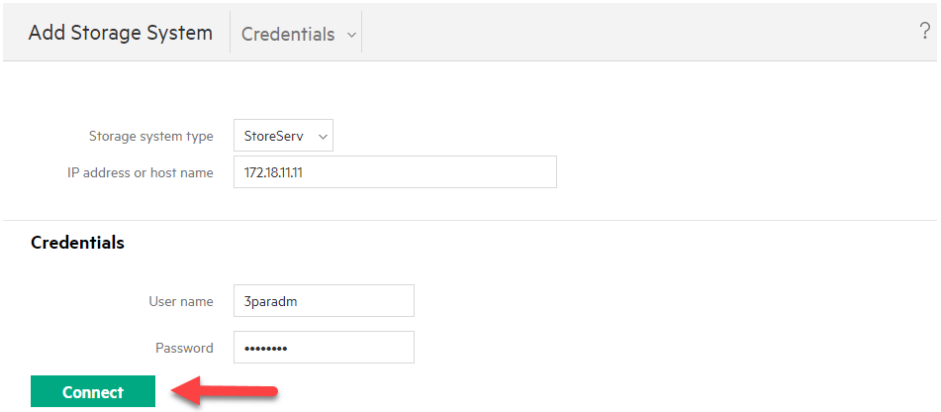
2. In the Storage Systems screen, click the + *Add storage system* button.



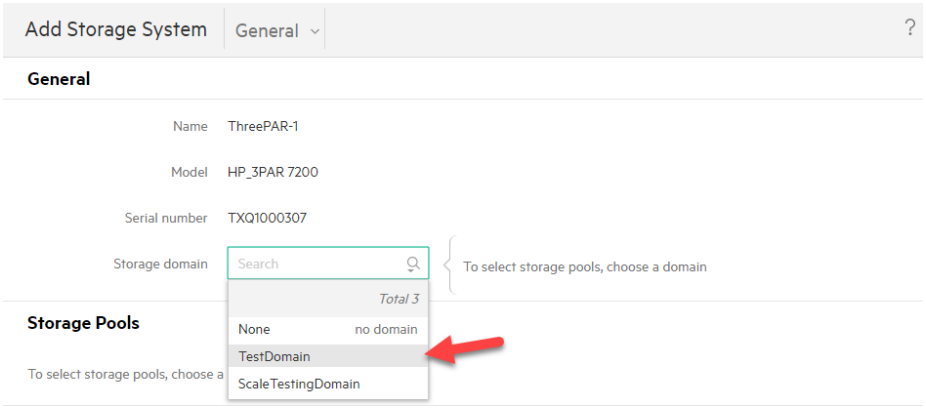
3. Select the type of storage system to be imported using the drop down menu, select Alletra, StoreServ, Primera or Nimble.



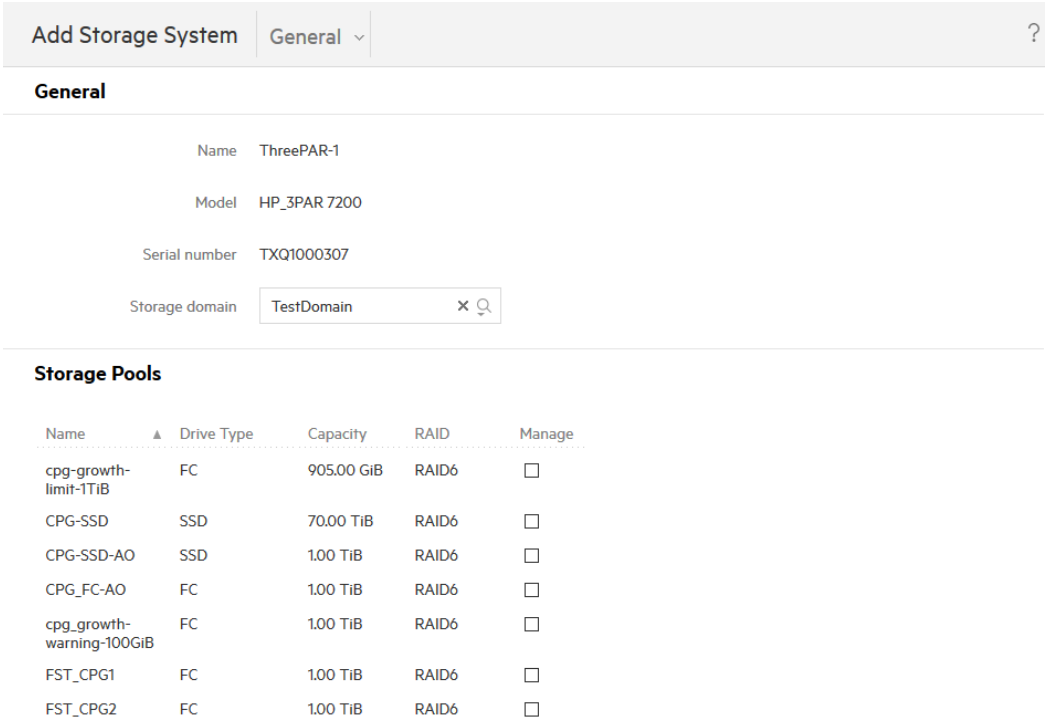
4. In the Add Storage System screen, add the *FQDN or IP Address* of the storage system to be added, along with Administrator credentials. Click the *Connect* button to connect to the storage system.



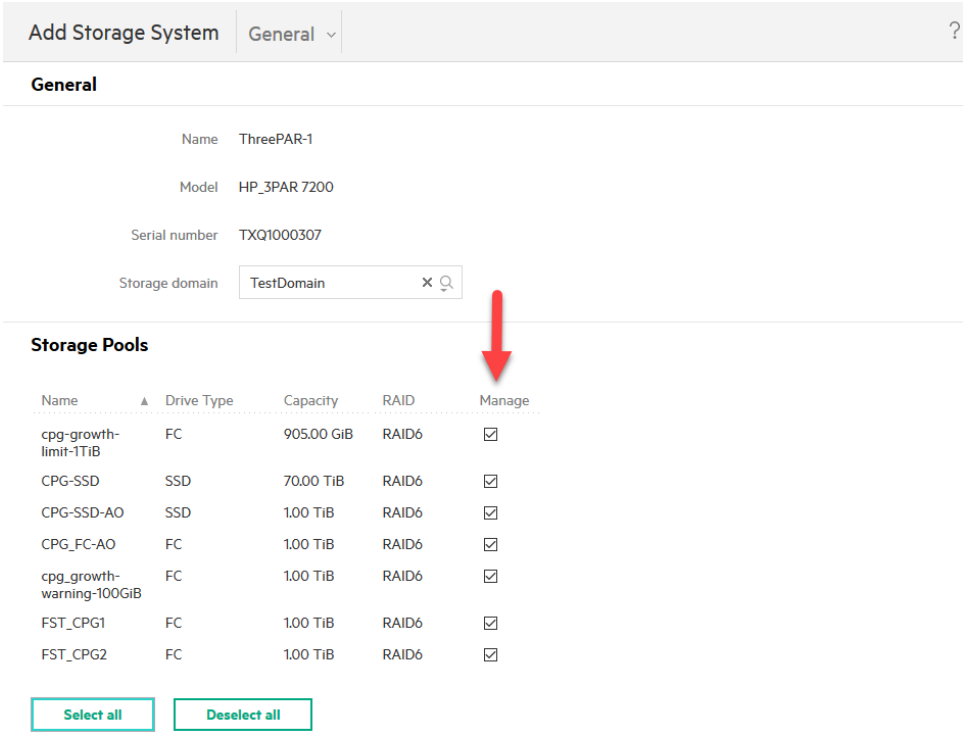
5. Once connected to the storage system, 3PAR StoreServ and Primera systems also require selecting the storage domain from the drop-down box if needed



6. Once the storage domain is selected the storage pools will be discovered and made available to be managed. This equates to CPG's on a 3PAR StoreServ and Primera systems, or storage pools on Nimble storage systems.



7. Select the *Manage* checkbox next to the storage pool(s) to be managed or use the *Select all* / *Deselect all* buttons to select or deselect all of the storage pools. HPE OneView will only provision volumes from managed storage pools.



Associating Storage System Ports to Networks / SANs

Storage System Ports must be associated with OneView Networks or SANs in order to establish connectivity to enclosures and servers in the environment. When adding SAN volume attachments to server profiles, only storage system ports on networks to which the profile has connections can be configured for storage paths by HPE OneView. HPE OneView establishes the storage system port's connectivity according to its Network (iSCSI) or *Expected SAN / Network (FC)* field setting.

On the Storage System Ports section of the *Add storage system* screen, set each port's Network or *Expected SAN / Network* value to the SAN or Network which is connected to the storage system port. Ports represent Nimble's iSCSI "Discovery IP" whereas, ports for FC storage systems are FC target ports identified by WWN's.

FC Ports whose connectivity is discovered on a managed SAN will already have its *Expected SAN / Network* value set. Ports whose connectivity cannot be discovered will have their *Expected SAN / Network* value set to *Auto*, which will cause the port's value to be set to the first managed SAN on which the port is discovered. When a port is connected to an unmanaged SAN network or iSCSI network, it will need its Network or *Expected SAN / Network* value to be set manually to an unassociated Network.

Any storage system port which you do not want HPE OneView to use to configure storage paths, such as an array's replication ports, should be set to *None*.

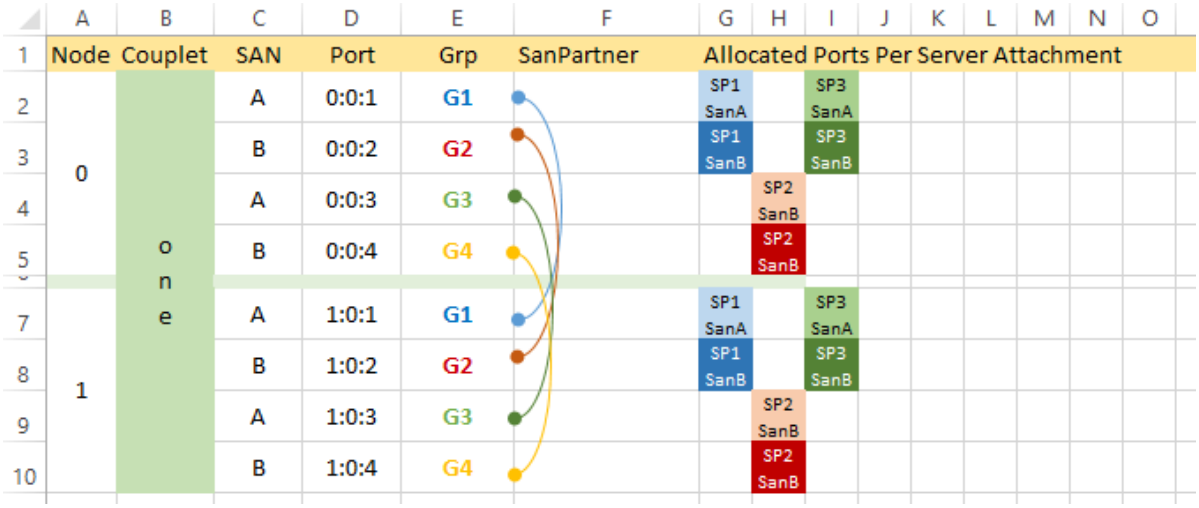
Repeat the process for the various ports on the storage system.

Creating FC Port Groups on Storage Systems

When HPE OneView attaches a volume to a server over Fibre Channel SANs, for each storage path, by default (using "auto" target ports), HPE OneView configures all storage system ports connected to the SAN connecting the storage system to the server as storage targets. If the storage administrator wishes to partition the storage system ports into smaller groups to be configured to each server, then assign a group name to the ports to be configured together. When Port Groups are defined, HPE OneView will choose the least configured port group to attach volumes to a server, achieving a load balancing across the storage system's ports. In this example, only 1 storage target will be configured per storage path per server even though there are two possible targets each server data path could be configure to access.

Best practice for creating FC port groups:

- StoreServ and Primera FC port groups generally will contain one or more persistent port pairs – connected to the same SAN.

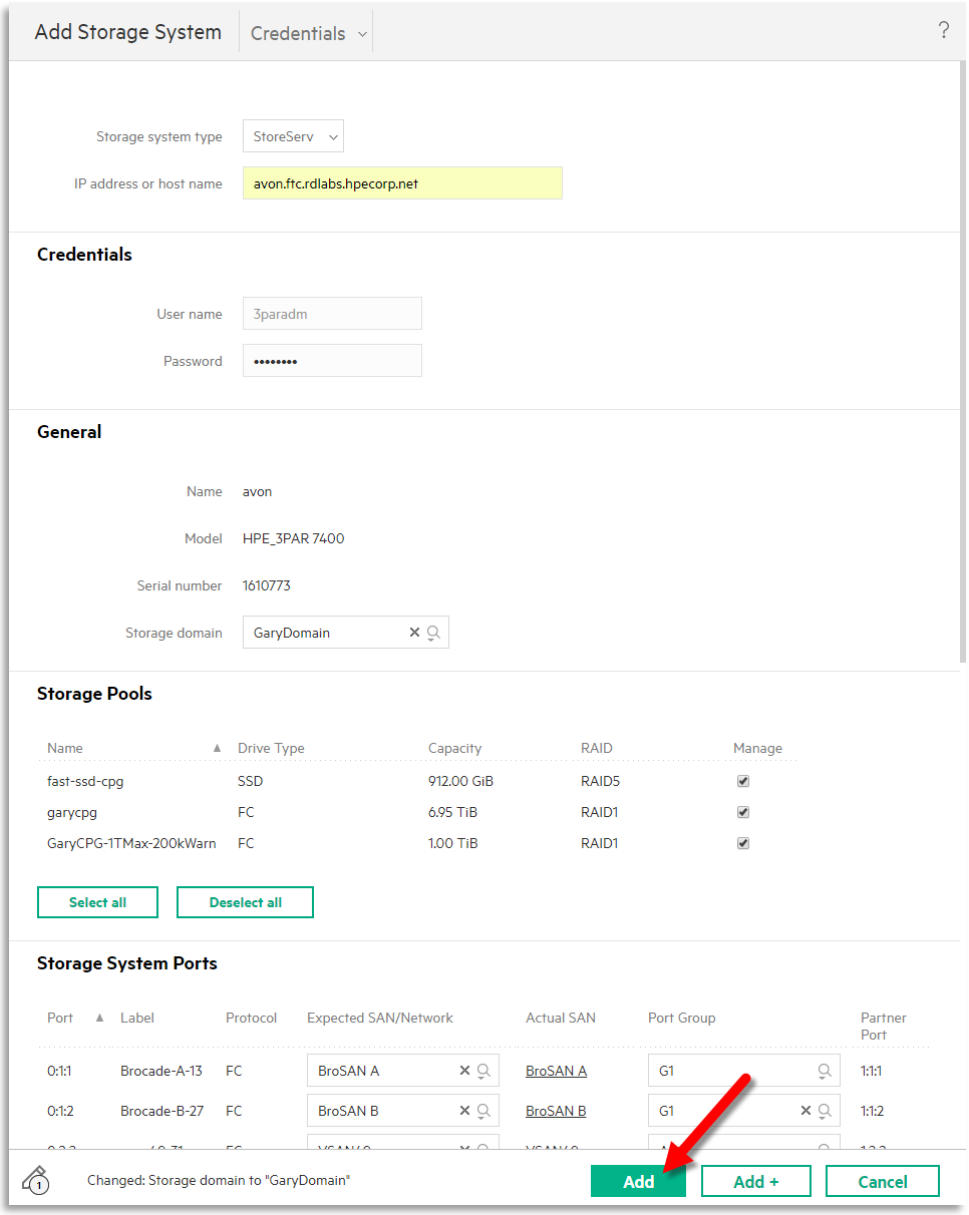


- Nimble FC port groups generally will contain a pair of ports, one on each of the controllers of an array – connected to the same SAN.

1. Set the port Group names for each port as desired.



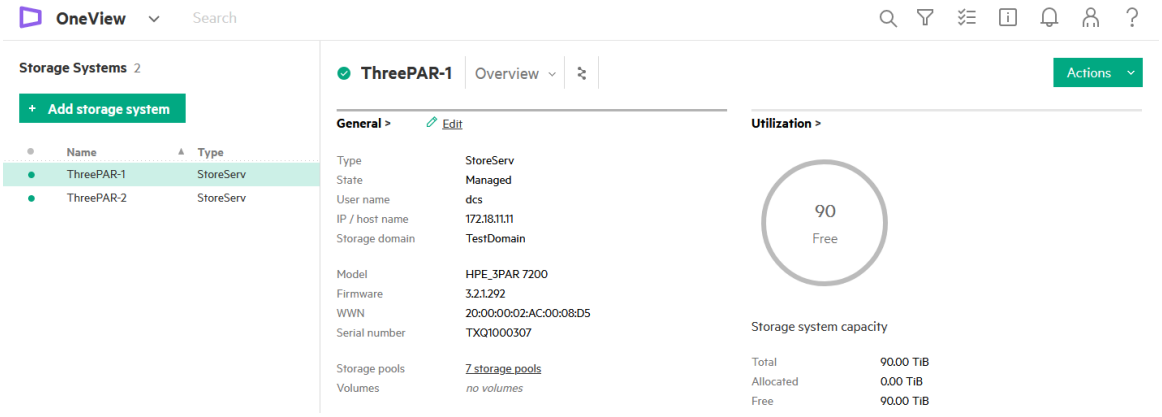
2. From the Add Storage System page, click the *Add* button to add the storage system, or select the *Add* + button to add other storage systems.



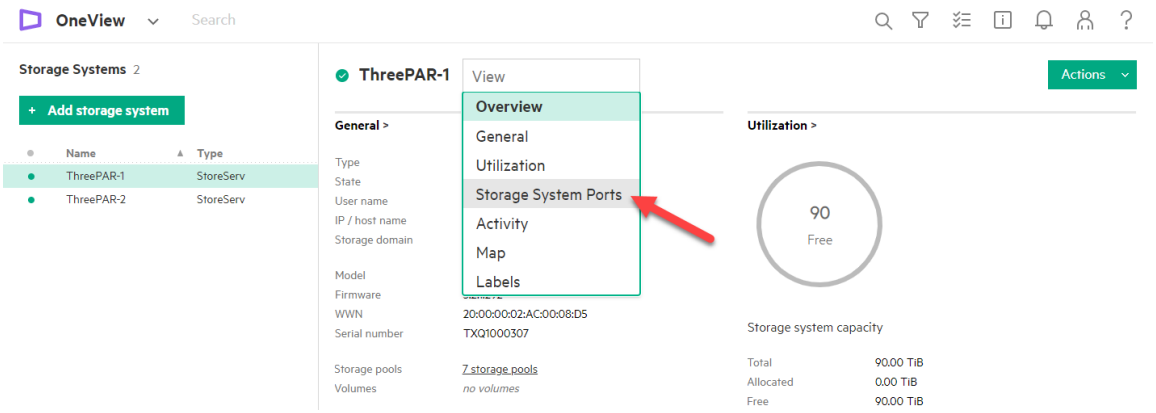
Examine Imported Storage System

After adding a Storage System, you can examine the details about the new resource.

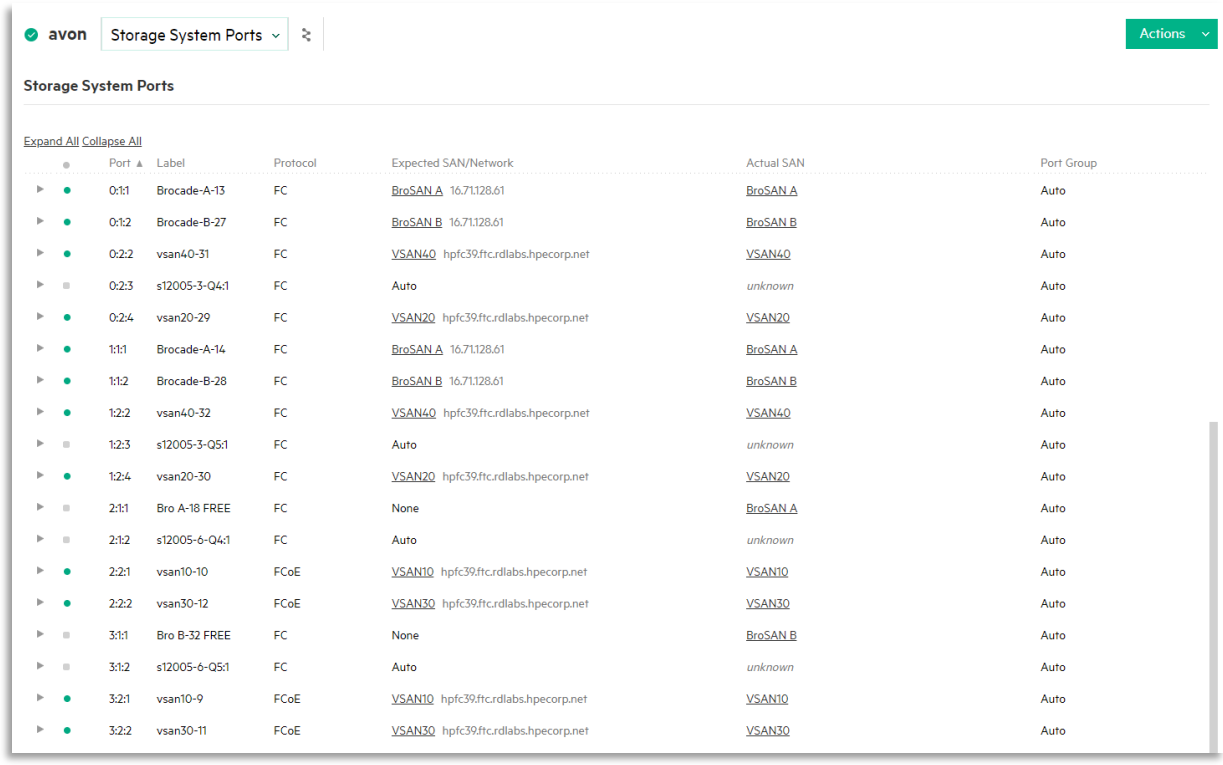
1. From the Storage Systems view, select the specific storage system in the resource list view.



2. Select *Storage System Ports* from the sub-menu.



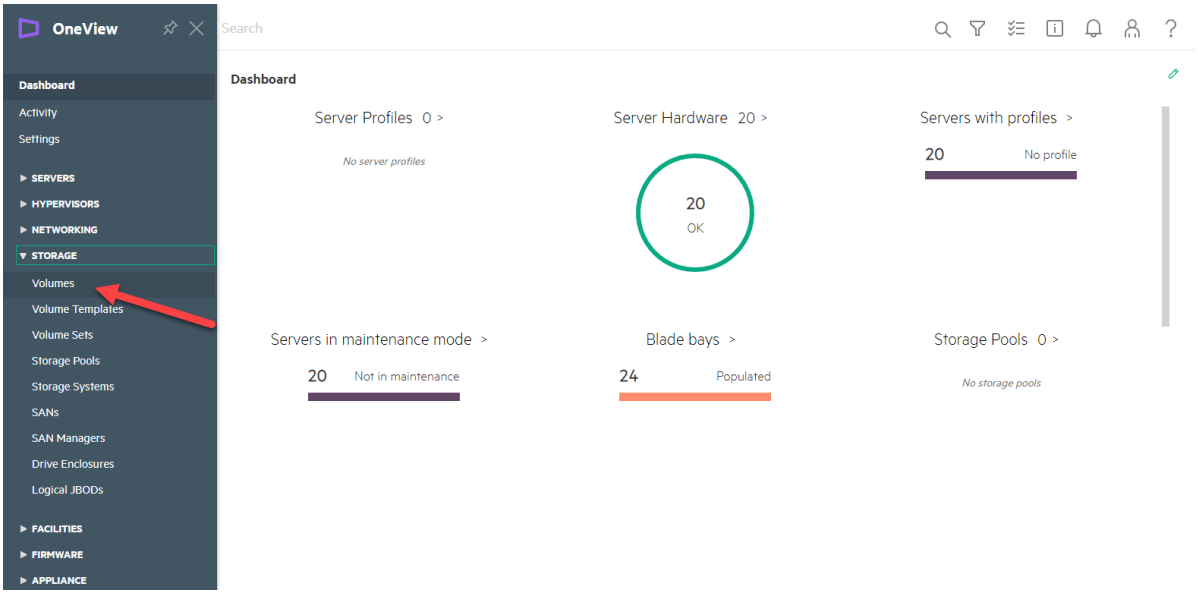
3. Here, you can view the matched storage system host ports, and the associated FC Networks and / or SAN Manager Fabrics.



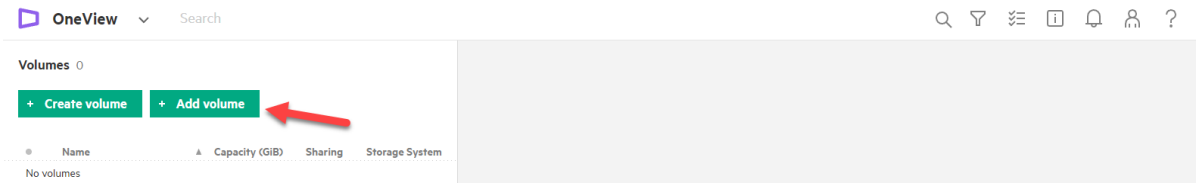
Import Existing Storage Volumes

HPE OneView can create new volumes but also allows existing volumes on the Storage System to be imported for attaching to servers in Server Profiles. Adding existing volumes can be performed as described below.

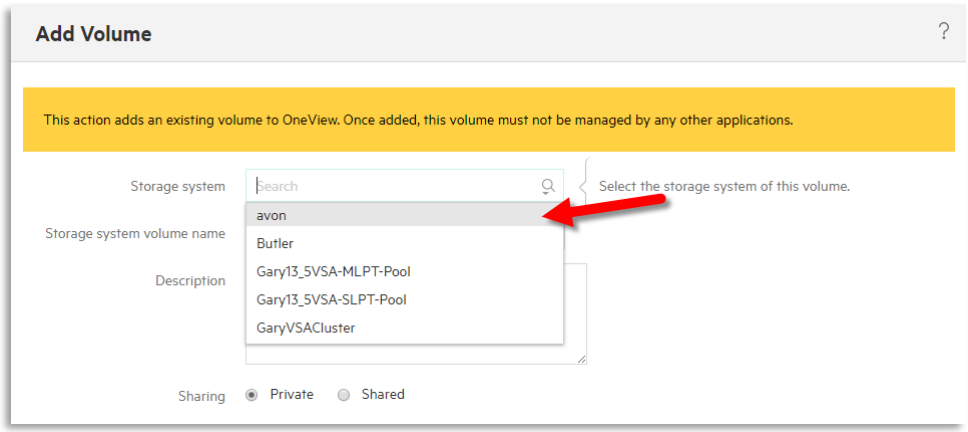
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Volumes*.



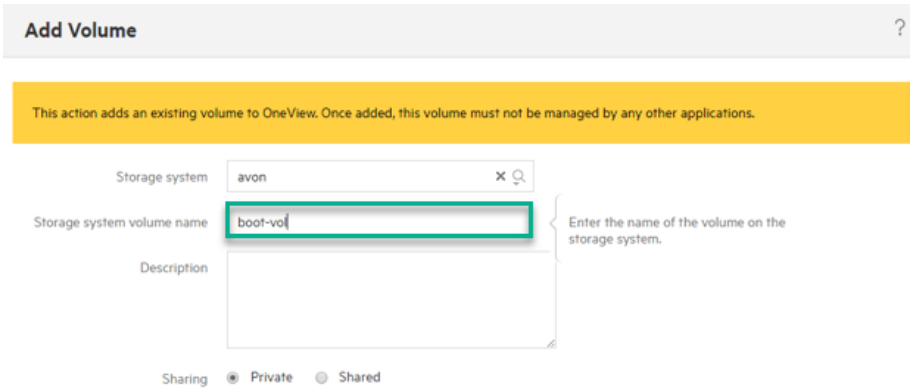
2. Select *Add volume* from the Volumes view.



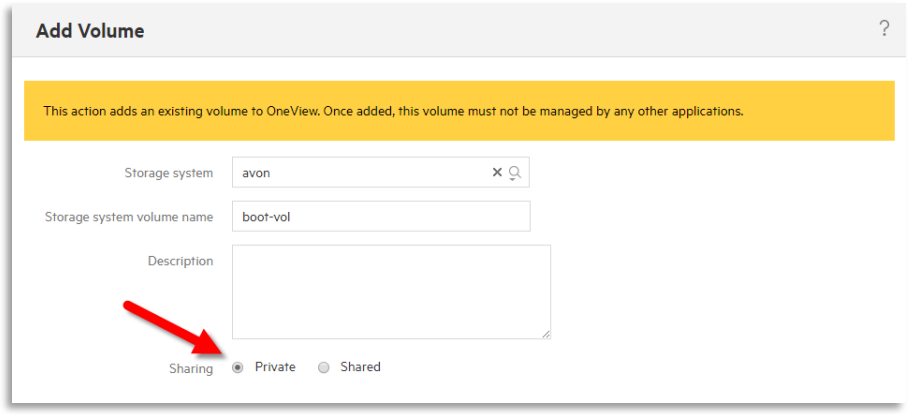
3. Select the *Storage system* form the drop-down list,



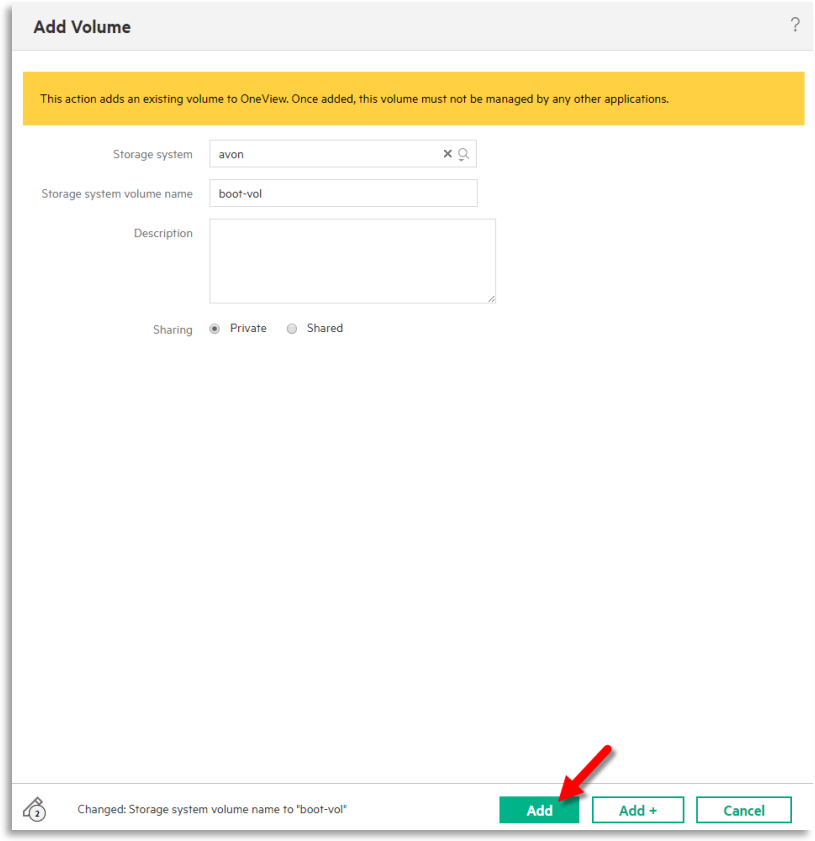
4. Enter the name of the volume to add. Optionally give it a description.



5. Select if the volume will be a *Private or Shared* volume. Private volumes are restricted to only being attachable to at most, one server at a time.



6. Select the *Add* or *Add +* button to add the volume. After being added, the volume can be attached to a server via its server profile.

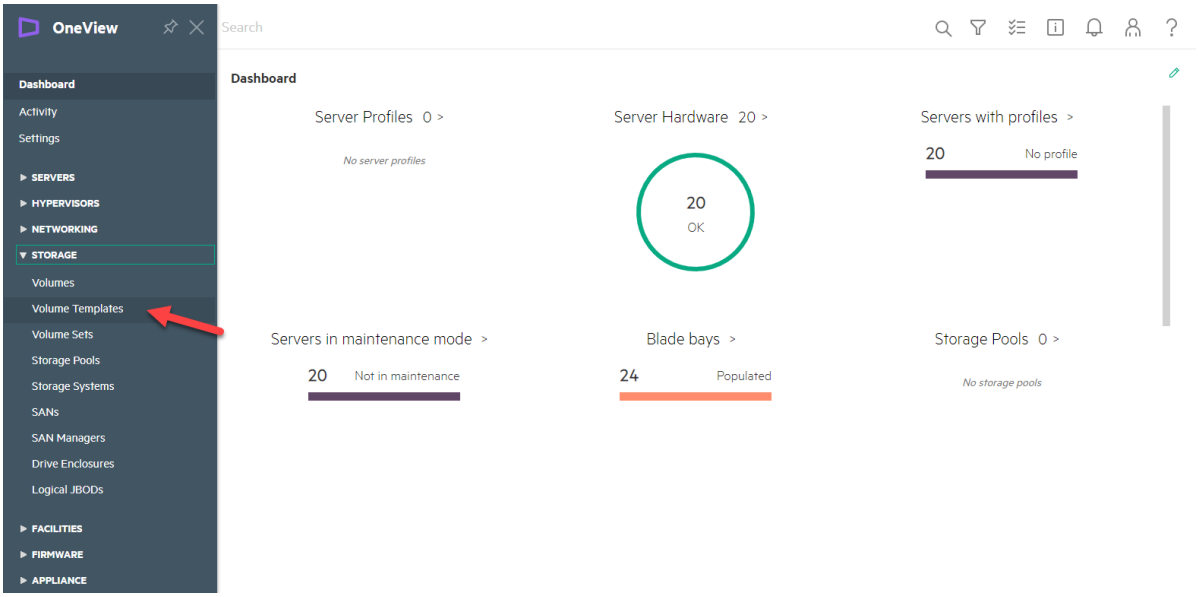


Create Storage Volume Templates to create Volumes

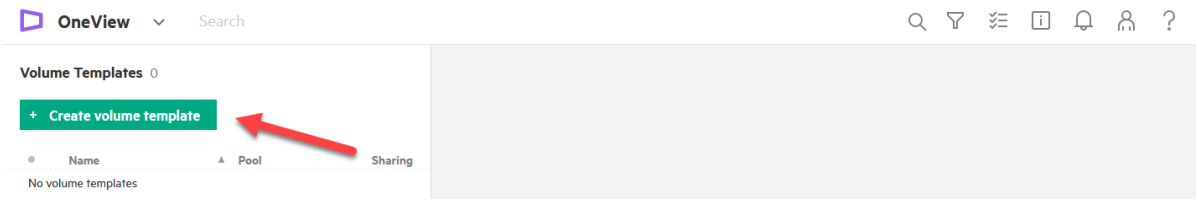
Storage Volume Templates allow the Storage Administrator to specify a set of volume properties when creating multiple volumes or to enforce certain volume property settings when other admins are creating volumes. Storage Volume Templates are not required in order to provision Storage Volumes (unless the HPE OneView global storage setting to require a volume template is enabled – described later).

Volume Templates contain settings specific to the type of storage pool being provisioned from. Create a StoreServ volume template by selecting a StoreServ storage pool for the volume template to create volumes from. Same for Alletra, Primera and Nimble. Create a storage volume template as follows.

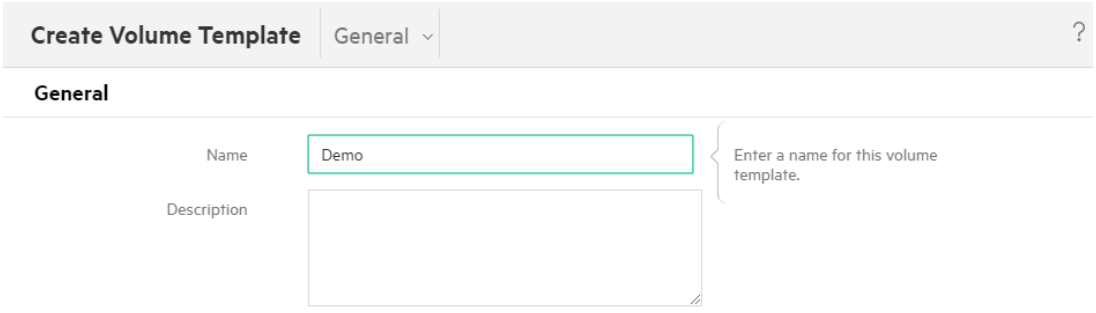
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Volume Templates*.



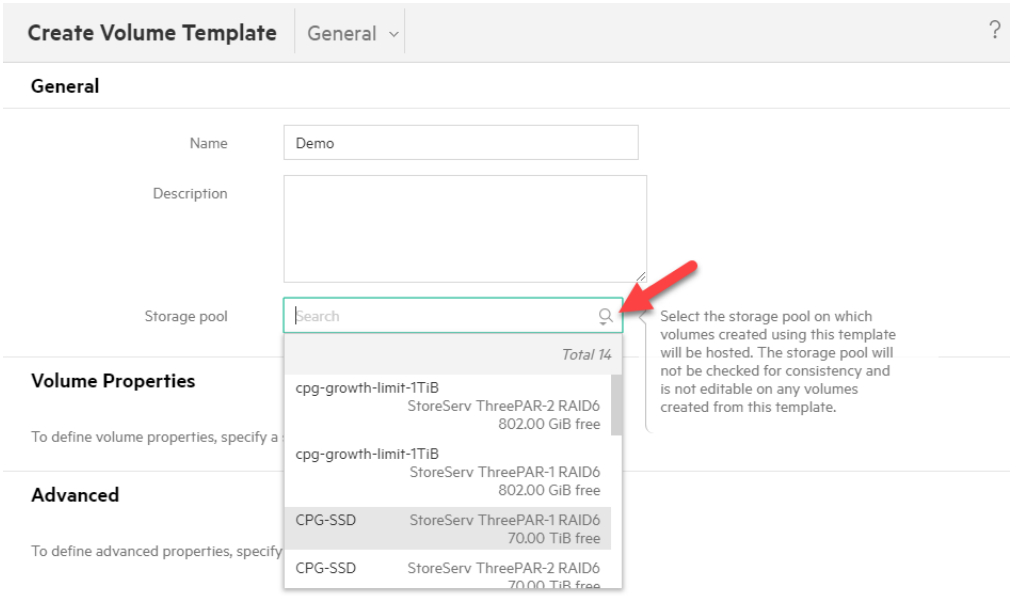
2. Click *Create volume template* button



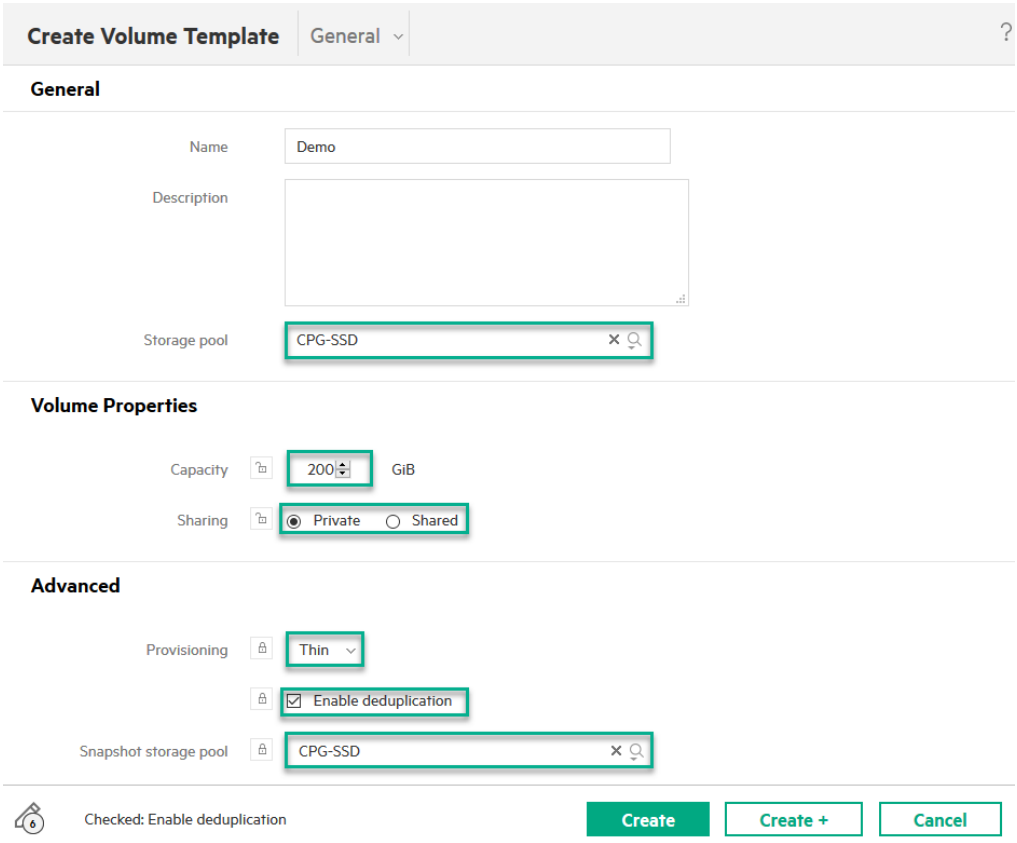
3. In the Create Volume Template screen, enter a *Name* for the Volume template and an optional description.



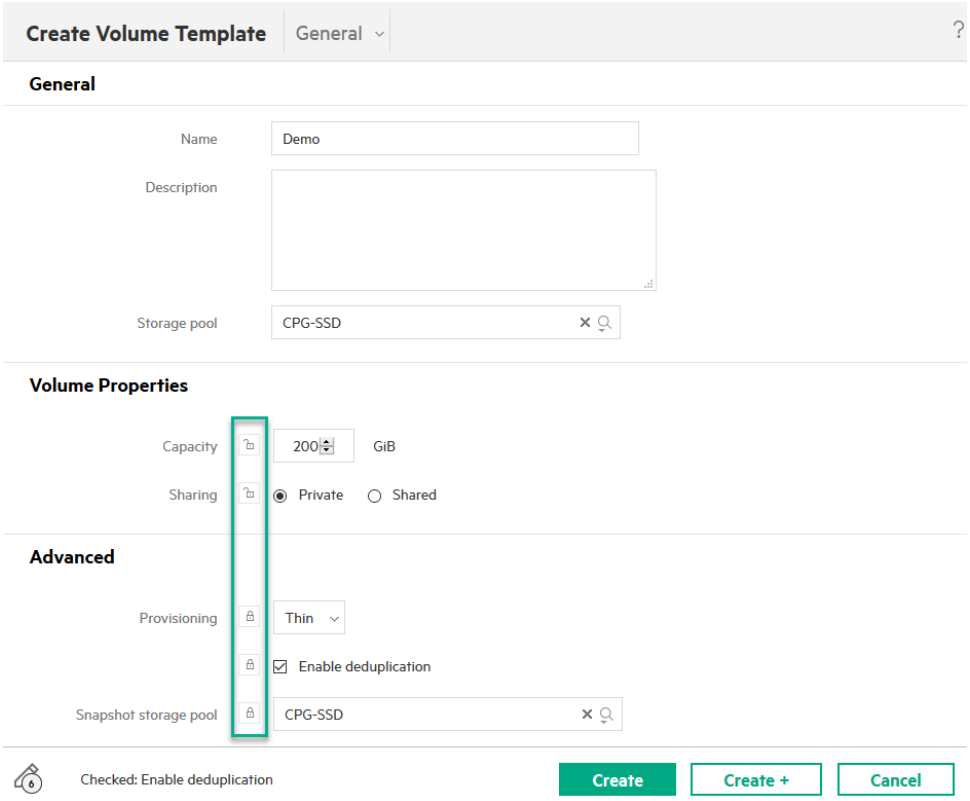
4. Using the storage pool drop down list, select the *Storage pool* the volume template will create volumes from.



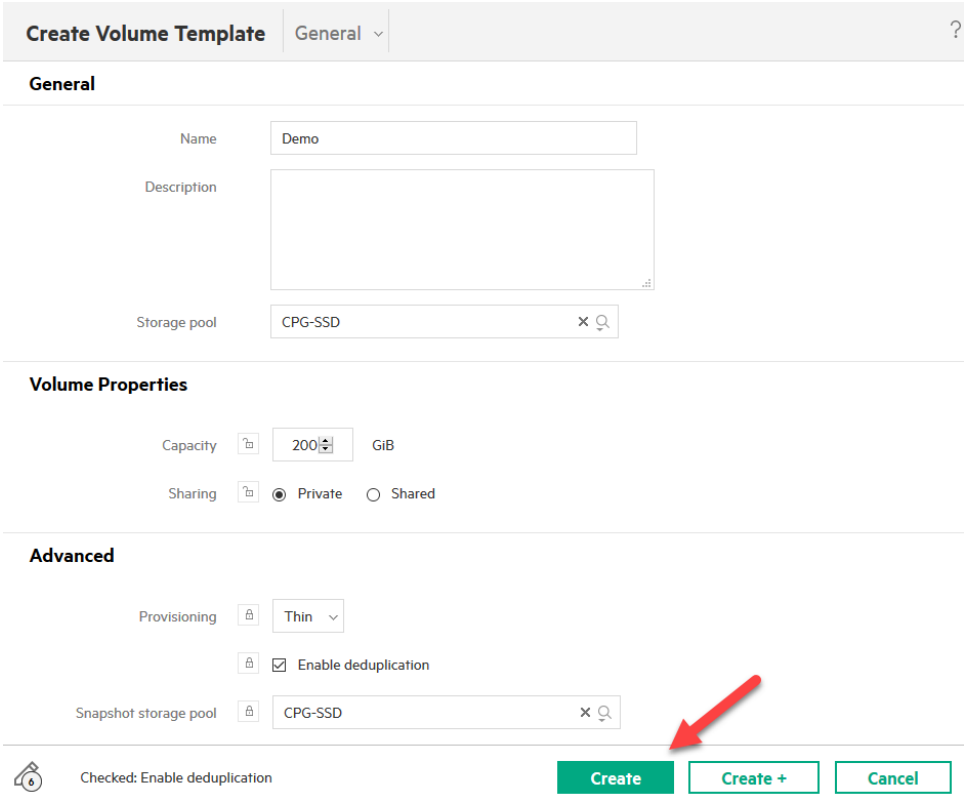
5. Once the volume template's storage pool is selected, the volume template is populated with the volume properties that can be set on volumes created within the selected pool. HPE 3PAR StoreServ pools (shown below) support different properties than HPE Primera or Nimble storage pools. Select the volume property settings as desired.



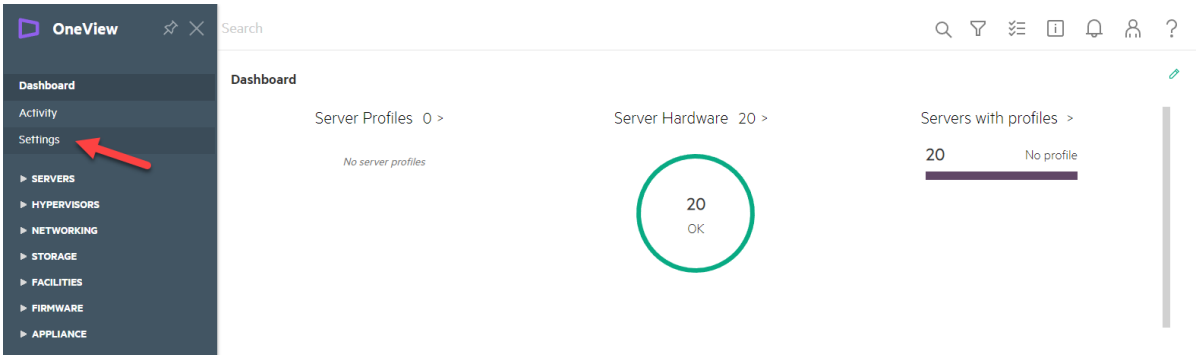
6. Next, select the enforcement mode for each volume property. Volume properties which are "locked" are not changeable when a volume is created using the template. Volume properties which are "unlocked" are changeable when a volume is created using the template.



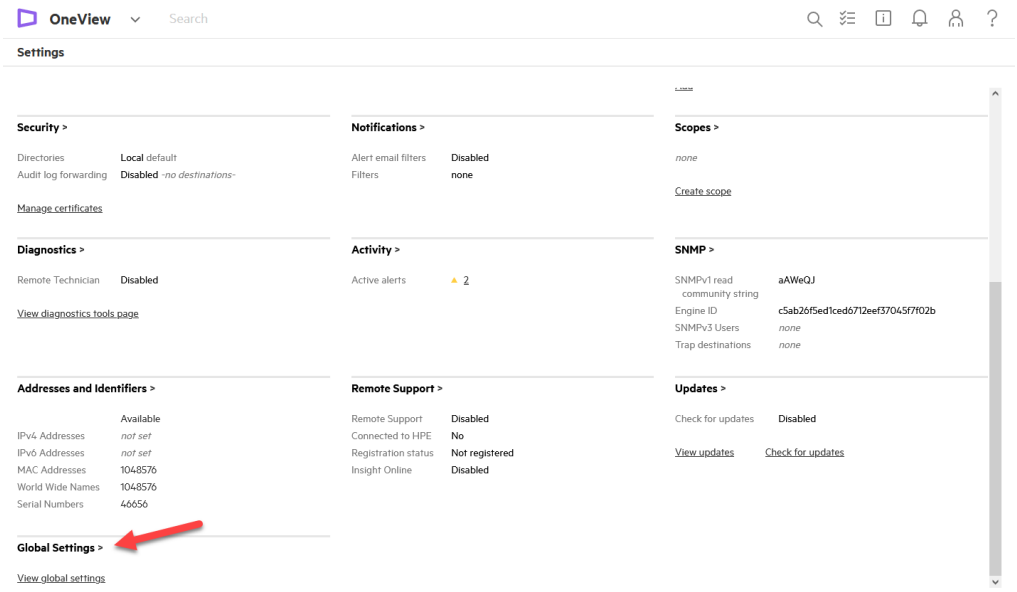
7. Then click the *Create* or *Create* + button to create the volume template.



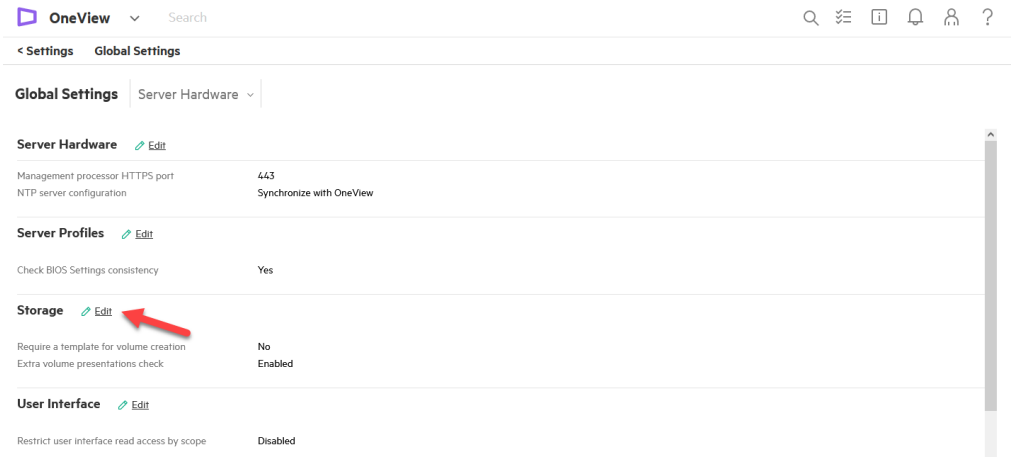
8. (Optional) If the Storage administrator wants to require that non-storage administrators must use storage volume templates when creating volumes, the *Require template for Volume Creation* Global Policy needs to be set, which is in the *Settings menu*.



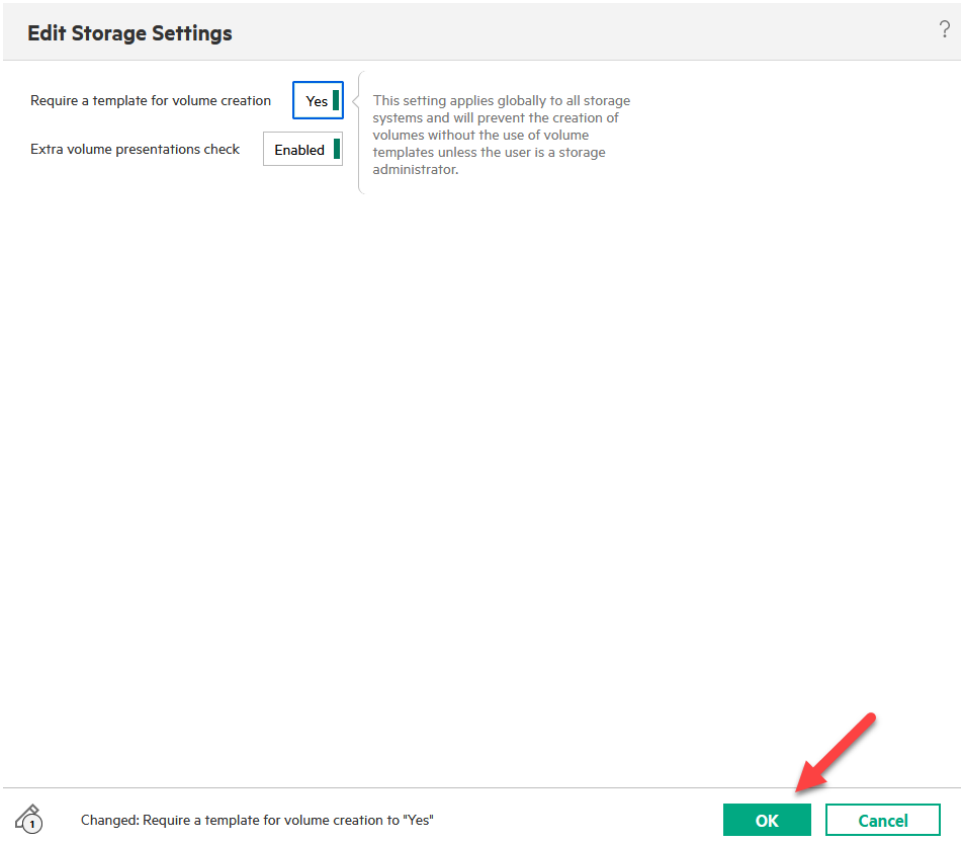
9. In the Settings click on *Global Settings*



10. Click on the Storage *Edit* to change the Global setting



11. Click the toggle to start requiring a storage volume template whenever non-storage administrators create volumes. Click *OK* to apply the setting

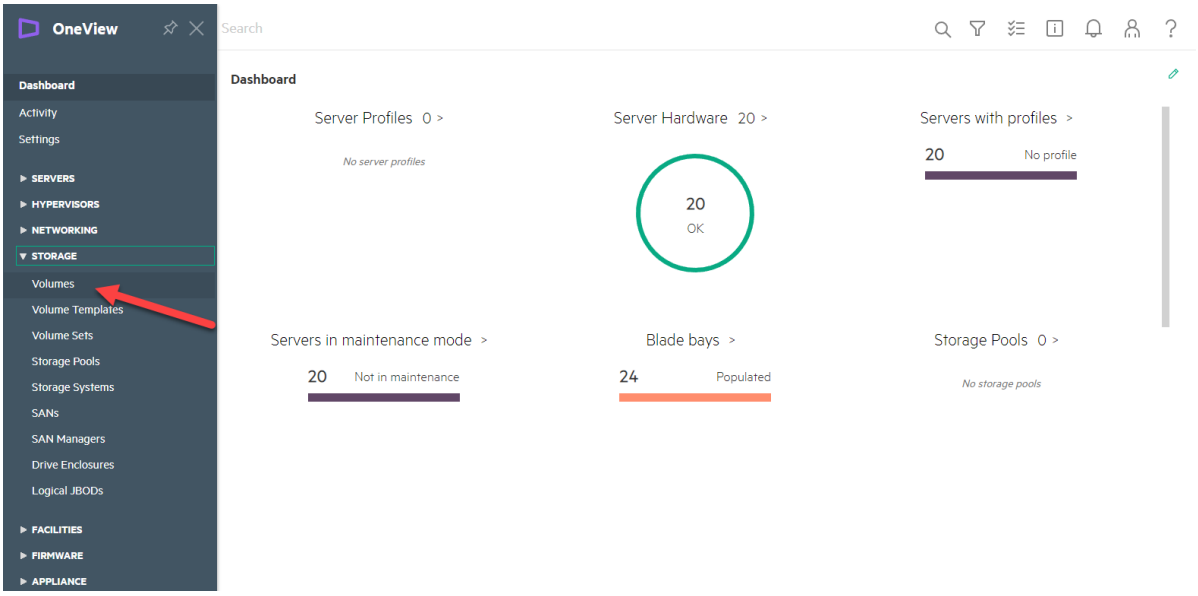


Creating StoreServ Storage Volumes

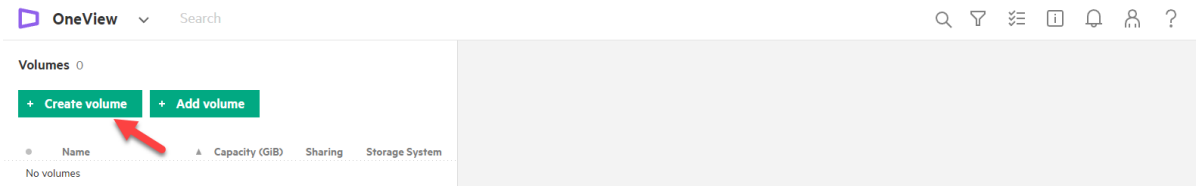
Volumes can be created independent of server profiles within the *Volumes* view, under the Storage column of the Top-Level Menu within the UI or created as part of a server profile. When created using the Volumes view, the volume's lifecycle will be independent of server profiles (i.e. "permanent"). When created as part of a server profile, the volume's lifecycle can optionally be tied to the server profile (i.e. "non-permanent", also called "Ephemeral") such that when the server profile is deleted, the volume will be deleted as well.

Volumes can be created by either server or storage administrator roles.

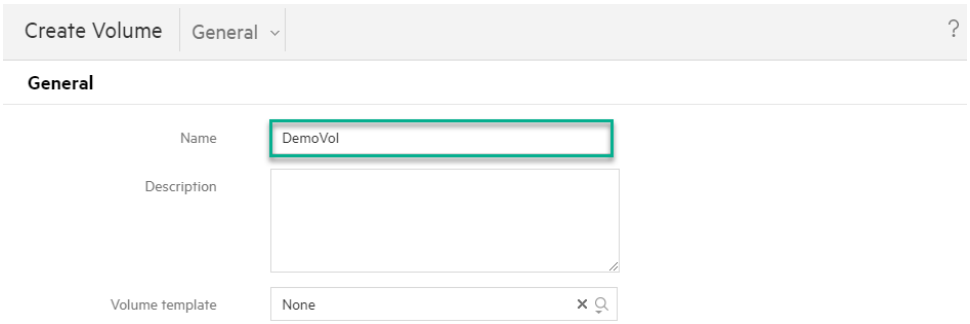
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Volumes*.



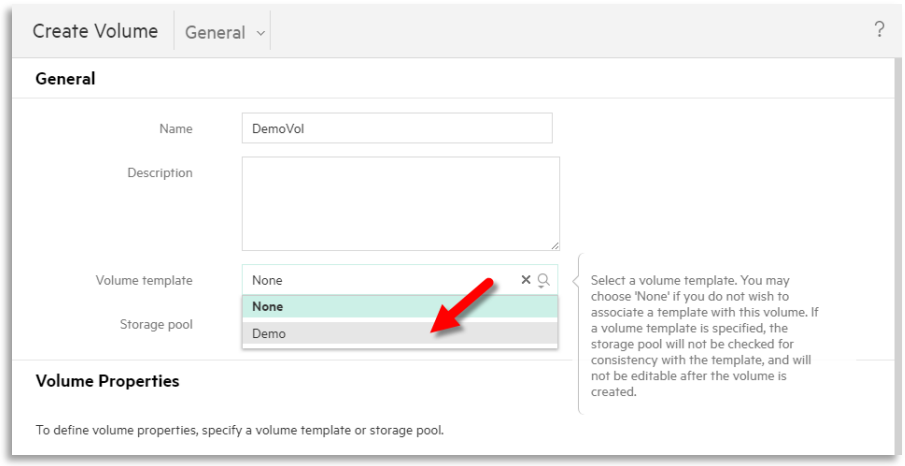
2. Click the *Create volume* button.



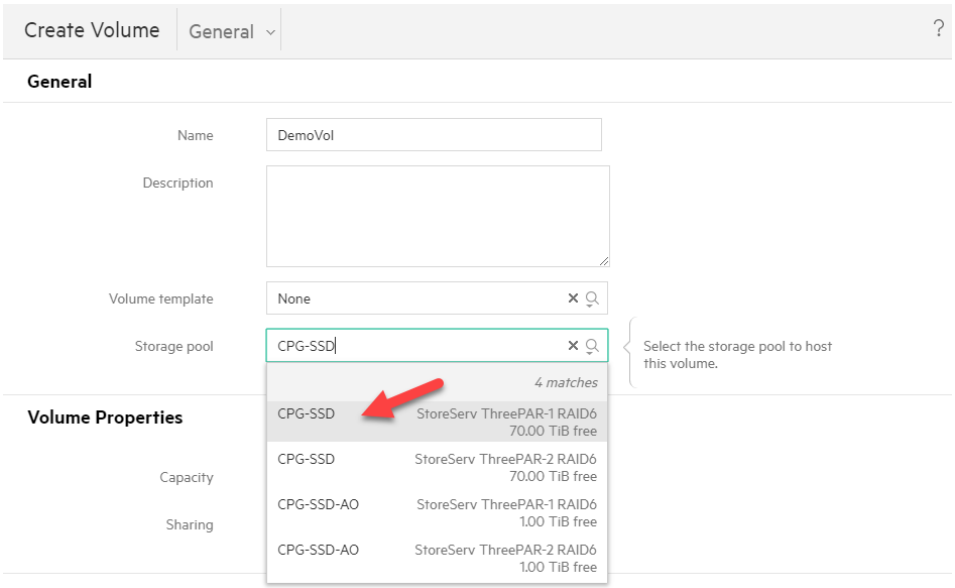
3. In the Create Volume screen, enter a *Name* and optionally a description for the volume.



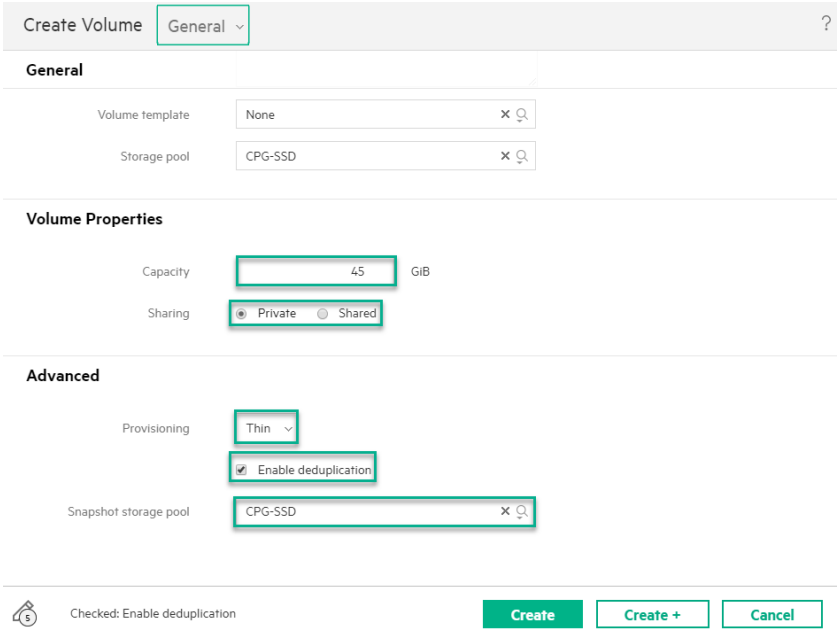
4. In the Create Volume screen, the options may be restricted if the Storage Administrator has forced Volume Creation to be provisioned from a Volume Template. Otherwise, the administrator creating the *Volume* may choose whether it will be associated with an available Volume Template or not. When creating a volume from a volume template select the template.



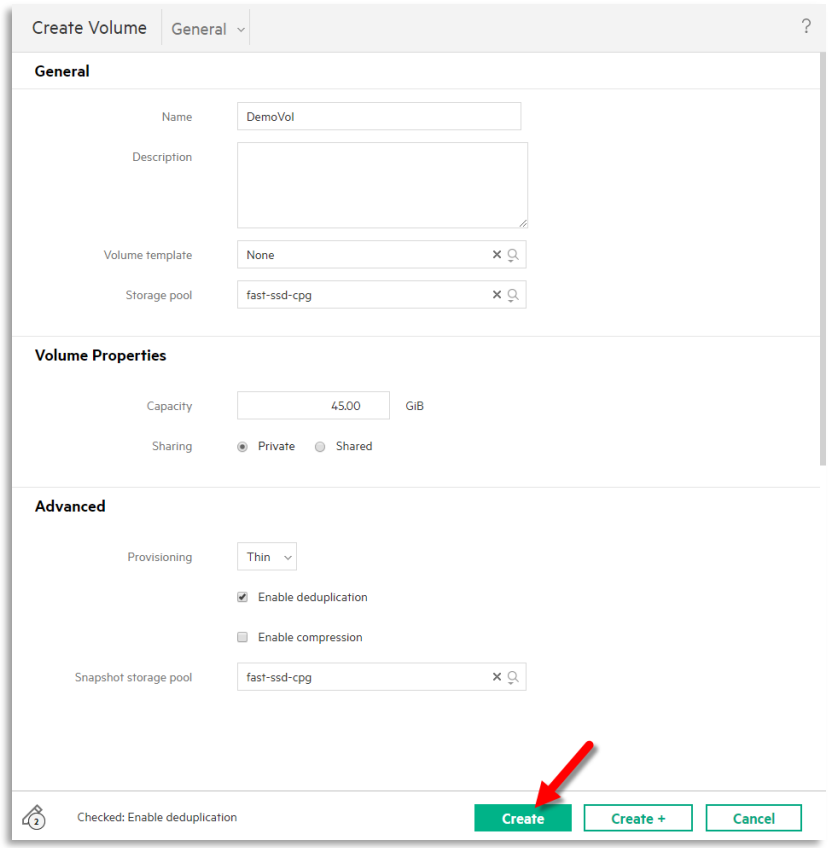
5. If not associated with a volume template, select the *Storage pool* for the volume



6. After selecting a volume template or storage pool, the Volume properties will be populated with the properties that can be set for the volume. HPE StoreServ storage pools allow different properties to be set on volumes than HPE Alletra, Primera or Nimble storage pools. Set the *Volume Properties* for the volume.



7. Click *Create* or *Create* + button to create the volume.

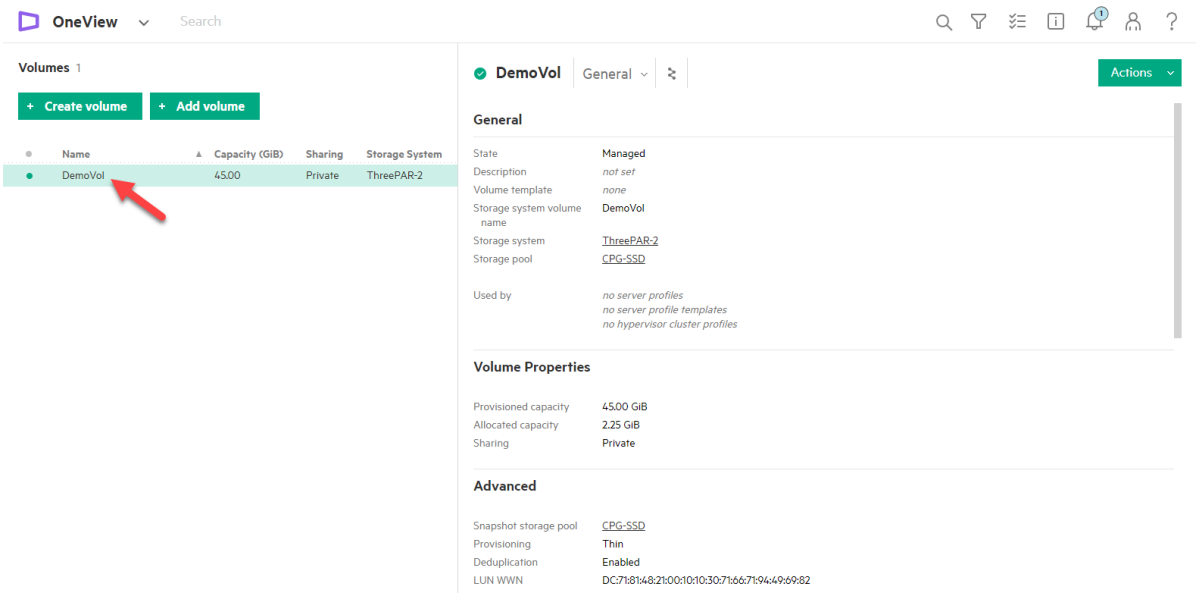


Note:
When creating volumes, HPE OneView attempts to name volumes on the storage system as close as possible to volume names in HPE OneView. When the HPE OneView volume name is not a valid volume name on the storage system (unsupported characters, name too long, name already exists, etc.), HPE OneView will remove illegal characters, shorten and ensure the name is unique to create a legal name on the storage system. Any scripting communicating with both systems needs to be aware of this.

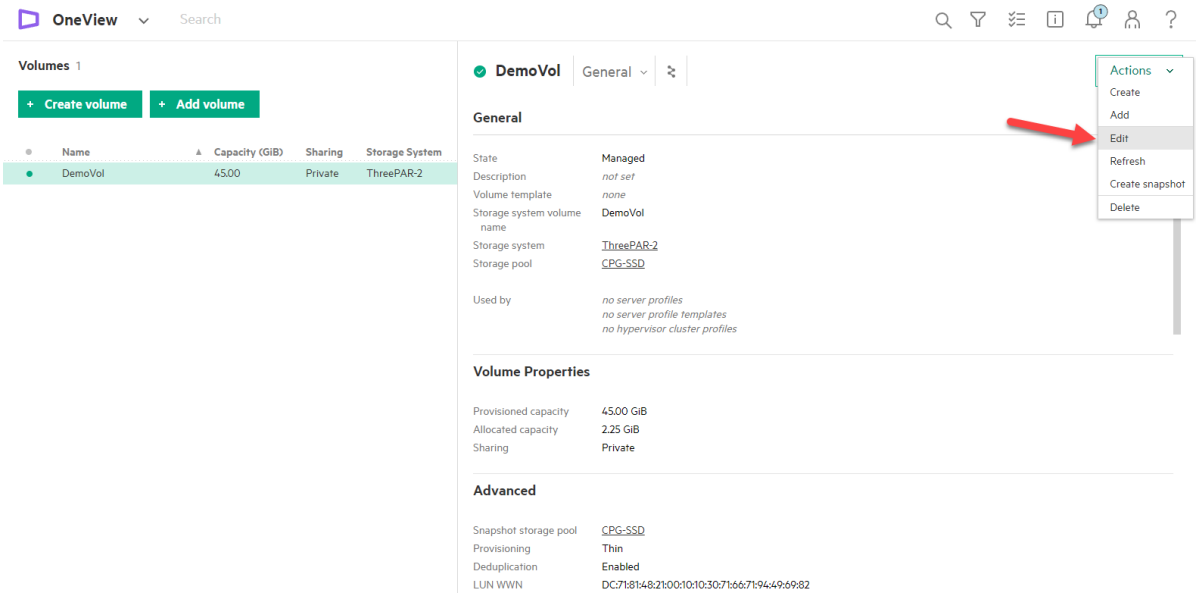
(Optional) Growing Volume Capacity

Growing a Volume or changing any other of its properties is performed by editing the volume. Grow the volume by increasing its capacity.

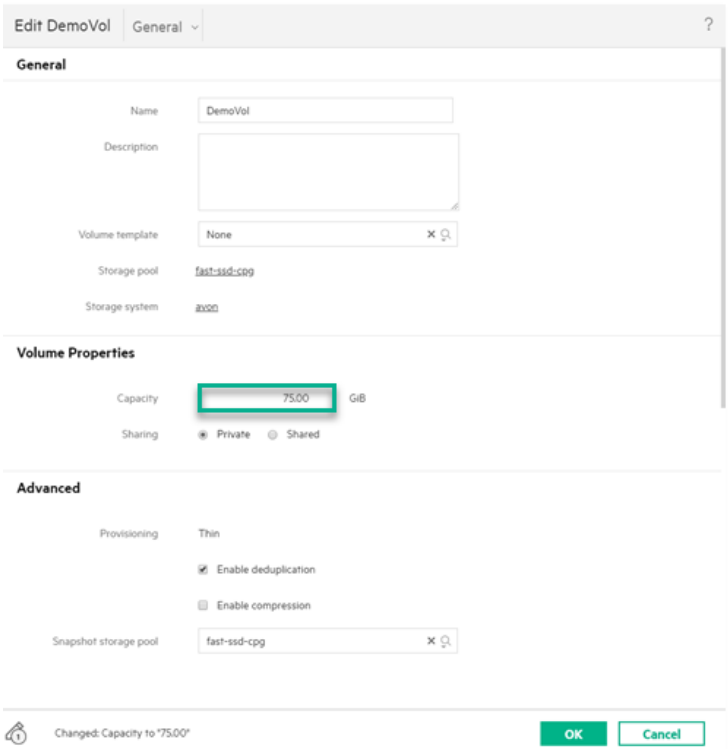
1. Select the *volume* from the menu



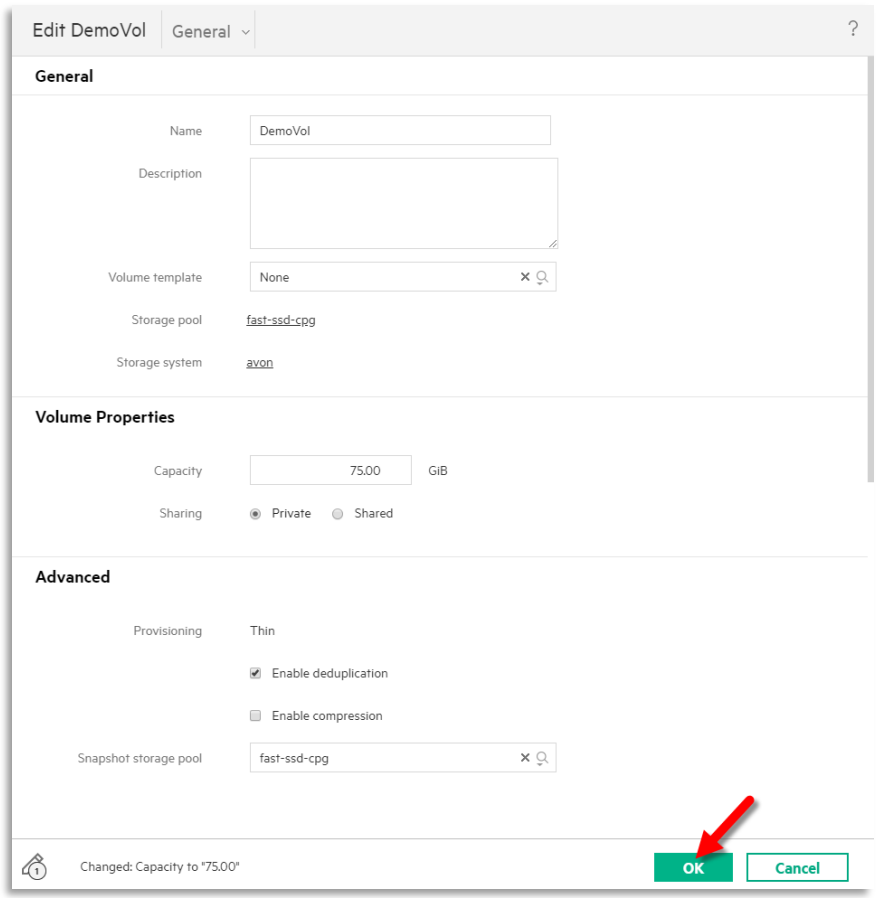
2. Select *Edit* from the Actions menu



3. In the Edit dialog box, edit the volume *Capacity*



4. Click *OK*.



Enabling StoreServ Compression and using Large Volumes

Using volumes with StoreServ compression enabled or creating / growing volumes larger than 16 TiB in size (up to 64 TiB) is performed by creating or editing an existing volume and setting these properties.

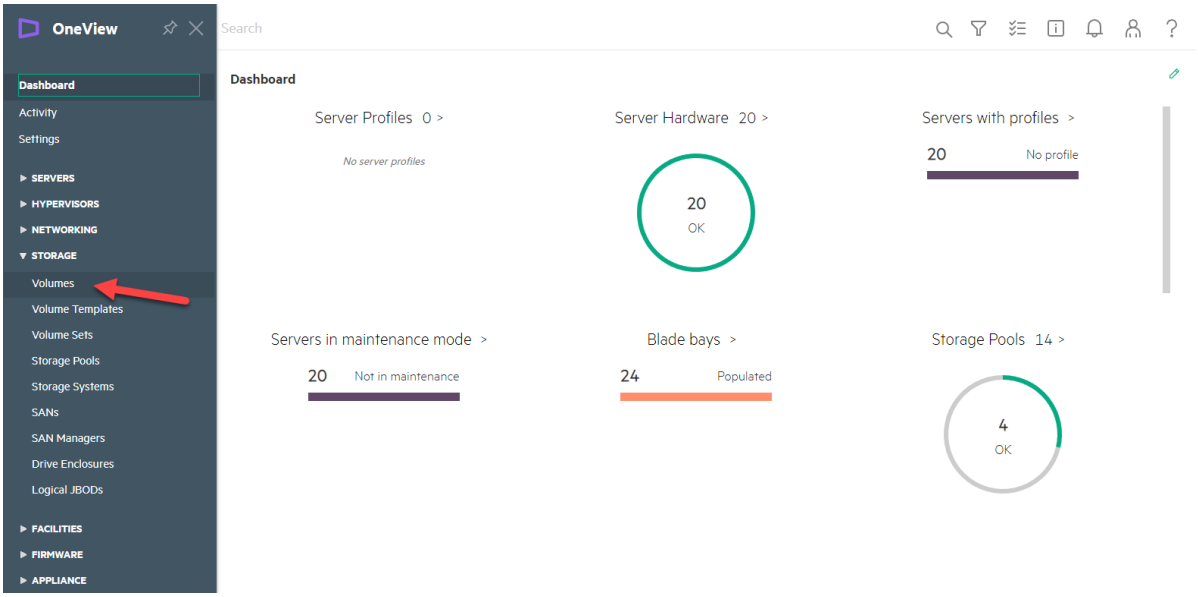
Note:
Volume compression and large volume sizes are only supported on 3PAR Storage Systems running 3.3.1 EGA or later.

Compression is only supported on Volumes created from Storage Pools with an SSD Drive type. When creating or modifying a Volume or Volume Template in a Storage Pool that does not support compression, the "Enable compression" volume setting will not appear.

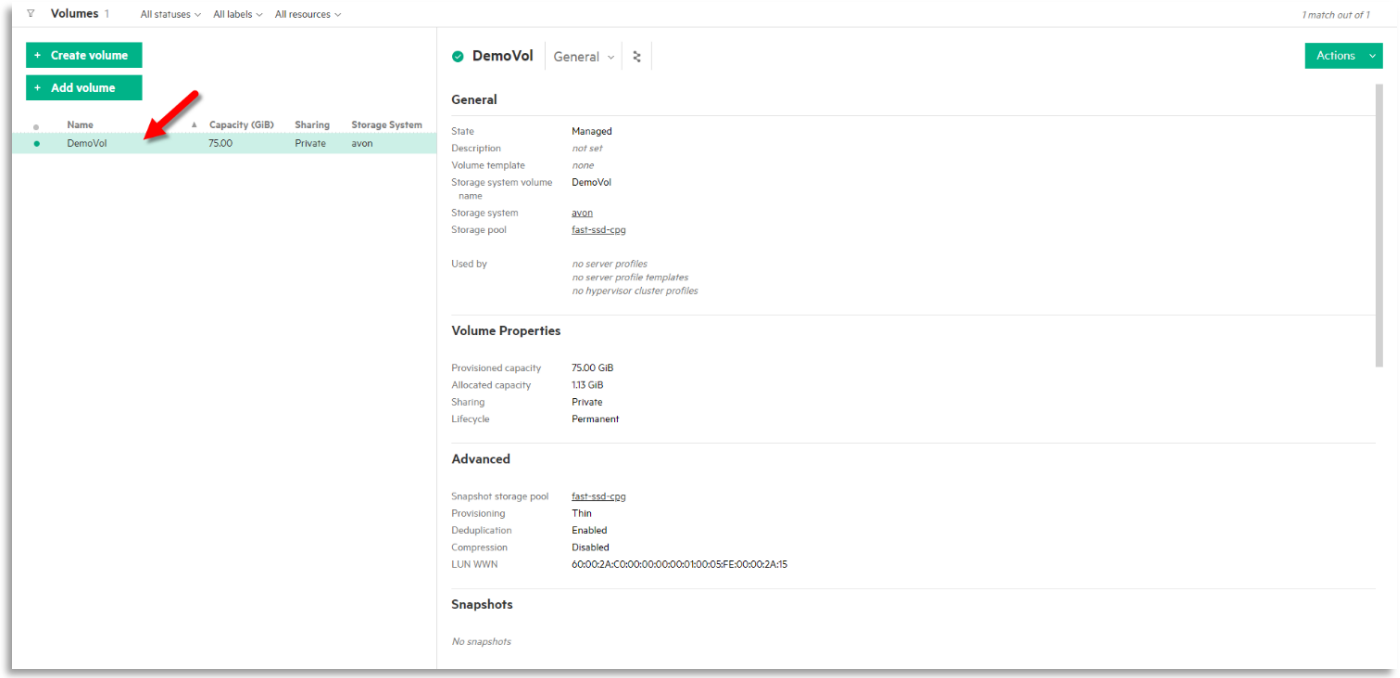
Large Volumes are supported only on Volumes with compression and deduplication disabled.

---

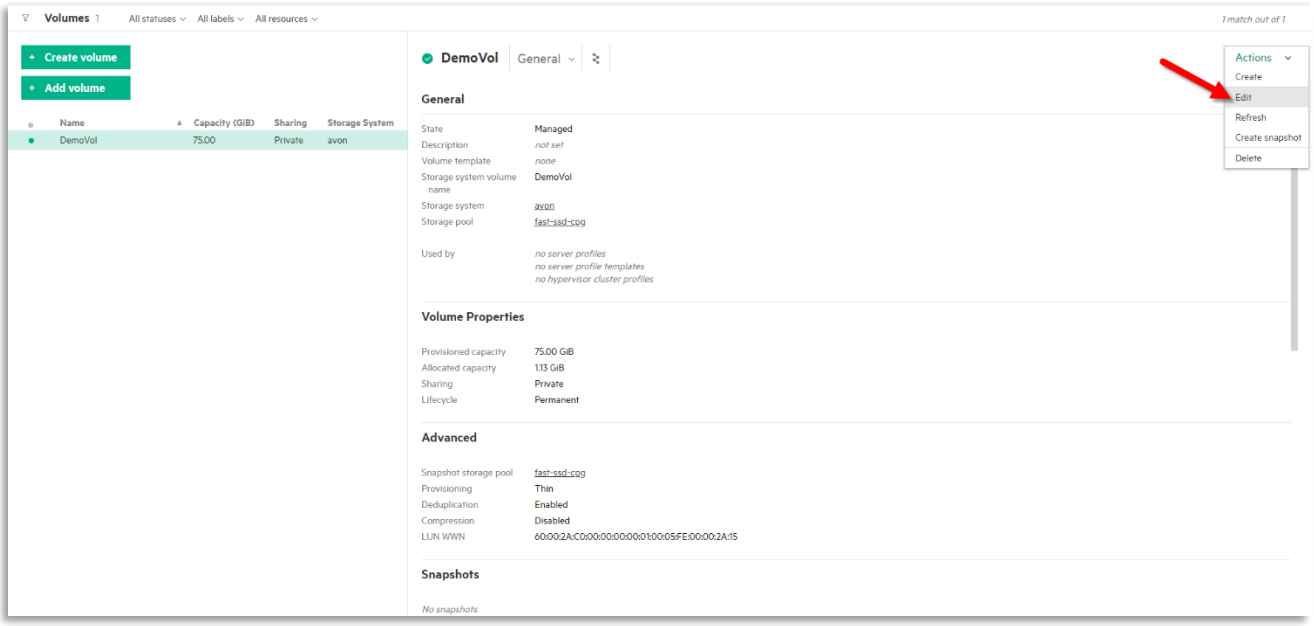
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Volumes*.



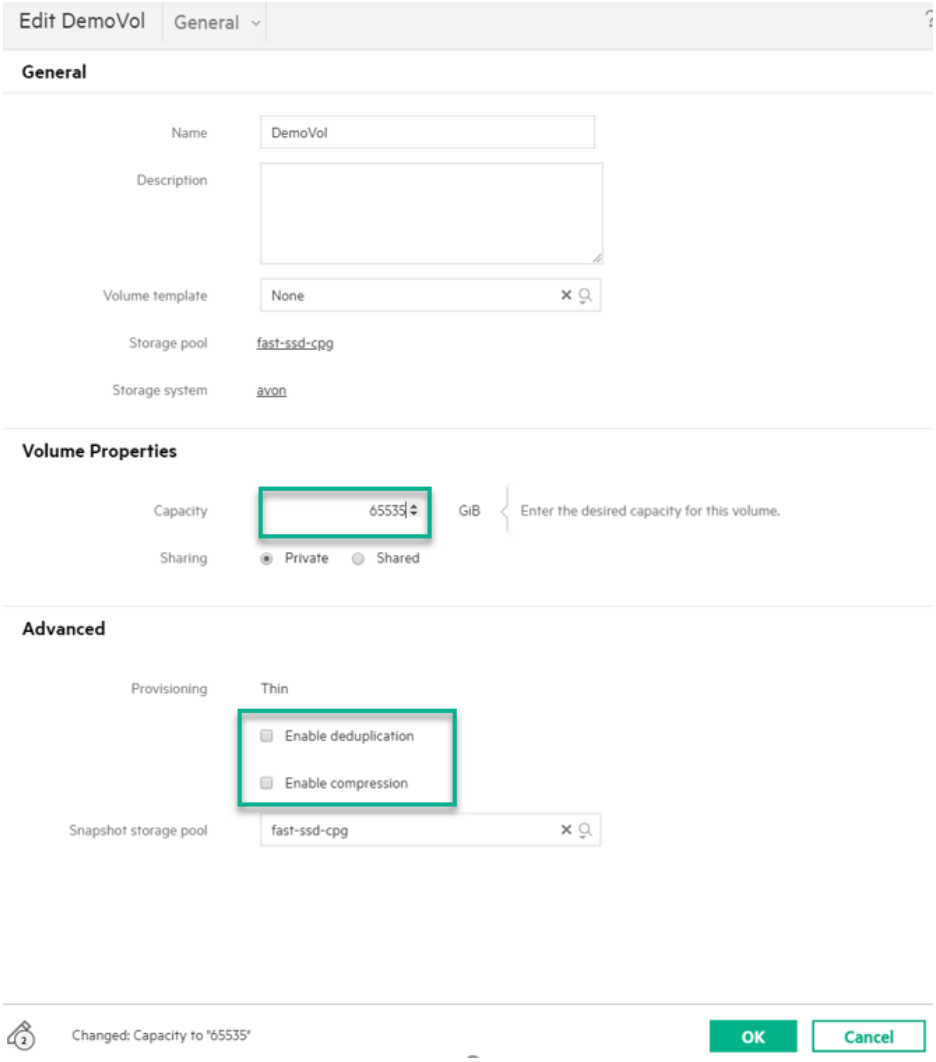
2. Select the *volume* that you wish to modify.



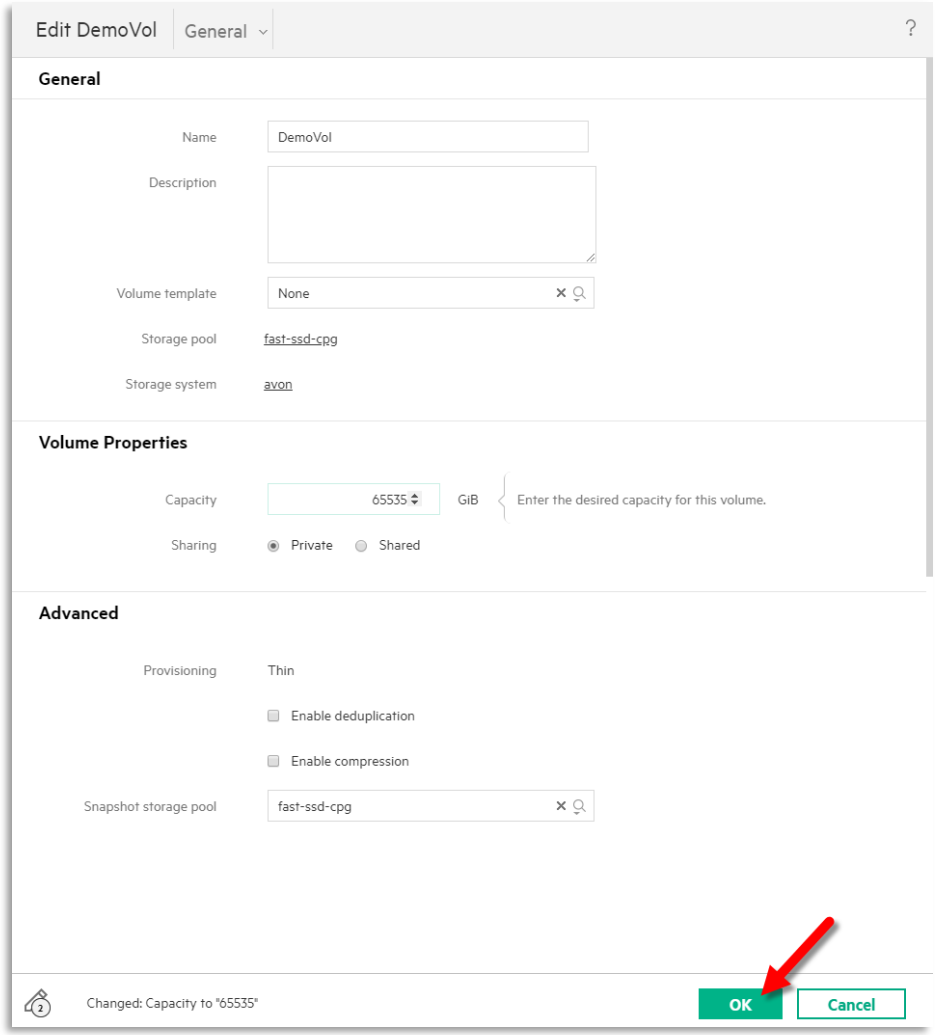
3. Select *Edit* from the actions menu



4. In the Edit dialog box, edit the volume *Capacity* to a size up to 64 TiB. Note that deduplication and compression must be disabled.



5. Click *OK*.

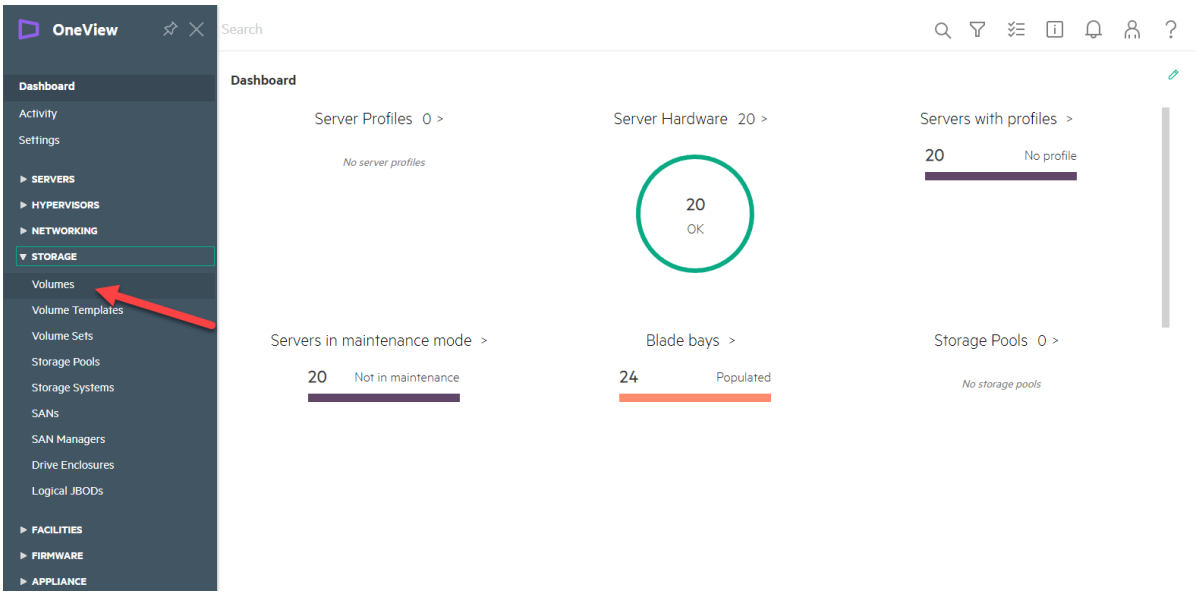

Edit DemoVol
General
General
Name
DemoVol
Description
Volume template
None
Storage pool
fast-ssd-cpg
Storage system
avon
Volume Properties
Capacity
65535
GiB
Enter the desired capacity for this volume.
Sharing
Private
Shared
Advanced
Provisioning
Thin
Enable deduplication
Enable compression
Snapshot storage pool
fast-ssd-cpg
Changed: Capacity to "65535"
OK
Cancel

Creating Nimble Storage Volumes

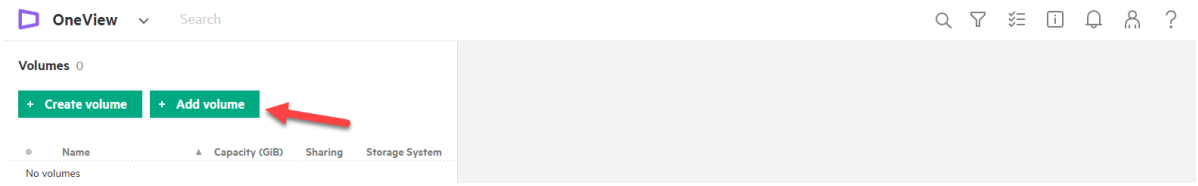
Nimble volumes can be created independent of server profiles within the *Volumes* view, under the Storage column of the Top-Level Menu within the UI or created as part of a server profile. When created using the Volumes view, the volume's lifecycle will be independent of all server profiles (i.e. "permanent"). When created as part of a server profile, the volume's lifecycle can optionally be tied to the server profile (i.e. "non-permanent", also called "Ephemeral") such that when the server profile is deleted, the volume will be deleted as well.

Volumes can be created by either server or storage administrator roles.

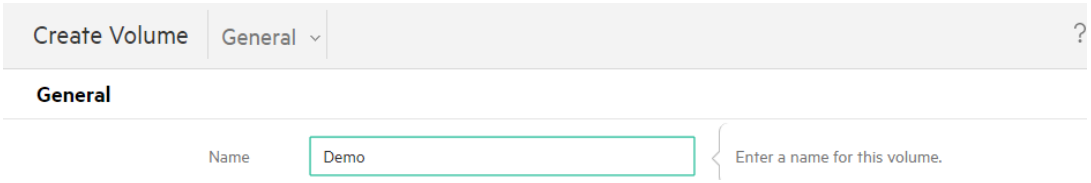
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Volumes*.



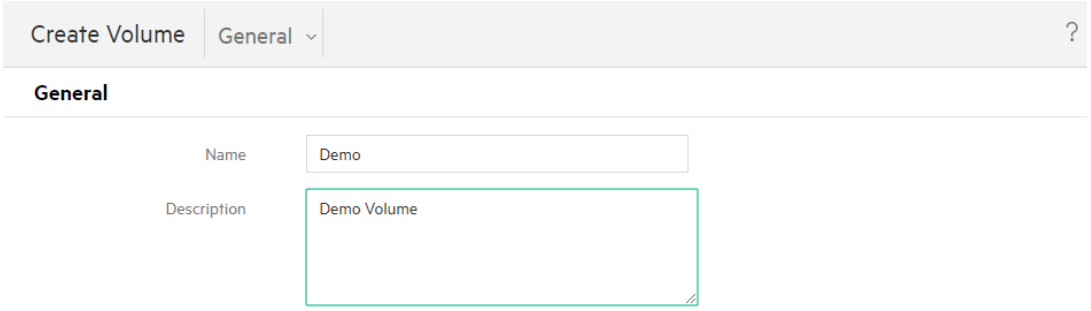
2. Click the Create volume button.



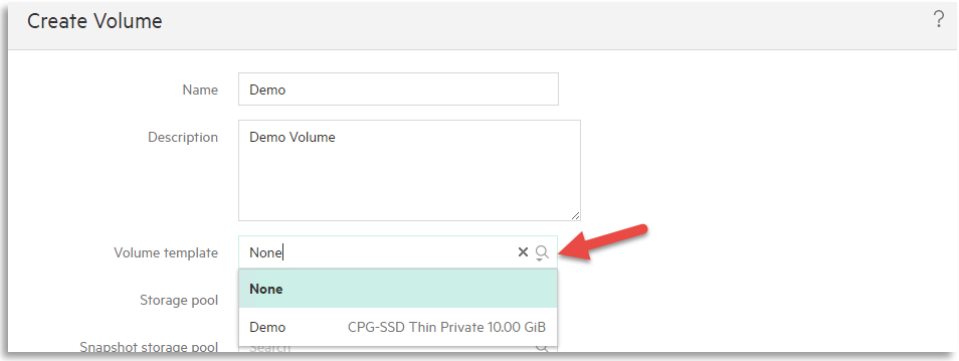
3. In the Create Volume screen, enter a *Name* for the volume



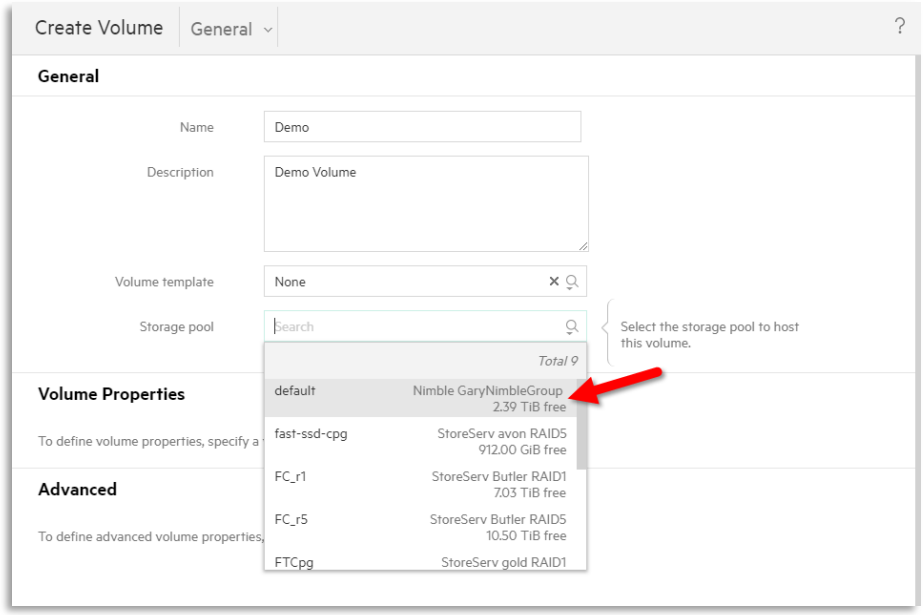
4. Enter a *Description* for the volume



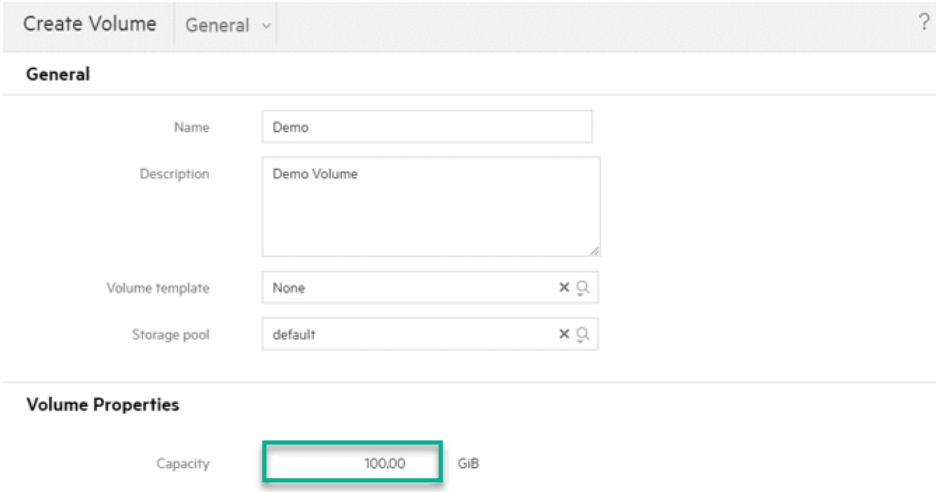
5. In the Create Volume screen, the options can be restricted if the Storage Administrator has forced Volume Creation to be provisioned from a Storage Volume Template. Otherwise, the administrator creating the *Volume* may choose whether it will be associated with an available Storage Volume Template.



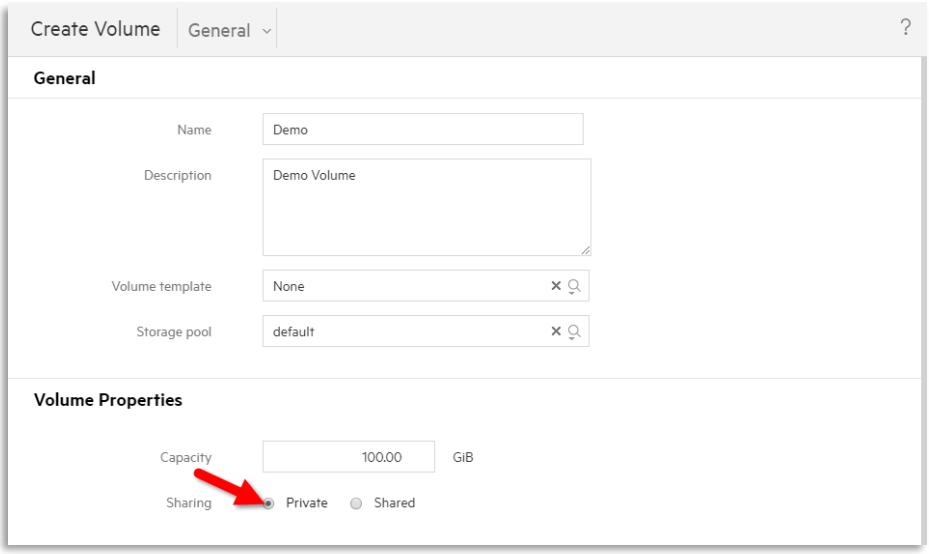
6. If not associated with a volume template, select a Nimble Storage System's *Storage Pool* for the volume



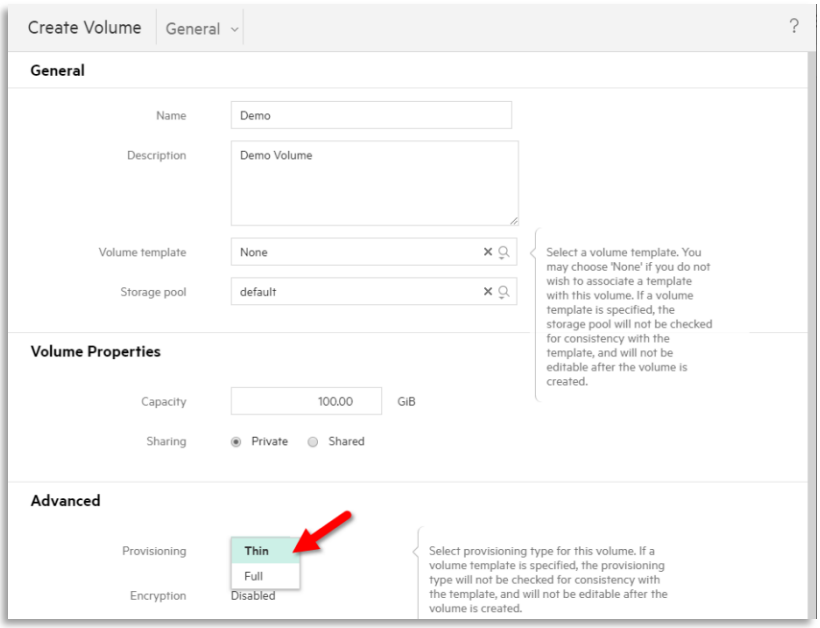
7. In the Volume Properties section, set the *Capacity* for the volume



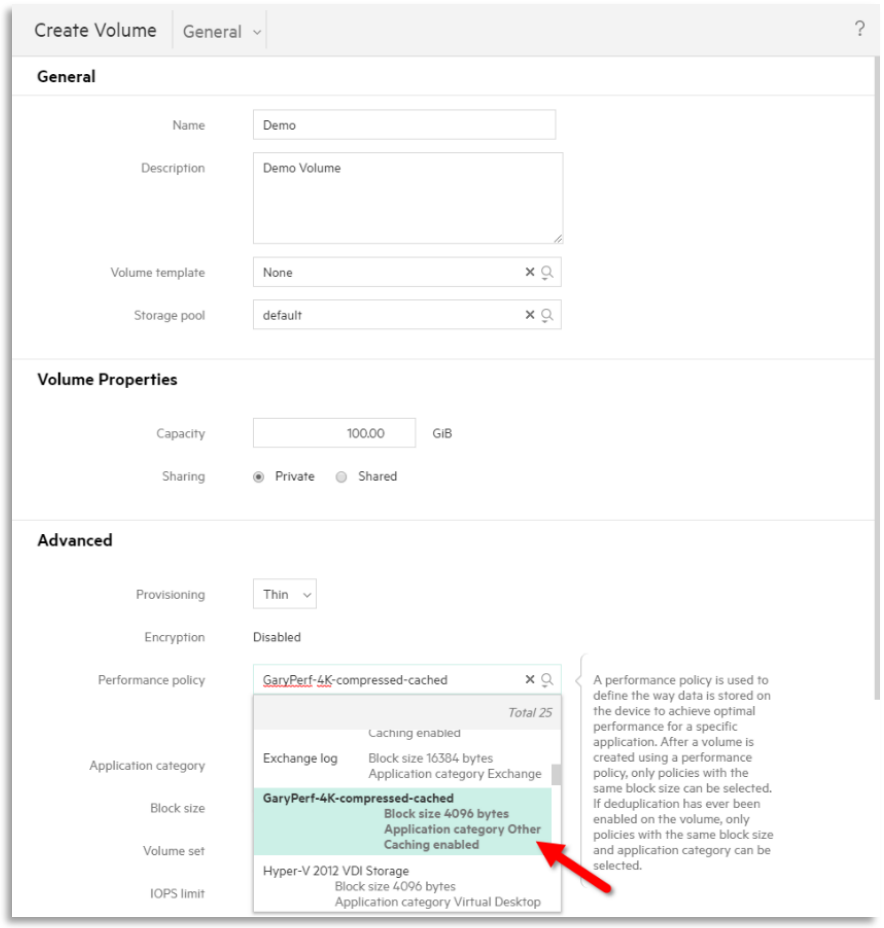
8. In the Volume Properties section, set the *Sharing* method for the volume



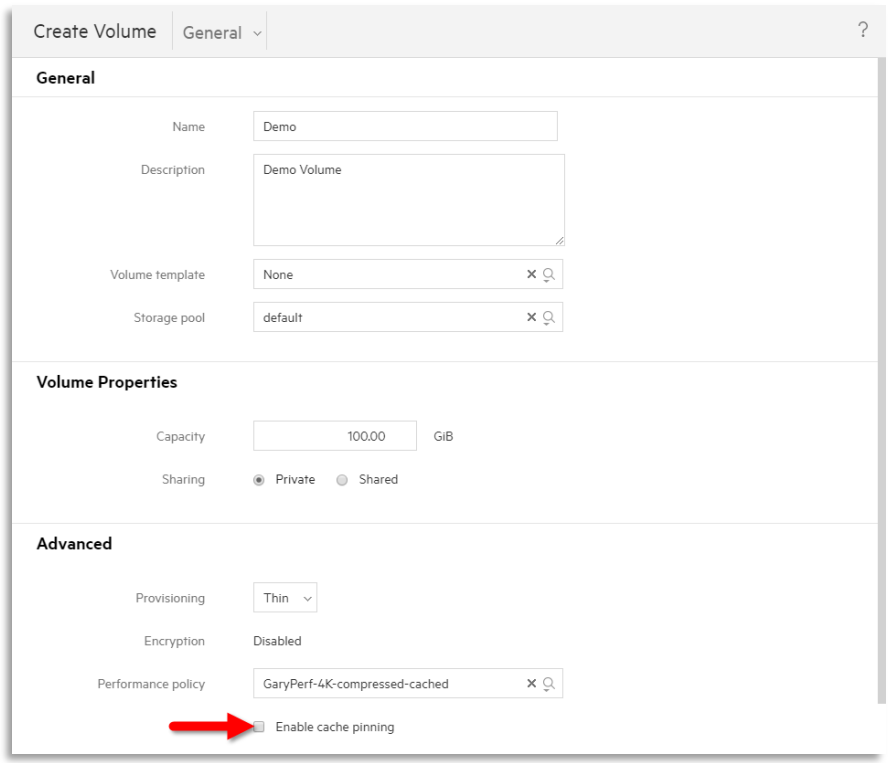
9. In the Advanced section, set the Nimble specific volume properties, starting with the *Provisioning* method for the volume



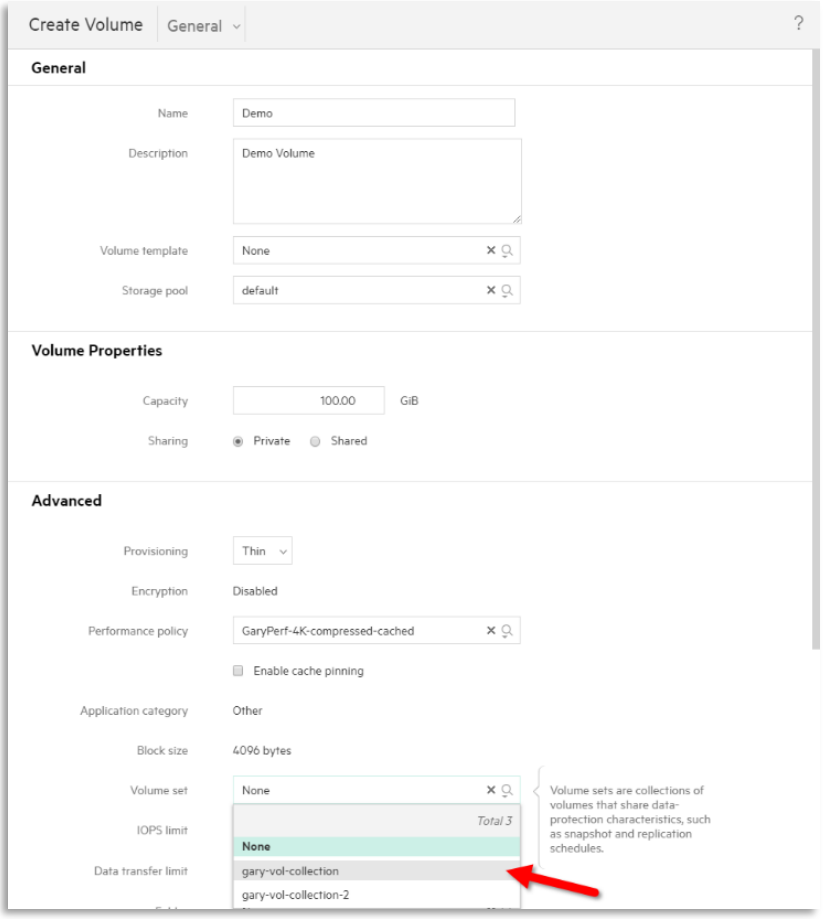
10. Performance policies are read from the Nimble Storage System and can be selected for the volume. The *Performance policy* sets the Application category and Block size as well.



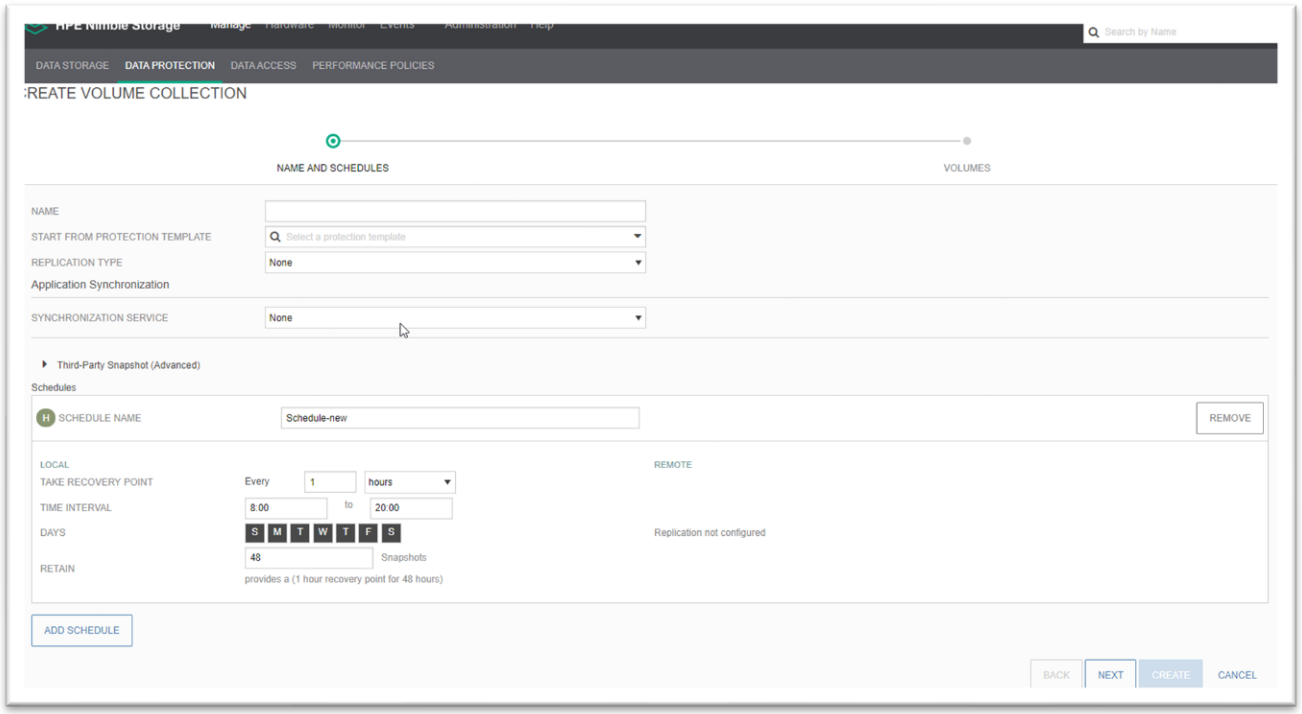
11. If the selected Performance policy allows cache pinning to be enabled, its value can be editable and can be selected. If the selected Performance policy does not allow cache pinning to be enabled, this value will be grayed out and statically set.



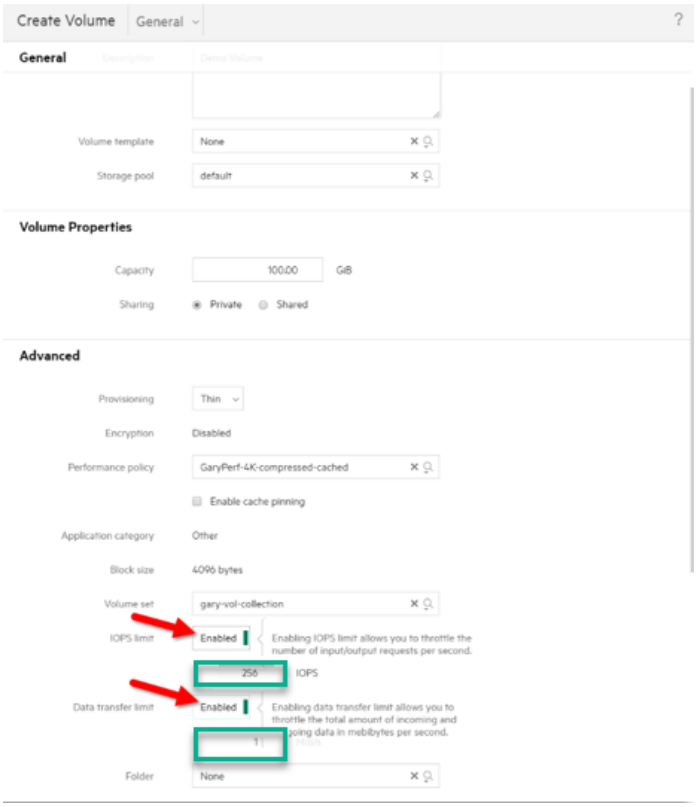
12. Volume sets are read from the Nimble Storage System and can be selected for the volume.



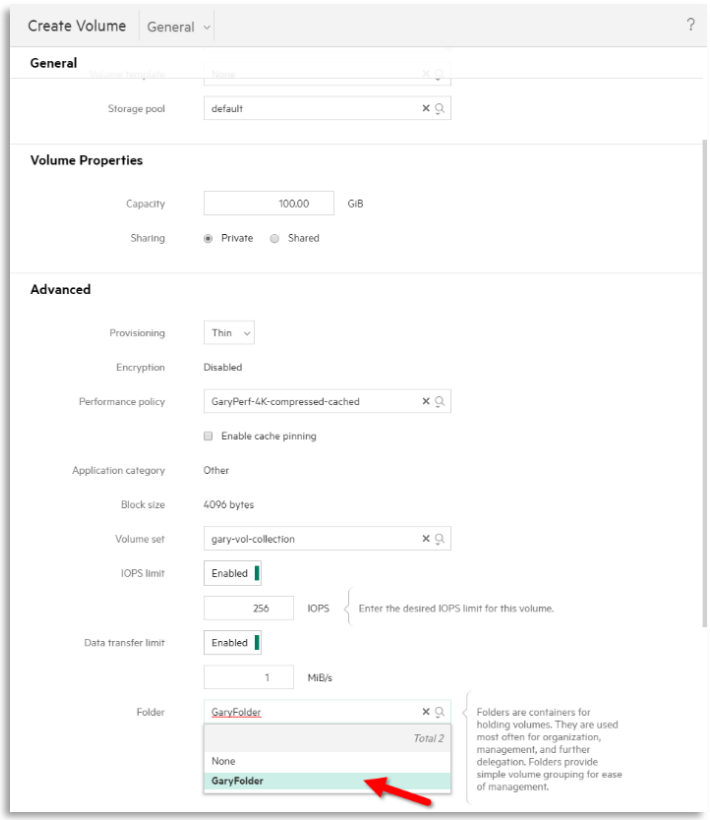
Volume sets (called Volume Collections on Nimble) define sets of volumes that share data-protection characteristics, such as snapshot and replication schedules.



13. Volume QoS throttling can be set on the volume by limiting the number of IOPS or MiB/s throughput.

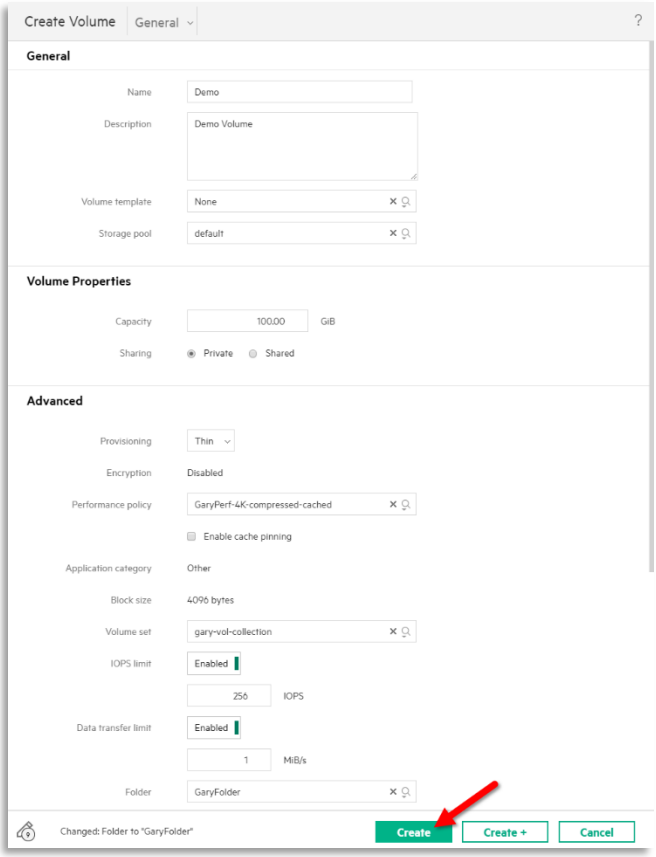


14. Folders are read from the Nimble Storage System and can be selected for the volume.



Nimble folders are containers for holding volumes. They are used most often for organization, management, and further delegation. Folders provide simple volume grouping for ease of management.

15. Click *Create* or *Create +* button to create the volume.

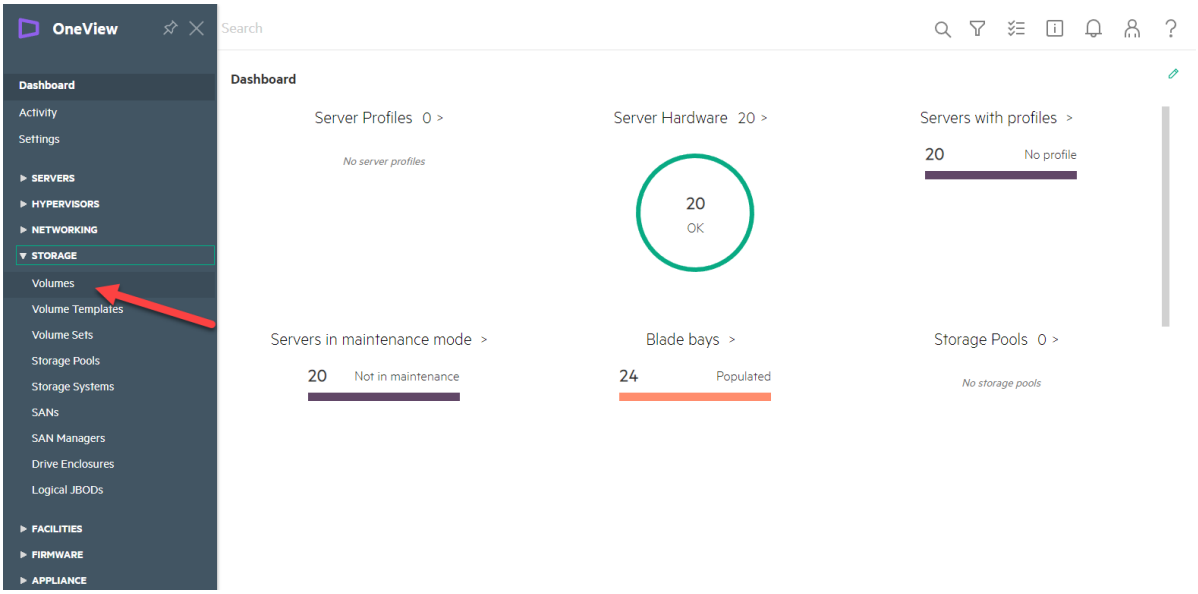


Creating Primera Storage Volumes

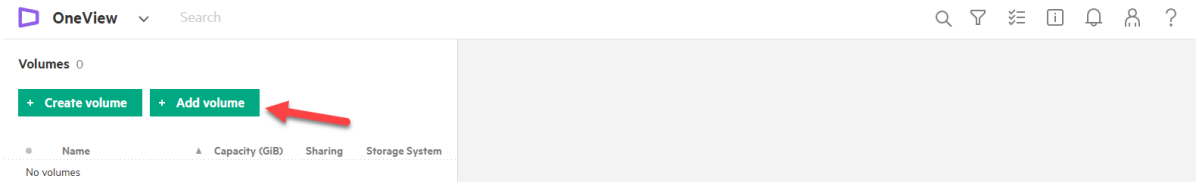
Volumes can be created independent of server profiles within the *Volumes* view, under the Storage column of the Top-Level Menu within the UI or created as part of a server profile. When created using the Volumes view, the volume's lifecycle will be independent of server profiles (i.e. "permanent"). When created as part of a server profile, the volume's lifecycle can optionally be tied to the server profile (i.e. "non-permanent", also called "Ephemeral") such that when the server profile is deleted, the volume will be deleted as well.

Volumes can be created by either server or storage administrator roles.

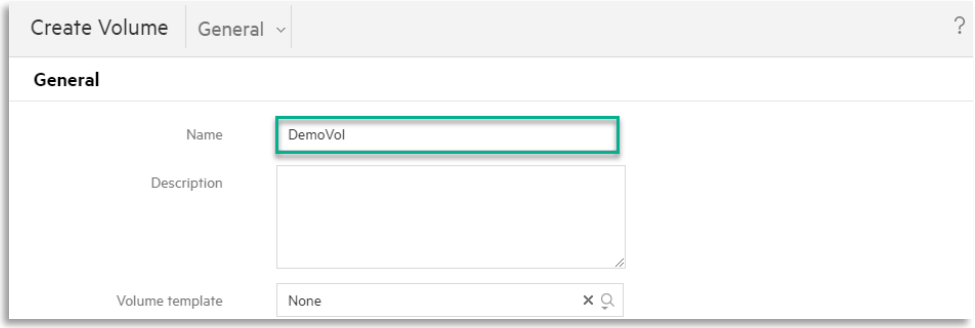
1. From the Top-Level Menu, expand the *STORAGE* option and then select *Volumes*.



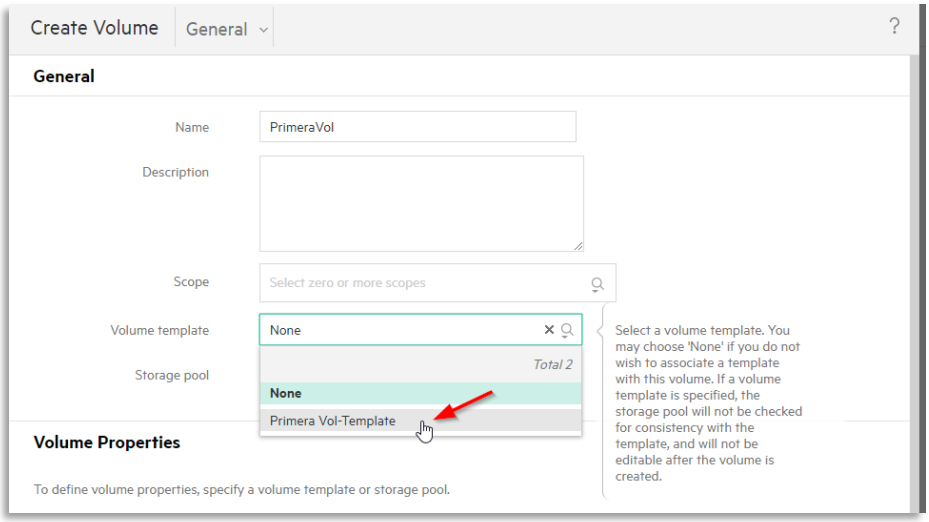
2. Click the *Create* volume button.



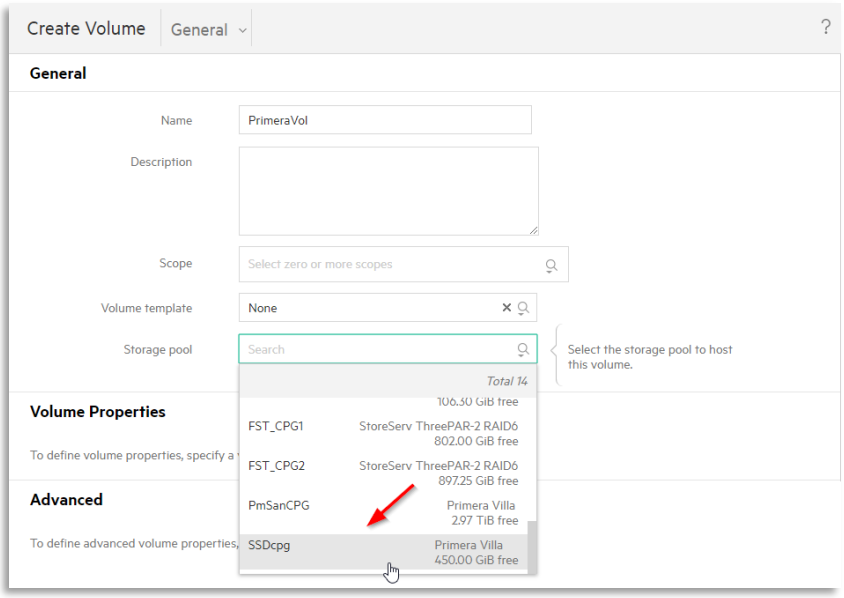
3. In the Create Volume screen, enter a *Name* and optionally a description for the volume.



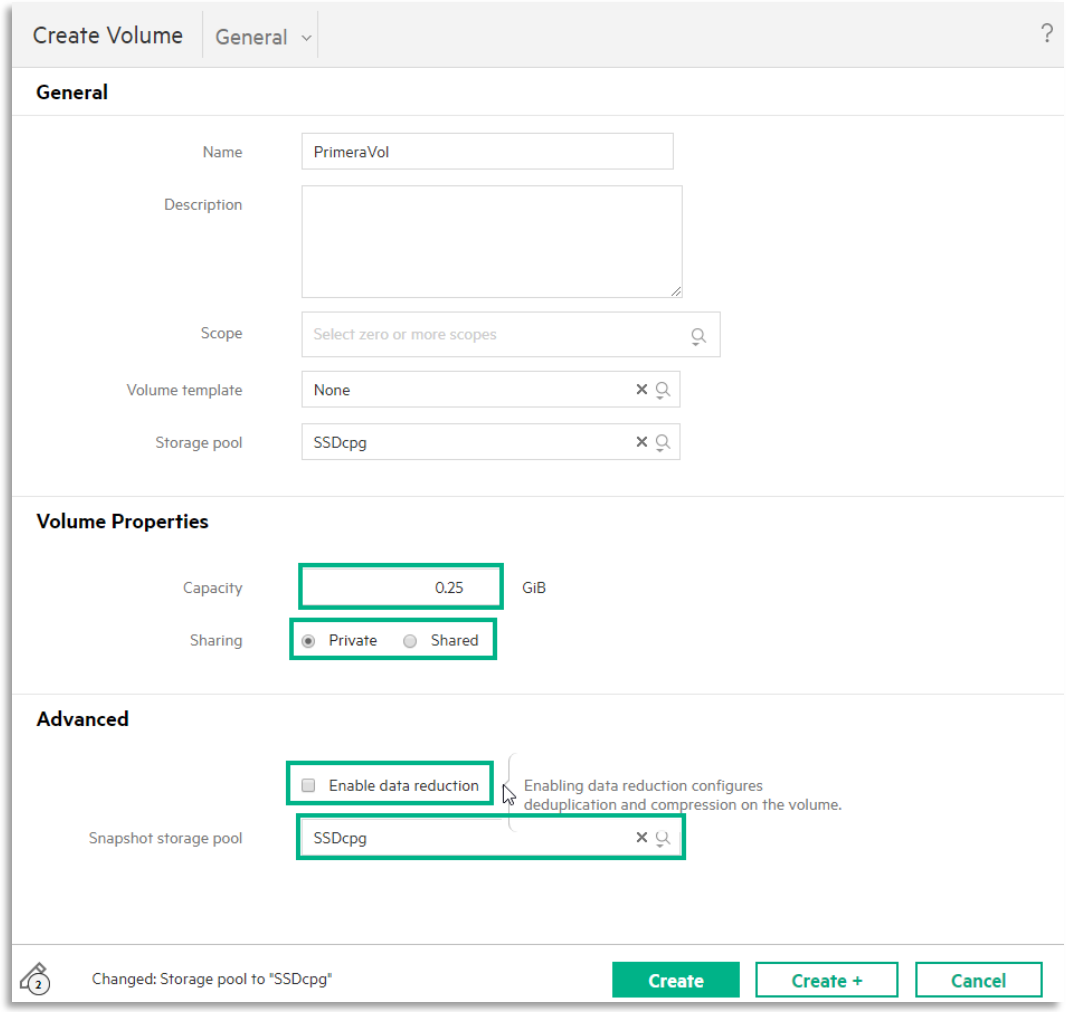
4. In the Create Volume screen, the options may be restricted if the Storage Administrator has forced Volume Creation to be provisioned from a Volume Template. Otherwise, the administrator creating the *Volume* may choose whether it will be associated with an available Volume Template or not. When creating a volume from a volume template select the template.



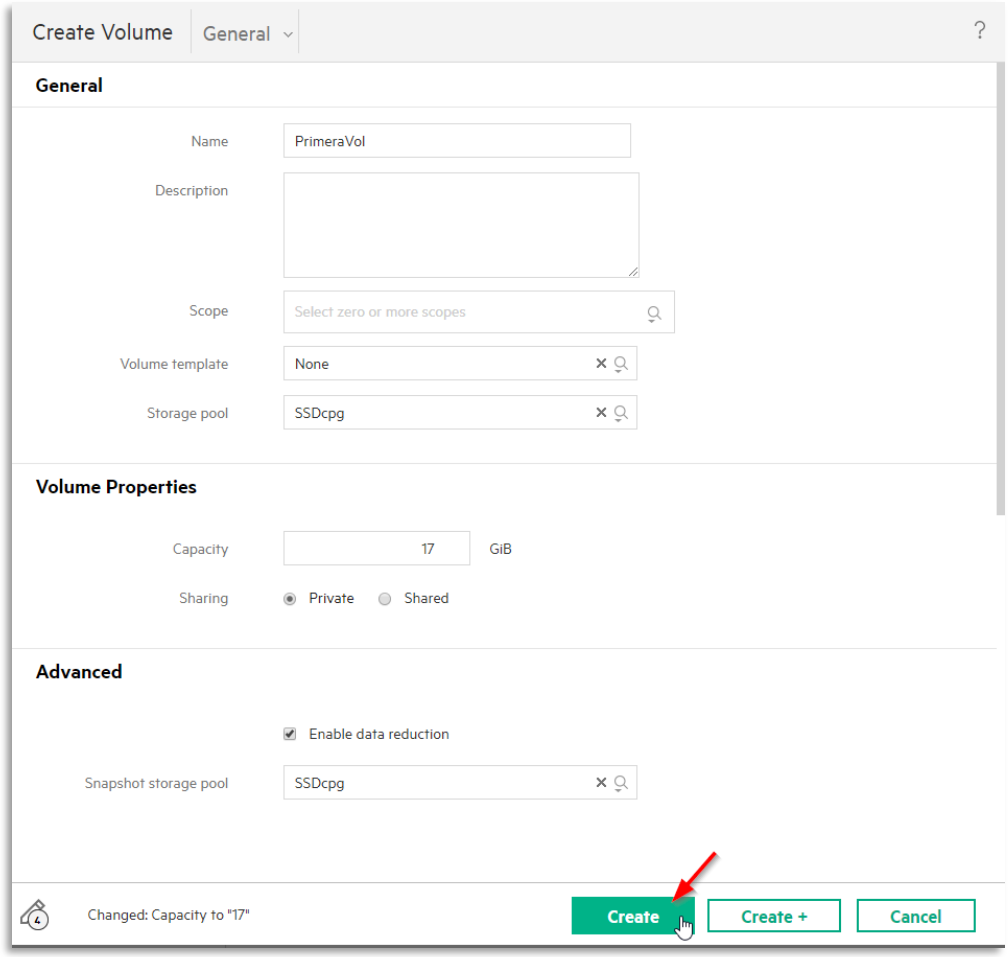
5. If not associated with a volume template, select the *Storage pool* for the volume



6. After selecting a volume template or storage pool, the Volume properties will be populated with the properties that can be set for the volume. HPE Primera storage pools allow different properties to be set on volumes than HPE StoreServ or Nimble storage pools. Set the *Volume Properties* for the volume.



7. Click *Create* or *Create +* button to create the volume.

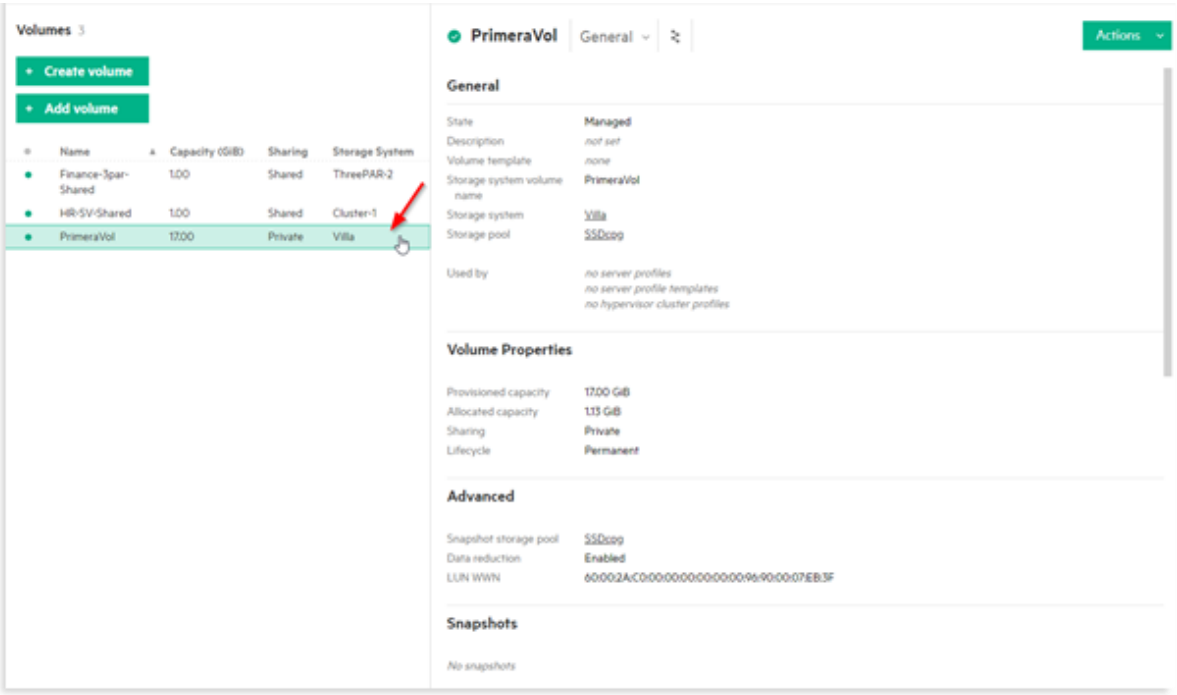


Note:
When creating volumes, HPE OneView attempts to name volumes on the storage system as close as possible to volume names in HPE OneView. When the HPE OneView volume name is not a valid volume name on the storage system (unsupported characters, name too long, name already exists, etc.), HPE OneView will remove illegal characters, shorten and ensure the name is unique to create a legal name on the storage system. Any scripting communicating with both systems needs to be aware of this.

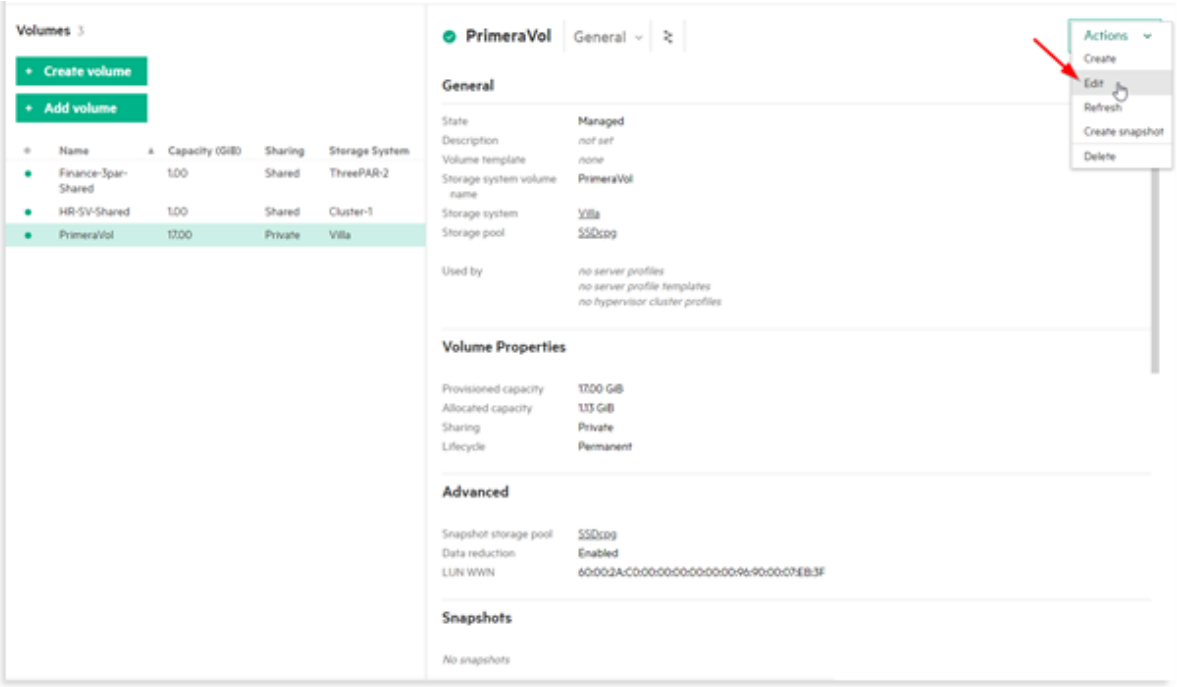
(Optional) Growing Volume Capacity

Growing a Volume or changing any other of its properties is performed by editing the volume. Grow the volume by increasing its capacity.

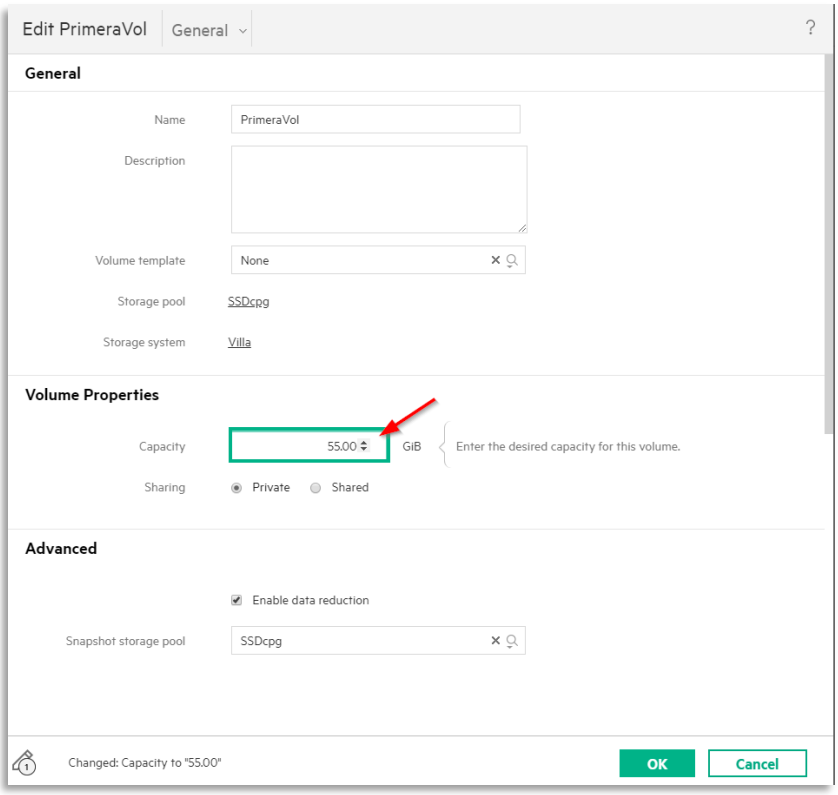
1. Select the *volume* from the menu



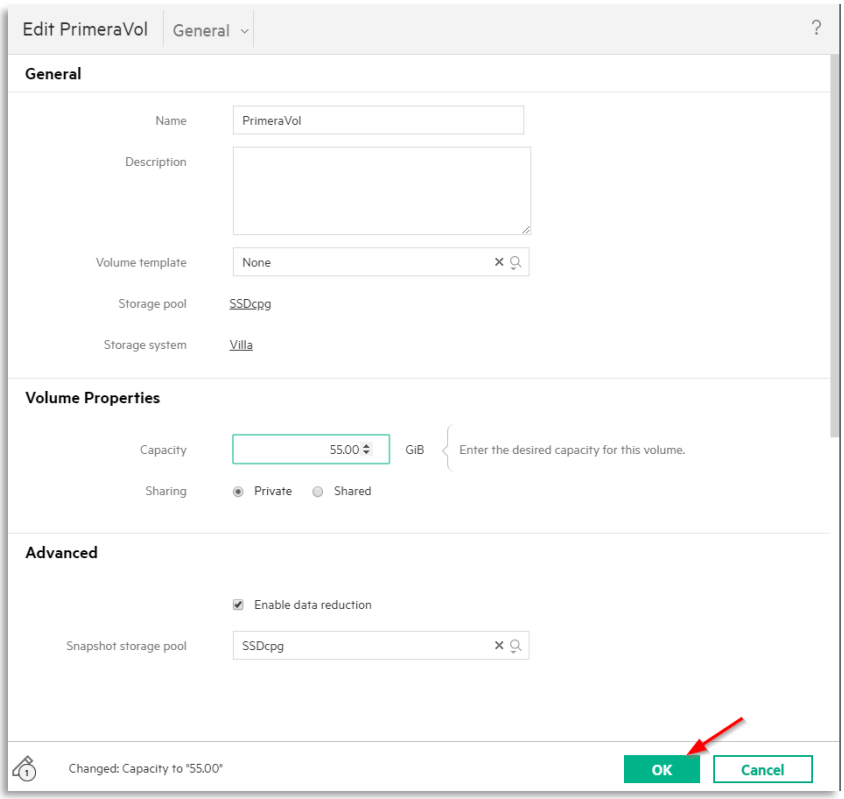
2. Select *Edit* from the actions menu



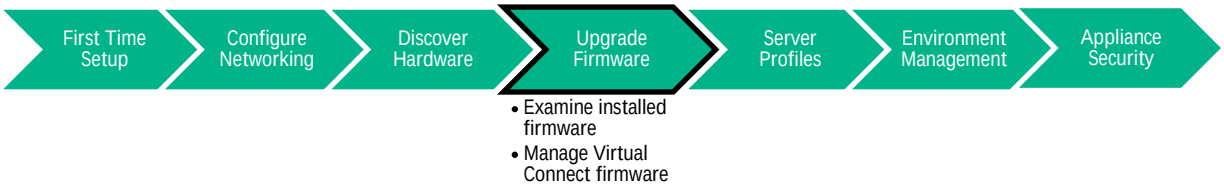
3. In the Edit dialog box, edit the volume *Capacity*



4. Click *OK*.



Upgrade Infrastructure Firmware

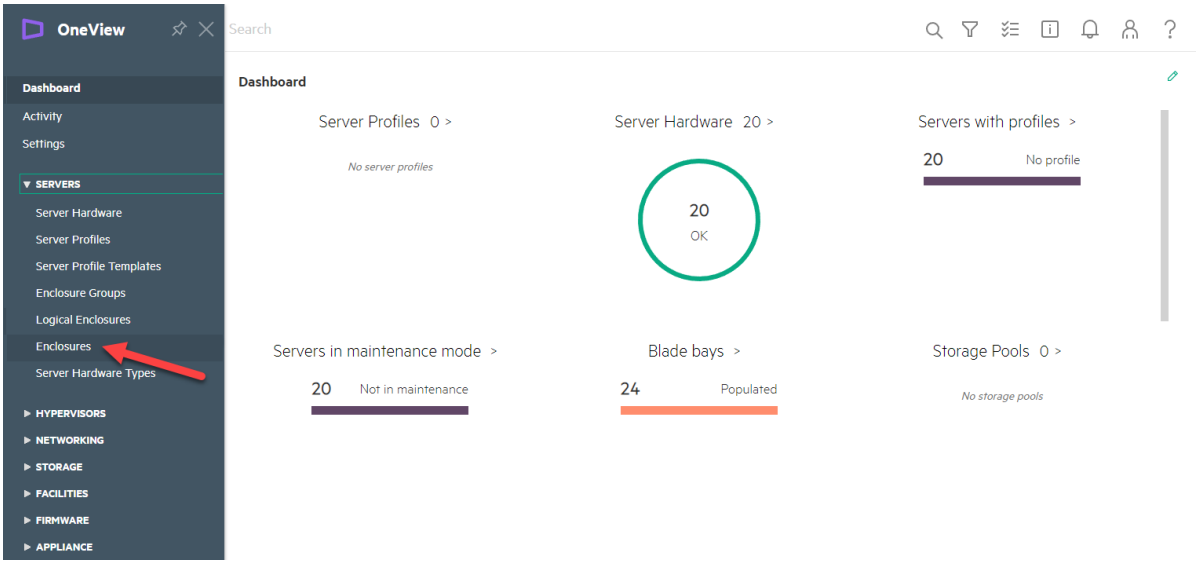


You will examine the firmware status of the discovered Enclosures and Servers.

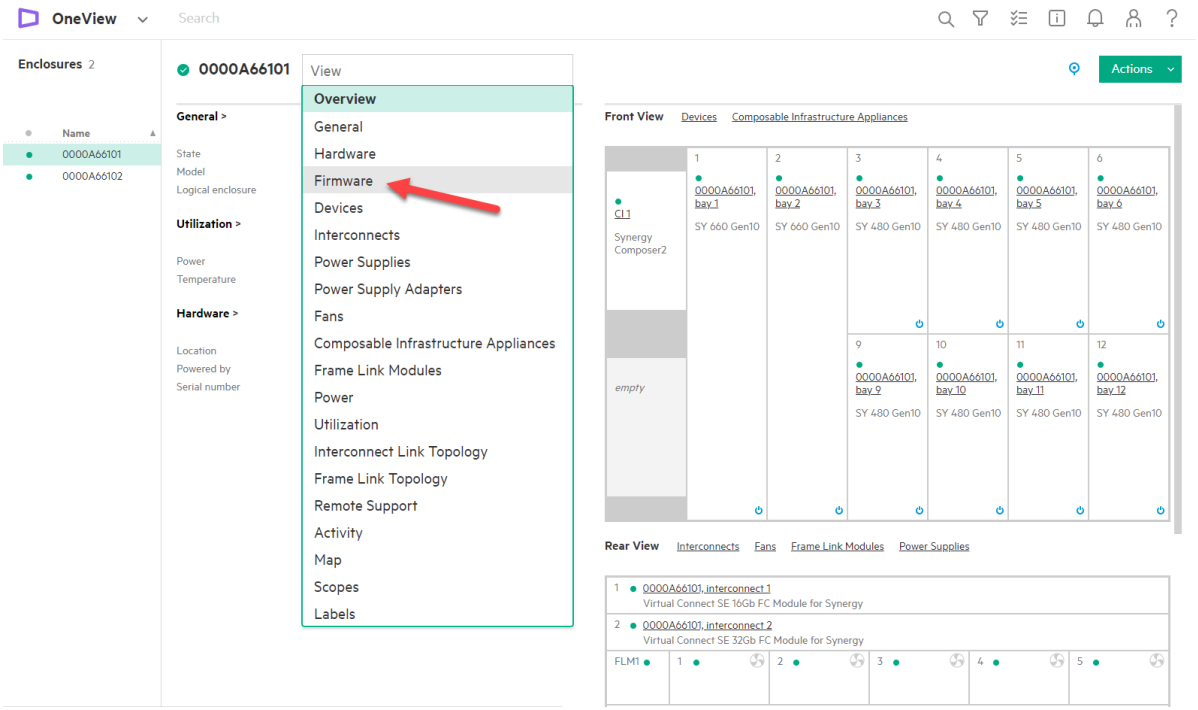
Examine Infrastructure Firmware

The first place to start is with the Enclosure. There is a *Firmware* sub-menu view that you can switch to, which will report the firmware installed.

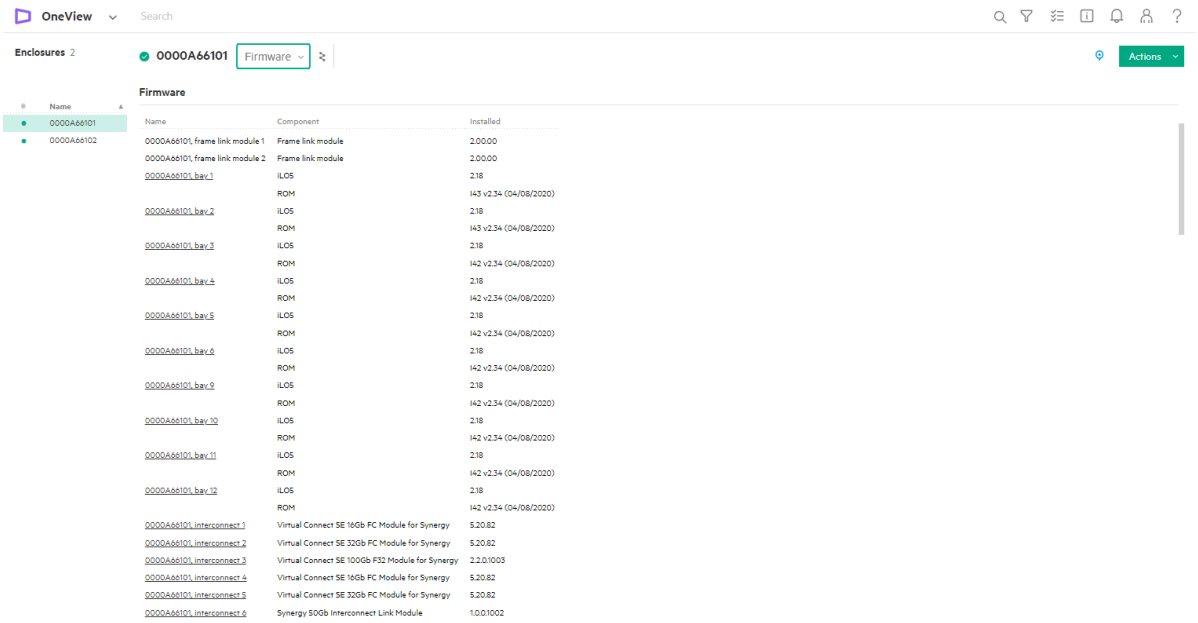
1. From the Top-Level menu, expand the *SERVERS* option and then select *Enclosures*.



2. Select *Firmware* in the submenu.



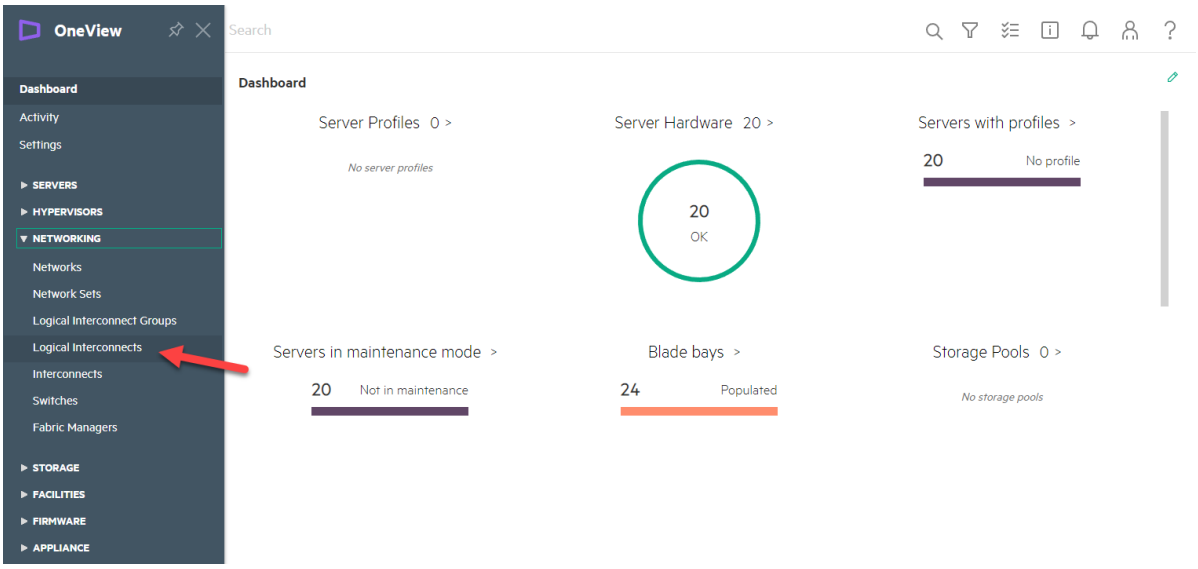
3. Examine what is installed.



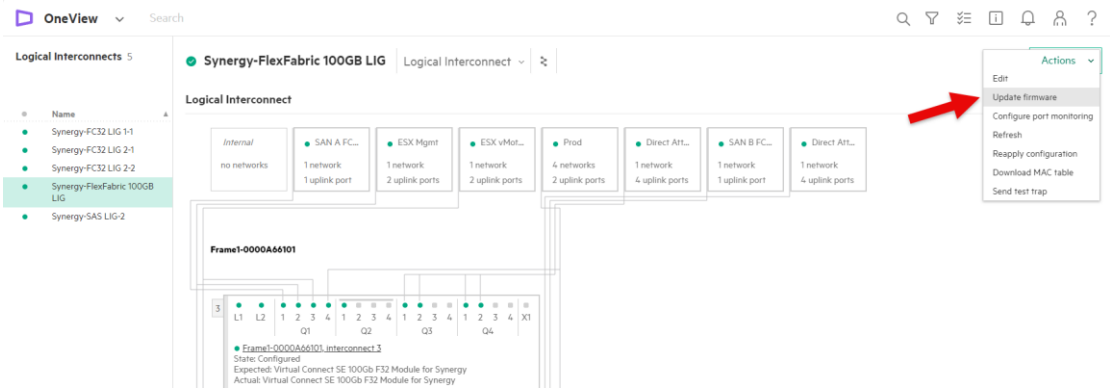
Managing Virtual Connect Firmware

HPE OneView provides the ability to manage Virtual Connect firmware from multiple locations; at the *Logical Interconnect* or *Enclosure* level. Managing Virtual Connect firmware at the *Logical Interconnect* would be used for those times where only VC firmware requiring updating.

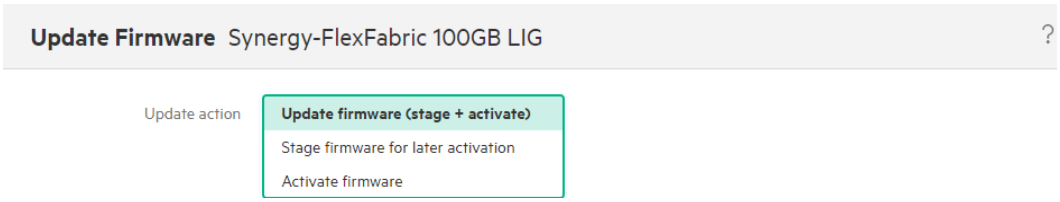
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Logical Interconnects*.



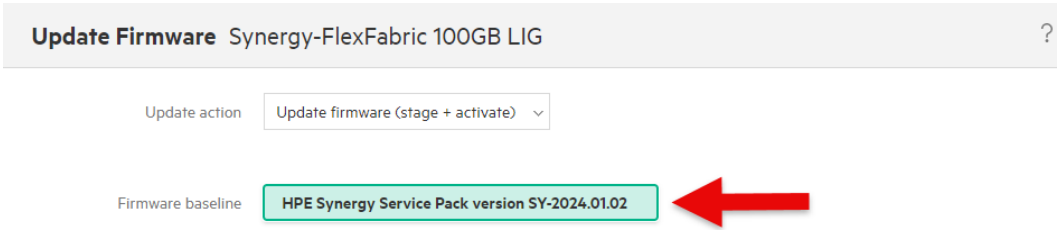
2. In the Logical Interconnects view, choose the Logical Interconnect, then select *Update firmware* from the Actions menu.



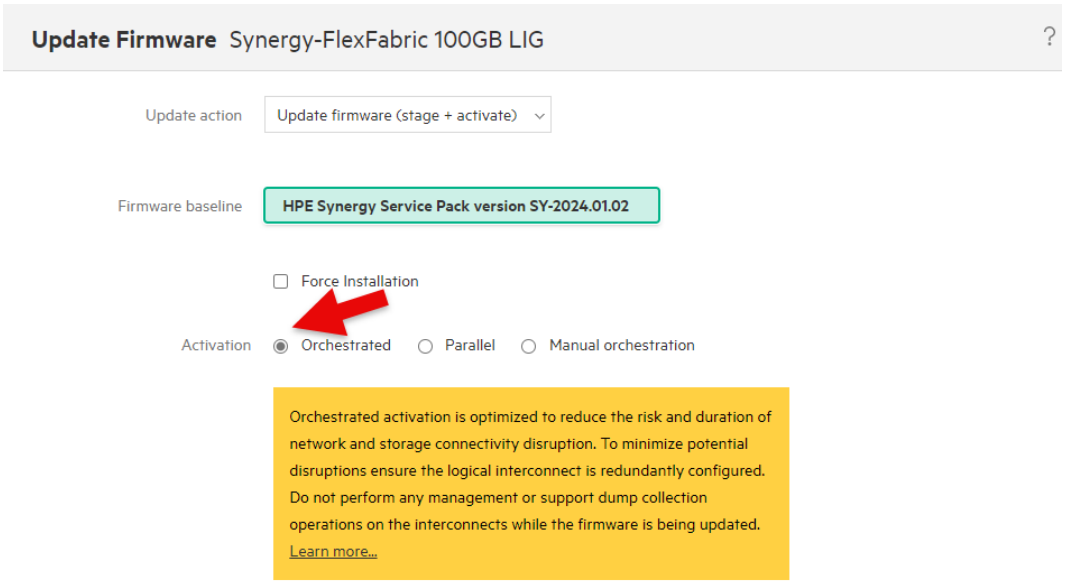
3. On the Update Firmware on Logical Interconnect window, select the update action from the drop-down list



4. Select the *Firmware baseline* from the firmware baseline dropdown list.

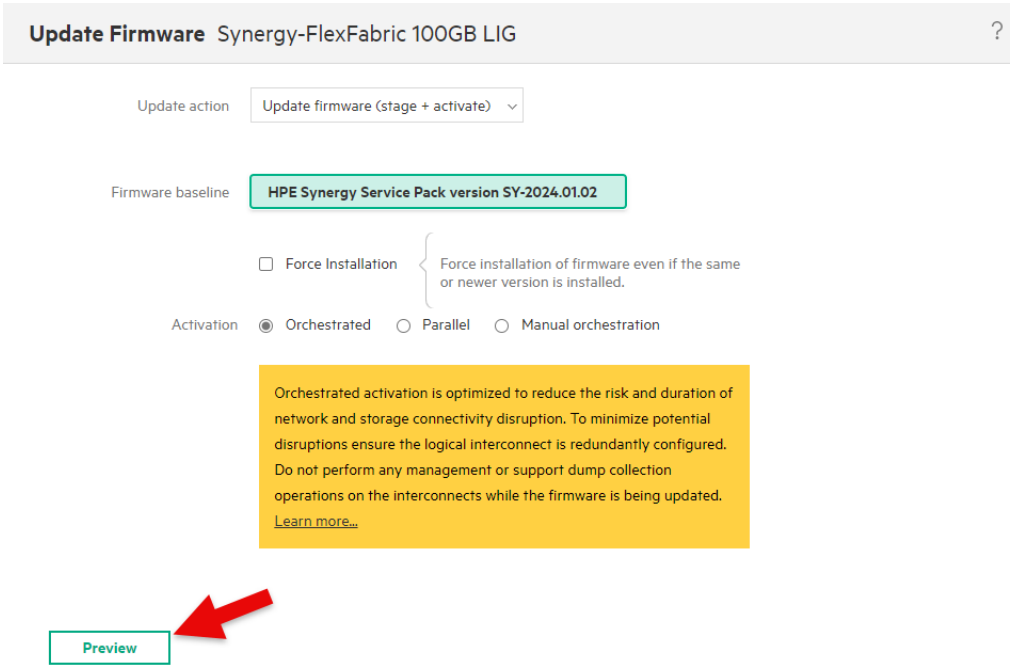


5. Select the Activation method required.

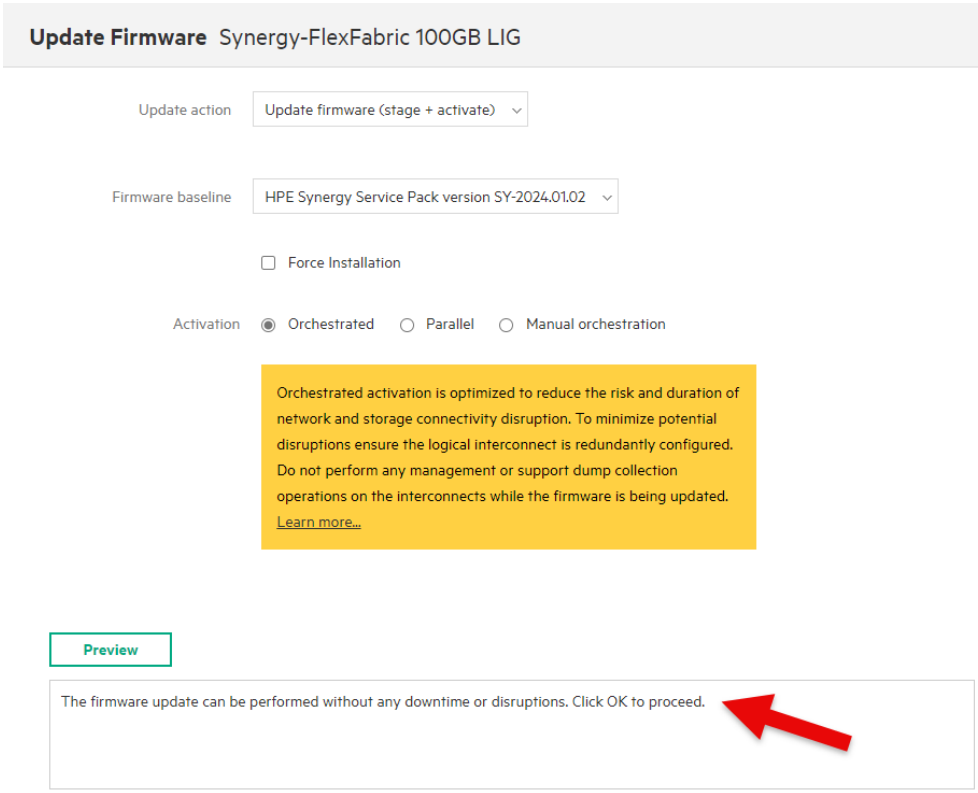


Note:
HPE OneView does not offer the ability to modify Activation order, and each module is activated independently or at the same time (which may cause a network outage). To control potential outages, consider staging and manual activation of Virtual Connect firmware.

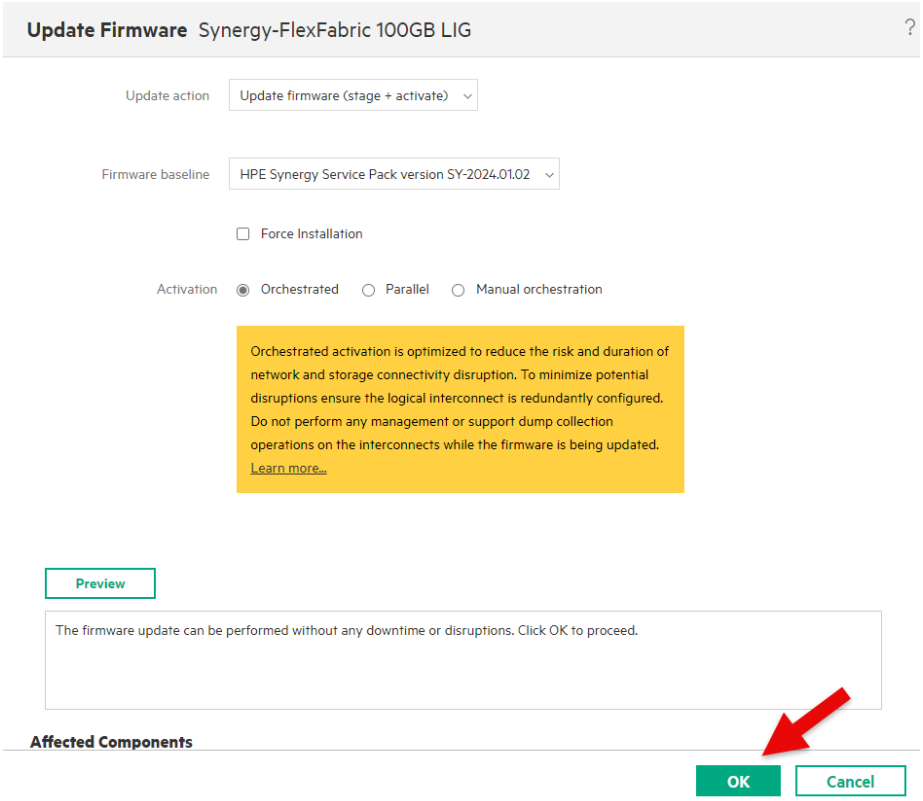
6. You can *Preview* what the upgrade process may affect.



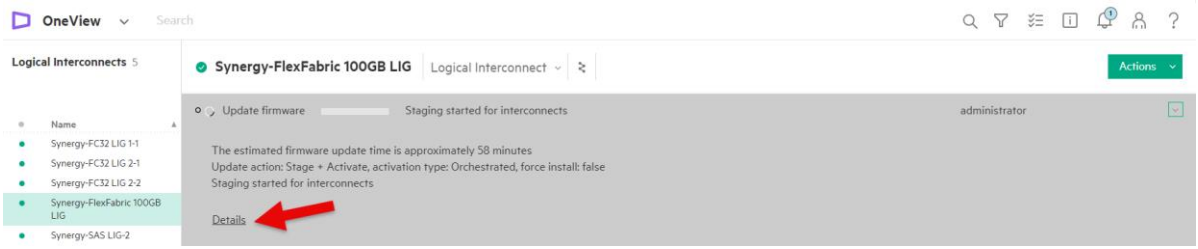
7. This shows that the Firmware upgrade should not cause any outages.



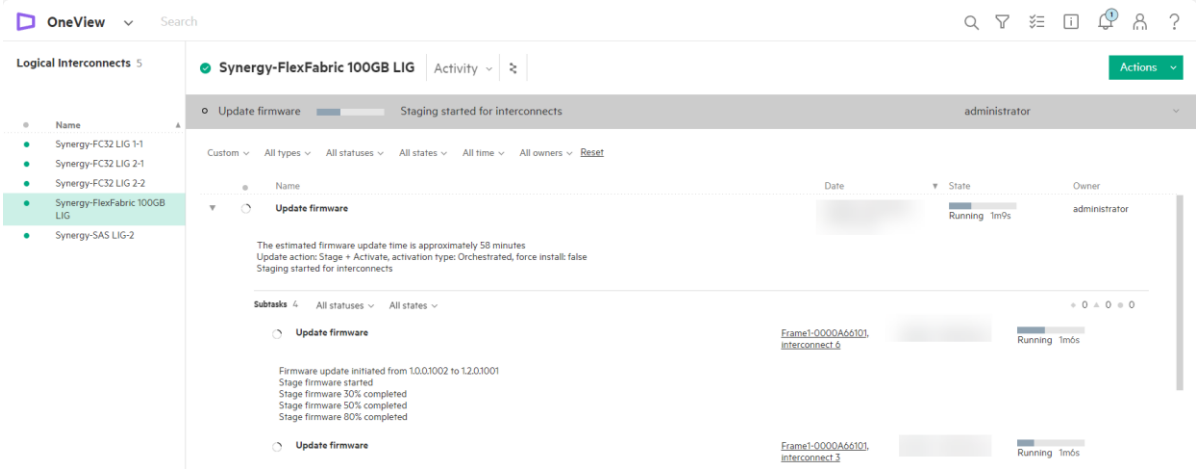
8. When you click *OK* the Firmware update process will begin



9. If you click on the *Details* link then you can look at what is happening



10. The Firmware update process begins and by looking at the Activity screen you can see what is happening.



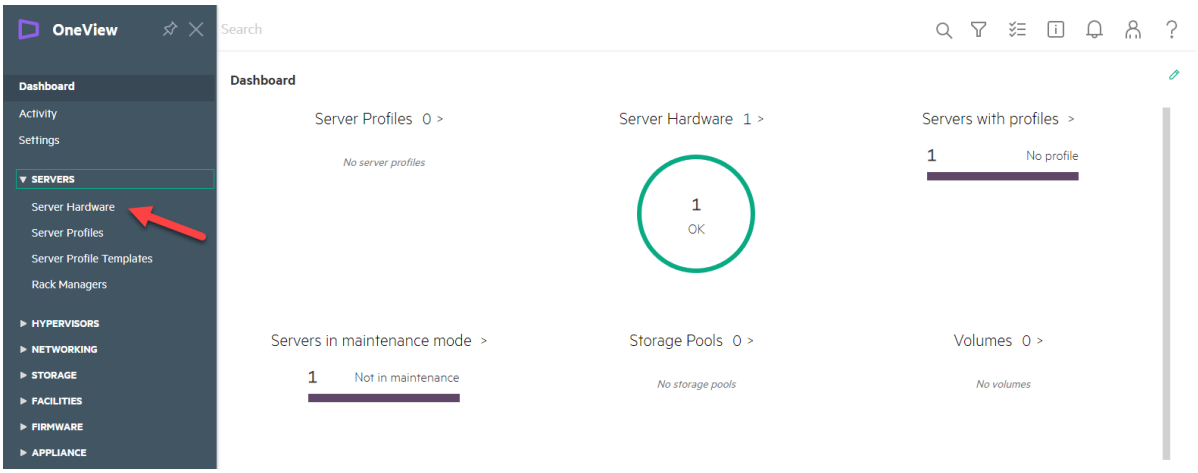
Updating Firmware on a Server without a Server Profile

With the release of HPE OneView 7.2 a new feature (Gen10 or later) has been introduced that allows you to manage / update the firmware for a Server in monitored mode. This feature will allow you to update the Server's firmware if the Server is powered off. OneView will power on the Server and apply the relevant Firmware based on the SPP that you have chosen. If the Server is already powered on, then you will need to power the Server down.

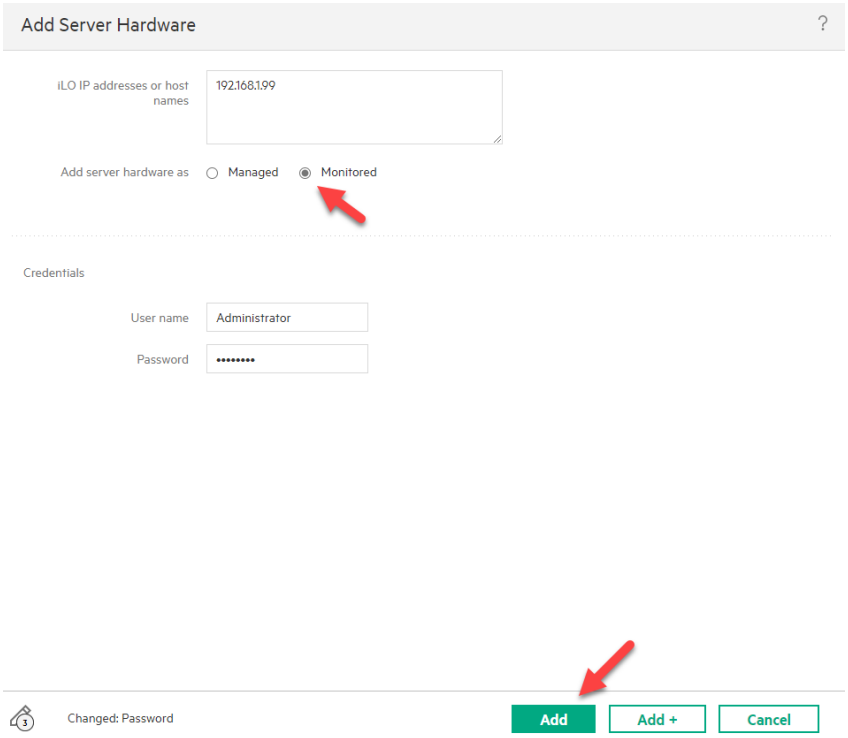
The Server will also need an iLO Advanced license installed to upgrade the firmware. As the upgrade takes place in Monitored mode a OneView license is NOT required.

Import the hardware that you wish to monitor

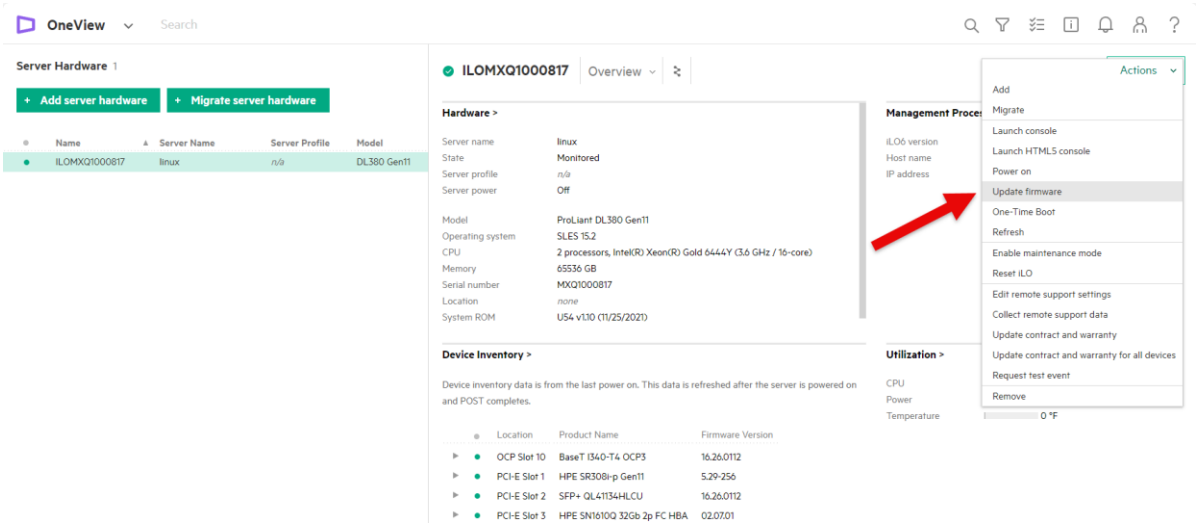
1. From the main menu, expand the *SERVERS* option and then select *Server Hardware*.



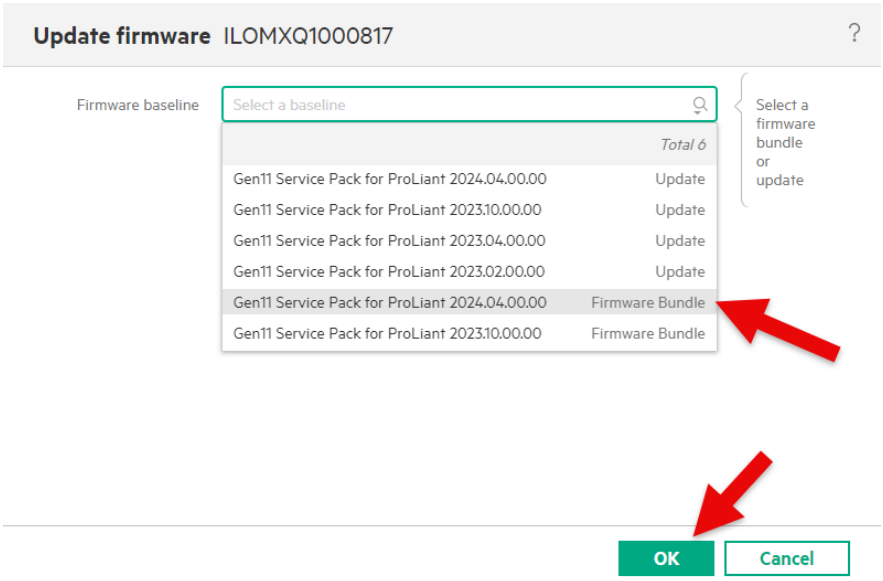
2. Add the iLO address and select *Monitored* and then click on *Add*.



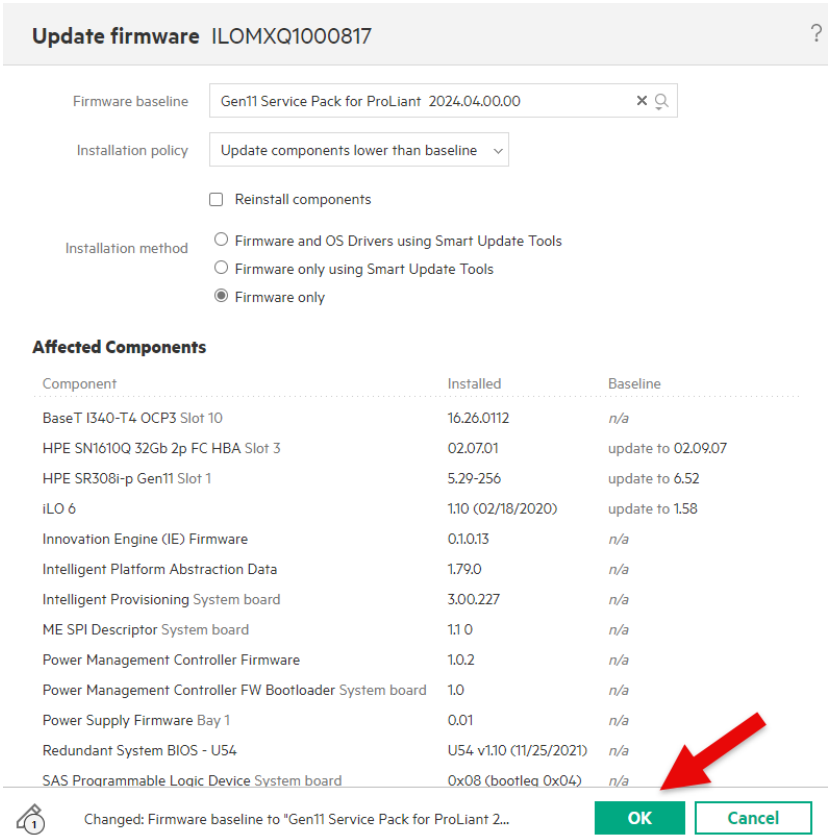
3. Once the hardware is added you can now update the firmware (assuming that the Server Power is off as the update can only happen offline). Click on the *Actions* menu and choose *Update firmware*.



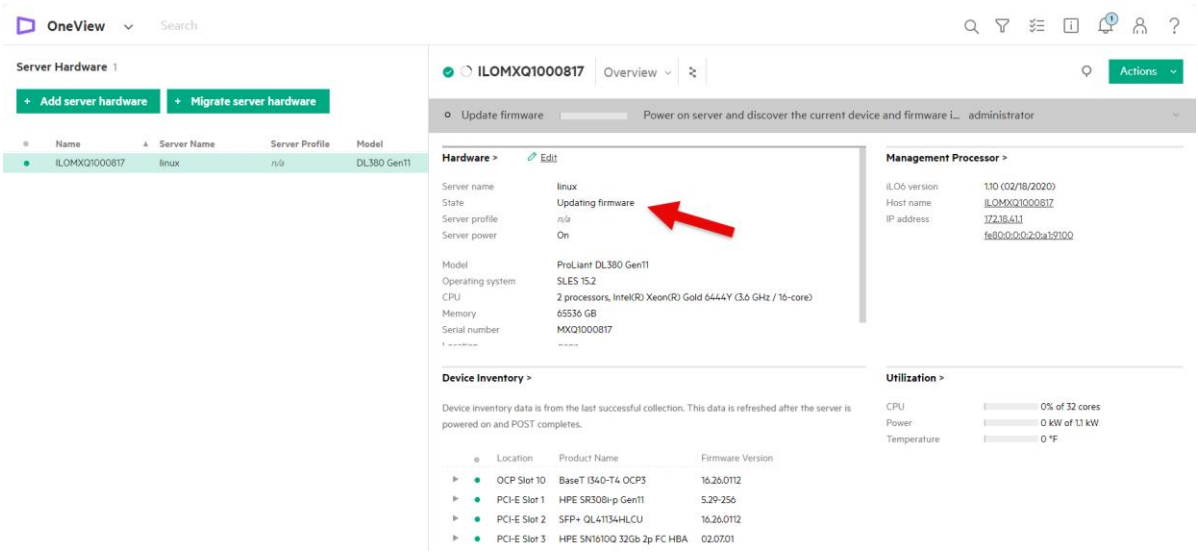
4. Choose the SPP that you want to deploy to the Server you have chosen and click *OK*



5. You are then shown the current firmware and what (if any) will be upgraded based on your selected Firmware baseline. Review and then click *OK* to continue.

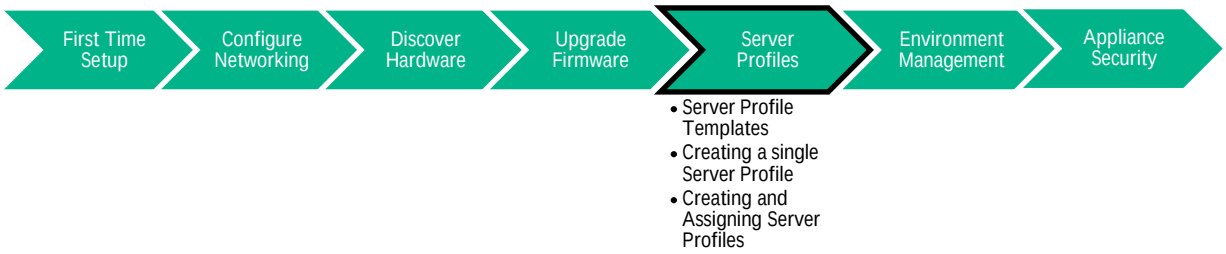


6. The Firmware upgrade will now proceed and when you look at the Server the State changes from Monitored to Updating firmware



7. Once completed the State will change back to Monitored

Creating Server Profiles



Server Profiles are managed resources that specify supported settings for the selected *Server Hardware Type* (e.g. Hardware Platform, Adapter Layout / Network Connections, BIOS Settings) and *Enclosure Group* (e.g. Networks based on *Logical Interconnect*) and can be left *Unassigned* for use as a *Template*. A *Firmware Baseline* (Policy) can be set within the *Server Profile* (for supported platforms), which will automatically update the firmware prior to assigning and configuring the *Server Profile*.

Server Profile Affinity is to provide and control if and when the Server Profile is reapplied to the server hardware during rip-and-replace procedures. When the Server Profile Affinity is set to *Device Bay*, the Server Profile will be reapplied (Connections, BIOS, Boot Order, Firmware, etc.) when any Synergy Compute Module is inserted into the device bay, as long as the Server Hardware Type (SHT) matches the original configured SHT. If the Server Profile Affinity is set to *Device Bay + Server Hardware*, then the Server Profile will only be applied in the event of the same Synergy Compute Module being reinserted into the same Device Bay. When the Server Hardware and its physical Serial Number do not match, the Server Profile will be flagged as Incompatible.

Managing SAN storage within server profiles will automate configuring access from the server to new (on-demand) or existing, private or shared SAN volumes. The Server Administrator can attach 1 or more Volumes to a Server Profile using 1 or more storage paths per volume. When the Server Profile is assigned to a Server, HPE OneView will orchestrate creating new volumes, configuring their presentation to the server (i.e. host, vlun and target port selection) on the HPE 3PAR StoreServ, Alletra, Primera and Nimble storage systems, as well as configuring any required FC Zones for Fabric Attach managed SANs.

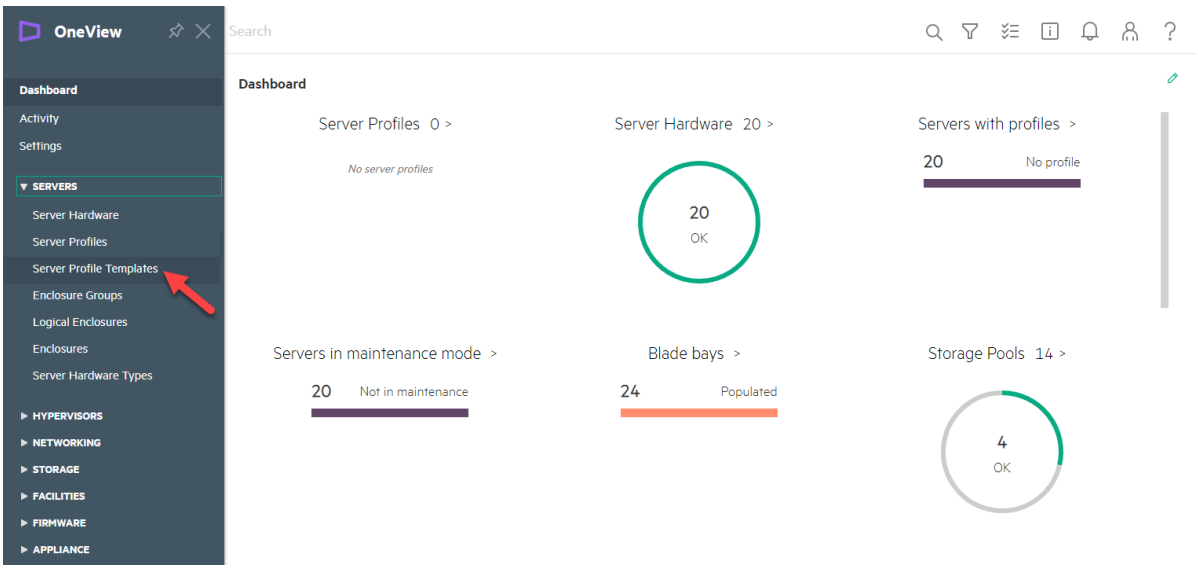
In this section, you will first create a *Server Profile Template* that defines specific elements. The *Server Profile Template* will then be used to create server profile assigned to a *Server Hardware* Device.

Create Server Profile Template

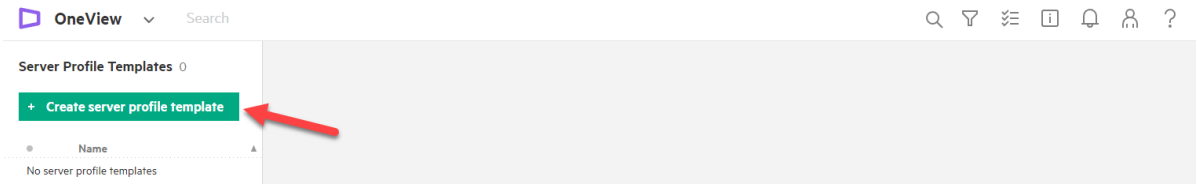
Server Profile Templates provide a powerful way to update and maintain your existing infrastructure. HPE OneView simplifies the one to many styles of update and management of server profiles using templates. This feature adds inheritance to HPE OneView templates where BIOS settings, firmware & driver updates, as well as other functions can be made in the template and then propagated out to the profiles created from that template.

Templates in HPE OneView provide a monitor and flag model. Profiles created from the template are monitored for compliance with the desired configuration. When inconsistencies are detected the profile is flagged as no longer being consistent with the template. So, when a new update is made at the template level, all profiles parented to that template will be flagged as not being consistent. From there, the user has control to bring individual profiles into compliance with the template or multi-select systems for update to the template.

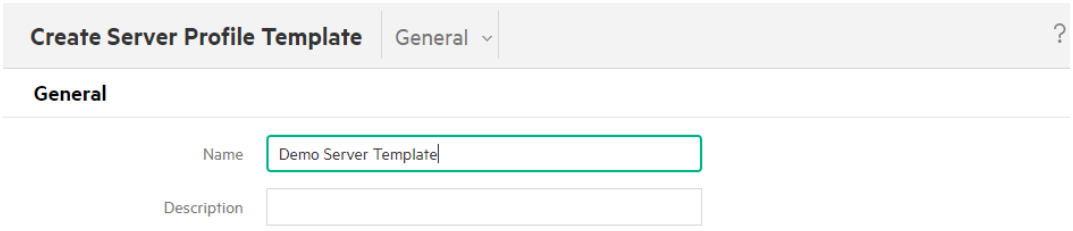
8. From the main menu, expand the *SERVERS* option and then select *Server Profile Templates*.



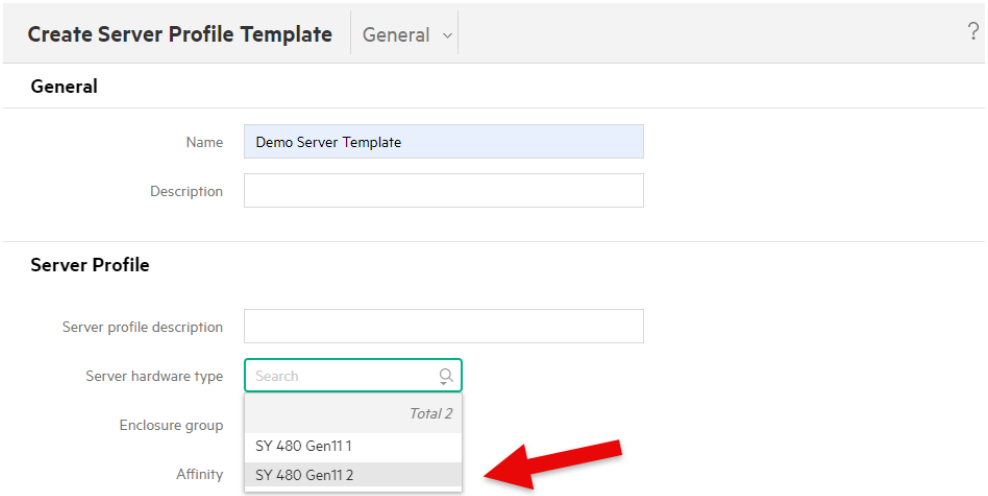
2. Once on the Server Profile Template screen, select the + *Create server profile template* button



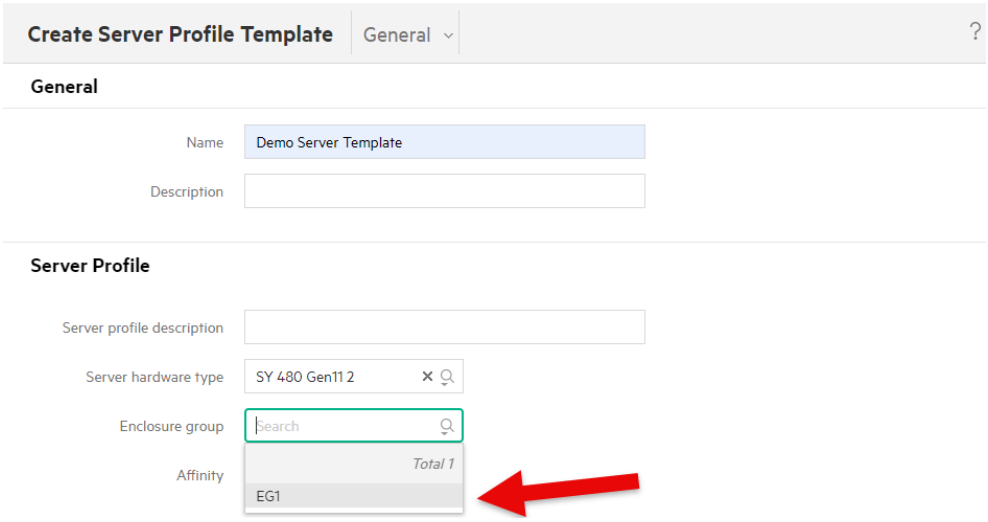
3. In the Server Profile section of the server profile template creation page, enter a *Name* and optionally a *Description* for the server profile template.



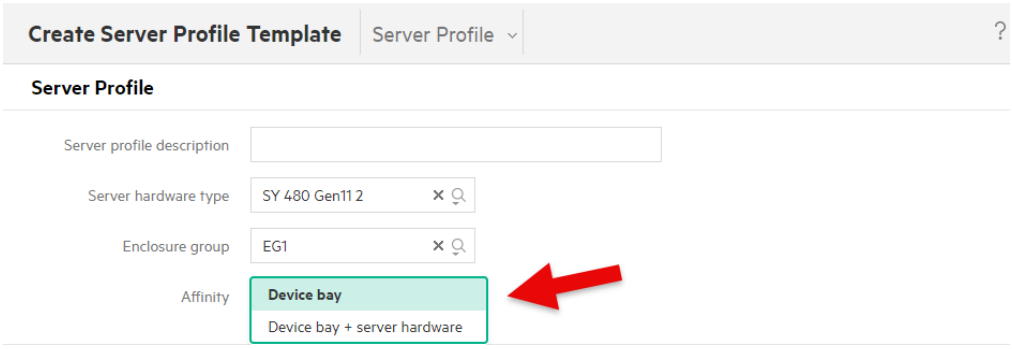
4. Select the *Server hardware type* using the dropdown menu.



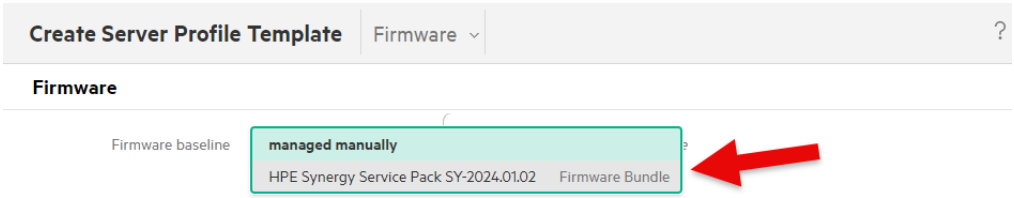
5. Select the *Enclosure group* from the dropdown menu that the server profile template will be associated with.



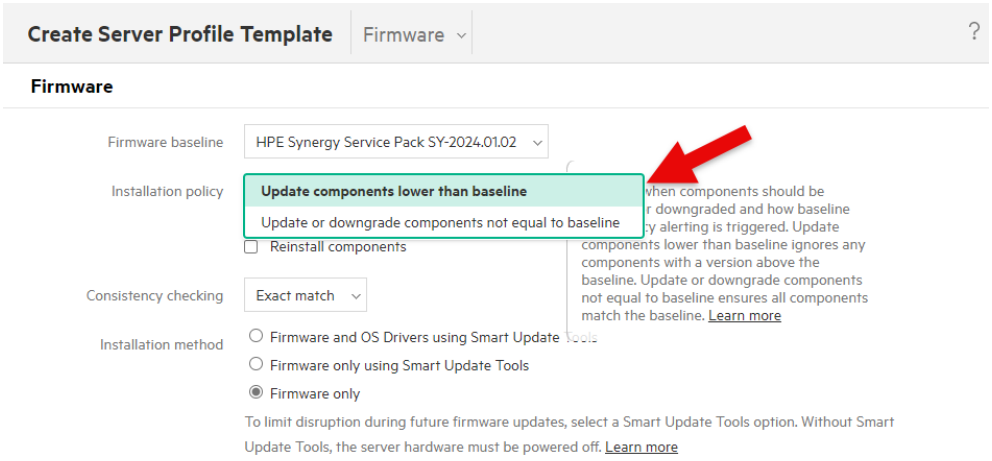
6. Specify the Server *Affinity* method you'd like to configure.



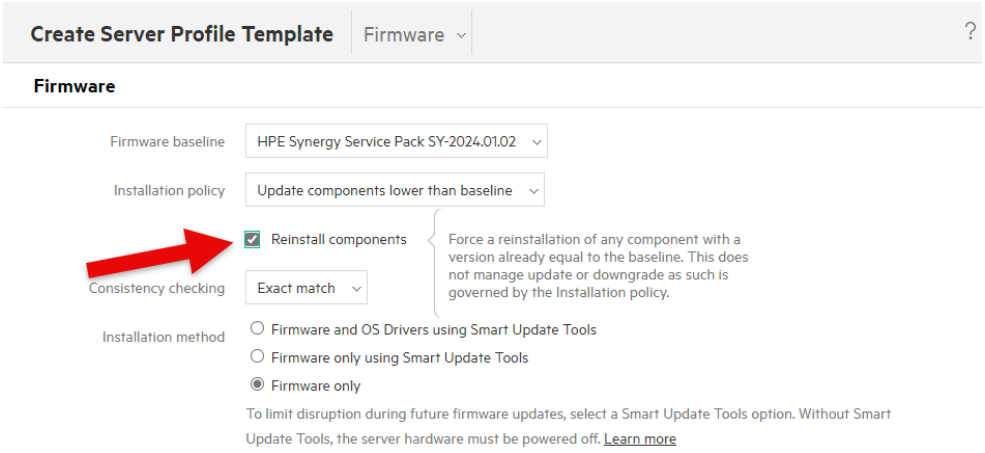
7. In the firmware section of the server profile template creation page, select a *Firmware baseline* from the dropdown menu.



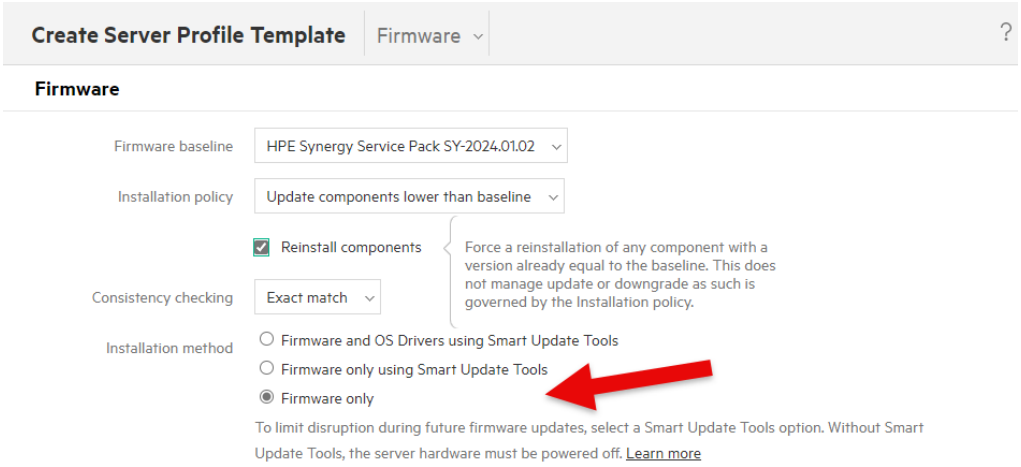
8. Now that the baseline has been selected you now options for the installation policy. Depending on what you choose for this policy will determine how the firmware will be applied. The default is to update everything that is lower than the selected baseline.



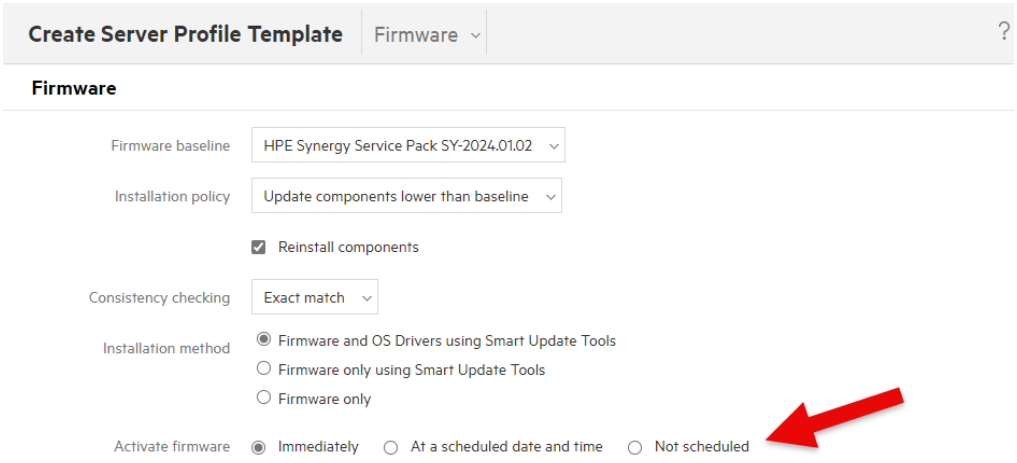
9. If you select *Reinstall components* all firmware from the baseline will be applied regardless if it is the lower, same or later to match baseline.



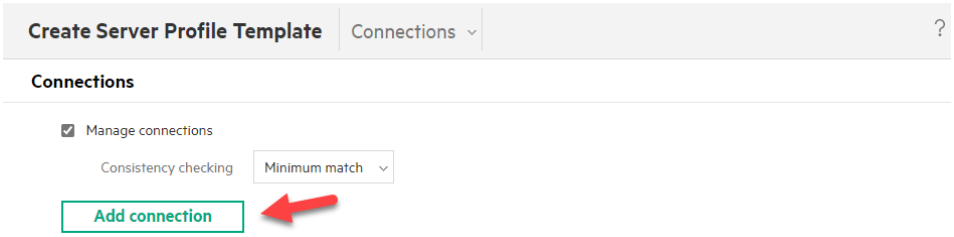
10. Once a baseline is selected, choose how the baseline will be applied to the servers used within this server profile template. If either of the options using the HPE Smart Update Tools is selected then the firmware or driver updates will be done while the systems are online (this assumes that an OS has already been deployed to the Server previously). If the firmware *only* option is selected then the firmware will be updated offline using Intelligent Provisioning.



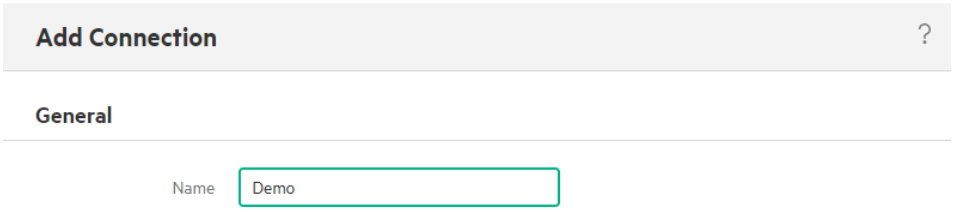
11. Select when the firmware updates will be deployed for this server profile template (only shown when Smart Update Tools options are chosen).



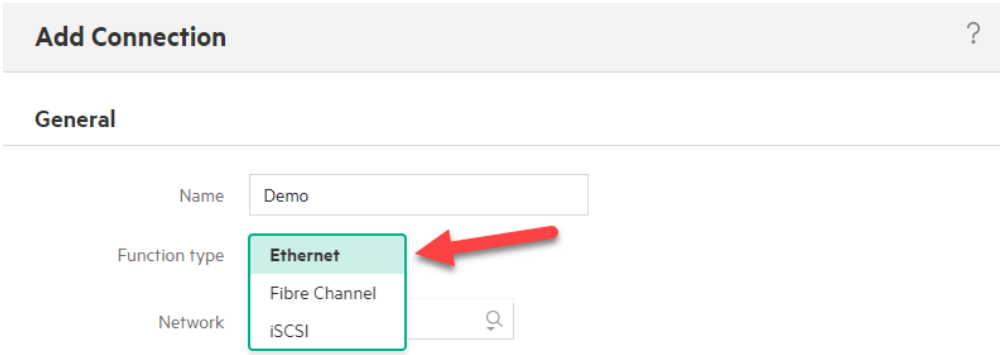
12. In the connections section of the server profile template creation page, click *Add connection*.



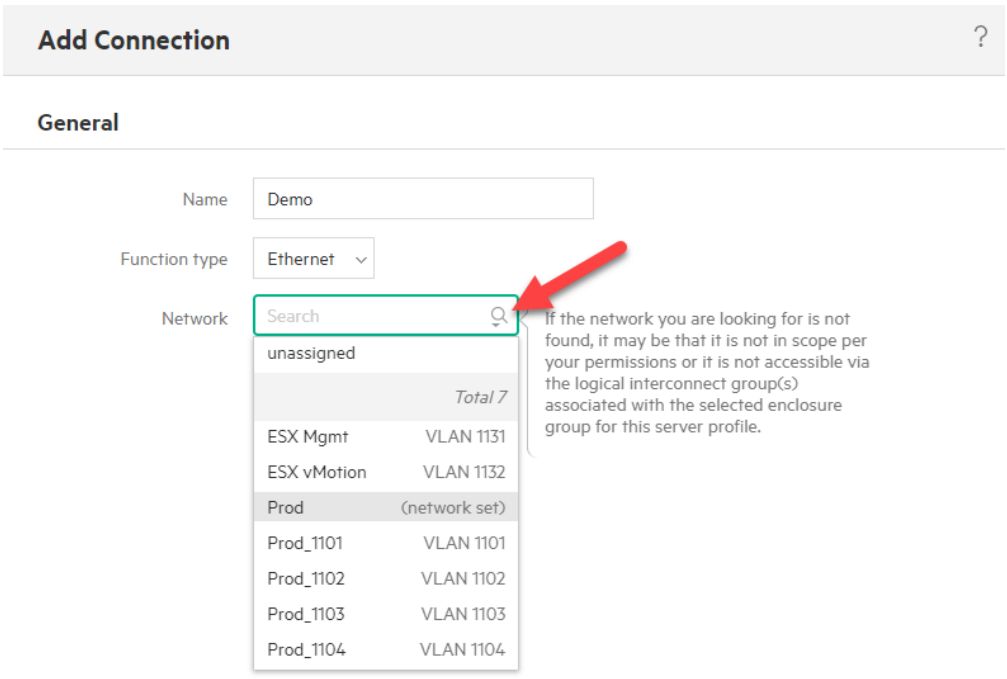
13. In the Add Connection dialog window, enter a *Name* for the connection



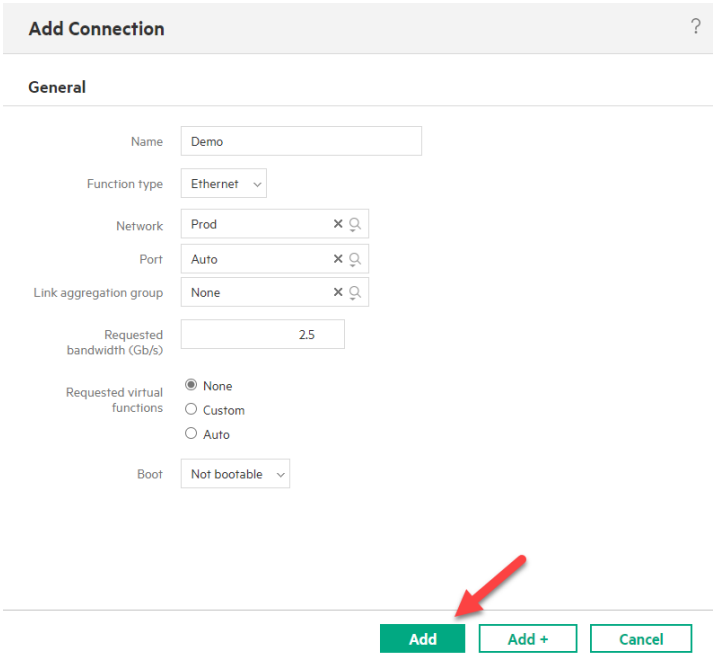
14. Using the dropdown list select the function type for the connection



15. Select the Network or Network Set to be associated with the function using the Network dropdown list



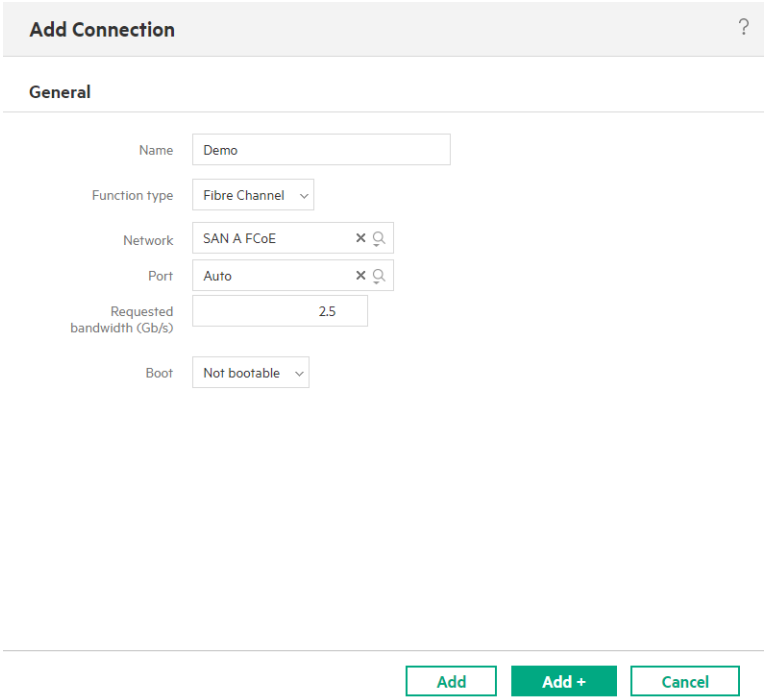
16. Click the *Add* to close the Add Connection dialog window or *Add+* button to continue adding Network Connections to the Server Profile.



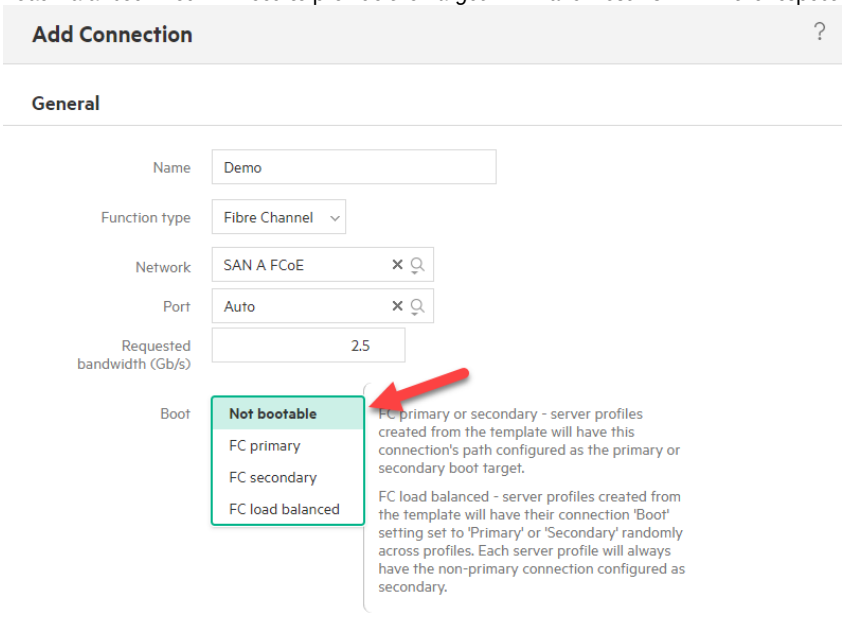
Note:
The Use user-specified IDs is for those customers that wish to provide their own MAC or WWN address for that connection.

Note:
You can specify which FlexNIC to assign the Network Connection to or leave it at the default of Auto. Auto will apply the same Network Connection to Adapter mapping Virtual Connect does today. Do know that you cannot create a FlexNIC B, C or D without first creating FlexNIC A.

17. (Optional) Adding *Fibre Channel Networks* is a similar operation as an Ethernet Device Type. FlexNIC B is reserved for FC Connections when FC Connection Types are added to the *Server Profile*. When choosing the FlexNIC, you can leave the default *Auto*. You can force the FlexNIC assignment, but the list will be filtered based on the connection location to the Interconnect Bay the FC Network is assigned to.

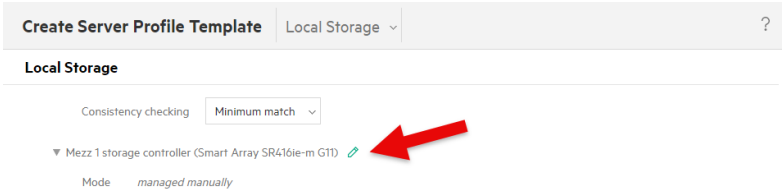


(Optional) If you wish to configure FC Boot From SAN (BFS), change the Boot setting from Not Bootable to either *FC Primary*, FC *Secondary or FC Load Balanced*. You will need to provide the *Target WWN* and *Host LUN ID* in the respective fields.

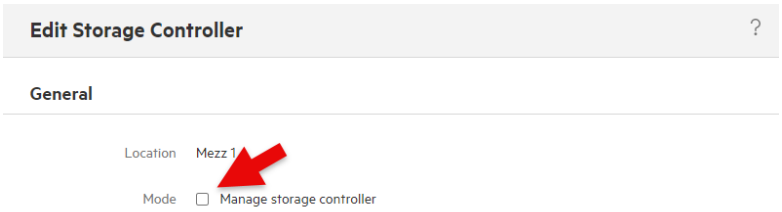


18. If desired, enable local storage management by editing the edit option.

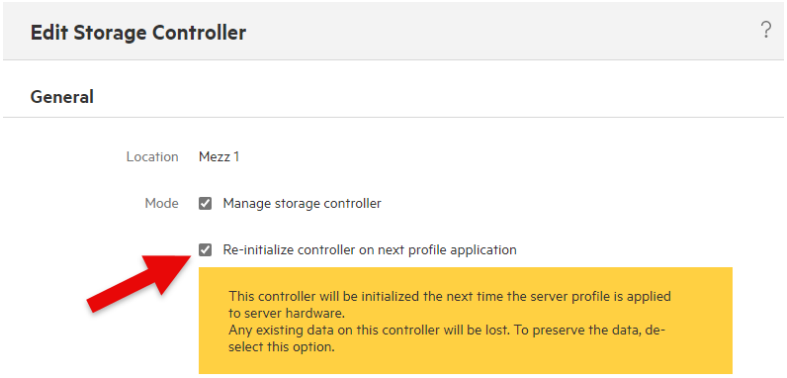
Note: *This will be different depending on the generation of the server due to different SMART Array Controller configs. The following is for a Gen11 Server.*



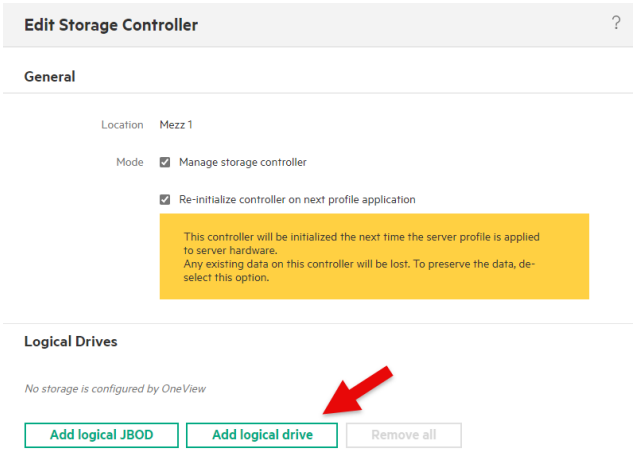
19. Select the *Slot 0 embedded storage controller*



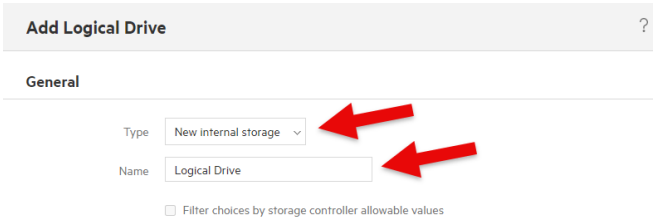
20. Enable or disable the option to Re-initialize controller on next profile application. A warning is shown about this option.



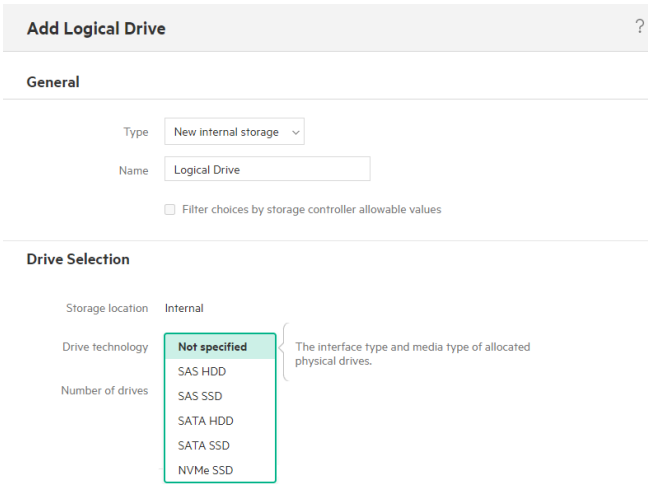
21. Click *Add logical drive*



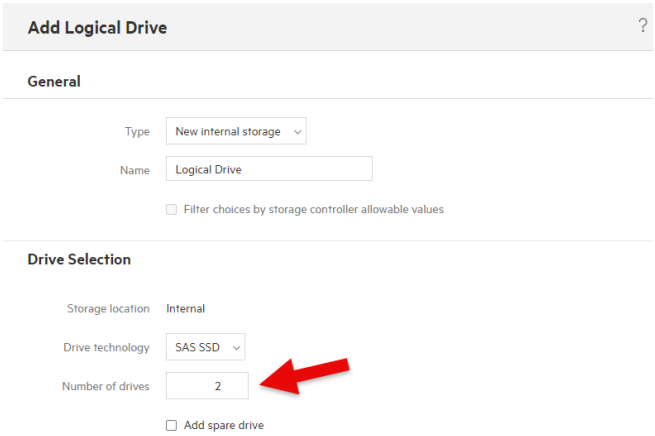
22. Choose whether the Storage is *internal* or *external* and in the Add Logical Drive dialog window, enter a *Name* for the logical drive



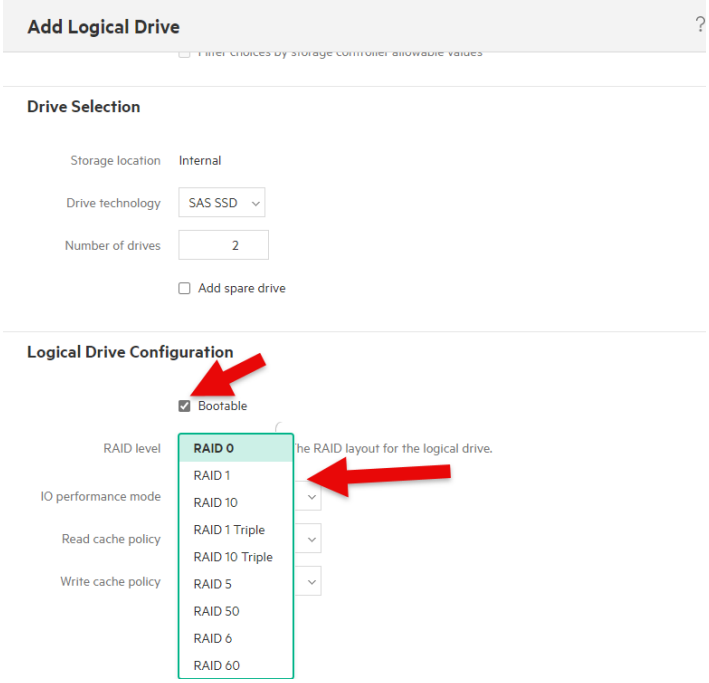
23. Select the *drive technology* for the logical drive



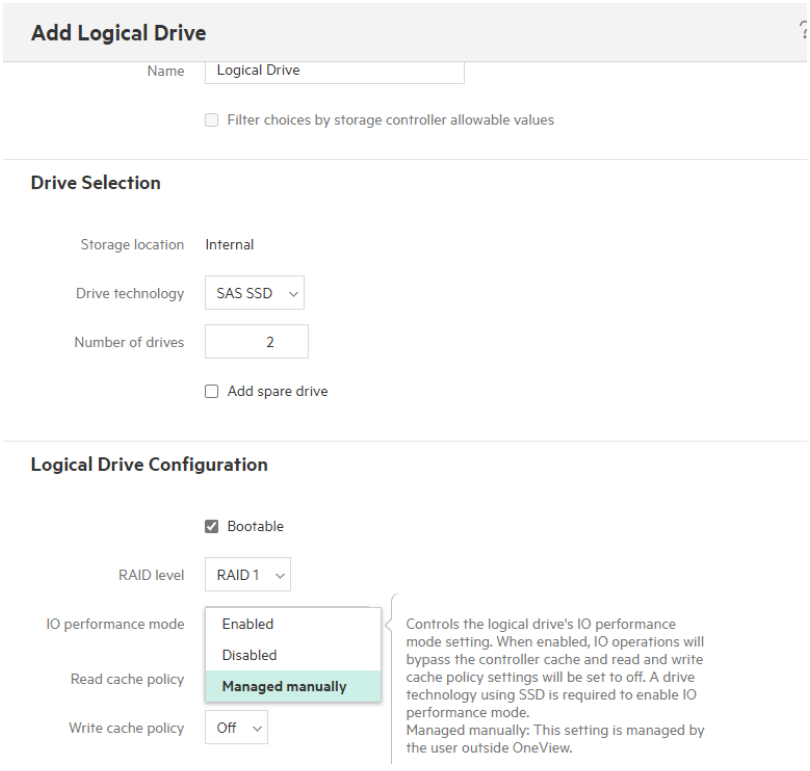
24. Depending on the server and RAID type you can set the *number of drives* for a RAID set.



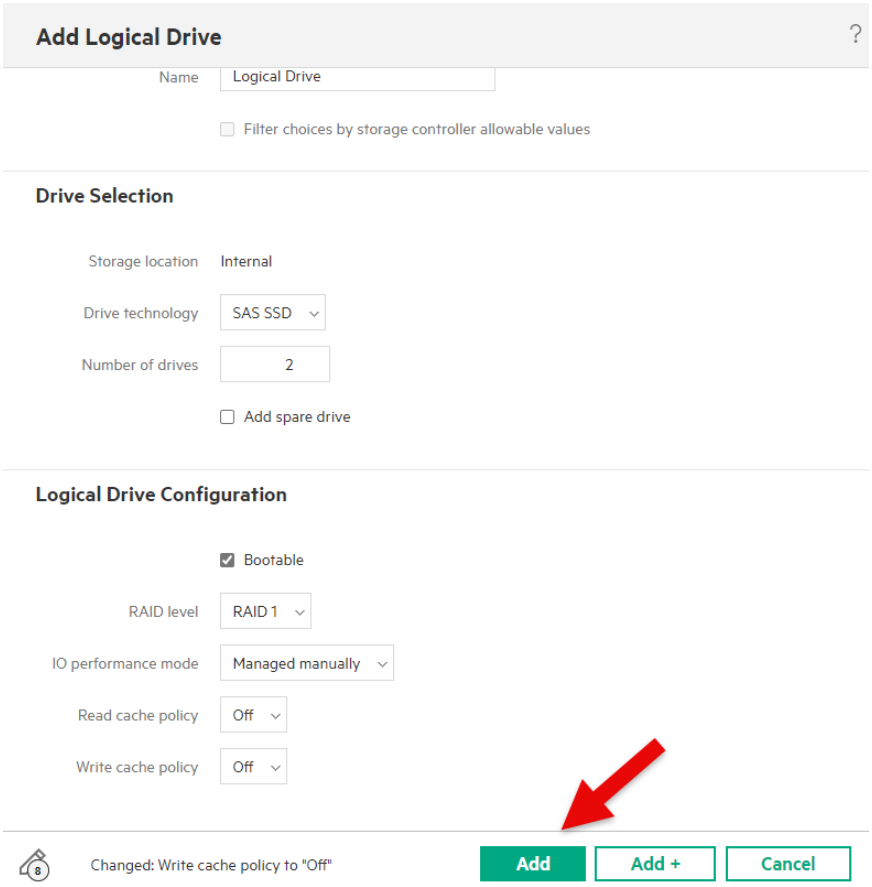
25. Select the *RAID level* and if this is a boot drive then click the *Bootable* box



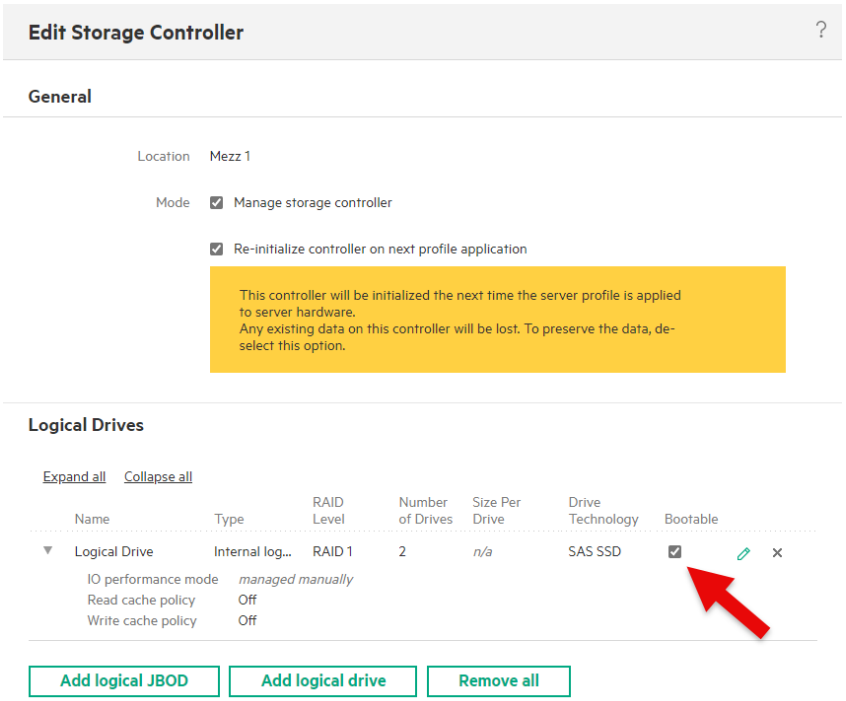
26. You can select how the Smart Array Accelerator is configured by clicking on the *IO performance mode*, *Read cache and Write cache policy* menus.



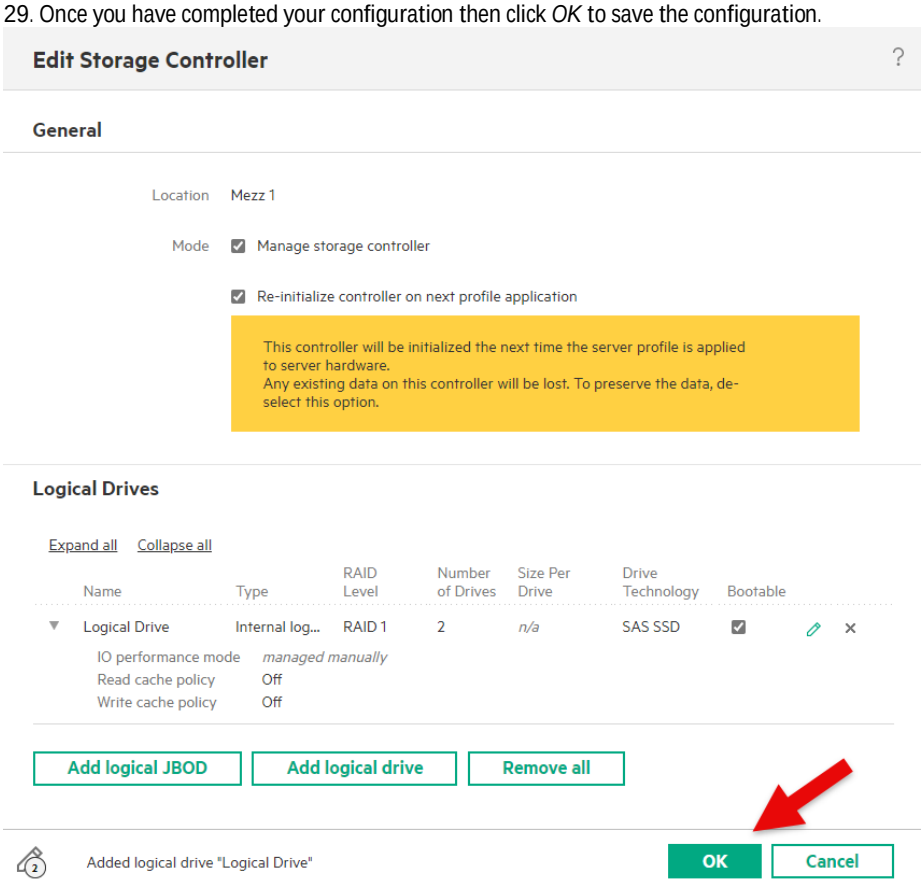
27. When you are satisfied with your choices then click *Add or Add+* to create the logical drive for the server profile template.



28. Now that all your logical drives have been created you have the option to select or change the Boot drive.



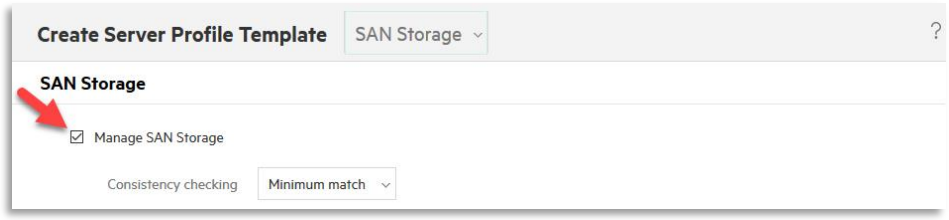
29. Once you have completed your configuration then click *OK* to save the configuration.



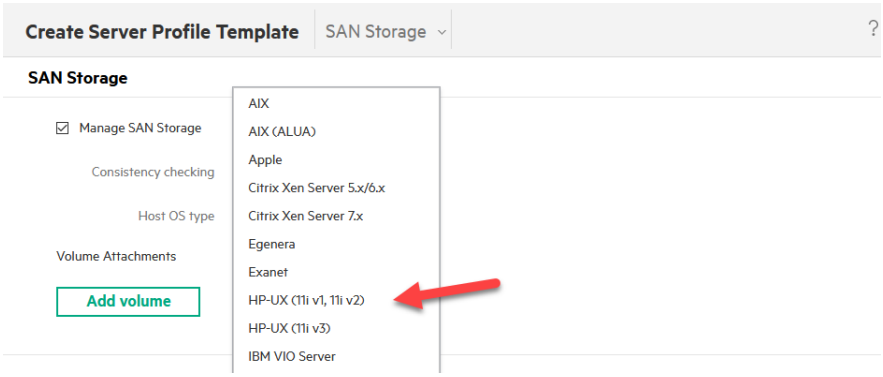
Note: *The Smart Array Accelerator is backed by a battery in the event of power failure. If you enable the drive "write cache" there is no protection for the data in the "drive write cache" in the event of a power outage on the server.*

30. Enable *SAN Storage* if necessary.

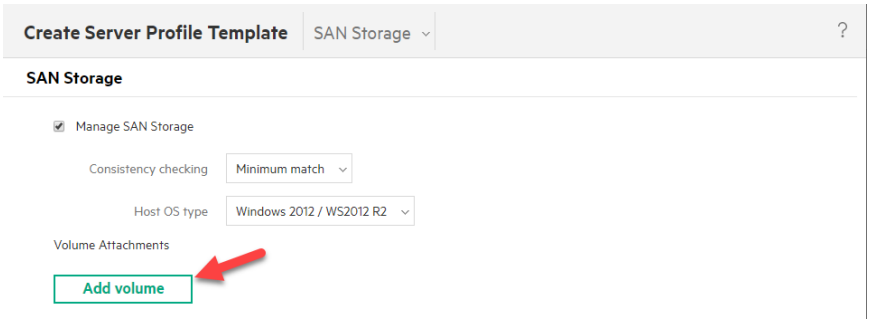
A. Check the box for *Manage SAN Storage*



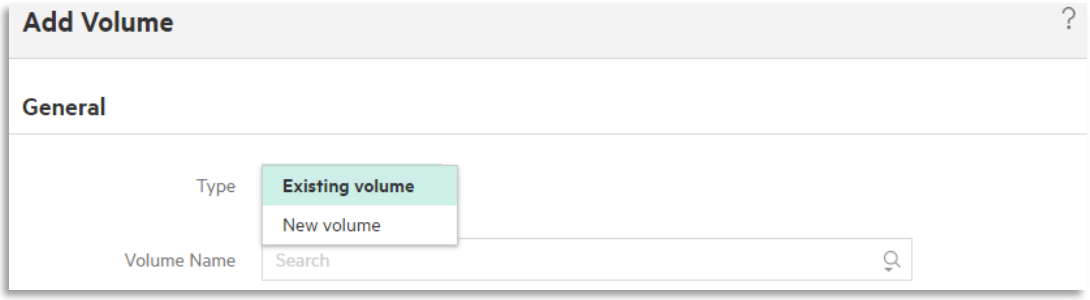
B. Specify the *Host OS type*, which controls the Host created on the 3PAR storage system.



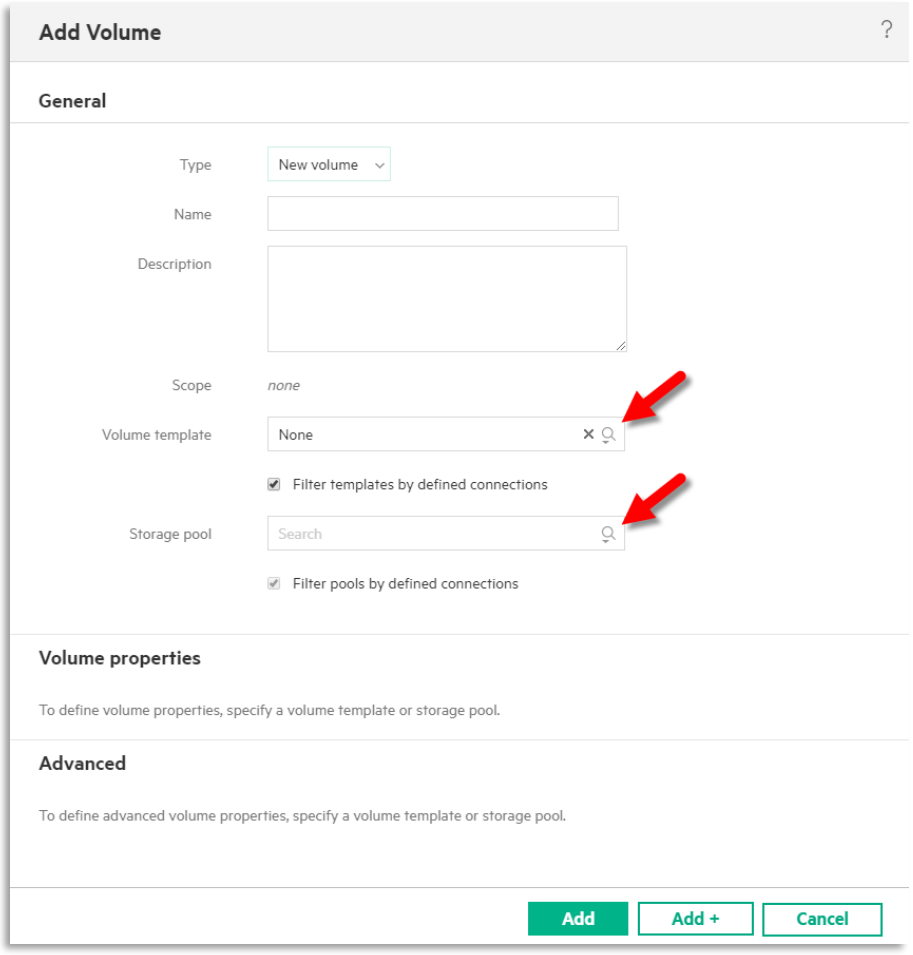
C. Click the *Add volume* button to display the list of volumes available for assignment.



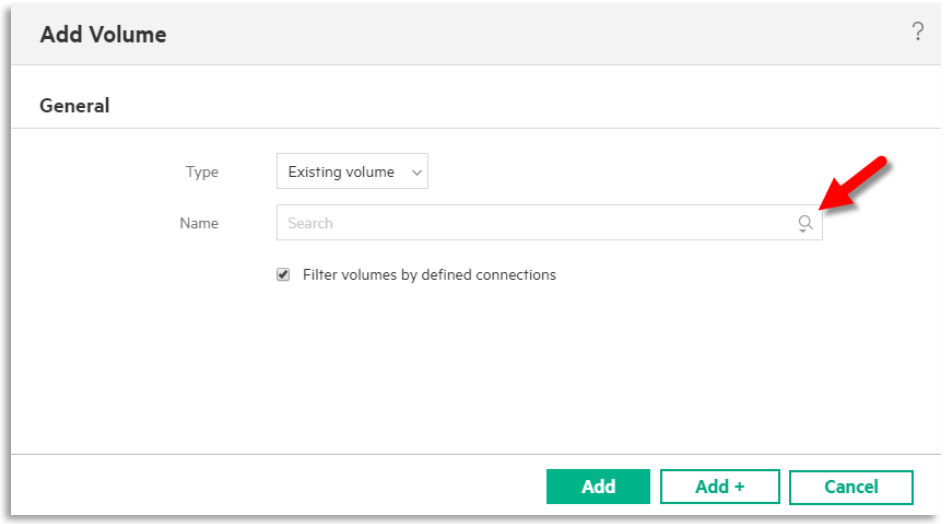
D. In the Add Volume dialog window, select Volume *Type* from the drop down list



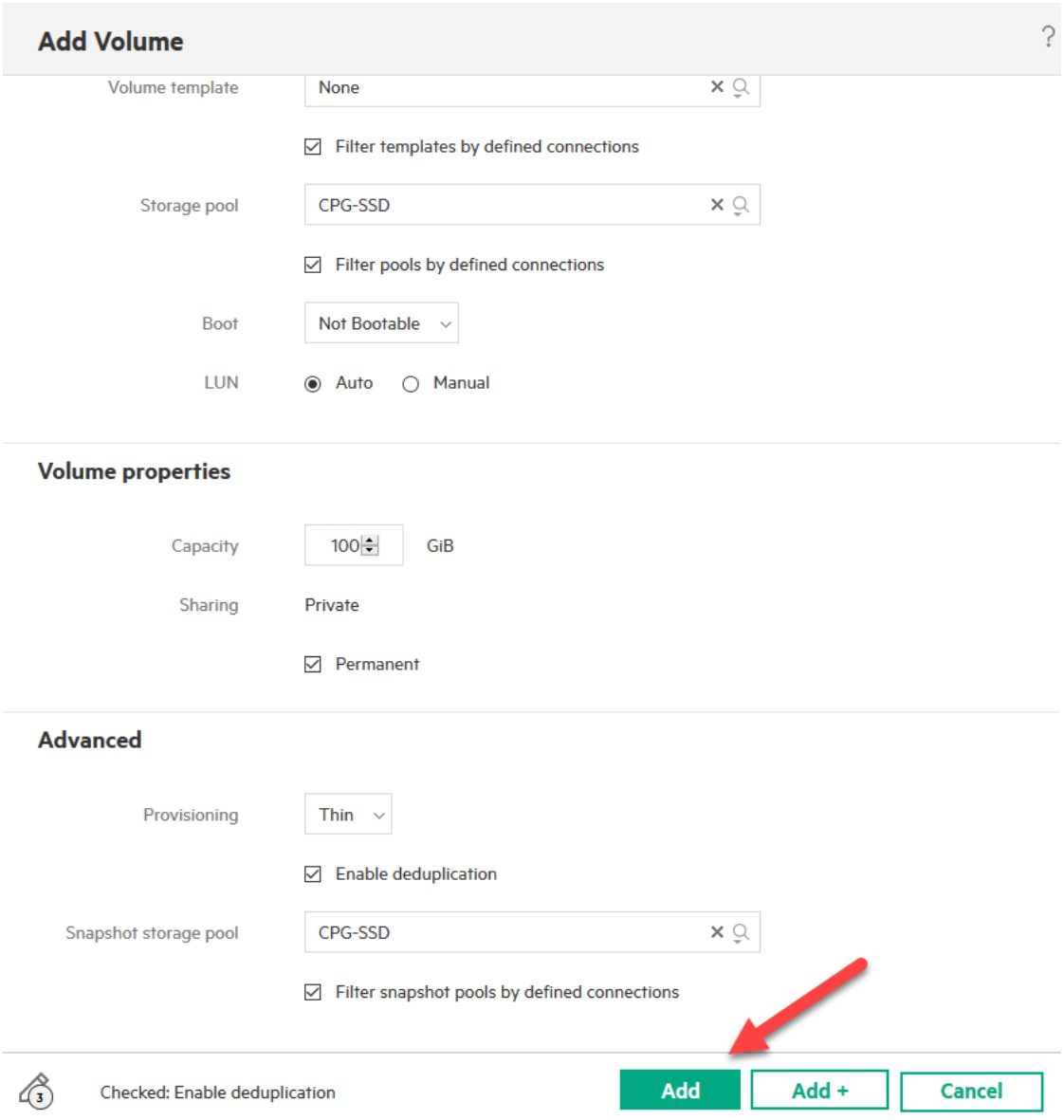
E. If creating a new volume, create the volume to the desired specifications. New volumes can be created from a volume template or directly from a storage pool. After selecting a template or pool, the volume properties supported by the selected storage pool will be displayed.



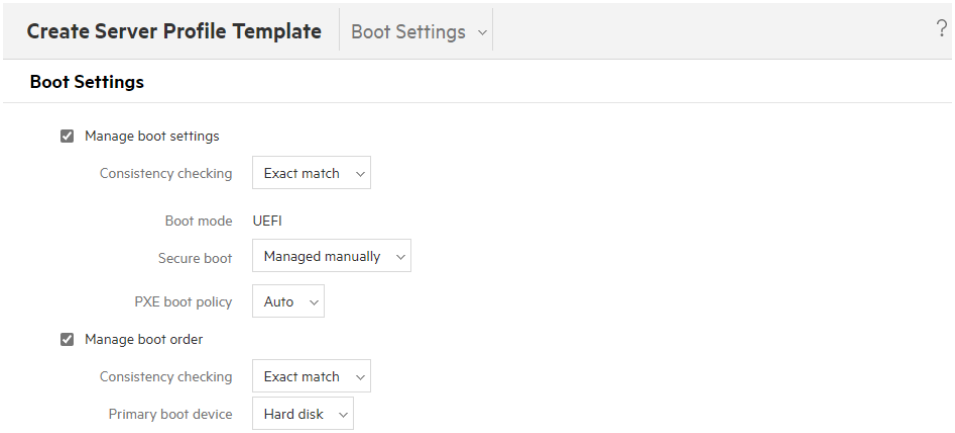
F. If using an existing volume select the Volume using the dropdown list or the SmartSearch feature.



G. Once the *Volume* has been configured, the available Storage Paths will be displayed. You can disable, remove or add Storage Paths. Click *Add or Add +* to add the volume.



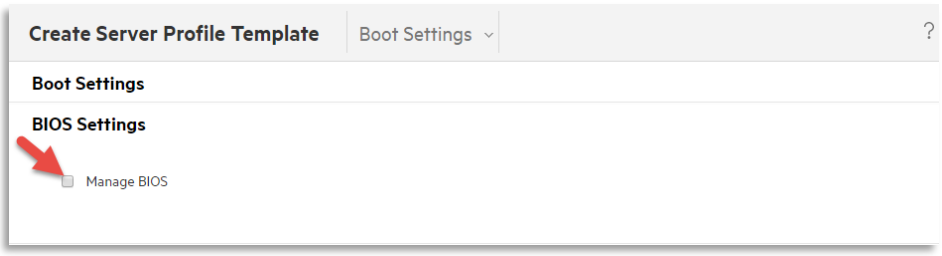
31. In the Boot Settings section, you can set the *Manage Boot settings* and set *Secure boot* to *Enabled* or *Disabled*



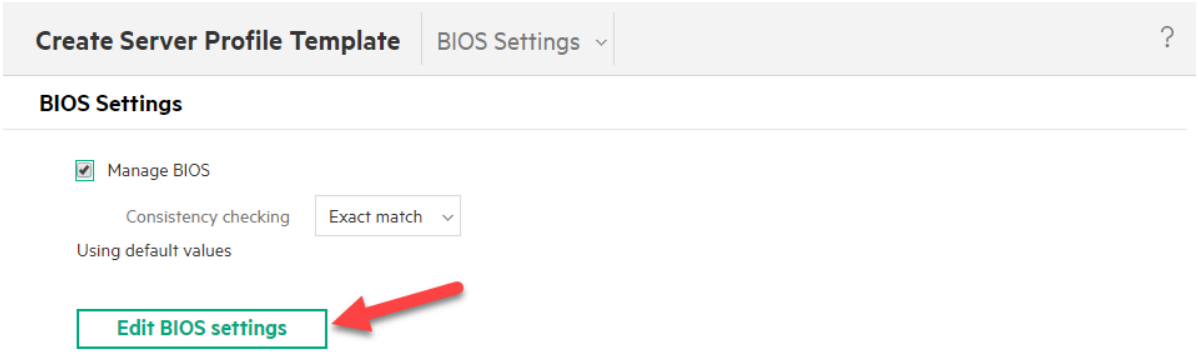
Warning
Disabling *Boot Order* in the Server Profile will also disable PXE and FC BfS configuration options.

---

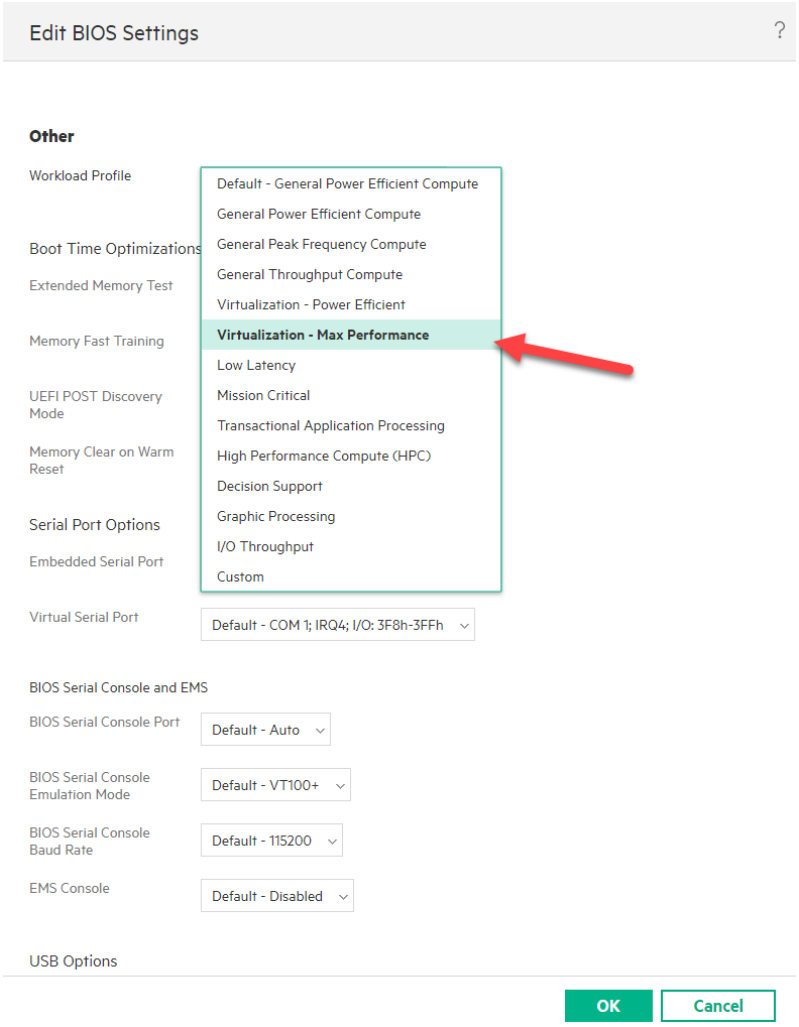
32. In the BIOS Settings section, if desired, check the box to *Manage BIOS*.



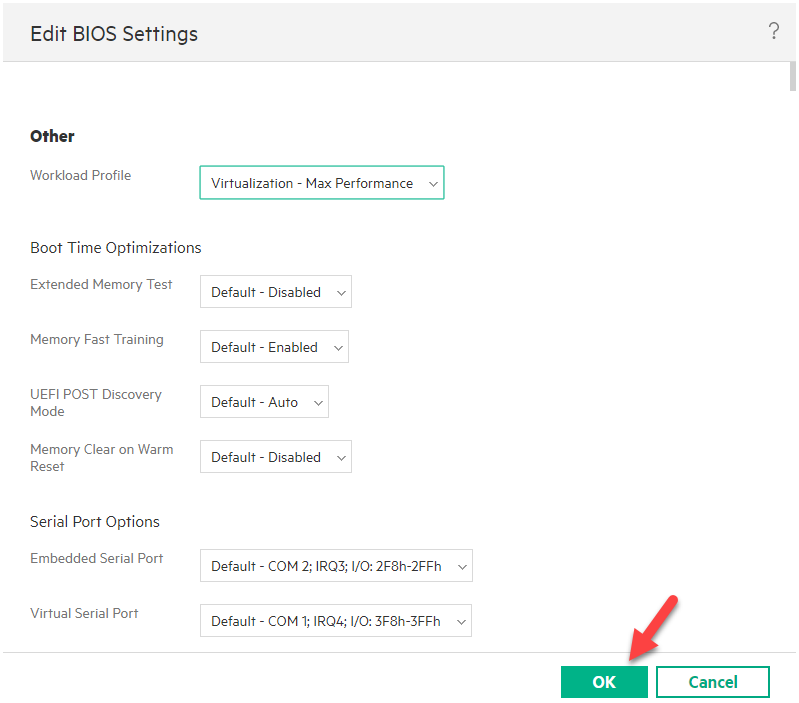
33. Click *Edit BIOS settings*



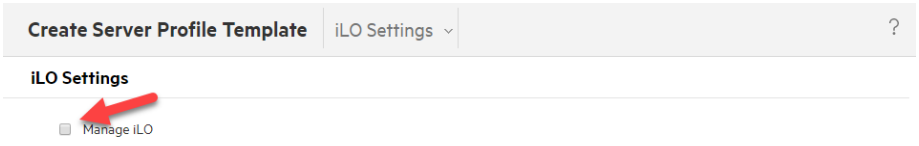
34. In the Edit BIOS settings dialog window, edit any desired BIOS settings. For Gen10 Server you can set the Workload Profile to set a number of BIOS settings to get the most out of your server based on HPE testing.



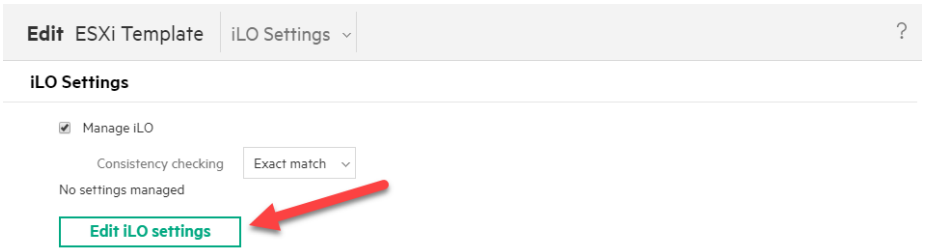
35. In the Edit BIOS settings dialog box, click *OK* after all of the desired BIOS settings are made.



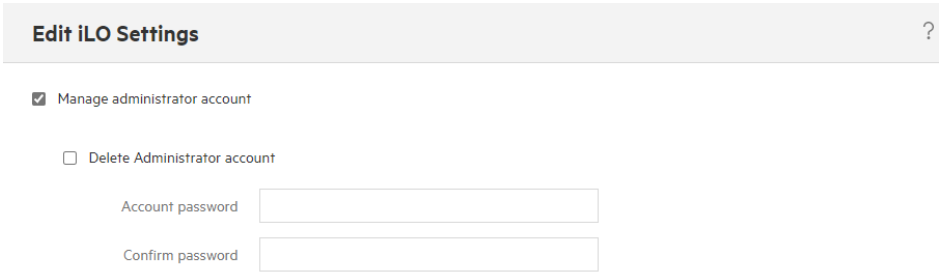
36. If desired, check the *Manage iLO* box in the iLO Settings section



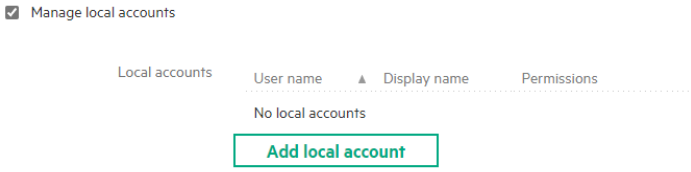
37. Click *Edit iLO settings*



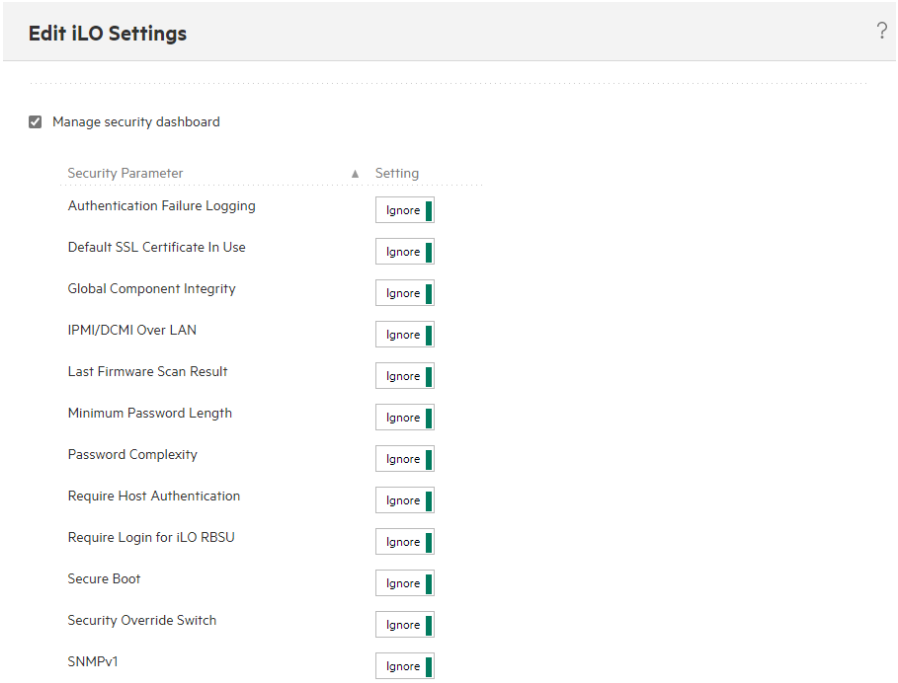
38. If desired, check the box *Manage administrator account* and edit the details as needed



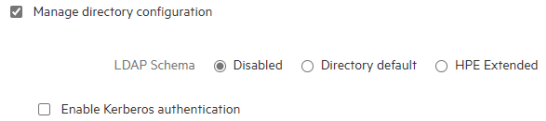
39. If desired, check the box *Manage local accounts* and edit the details as needed



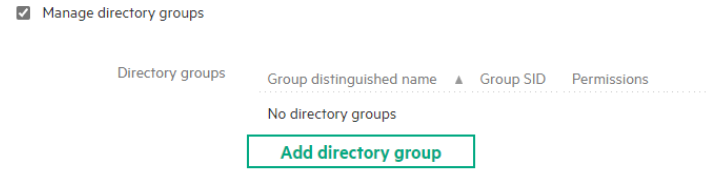
40. If desired, check the box *Manage security dashboard* and edit the details as needed. This will change the iLO Security Parameters for iLO Alerts



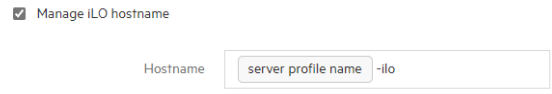
41. If desired, check the box *Manage directory configuration* and edit the details as needed



42. If desired, check the box *Manage directory groups* and edit the details as needed



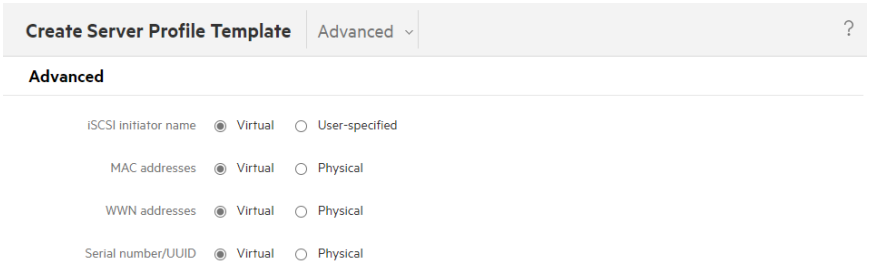
43. If desired, check the box *Manage iLO hostname* and edit the details as needed



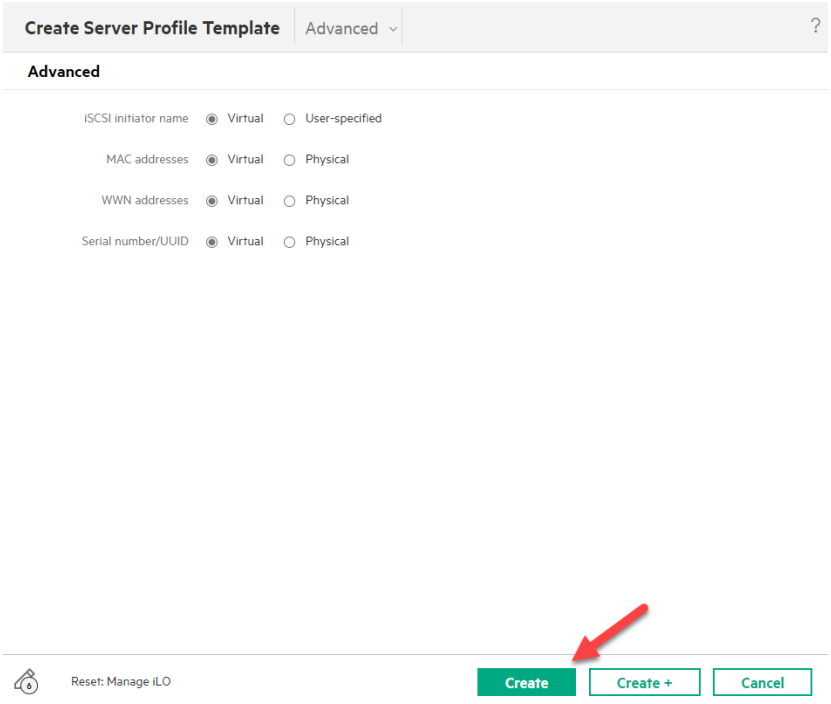
44. If desired, check the box *Manage key manager* and enter the Primary key server address



45. The HPE recommendation is to leave the Advanced section as default, which would be Virtual Managed Addresses.

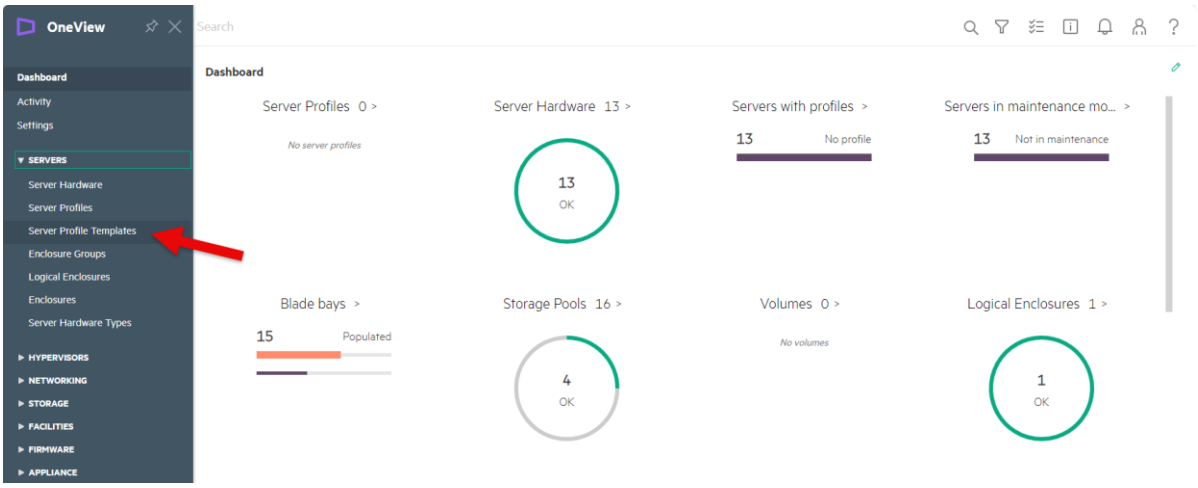


46. Click *Create or Create +*.

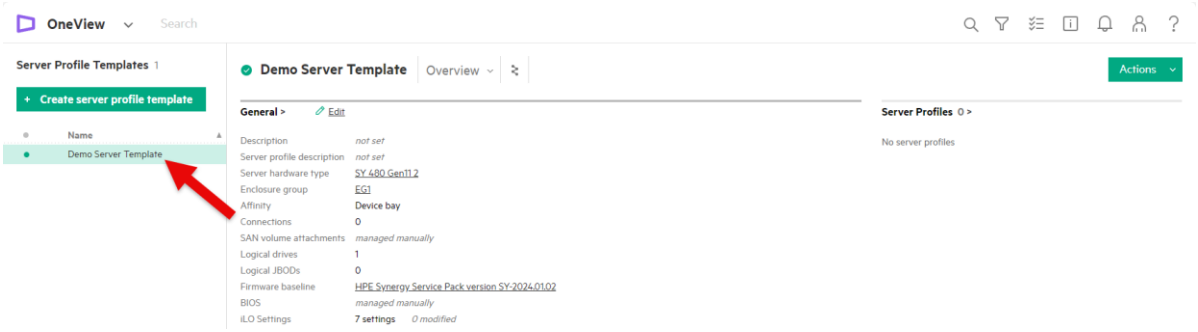


Creating Server Profiles from a Server Profile Template

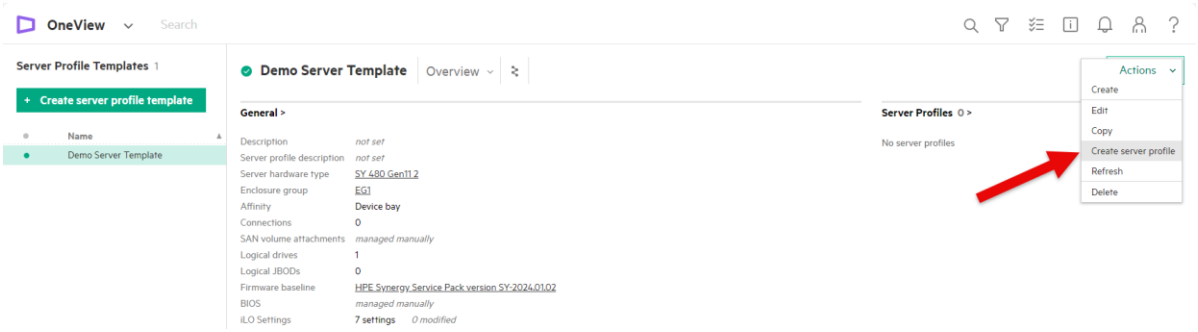
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profile Templates*.



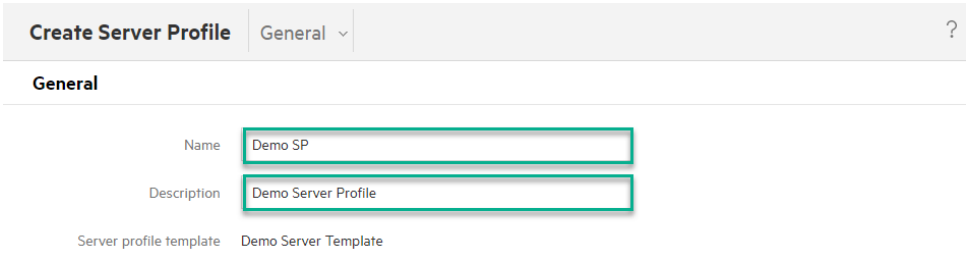
2. From the menu, select the server profile template to be used.



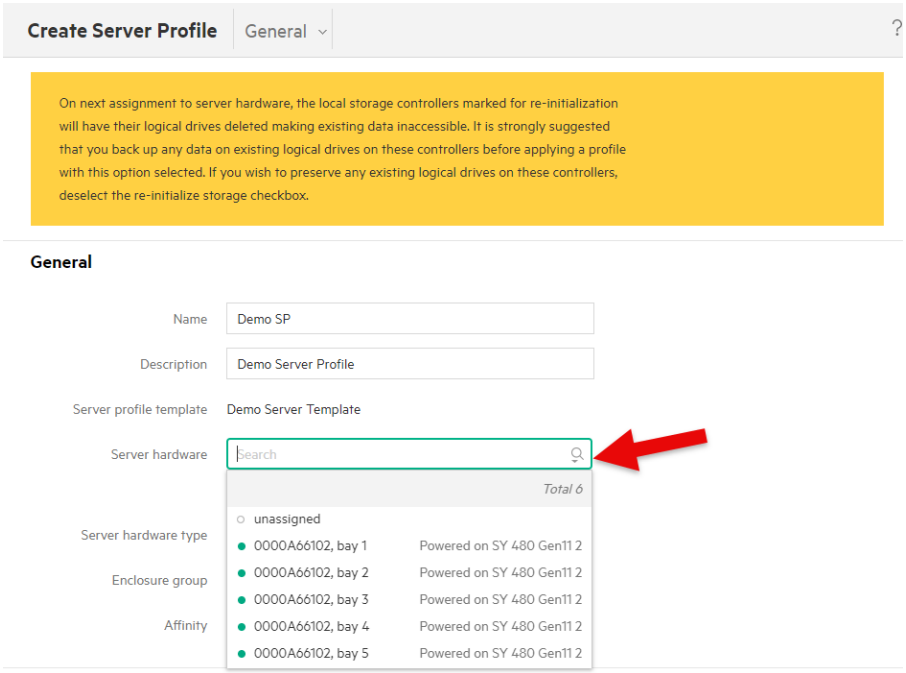
3. From the actions menu on the right hand side, select *Create server profile*



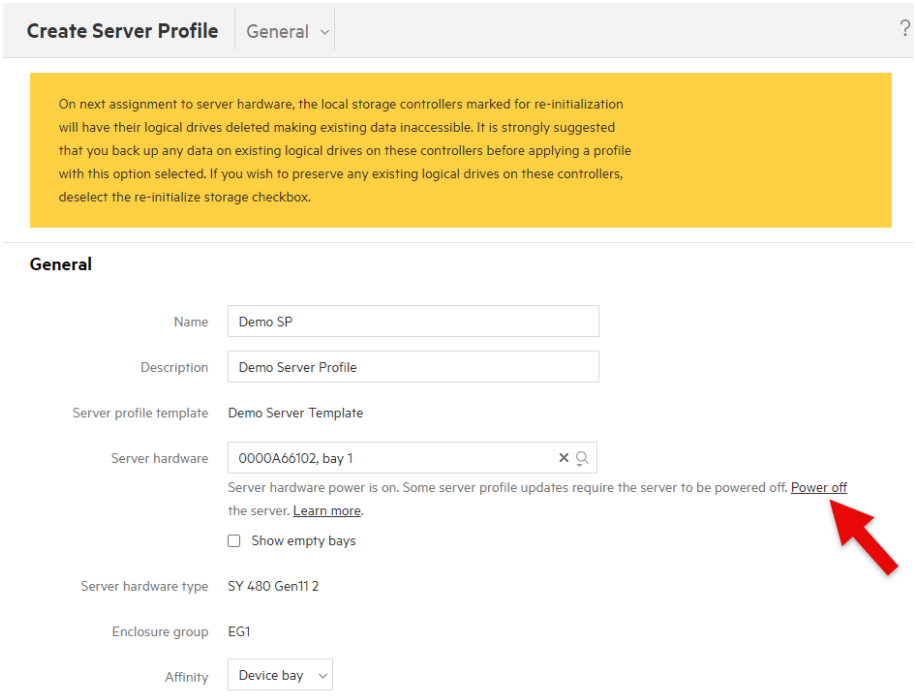
4. In the General section of the Create Server Profile dialog window, enter a *Name* and *Description* for the server profile



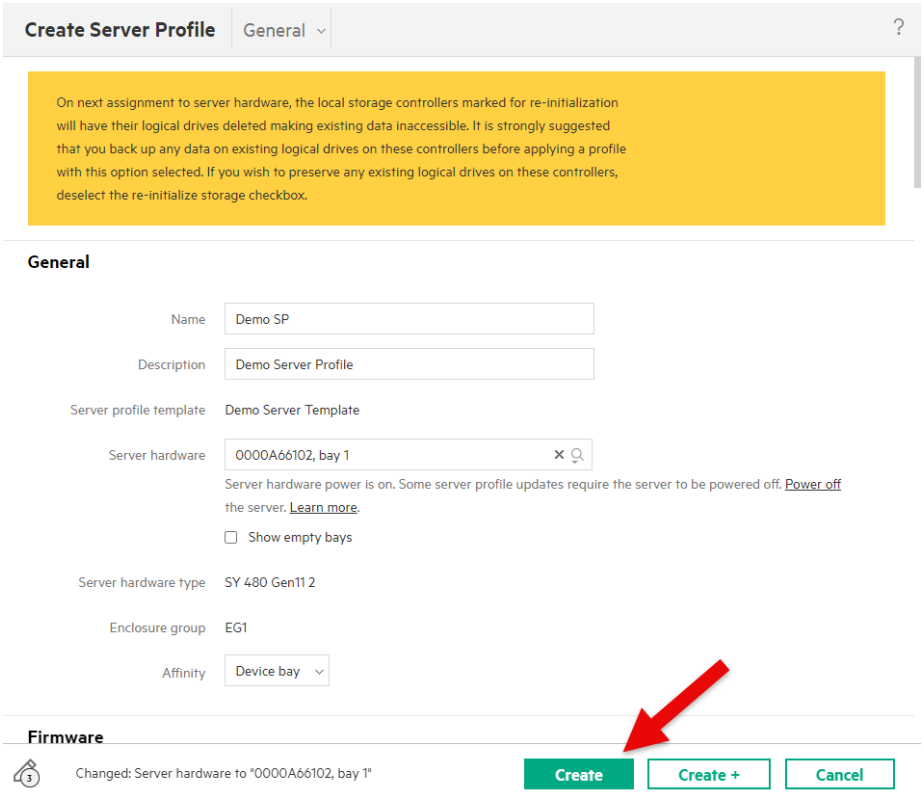
5. Using the dropdown menu, select the *Server hardware* that the server profile will be assigned to.



6. If the Server is powered on then it will need to be off as a Server Profile cannot be applied to a powered on Server.

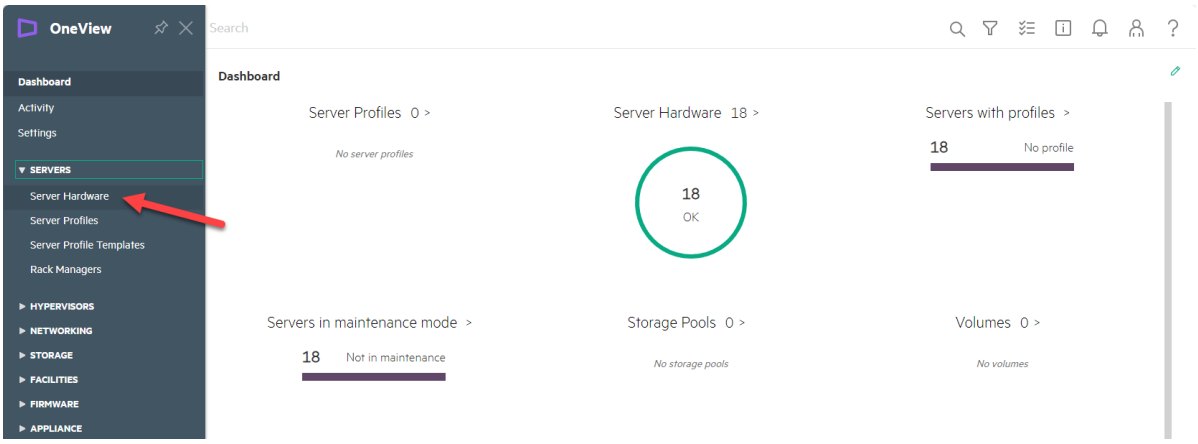


7. Click *Create* or *Create +* to create the Server Profile.

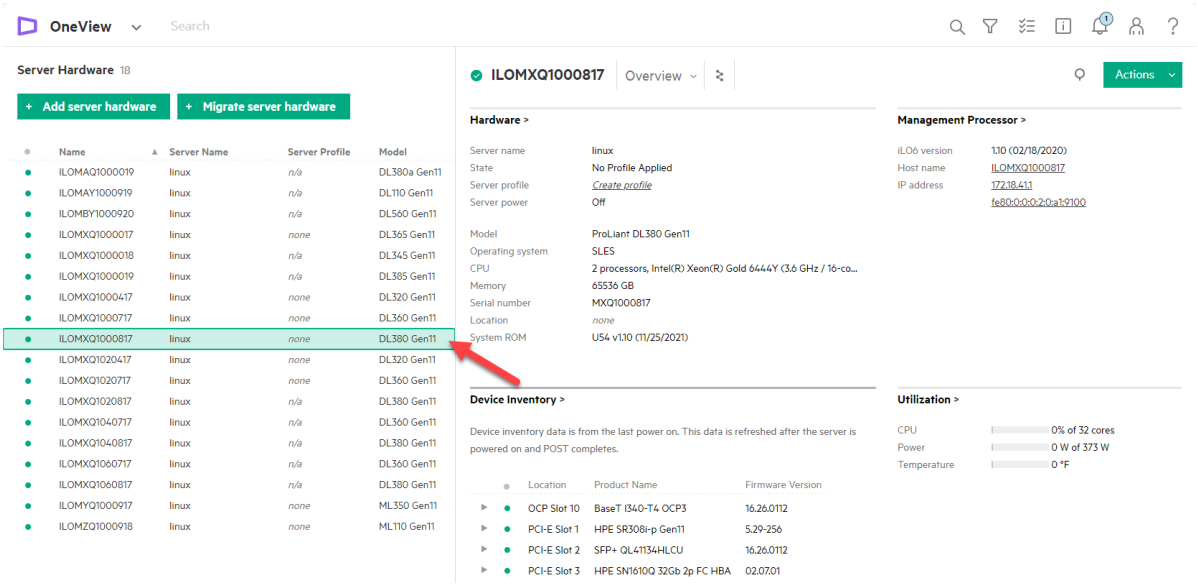


Assign a Server Profile to a newly discovered / imported server

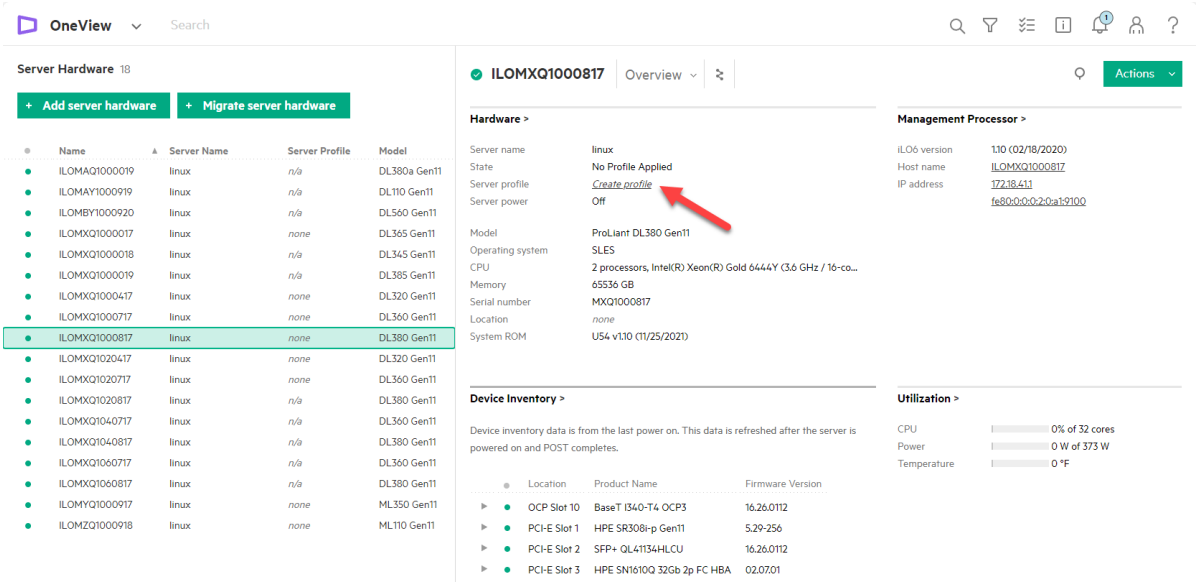
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Hardware*.



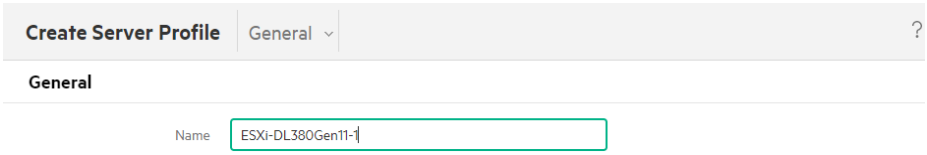
2. From the menu, select the server that you want to create a Server Profile for.



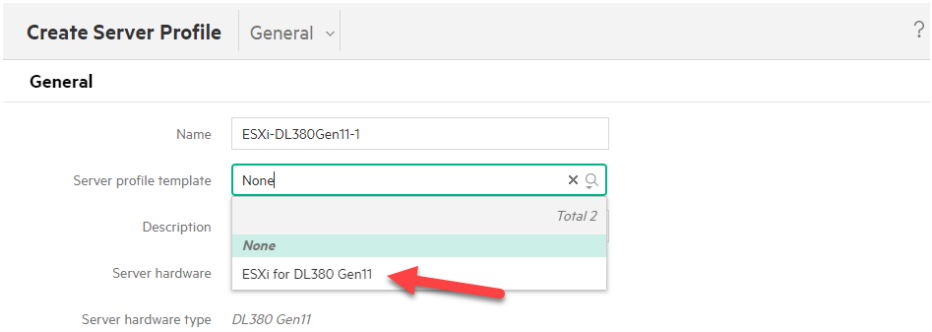
3. In the Overview section of the server hardware, select *Create profile*



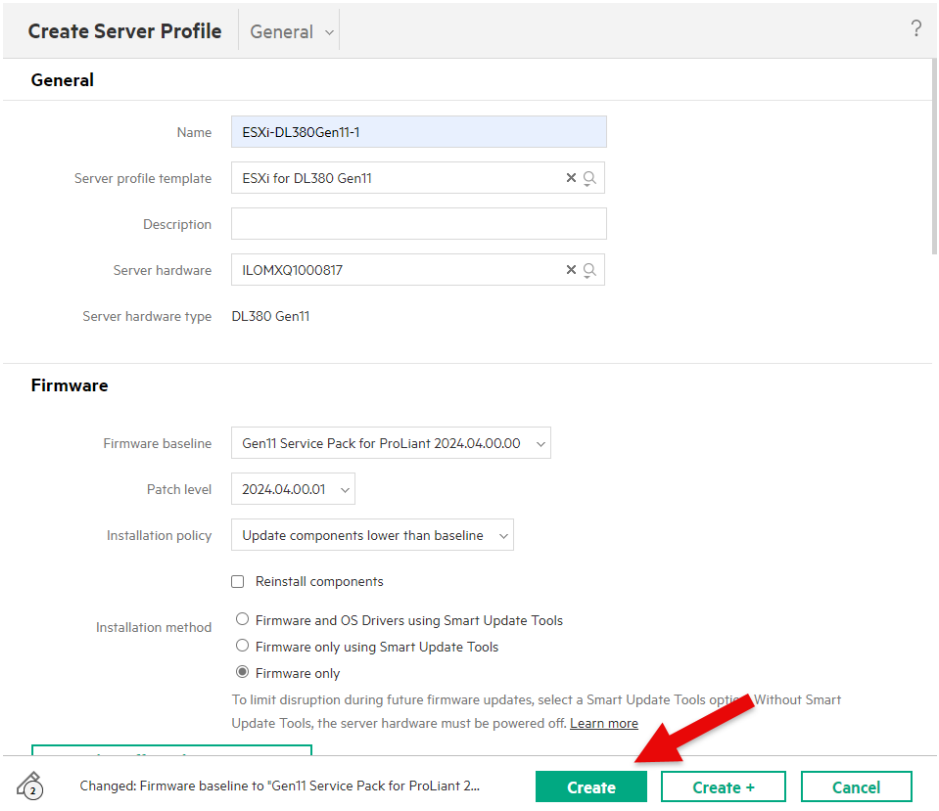
4. Enter a *Name* for the Server Profile



5. If applicable, from the drop-down list, select the server profile template to be used.

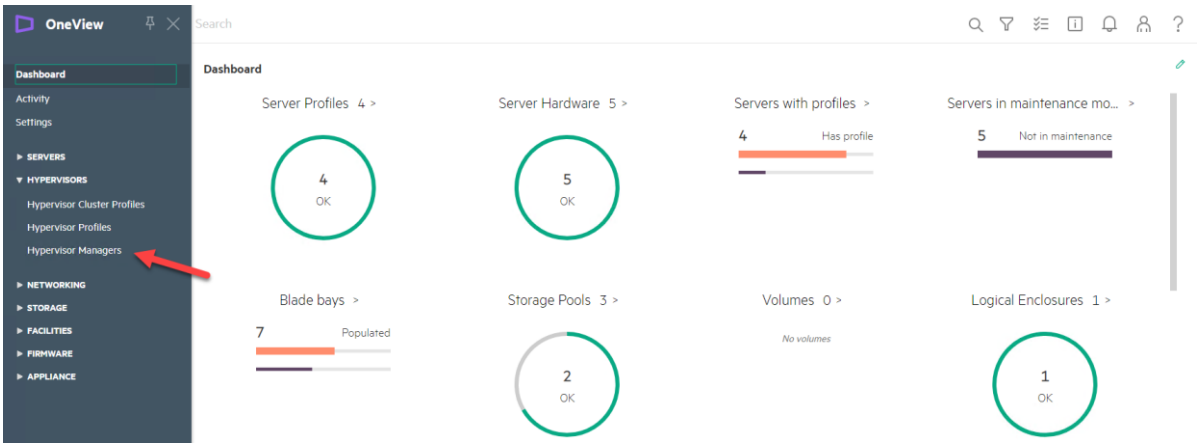


6. Click *Create* or *Create +*.

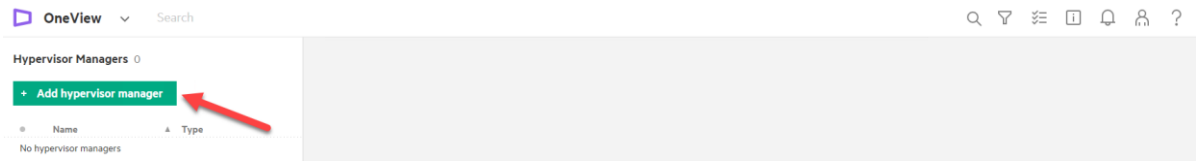


Add Hypervisor Manager

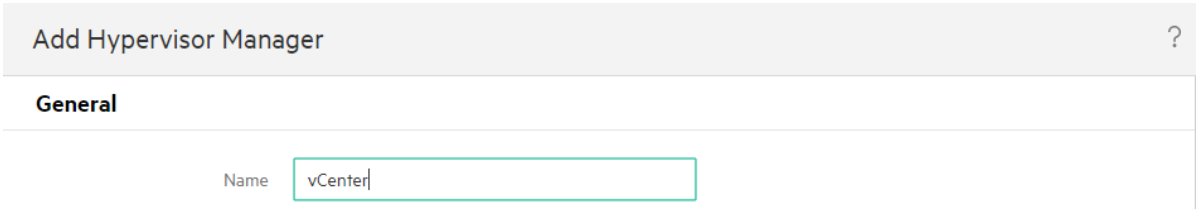
1. From the Top-Level Menu, expand the *HYPERVISORS* option and then select *Hypervisor Managers*.



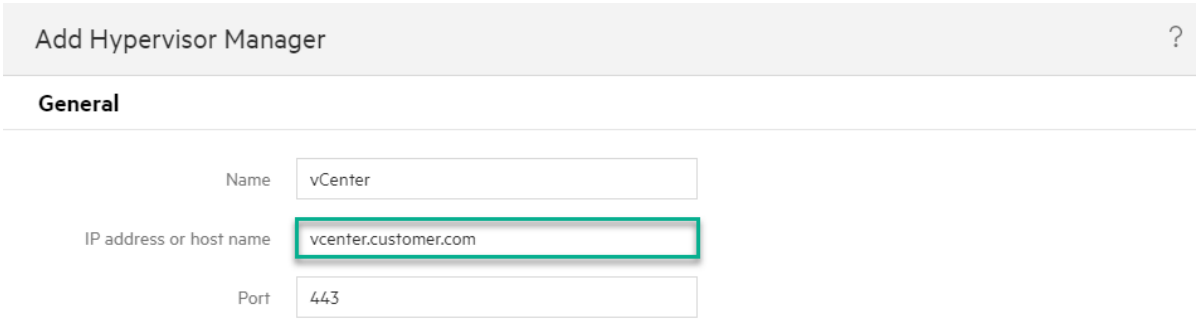
2. From the menu select the Add hypervisor manager



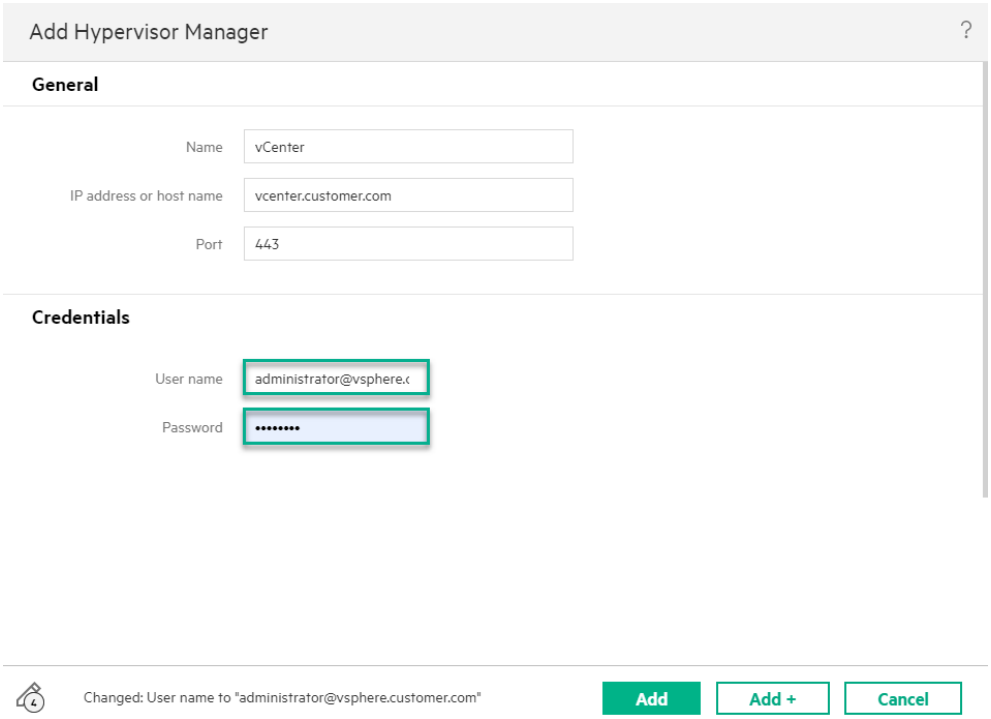
3. Enter the *Name* for the hypervisor manager



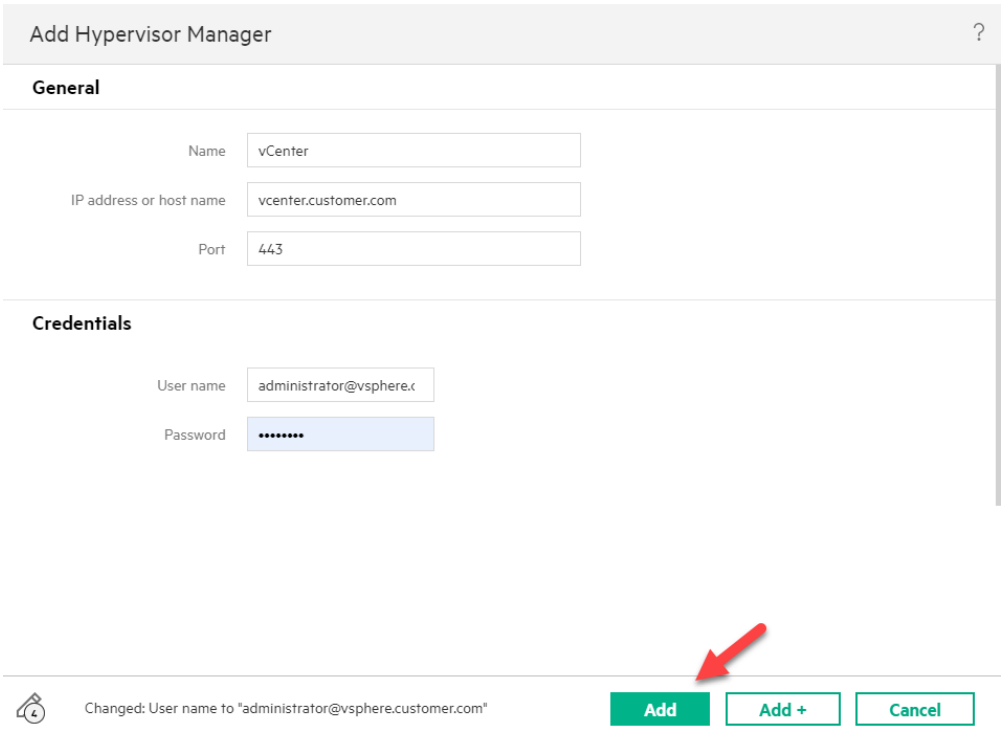
4. Enter the *IP address / hostname* of the hypervisor manager



5. Enter the *Credentials* for the Hypervisor Manager



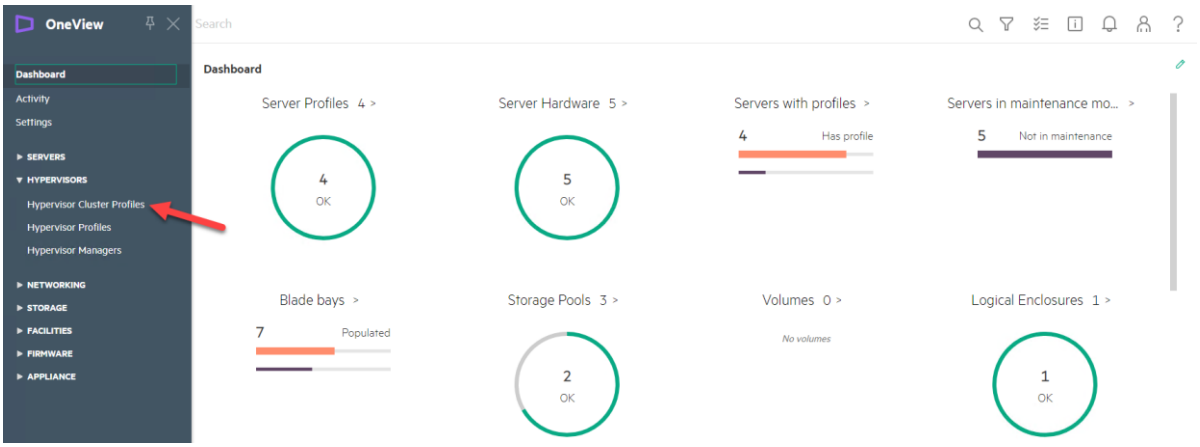
6. Click *Add*



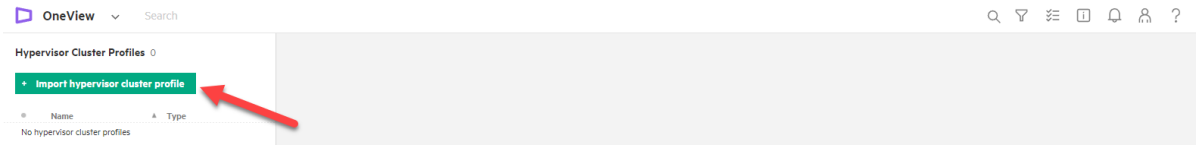
7. Accept Yes, Trust to accept the certificate from the Hypervisor Manager

Import VMware Cluster Profile

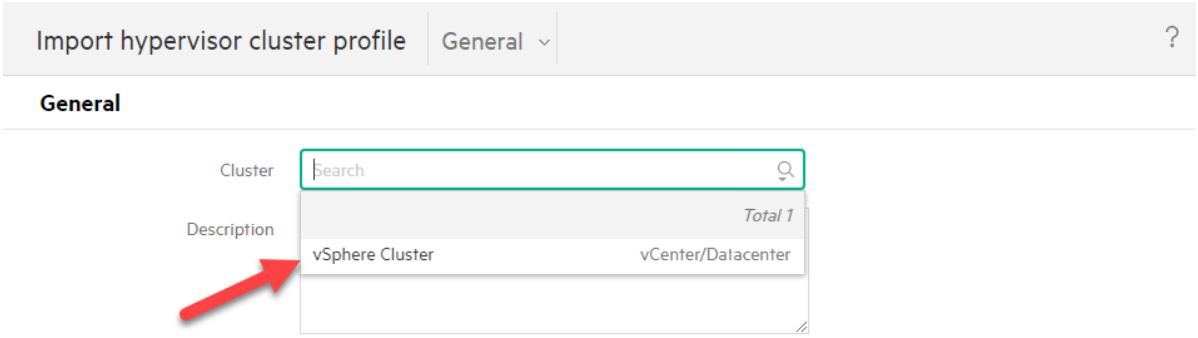
1. From the Top-Level Menu, expand the *HYPERVISORS* option and then select *Hypervisor Cluster Profiles*.



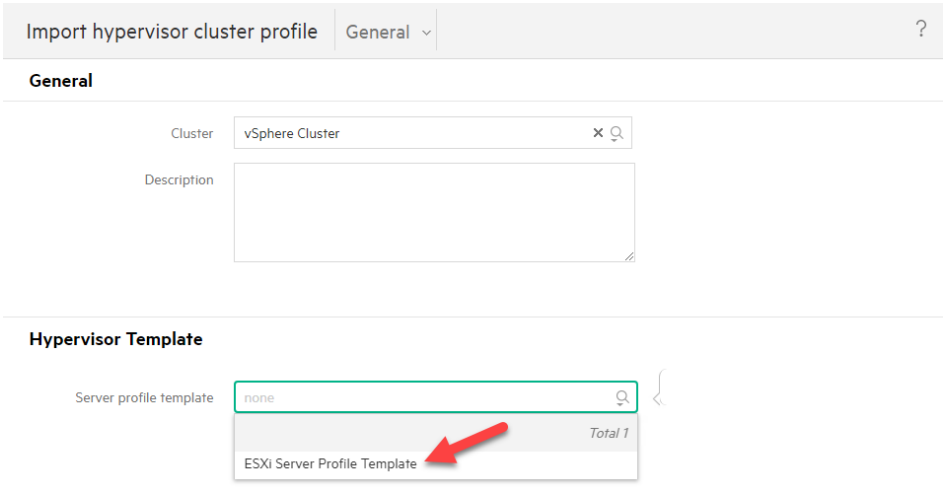
2. From the left hand menu select the *Import hypervisor cluster profile*



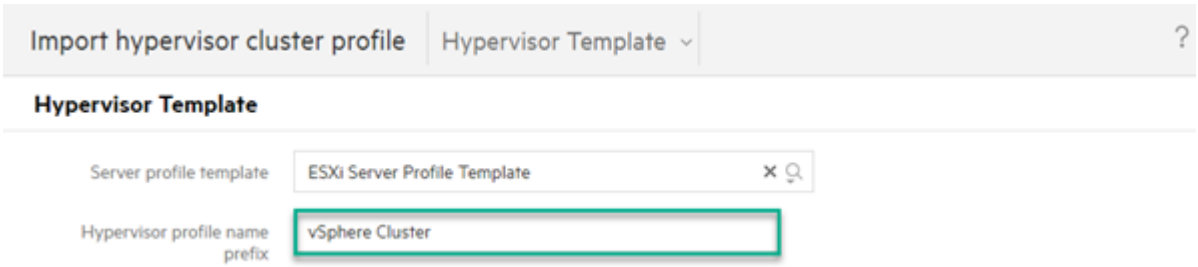
3. Select the Cluster that you want to Import.



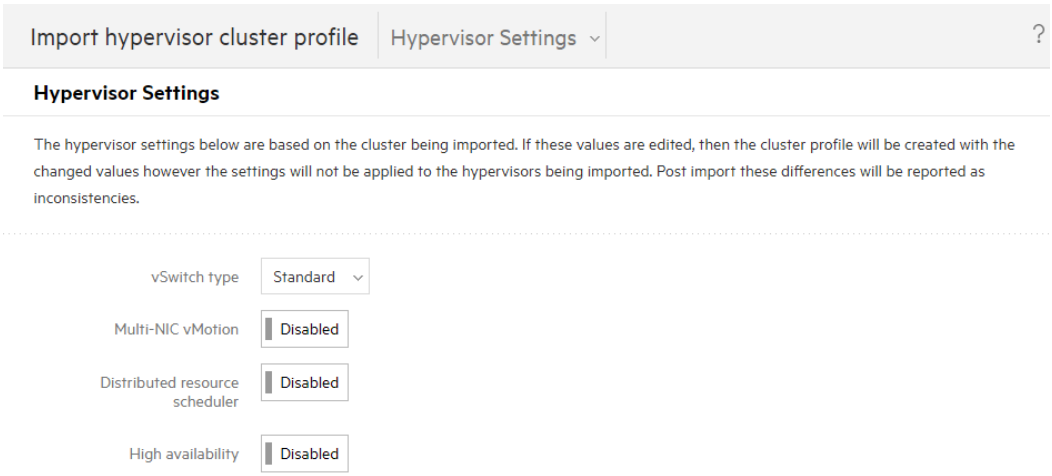
4. Select the Hypervisor Template for the cluster profile



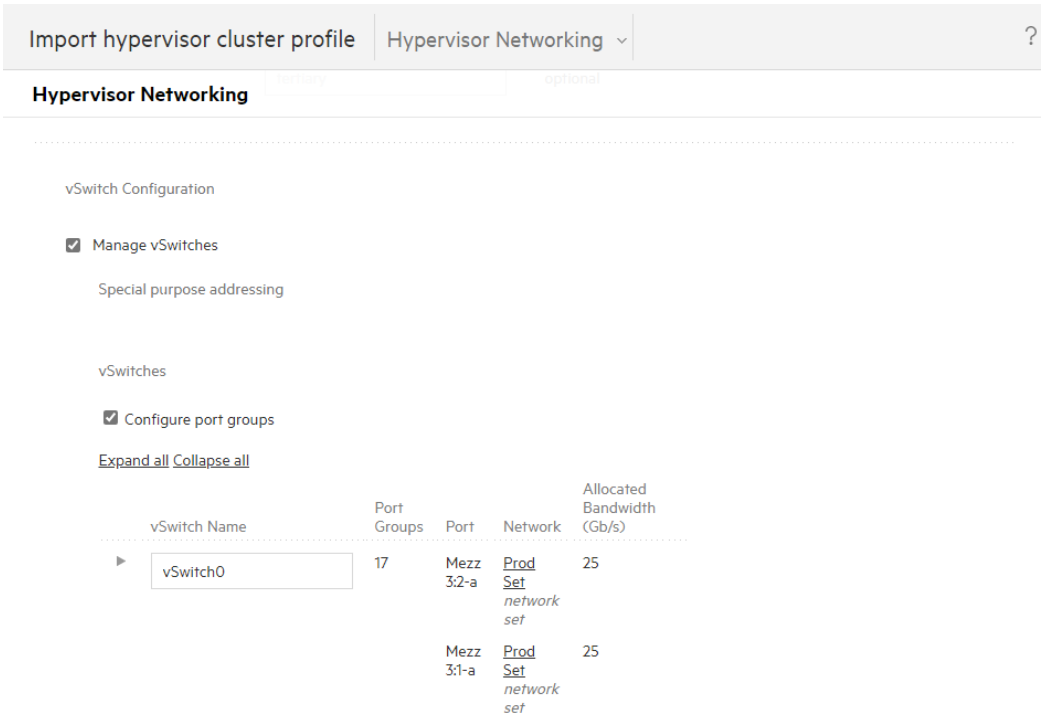
5. Create the prefix that will be used for the Hypervisor profile name



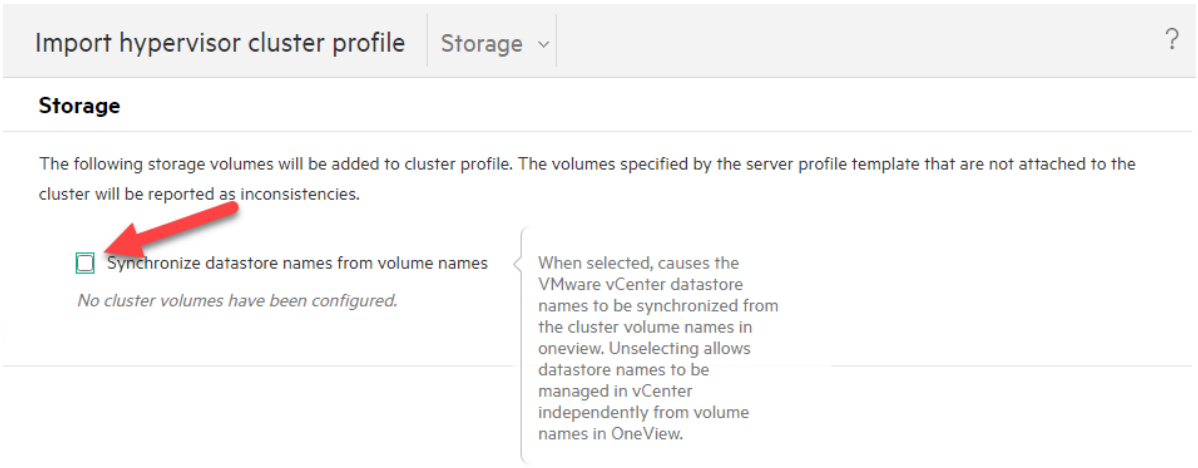
6. Verify the Hypervisor Settings



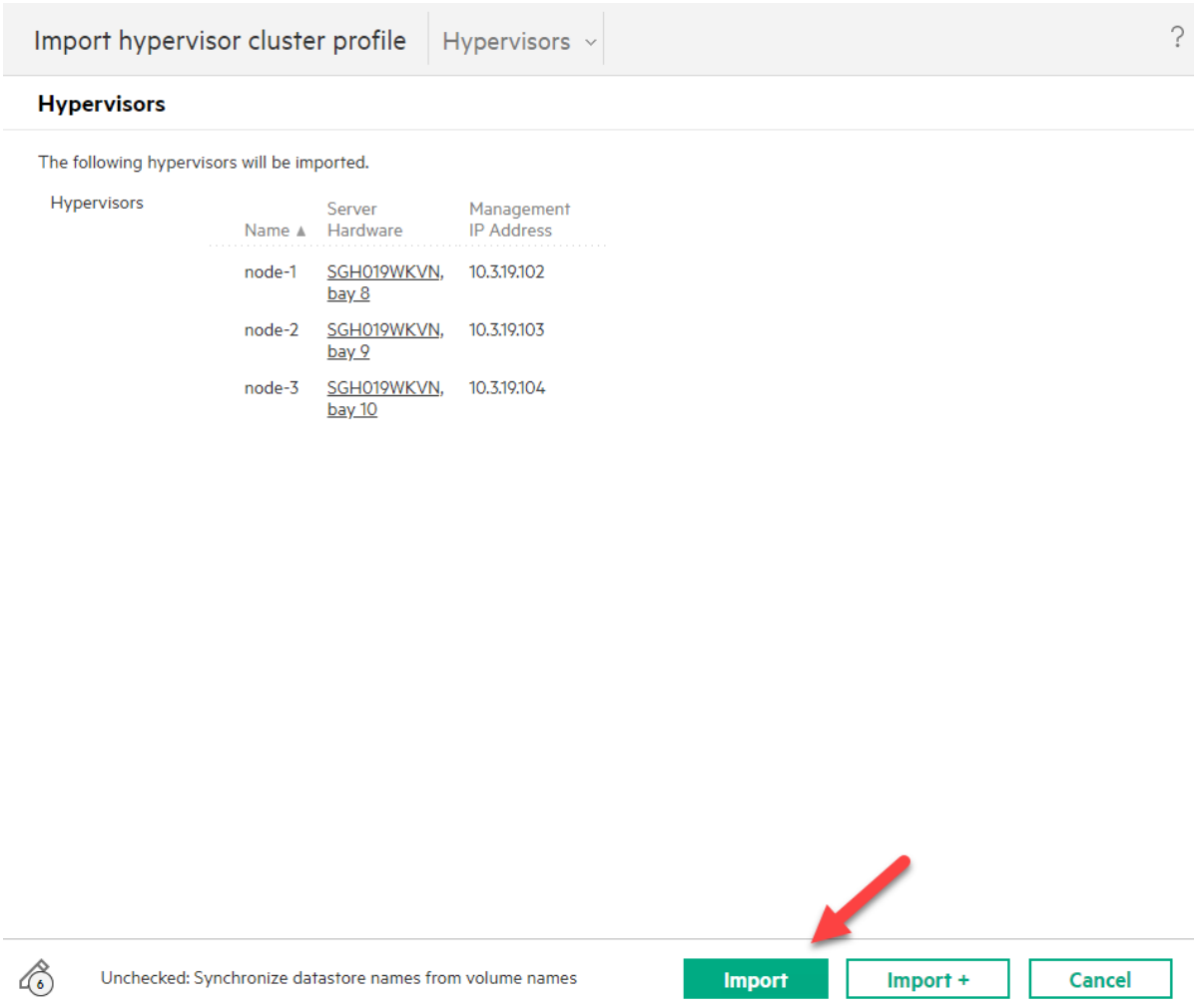
7. Enter the appropriate Hypervisor Networking settings



8. Choose whether you require the Volume Names synchronized from vCenter.

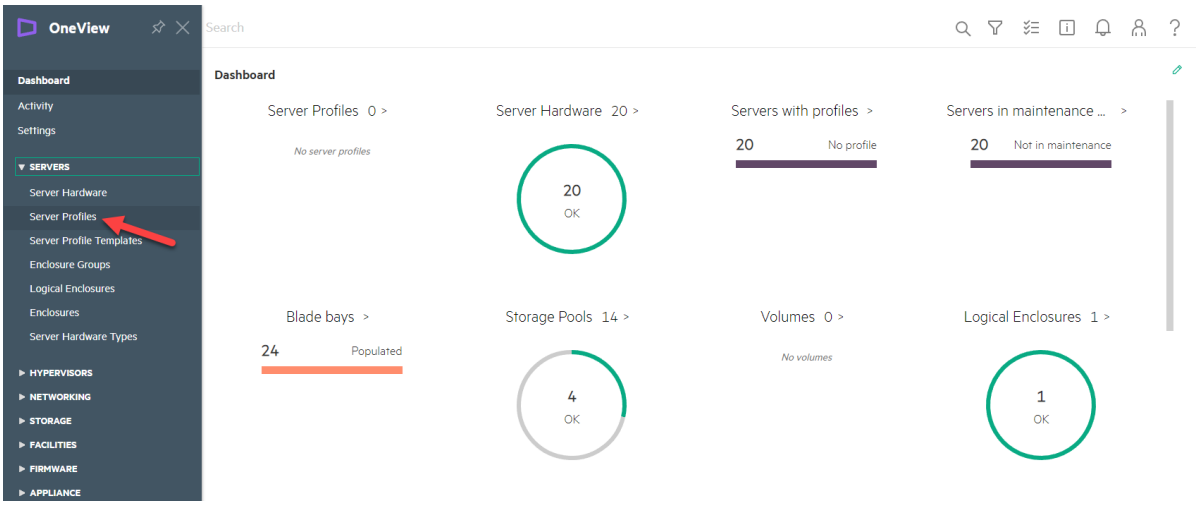


9. As you are importing an existing Hypervisor cluster the Hypervisors will be selected automatically. Click on *Import* to import the Cluster

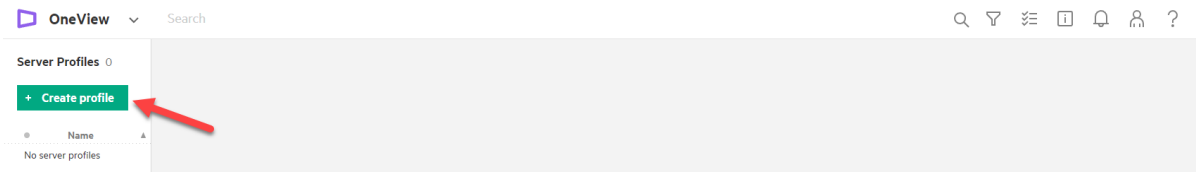


Create One-Off Server Profile

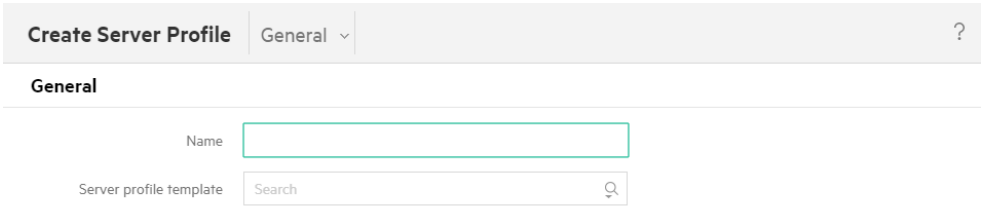
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



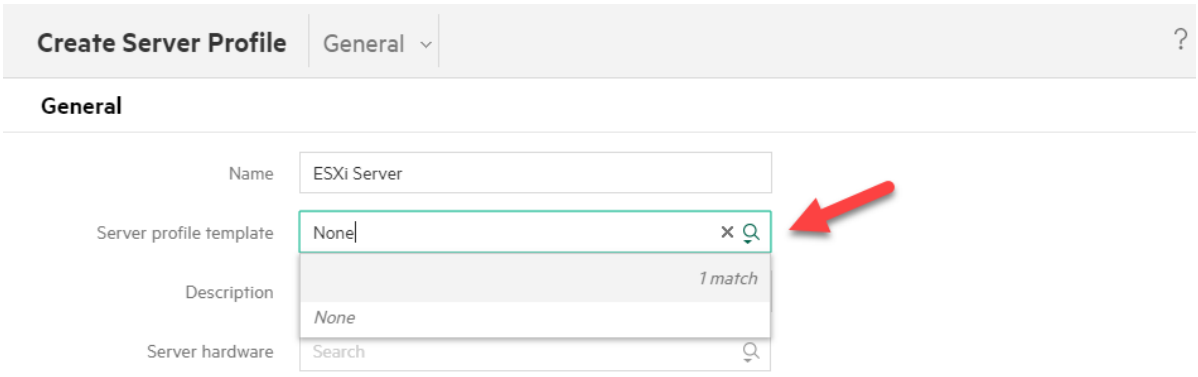
2. Once on the Server Profiles screen, select the + *Create profile* button



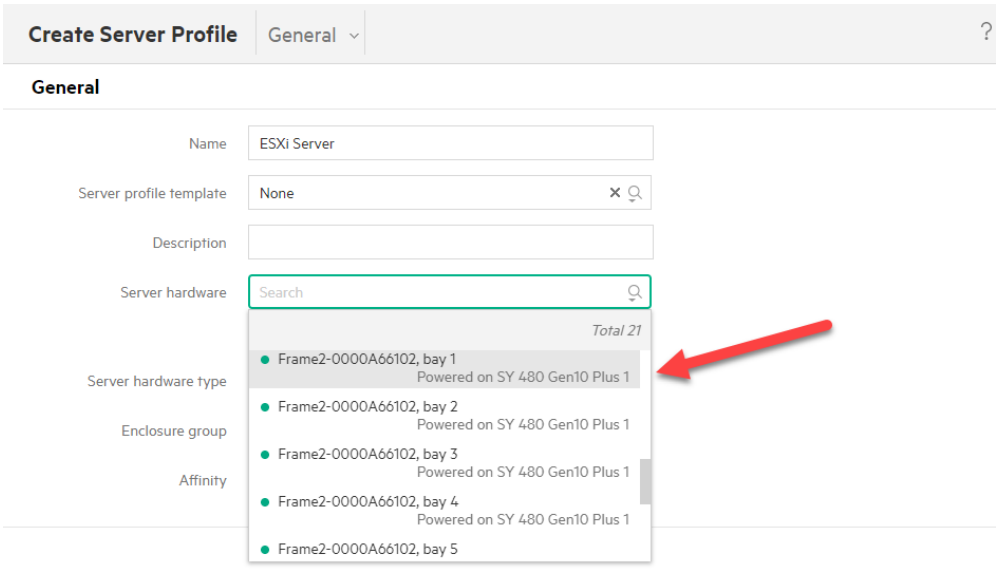
3. In the General section of the server profile creation page, provide a *Name* for the Server Profile.



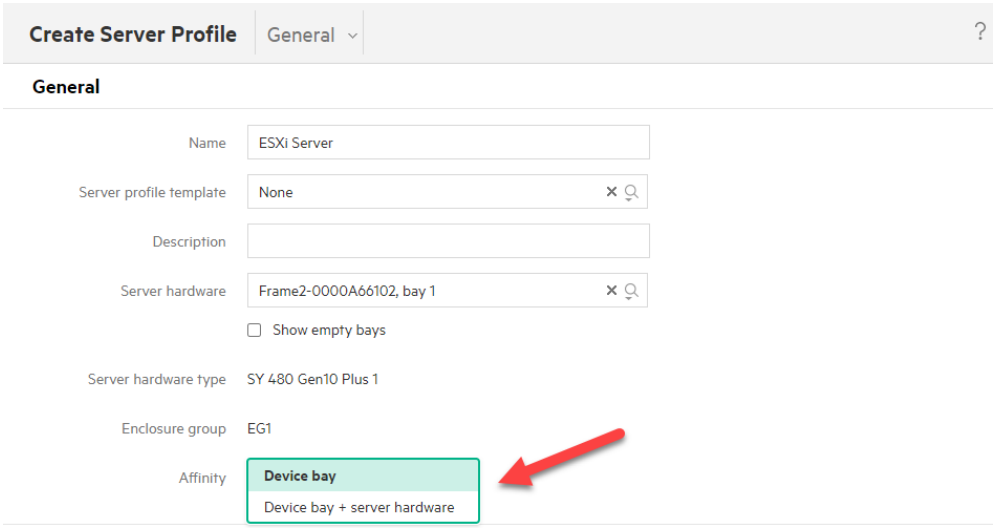
4. You have to choose a Server profile template in this case because we do not want the profile based on one you have to select *None*.



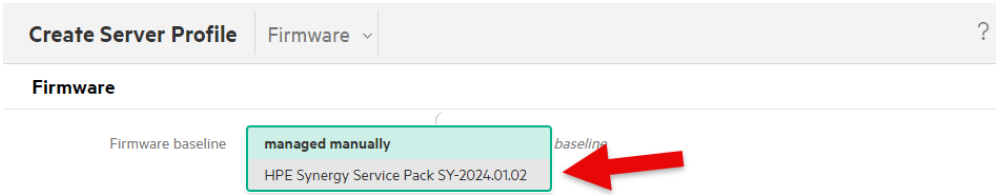
5. Select the *Server hardware* that the profile will be applied to using the dropdown menu.



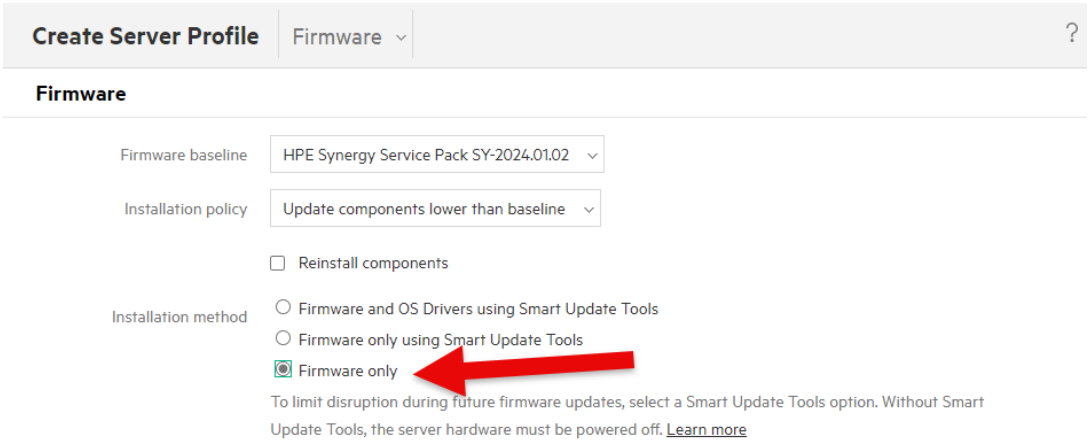
6. Specify the *Affinity* method you'd like to configure.



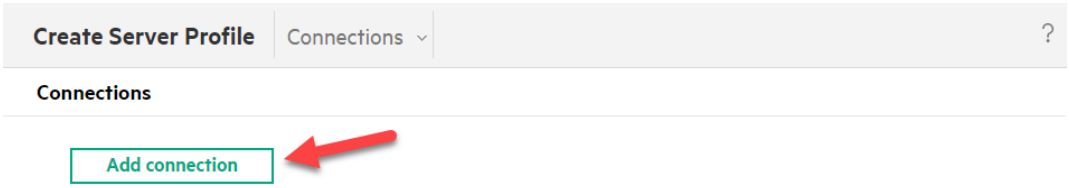
7. In the firmware section, select a *Firmware baseline* from the dropdown menu.



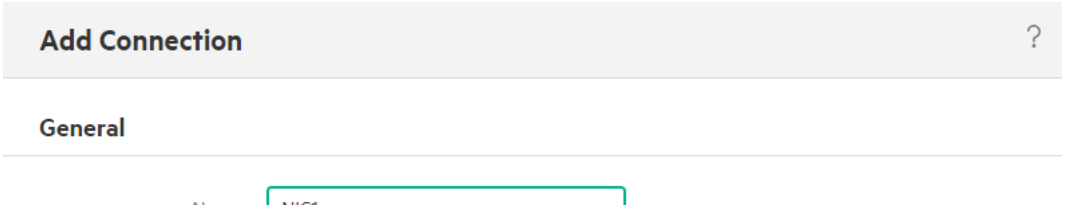
8. Once a baseline is selected, choose how the baseline will be applied to the server. If either of the options using the HPE Smart Update Tools is selected then the firmware or driver updates will be done while the systems are online. If the firmware only option is selected then the firmware will be updated offline using Intelligent Provisioning.



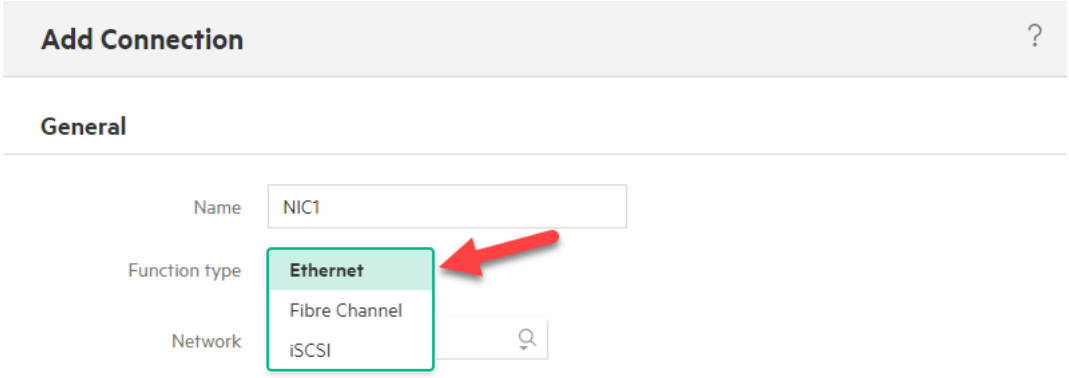
9. In the connections section, click *Add connection*.



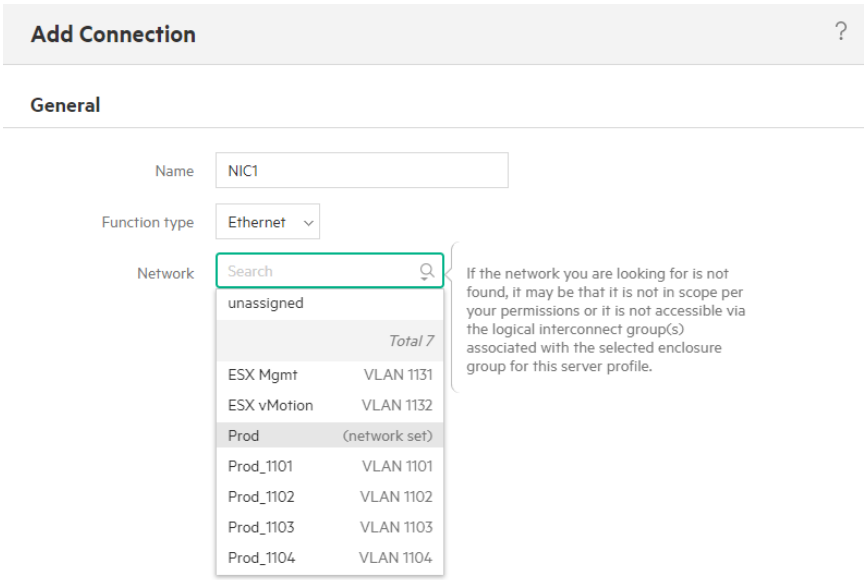
10. In the Add Connection dialog window, enter a *Name* for the connection



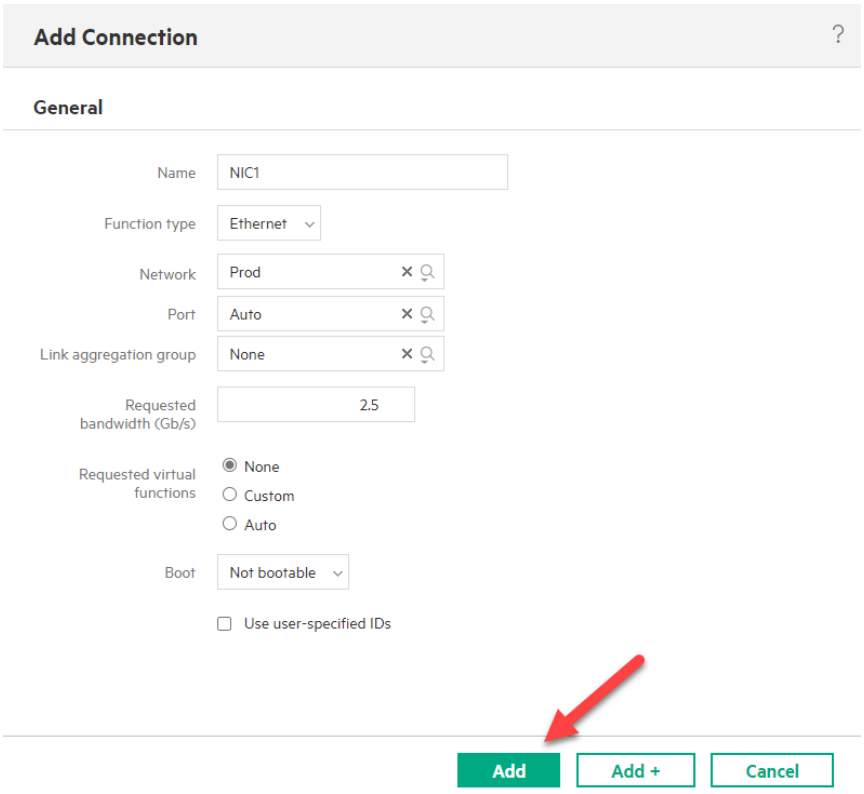
11. Using the dropdown list select the function type for the connection



12. Select the network to be associated with the function using the Network dropdown list



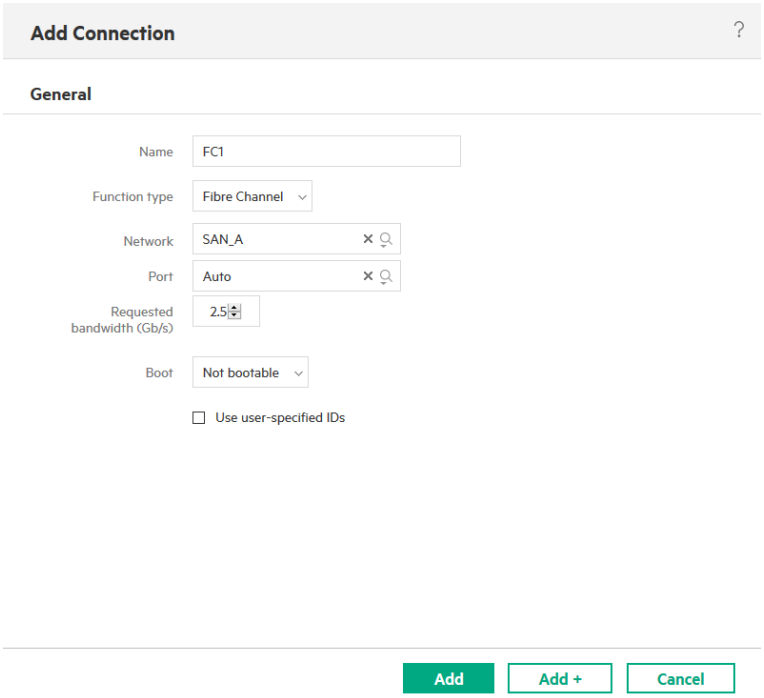
13. Click the *Add* to close the Add Connection dialog window or *Add+* button to continue adding Network Connections to the Server Profile.



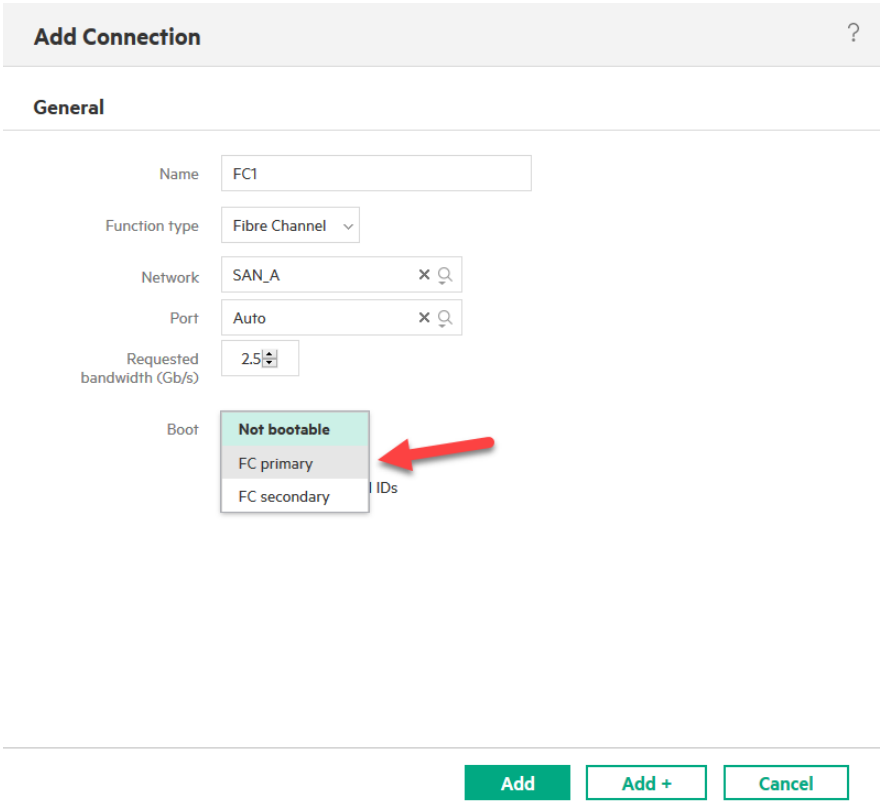
Note:
The Use user-specified IDs is for those customers that wish to provide their own MAC or WWN address for the connection.

Note:
You can specify which FlexNIC to assign the Network Connection to or leave it at the default of Auto. Auto will apply the same Network Connection to Adapter mapping Virtual Connect does today. Do know that you cannot create a FlexNIC B, C or D without first creating FlexNIC A.

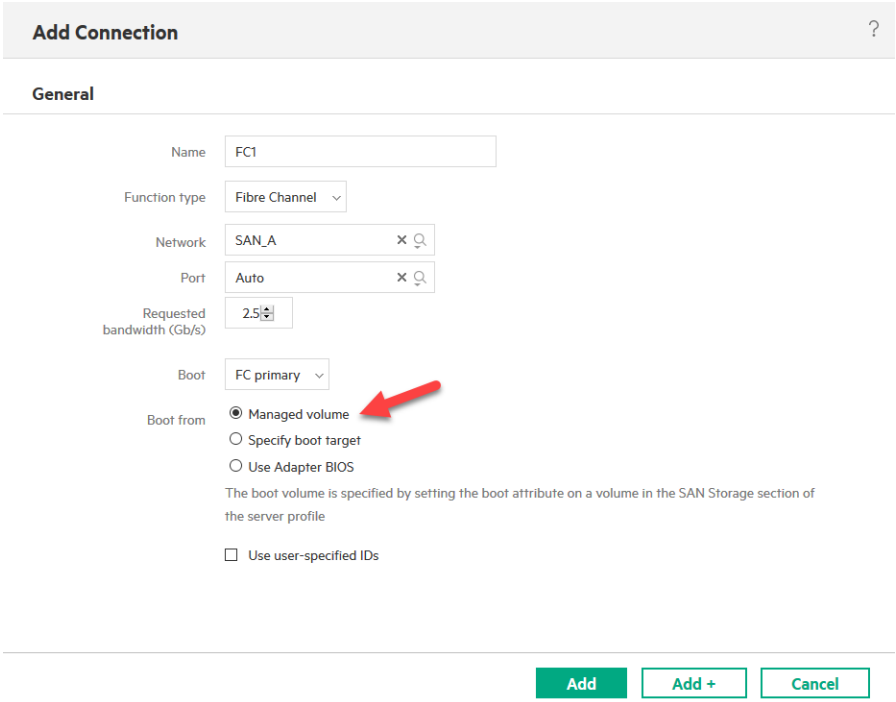
14. (Optional) Adding *Fibre Channel Networks* is a similar operation as an Ethernet Device Type. FlexNIC B is reserved for FC Connections when FC Connection Types are added to the *Server Profile*. When choosing the FlexNIC, you can leave the default *Auto*. You can force the FlexNIC assignment, but the list will be filtered based on the connection location to the Interconnect Bay the FC Network is assigned to.



A. (Optional) If you wish to configure FC Boot From SAN (BFS), change the *Boot* setting from *Not Bootable* to either *FC Primary* or *FC Secondary*.

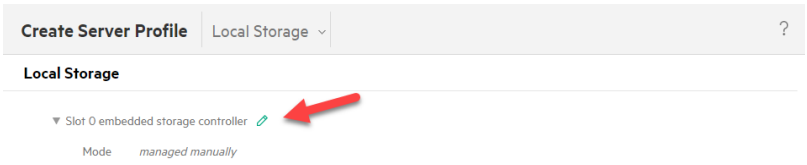


15. Select the connection's boot source, here selected to be a managed SAN volume. Later in the SAN storage configuration section you can select which managed volume will be configured as the boot volume.

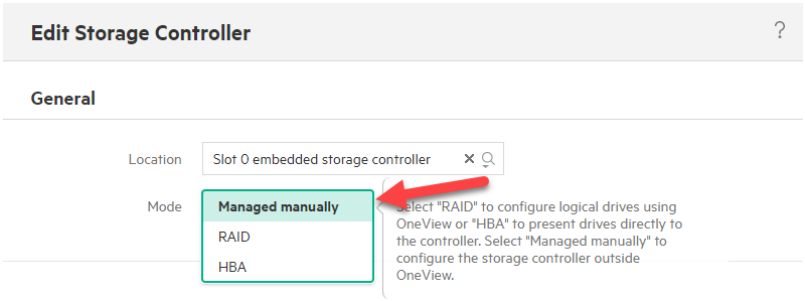


16. If desired, enable local storage management by editing the option.

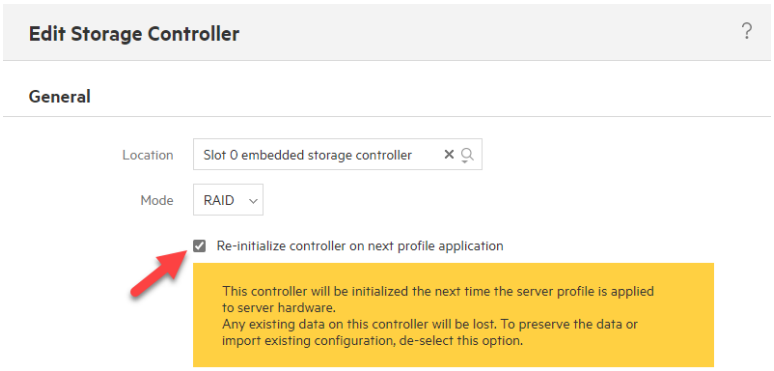
Note: *This will be different depending on the generation of the server due to different SMART Array Controller configs. The following is for a Gen9 Server.*



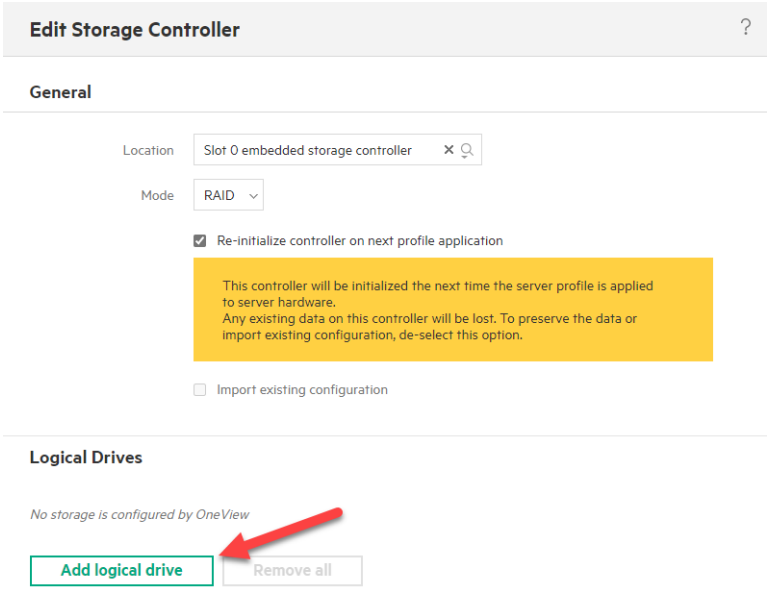
17. In the Edit *Slot 0 embedded storage controller* dialog box, select the mode of the storage controller using the dropdown list



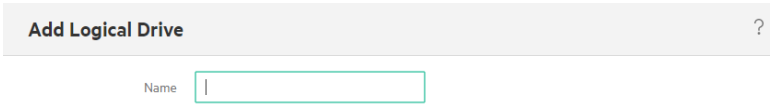
18. Enable or disable the option to Re-initialize controller on next profile application. A warning will be shown about this option



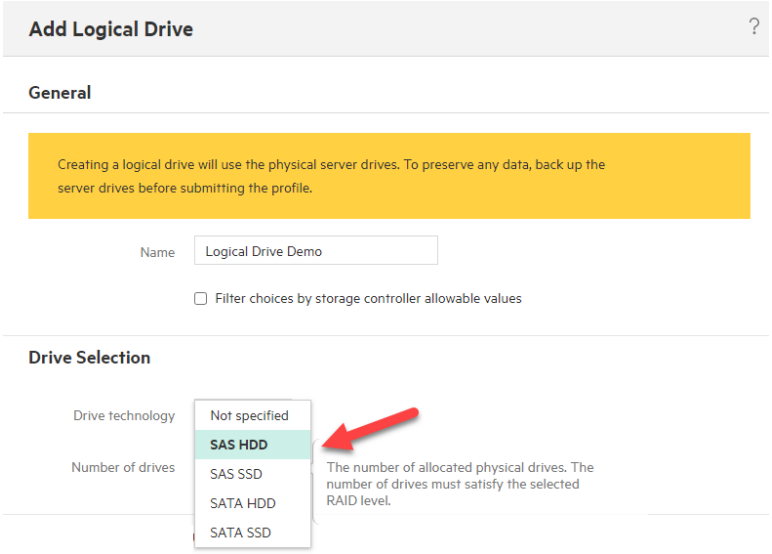
19. Click *Add logical drive*



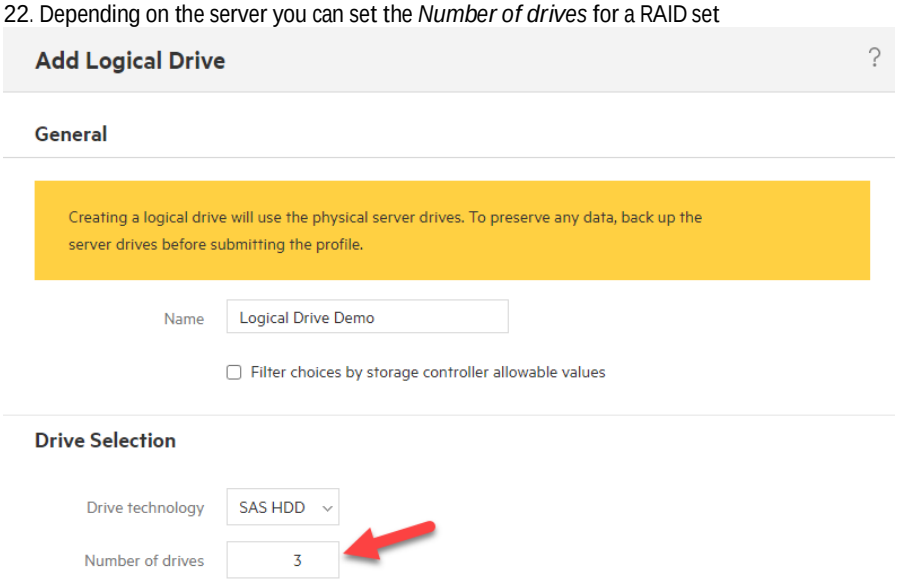
20. In the Add Logical Drive dialog window, enter a *Name* for the logical drive



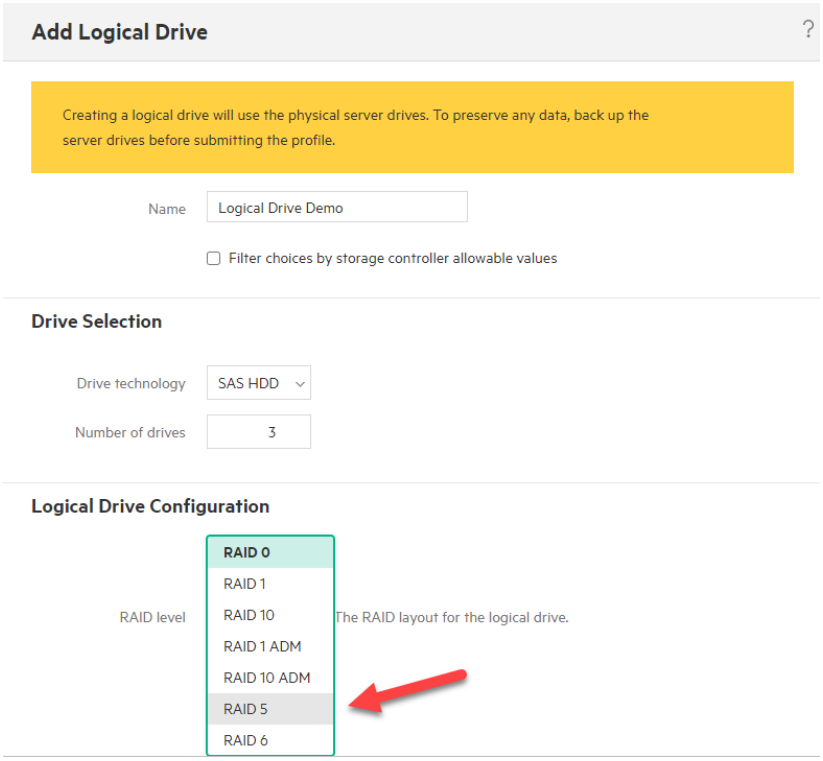
21. Select the *drive technology* for the logical drive



22. Depending on the server you can set the *Number of drives* for a RAID set

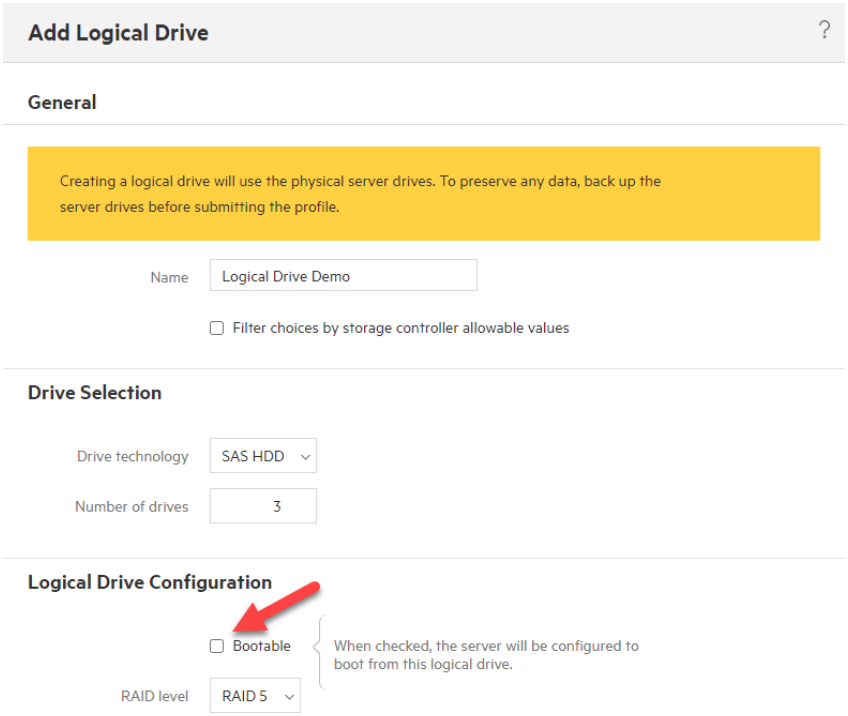


23. Select the *RAID level* of that RAID set.

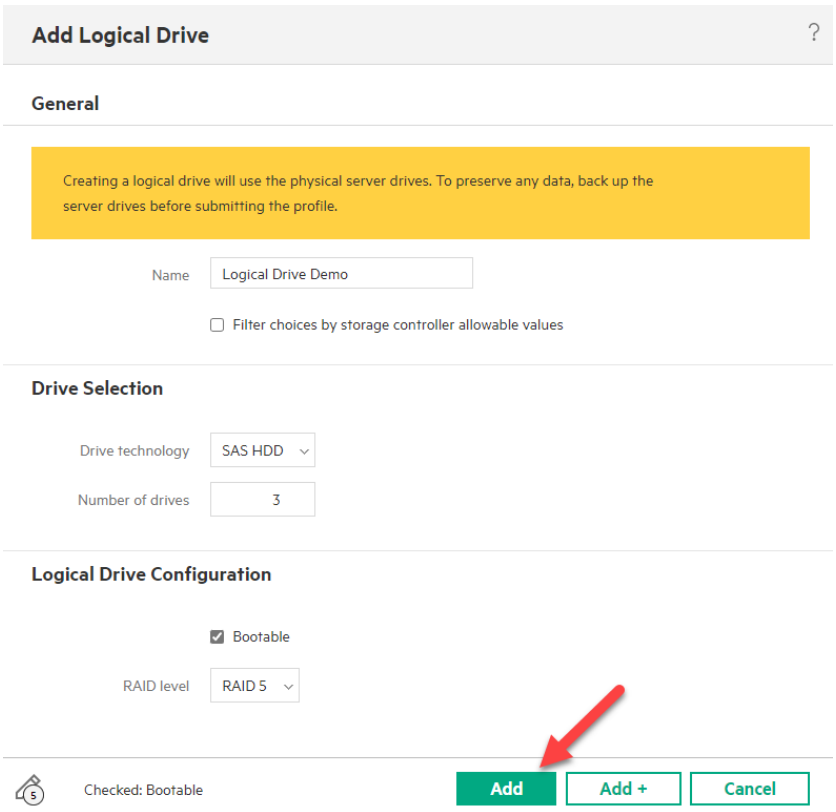


24. You can set whether this Logical Drive is the Boot volume by clicking on *Boot*.

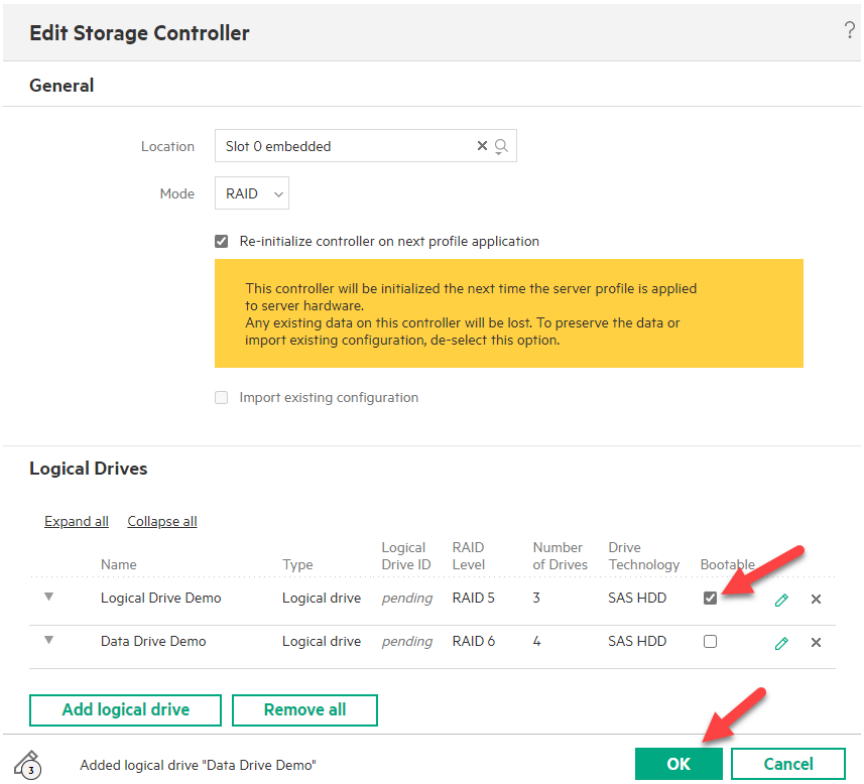
Note: *The boot option is only used when the BIOS mode is set to Legacy BIOS mode (set later in this section).*



25. Click *Add or Add +* to create the logical drive for the server profile.



26. Once all of your logical drives are created, you can still select which one is the boot drive. Click *OK* to finish configuring the Slot 0 embedded storage controller.

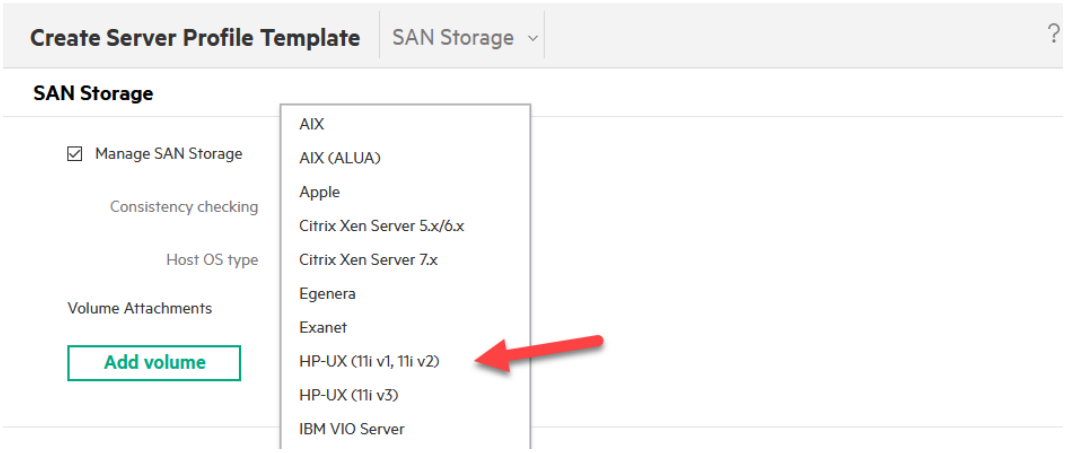


27. Enable *SAN Storage* if necessary.

A. Check the box for *Manage SAN Storage*



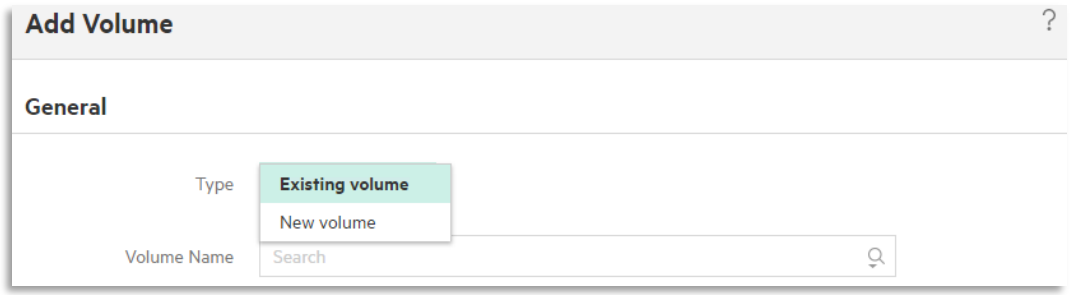
B. Specify the *Host OS type*, which controls the Host's OS / personna created on the HPE 3PAR StoreServ storage system.



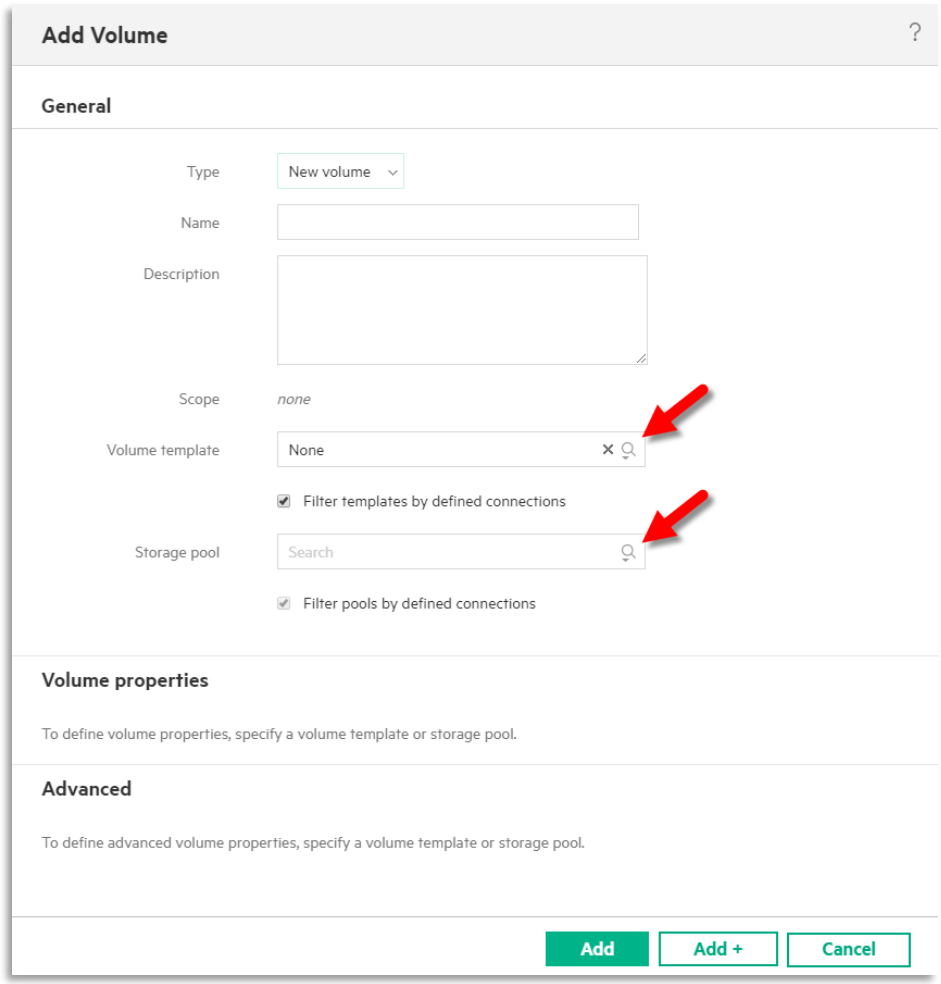
C. Click the *Add Volume* button to display the list of volumes available for assignment.



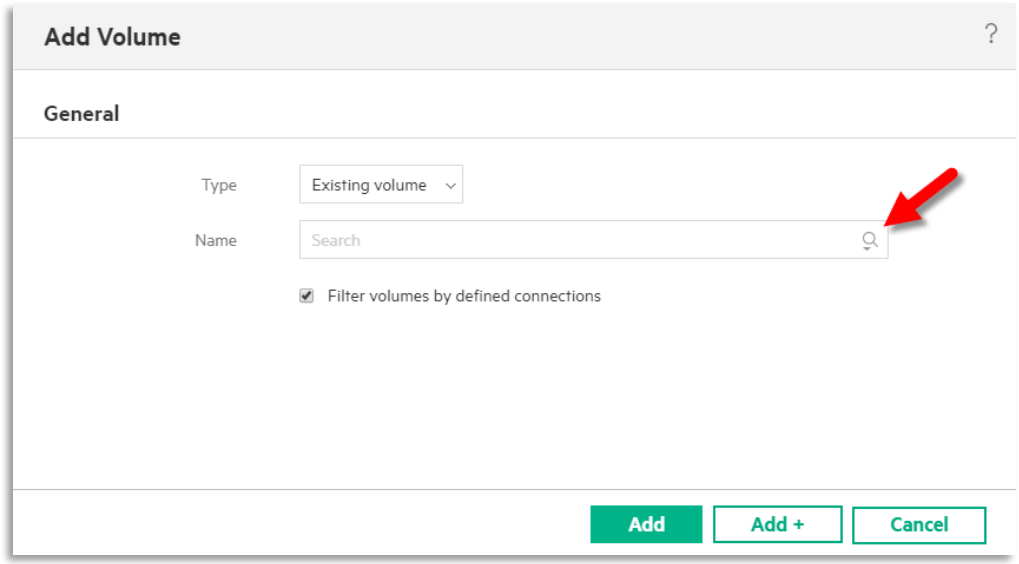
D. In the Add Volume dialog window, select Volume *Type* from the drop down list



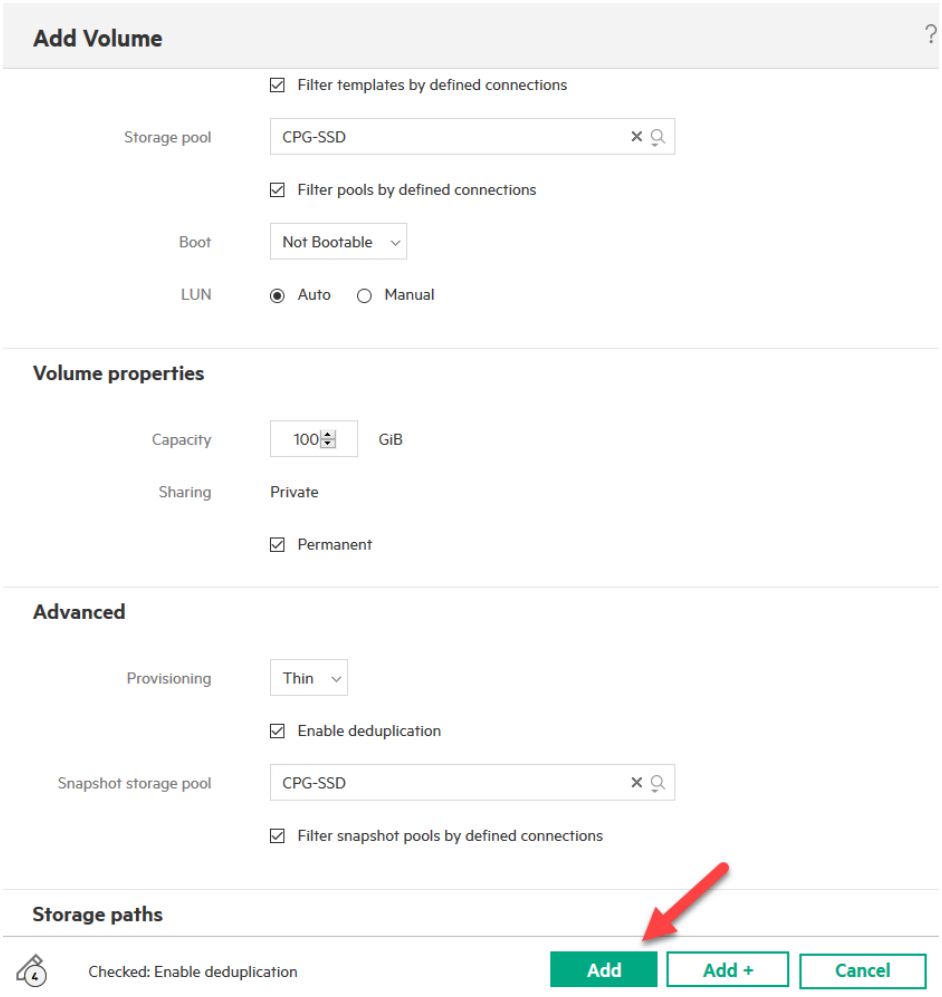
E. If creating a new volume, select a volume template or storage pool to create from and select the desired volume settings.



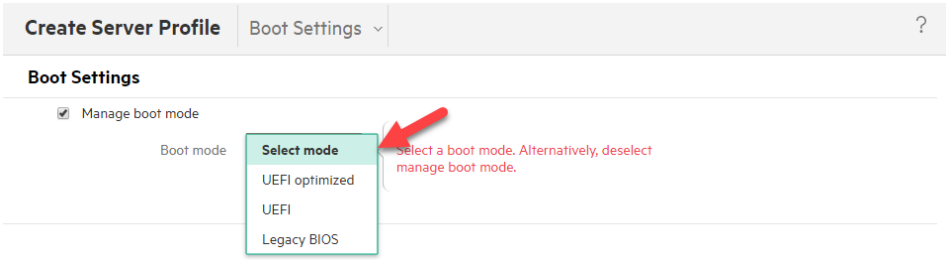
F. If using an existing volume, select the Volume using the dropdown list or the SmartSearch feature.



G. Once the *Volume* has been selected or configured, the default Storage Paths will be displayed. You can disable, remove or add Storage Paths. Click *Add or Add +* to add the volume.

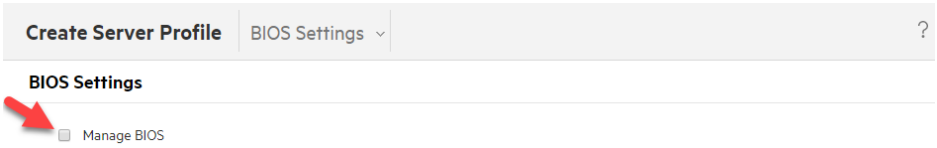


28. In the Boot Settings section, set the *boot* mode from the dropdown list

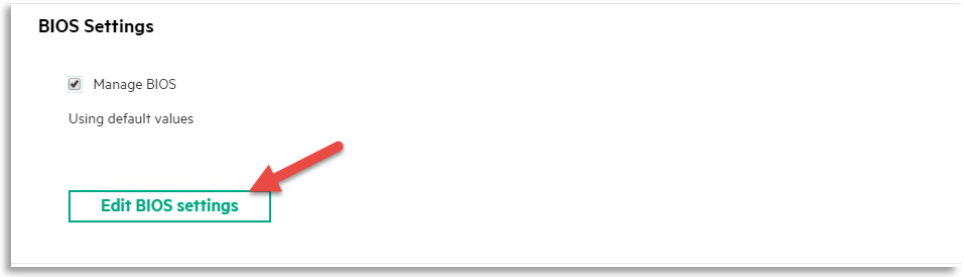


Warning
Disabling *Boot Order* in the Server Profile will also disable PXE and FC BfS configuration options.

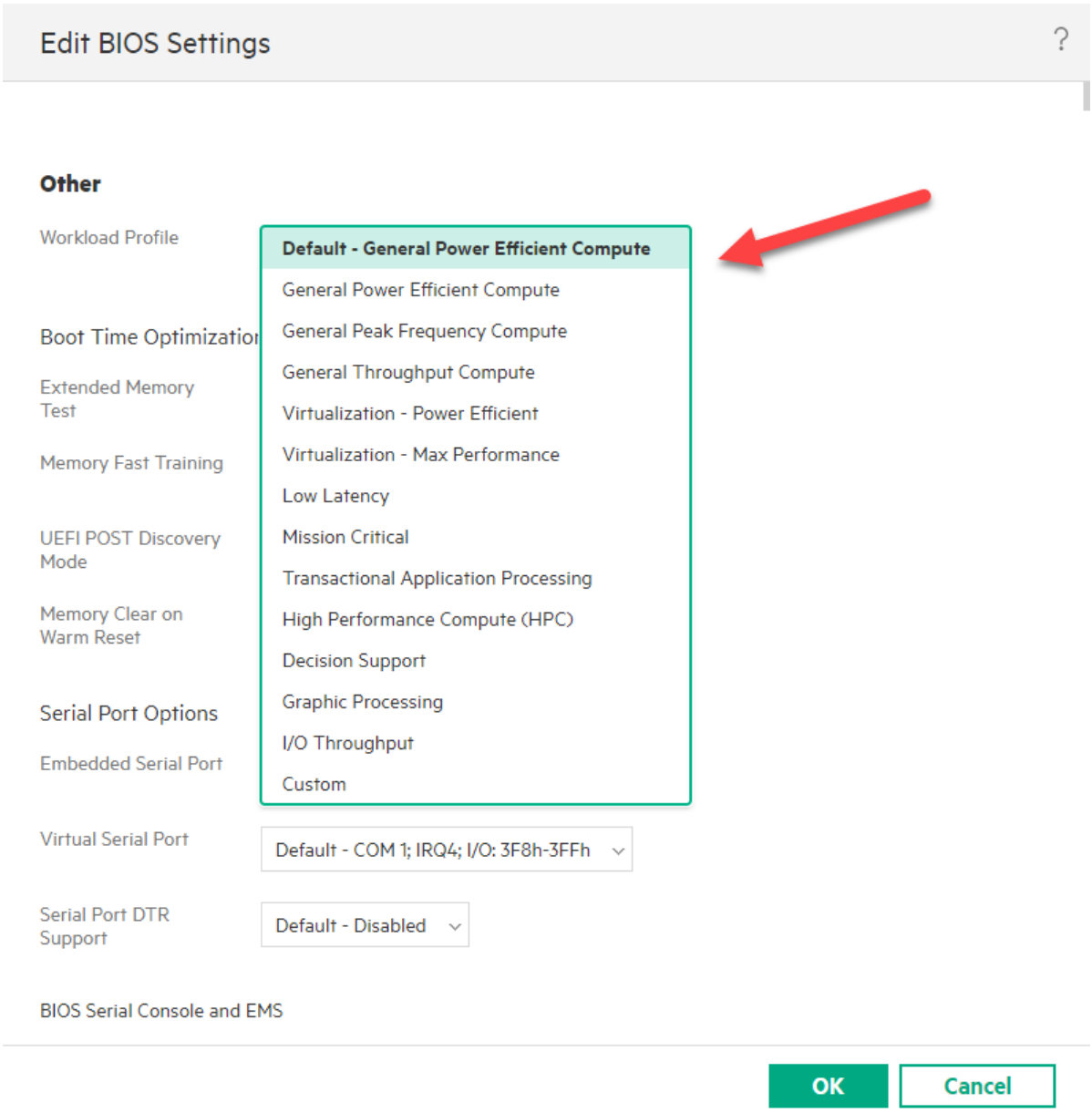
29. In the BIOS Settings section, if desired, check the box to *Manage BIOS*.



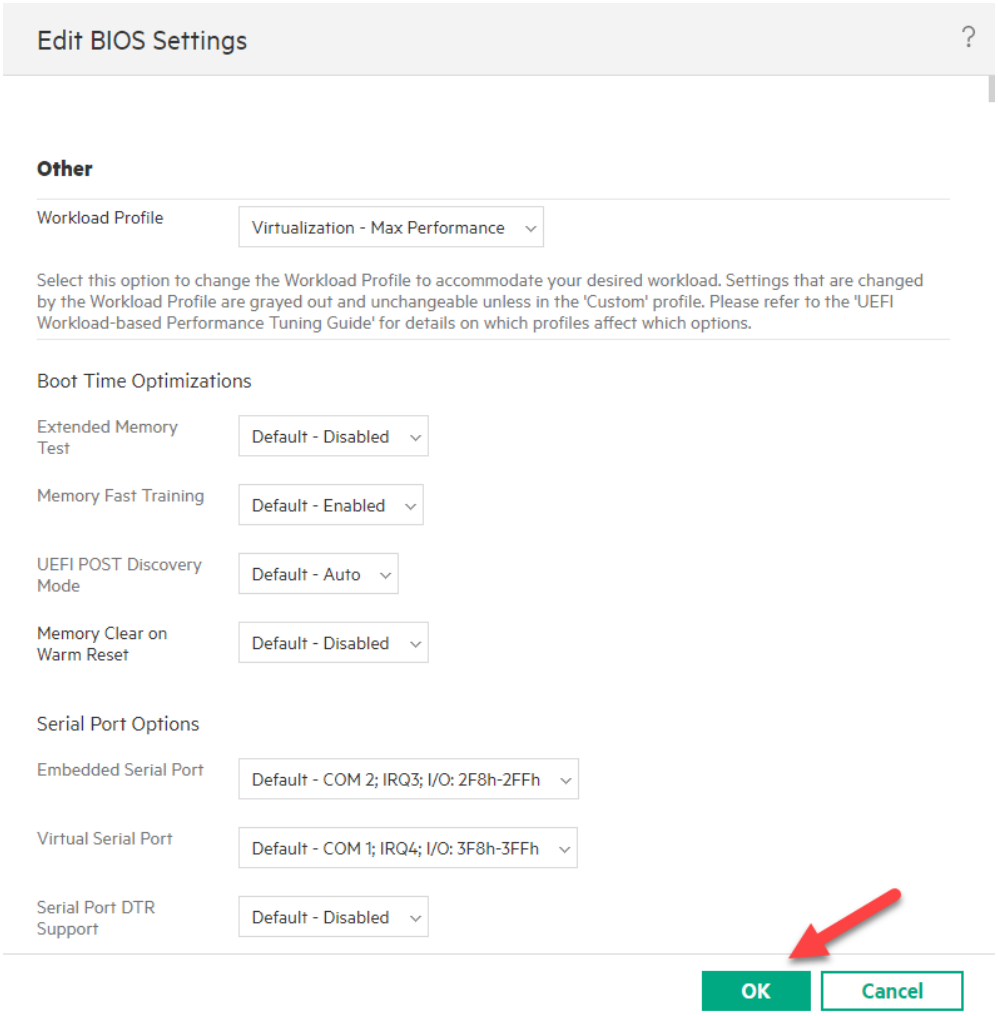
30. Click *Edit BIOS settings*



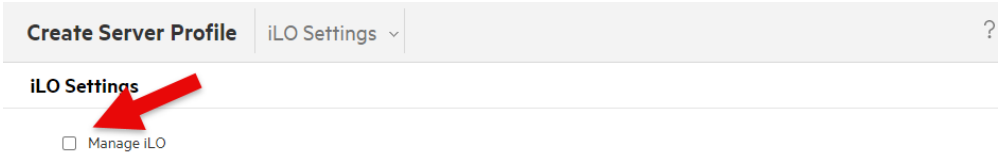
31. In the Edit BIOS settings dialog window, edit any desired BIOS settings or for Gen10 Servers choose a Workload Profile



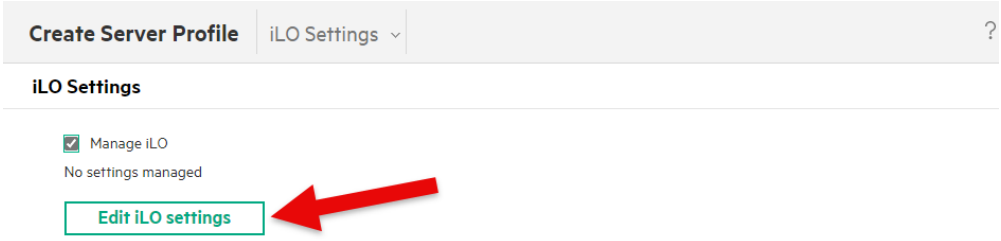
32. In the Edit BIOS settings dialog box, click *OK* after all of the desired BIOS settings are made.



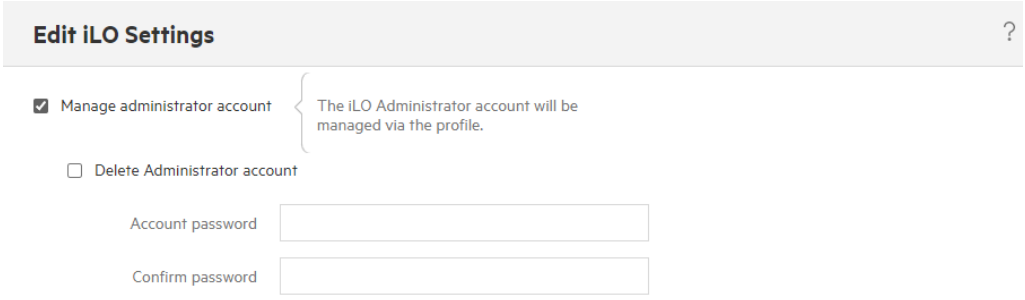
33. If desired, check the *Manage iLO* box in the iLO Settings section



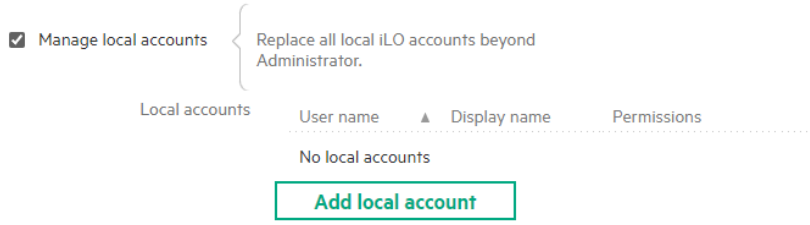
34. Click *Edit iLO settings*



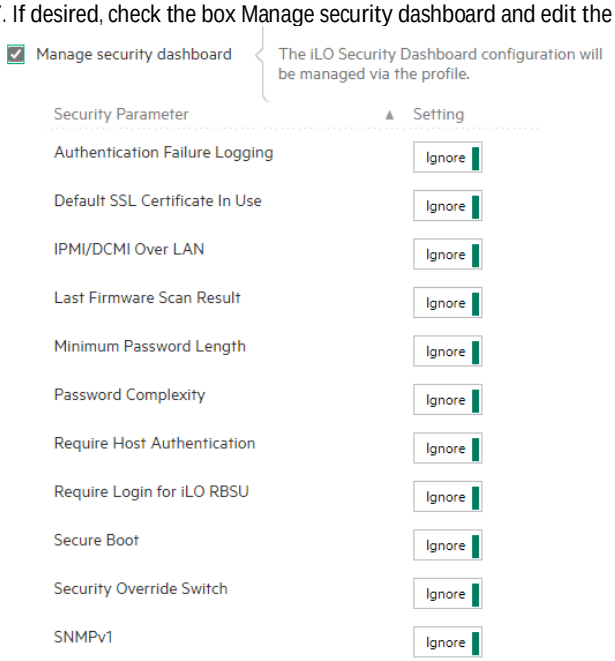
35. If desired, check the box *Manage administrator account* and edit the details as needed



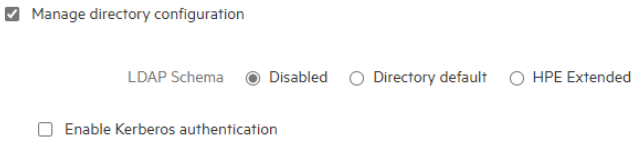
36. If desired, check the box *Manage local accounts* and edit the details as needed



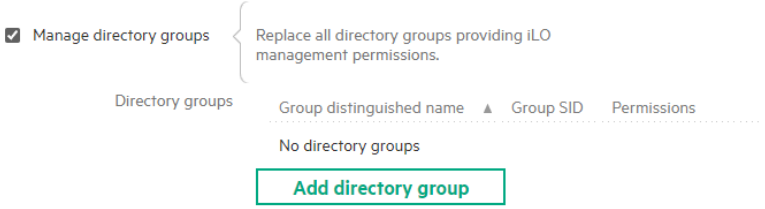
37. If desired, check the box Manage security dashboard and edit the details as needed



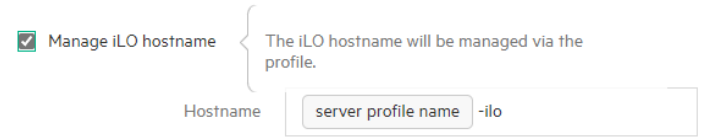
38. If desired, check the box *Manage directory configuration* and edit the details as needed



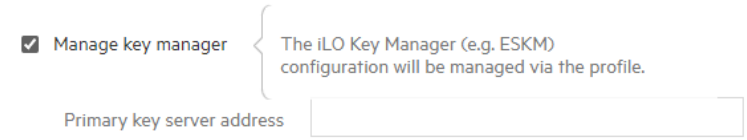
39. If desired, check the box *Manage directory groups* and edit the details as needed



40. If desired, check the box *Manage iLO hostname* and edit the details as needed

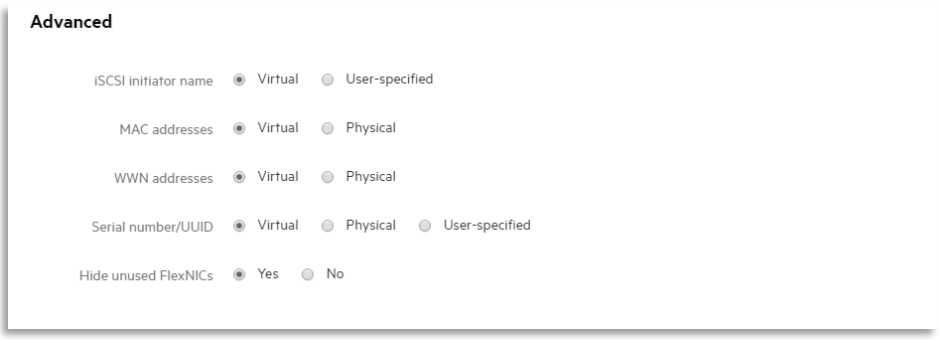


41. If desired, check the box *Manage key manager* and enter the Primary key server address

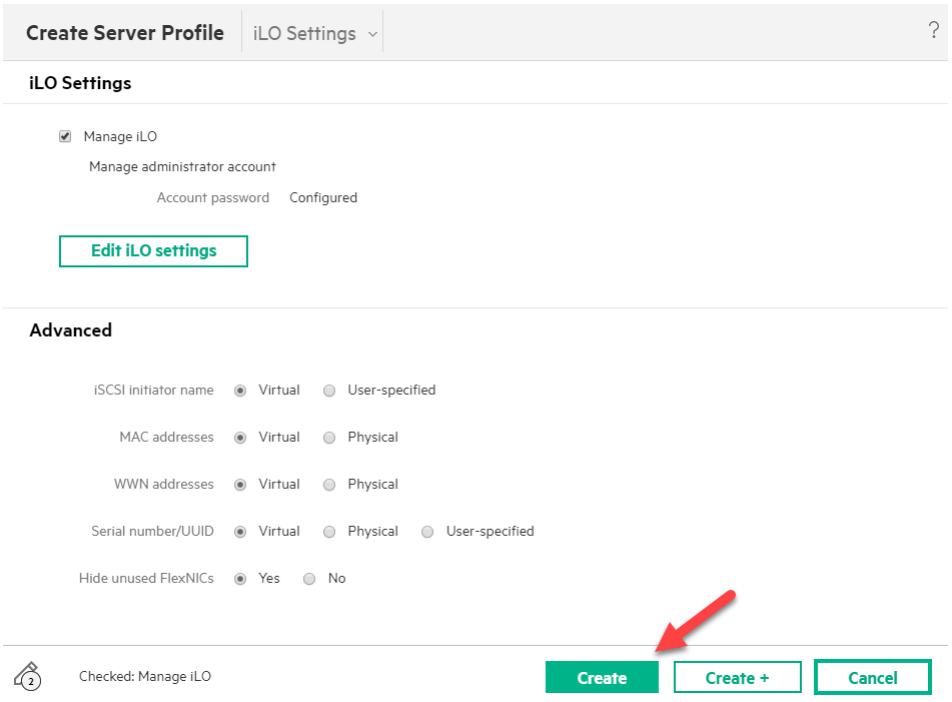


42. Click *OK* to save your iLO settings

43. The HPE recommendation is to leave the Advanced section as default, which would be Virtual Managed Addresses.

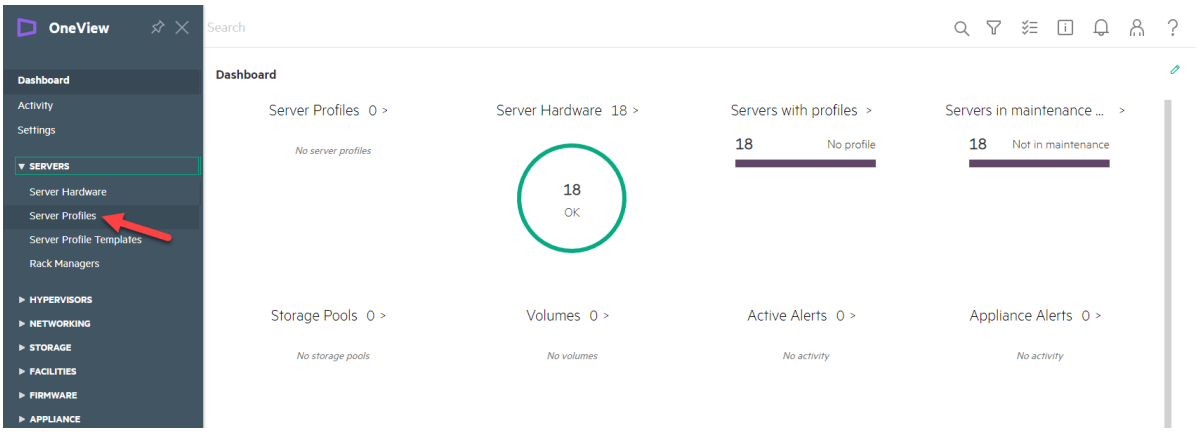


44. Click *Create or Create +*.

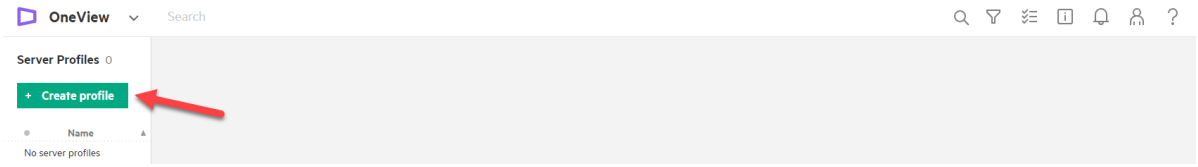


Create a Server Profile for Gen10 or newer DL Servers

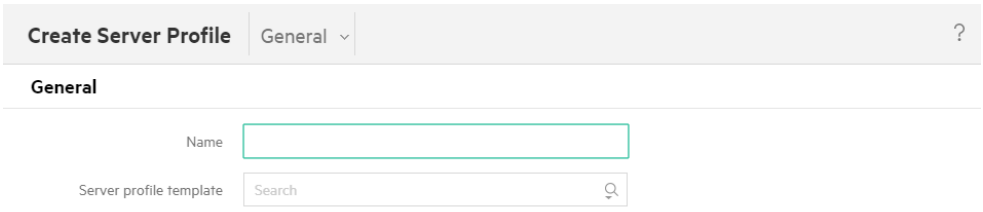
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



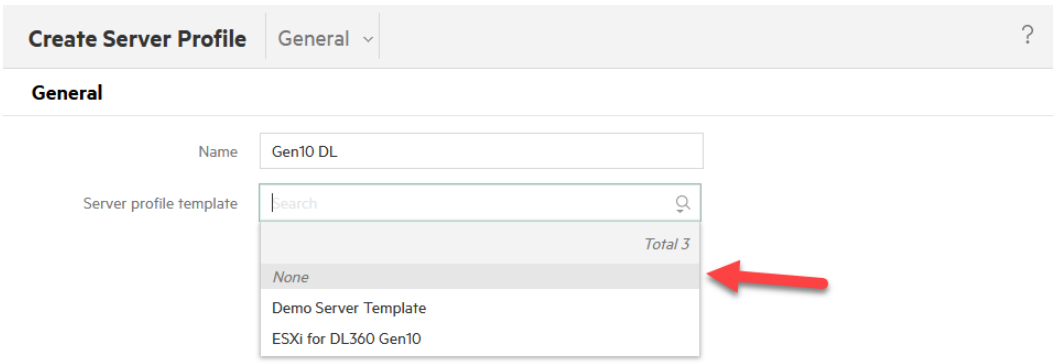
2. Click the + *Create profile* button.



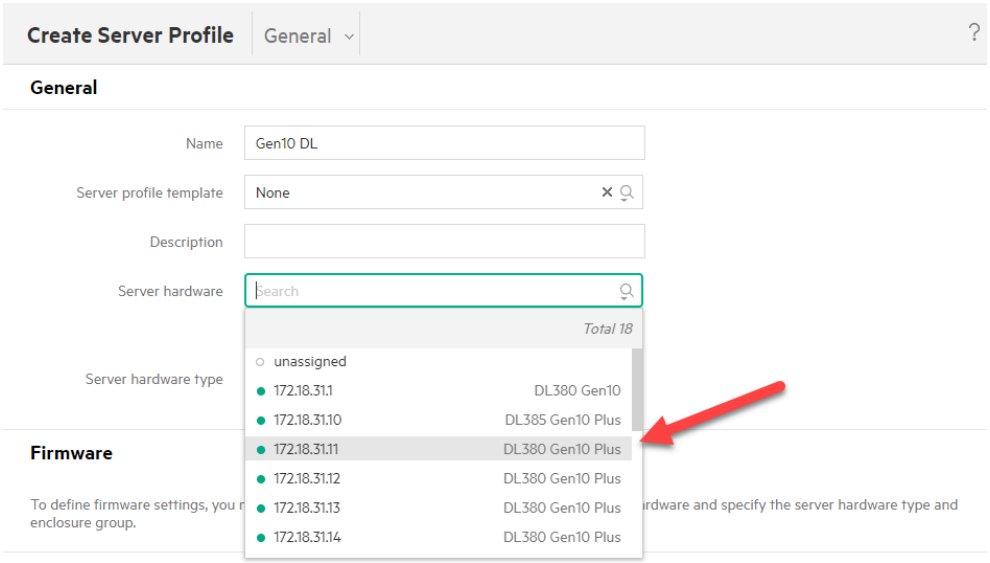
3. In the General section of the server profile creation page, provide a *Name* and optionally a *Description* for the Server Profile.



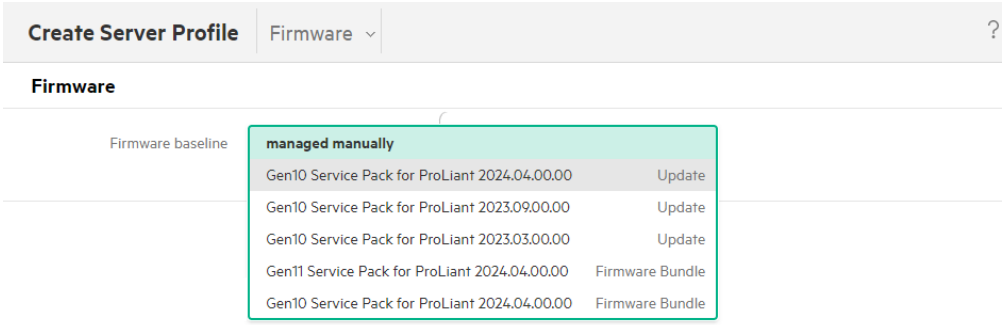
4. You have to choose a Server profile template, in this case because we do not want the profile based on one, you have to select *None*.



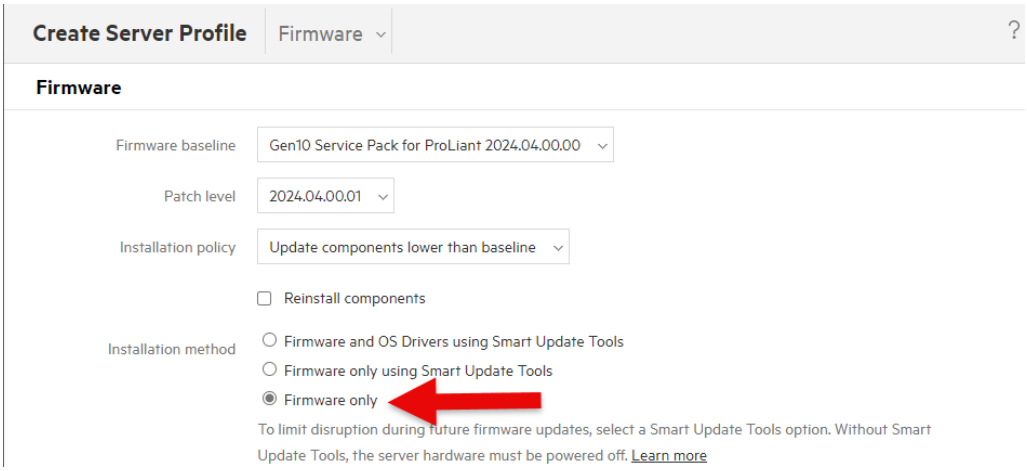
5. Select the *Server hardware* for the Server Profile



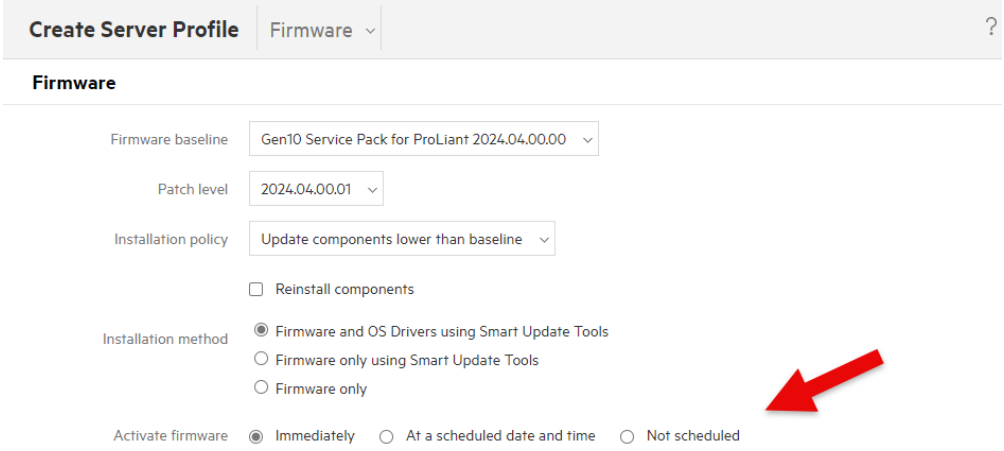
6. In the firmware section, select a *Firmware baseline* from the dropdown menu.



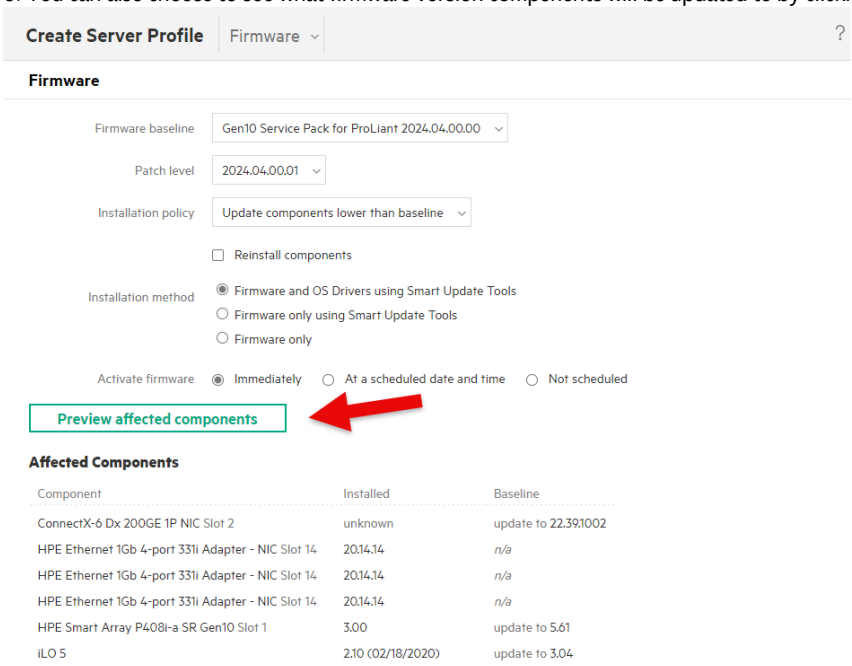
7. Once a baseline is selected, choose how the baseline will be applied to the servers used within this server profile template. If either of the options using the HPE Smart Update Tools is selected then the firmware or driver updates will be done while the systems are online. If the firmware *only* option is selected then the firmware will be updated offline using Intelligent Provisioning.



8. Select when the firmware updates will be deployed for this server profile template (if Smart Update Tools option has been selected).

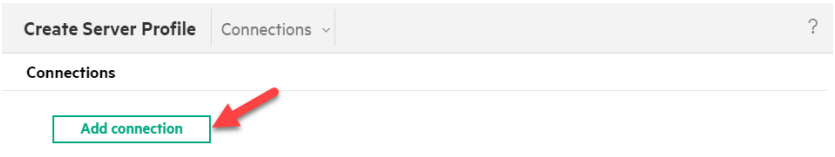


9. You can also choose to see what firmware version components will be updated to by clicking *Preview affected components*

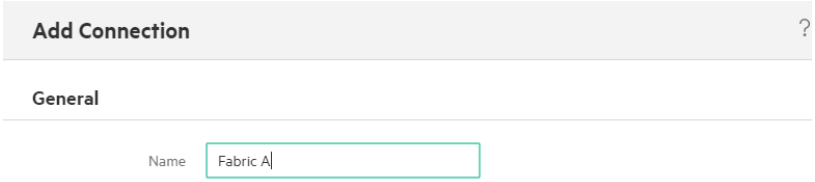


10. (Optional) You can set the SAN Fabric connection or Ethernet information, the following is for SAN Fabric

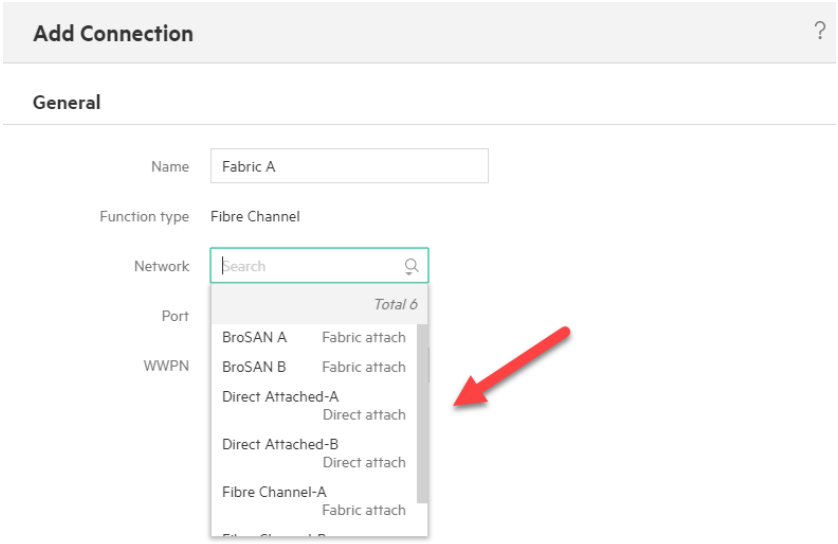
A. Choose *Add connection*.



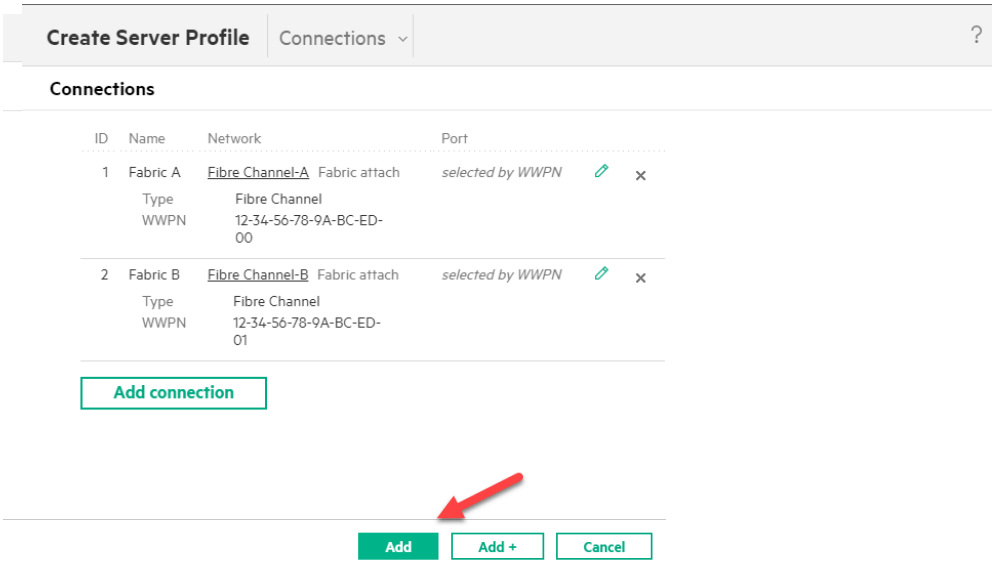
B. Type in a *Name* for the connection



C. Select a *Network* to attach this connection to.



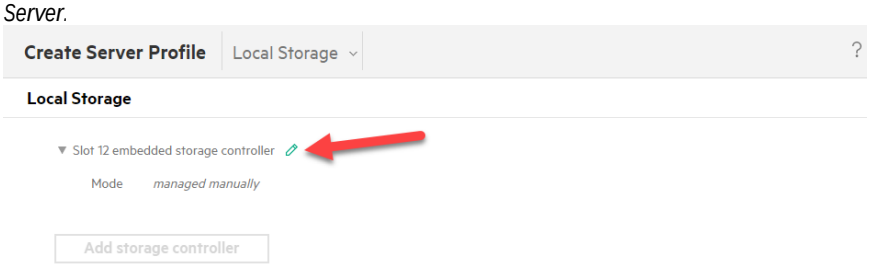
D. Input the WWPN number from the information that can be found in the iLO settings of the server you are creating the profile for. Once entered click *Add* to save the connection information.



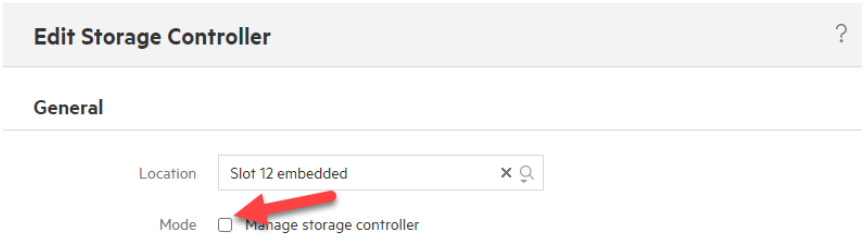
E. Once complete do the same for the second port assuming that you have either two single port cards or a single dual port FC card.

11. If desired, enable local storage management by editing the *edit* option on the Slot 0 embedded storage controller.

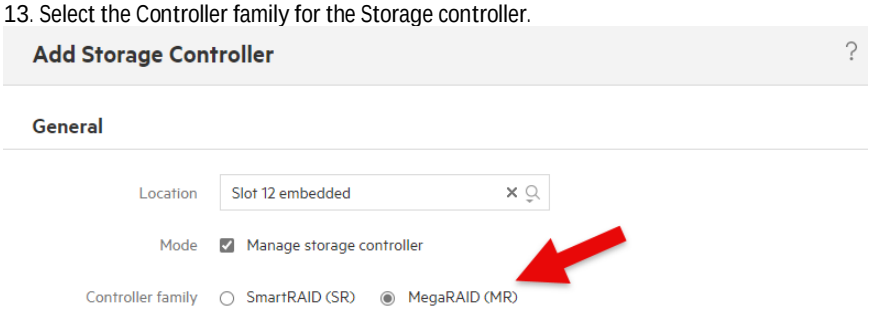
Note: *This will be different depending on the generation of the server due to different SMART Array Controller configs. The following is for a Gen9 Server.*



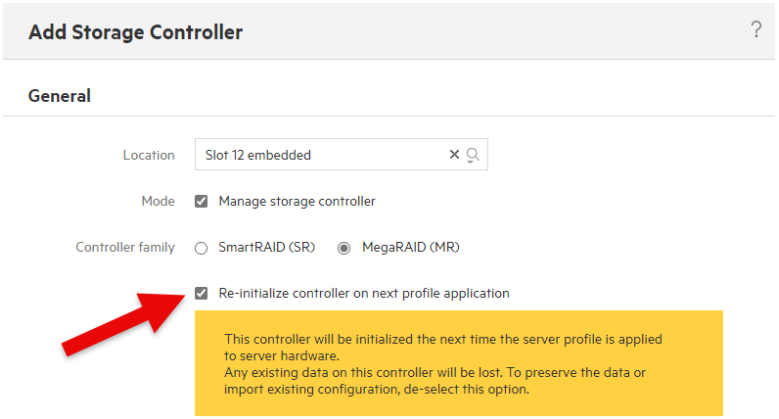
12. Click on *Manage storage controller* to configure the local storage on the Slot 0 embedded storage controller



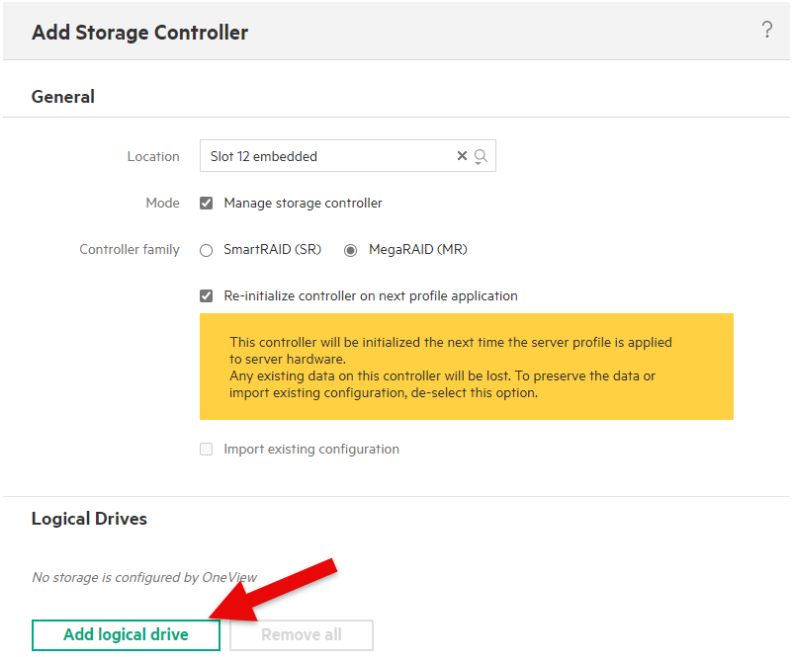
13. Select the Controller family for the Storage controller.



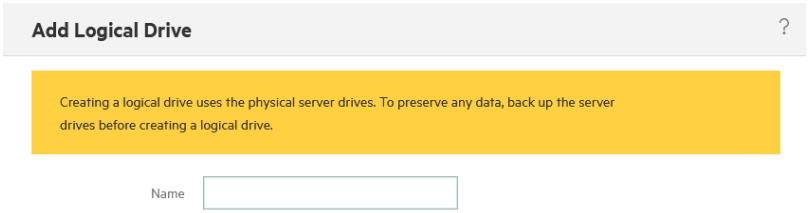
14. Enable or disable the option to Re-initialize controller on next profile application. A warning will be shown about this option



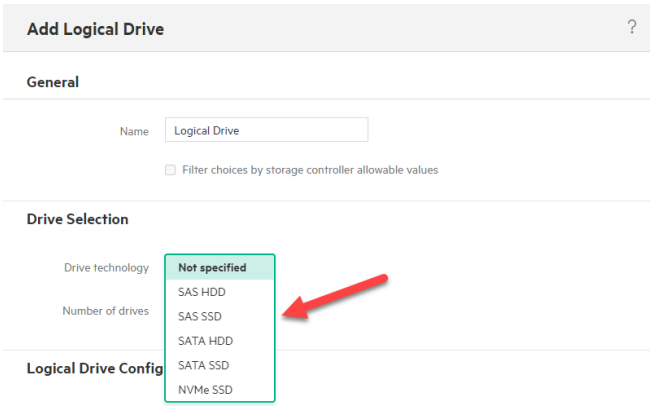
15. Click *Add logical drive*



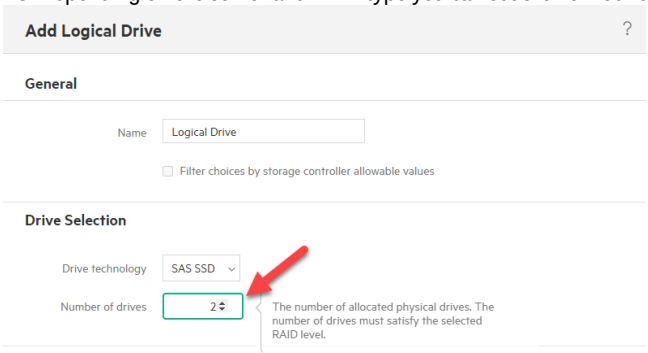
16. In the Add Logical Drive dialog window, enter a *Name* for the logical drive



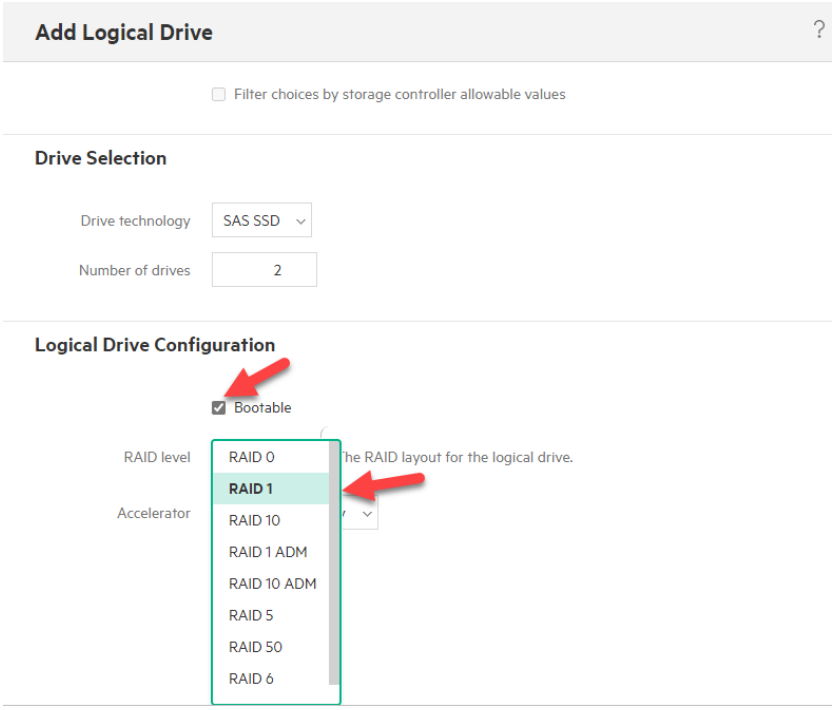
17. Select the *drive technology* for the logical drive



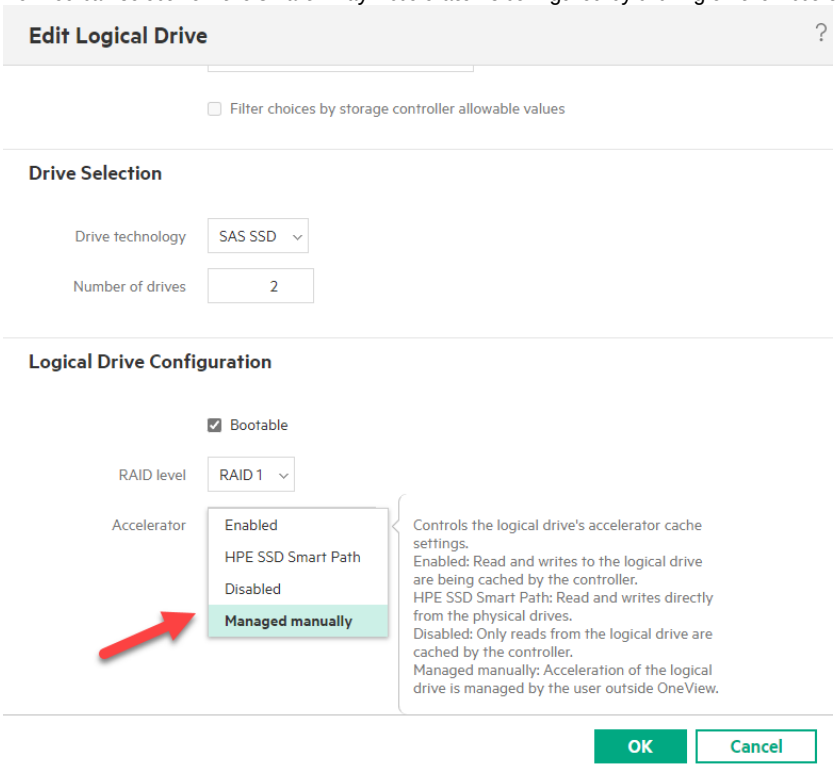
18. Depending on the server and RAID type you can set the *number of drives* for a RAID set



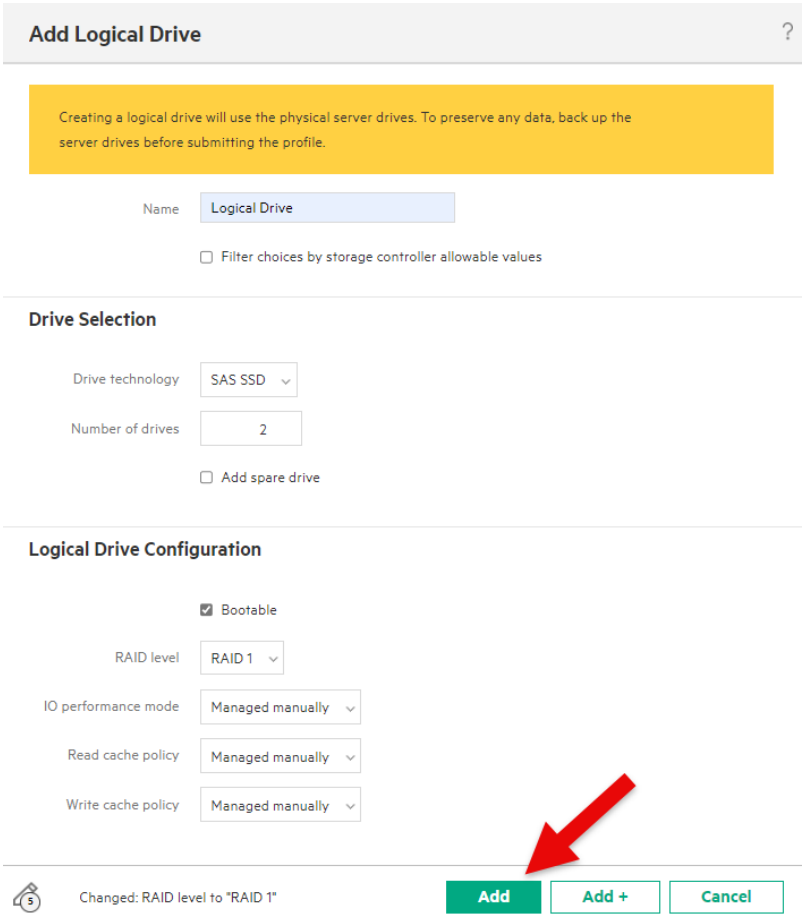
19. Select the *RAID level* and if this is a boot drive then click the *Bootable* box.



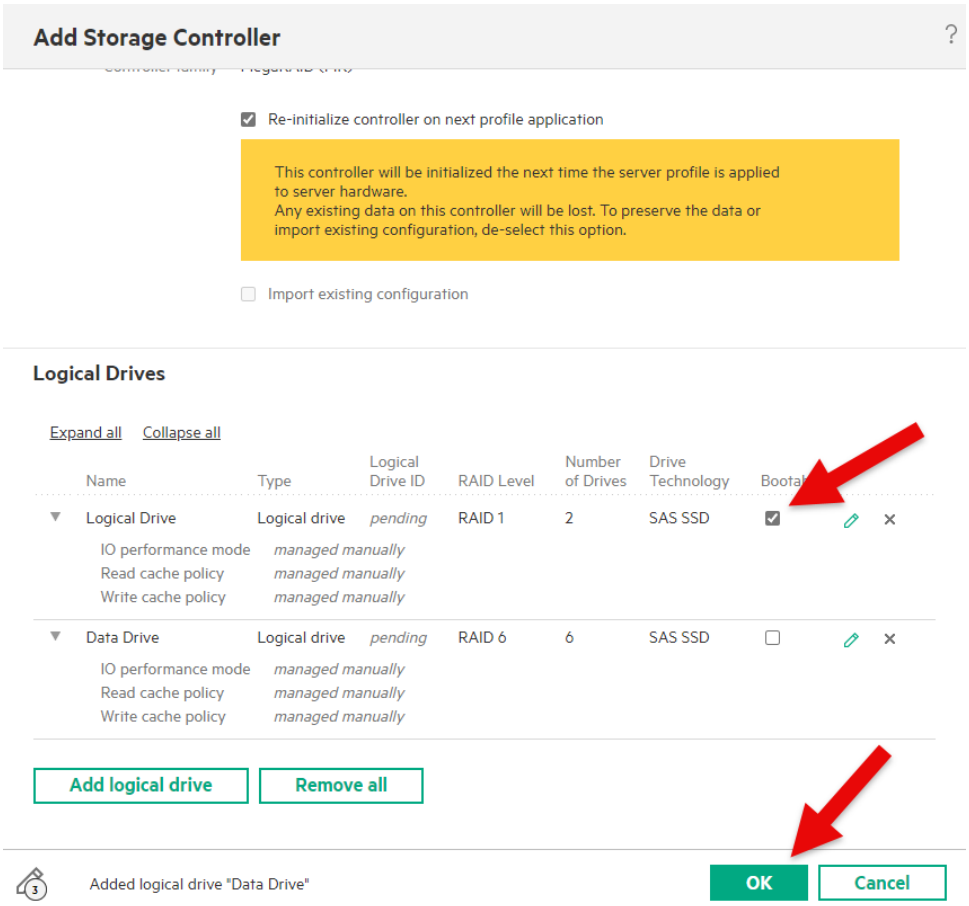
20. You can select how the Smart Array Accelerator is configured by clicking on the *Accelerator* menu



21. Click *Add or Add +* to create the logical drive for the server profile.



22. Once all of your logical drives are created, you can still select which one is the boot drive. Click *OK* to finish configuring the Slot 0 embedded storage controller.

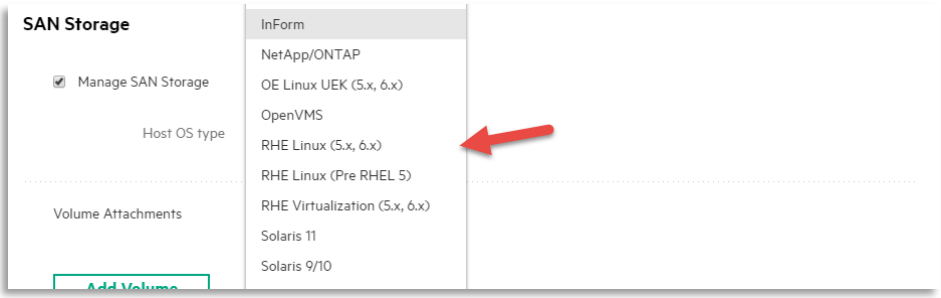


23. Enable *SAN Storage* if necessary.

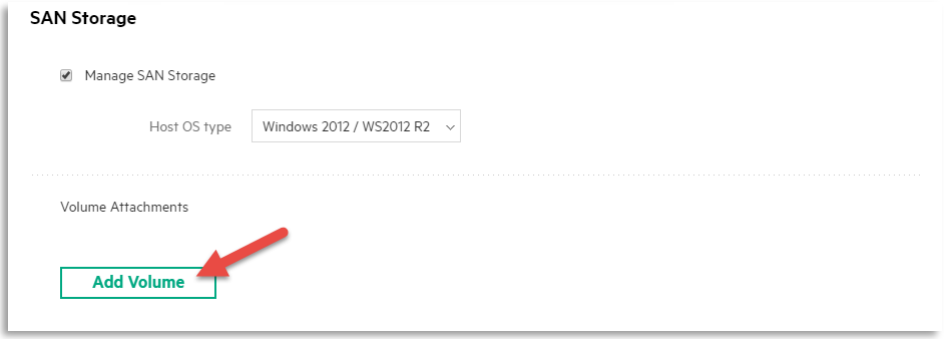
A. *Check the box* for *Manage SAN Storage*



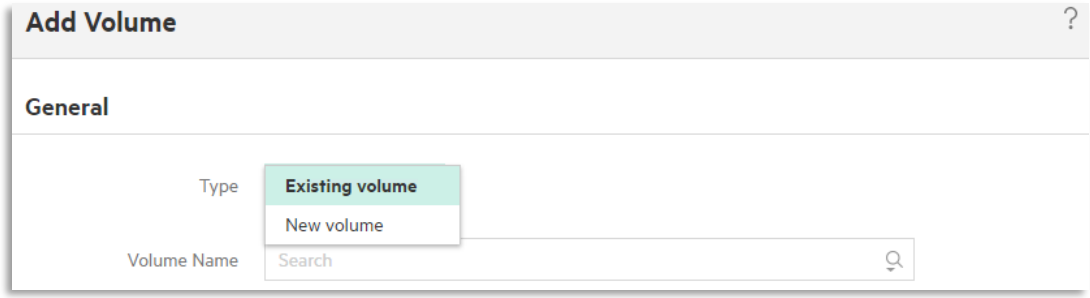
B. Specify the *Host OS type*, which controls the Host's OS / personna created on the HPE 3PAR StoreServ storage system.



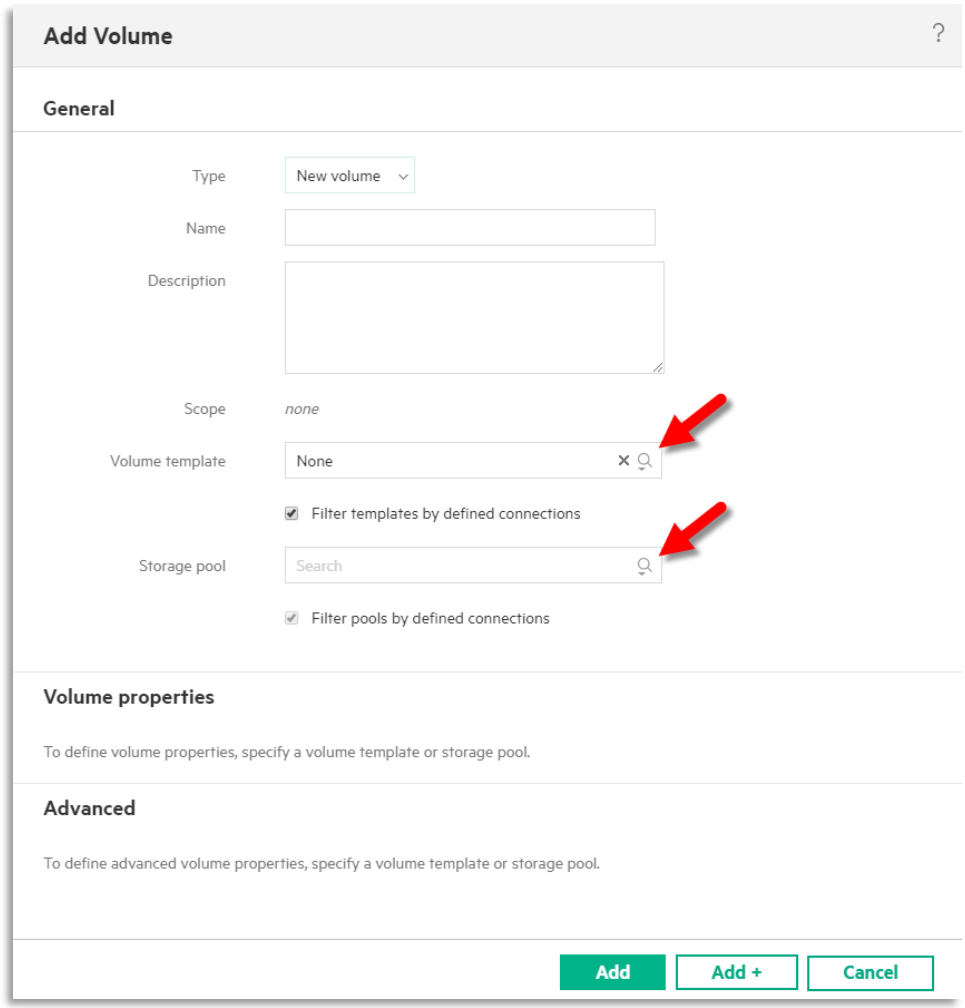
C. Click the *Add Volume* button to display the list of volumes available for assignment.



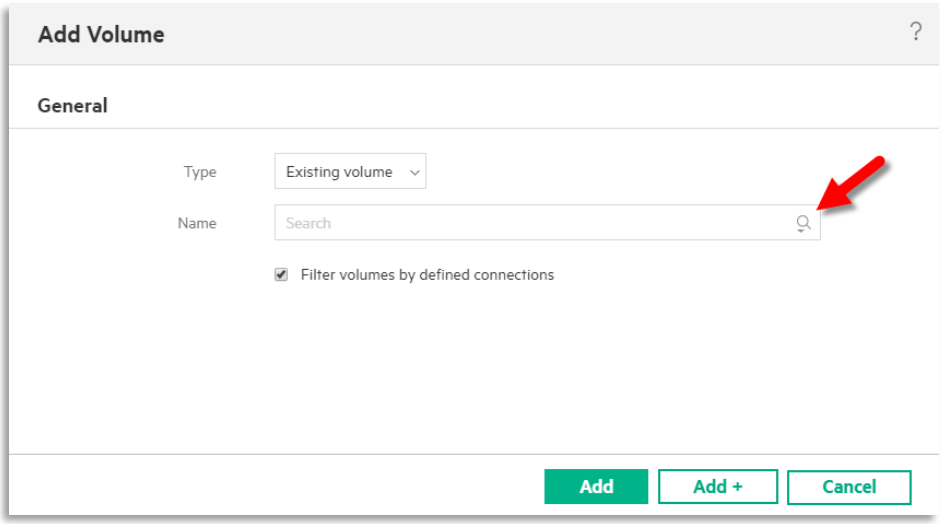
D. In the Add Volume dialog window, select volume *Type* from the drop down list



E. If creating a new volume, select a volume template or storage pool to create from and select the desired volume settings.

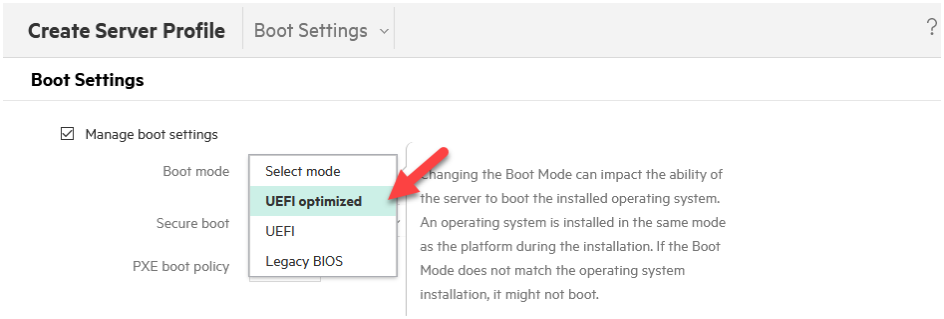


F. If using an existing volume, select the Volume using the dropdown list or the SmartSearch feature.



G. Once the *Volume* has been selected or configured, the default Storage Paths will be displayed. You can disable, remove or add Storage Paths. Click *Add or Add +* to add the volume

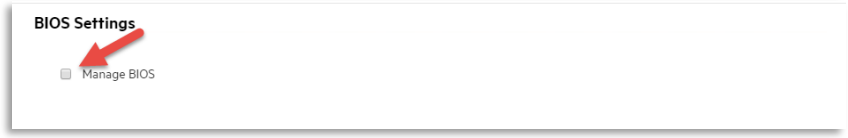
24. In the Boot Settings section, set the *Boot mode* from the dropdown list



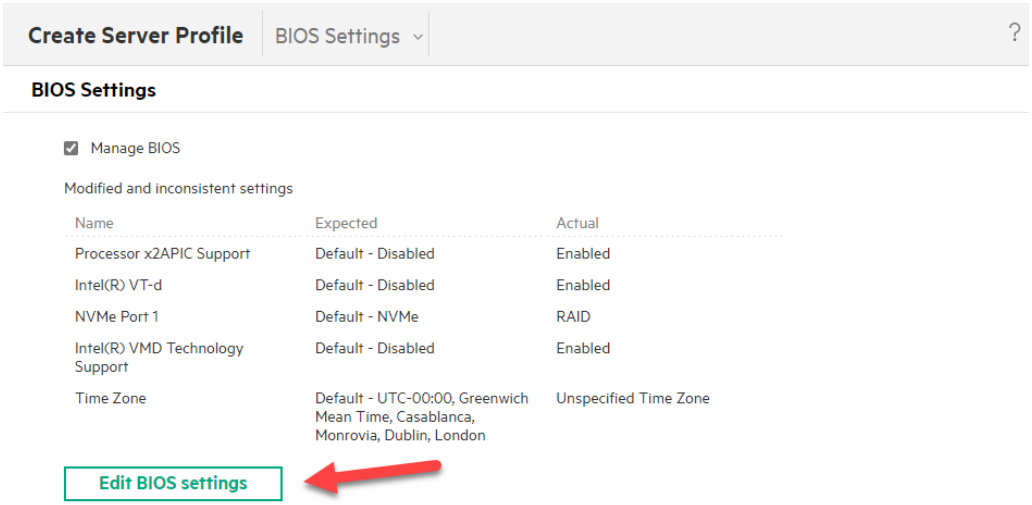
Warning
Disabling *Boot Order* in the Server Profile will also disable PXE and FC BfS configuration options.

---

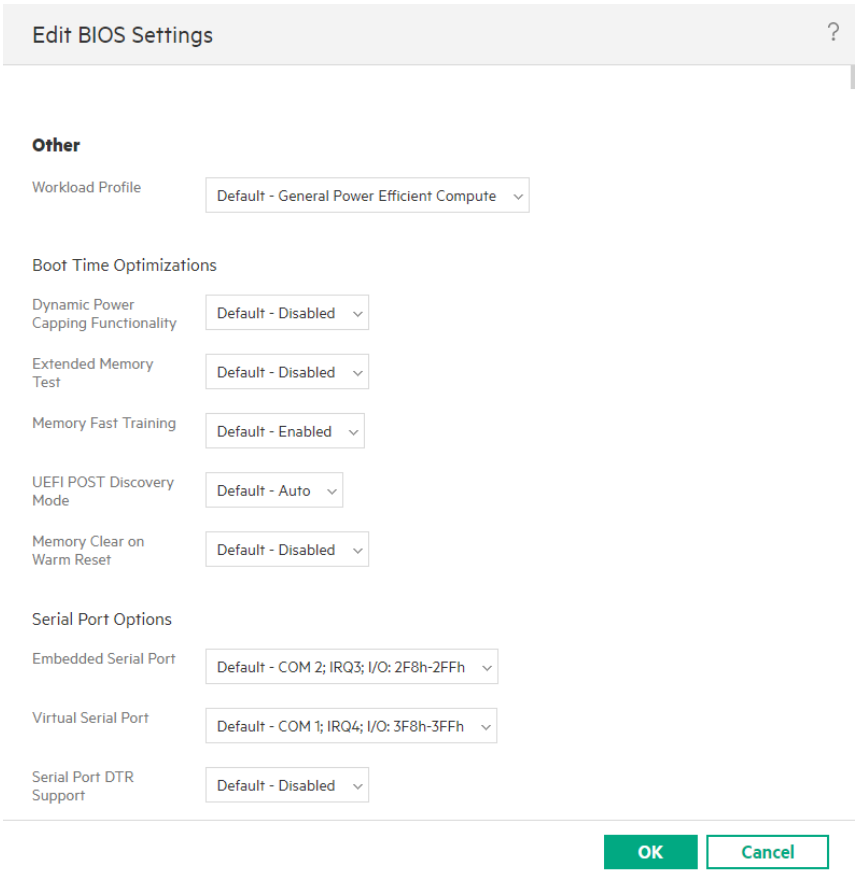
25. In the BIOS Settings section, if desired, check the box to *Manage BIOS*.



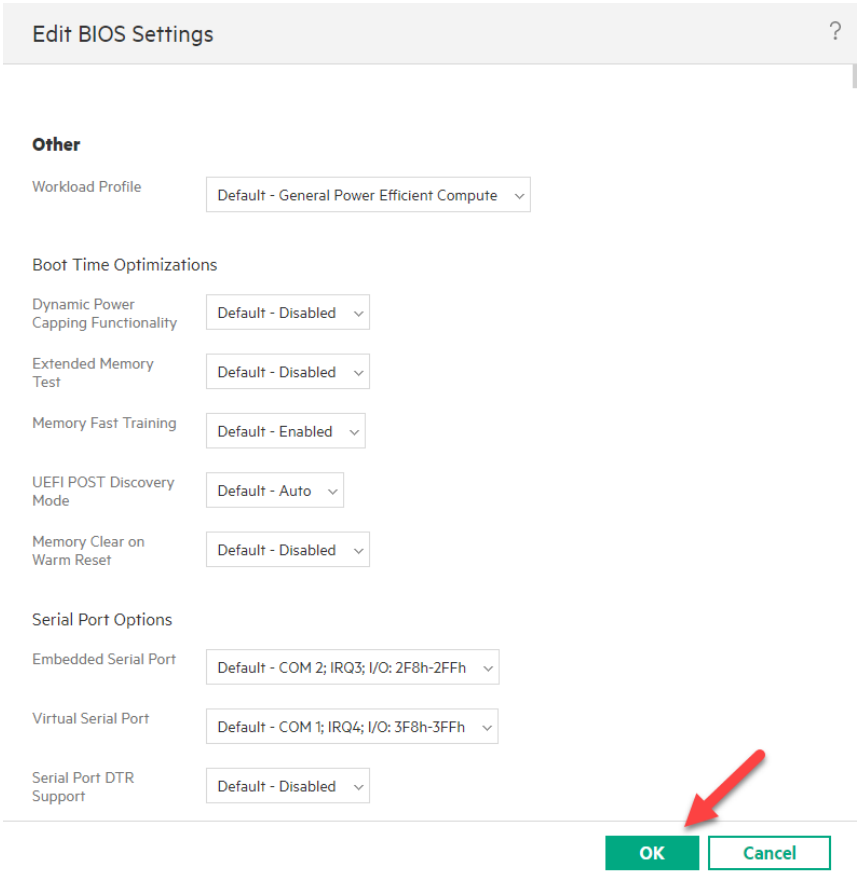
26. Click *Edit BIOS settings*



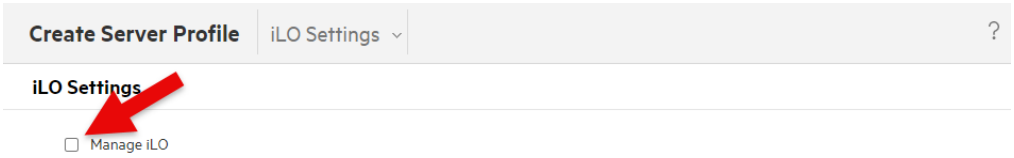
27. In the Edit BIOS settings dialog window, *edit* any desired BIOS settings.



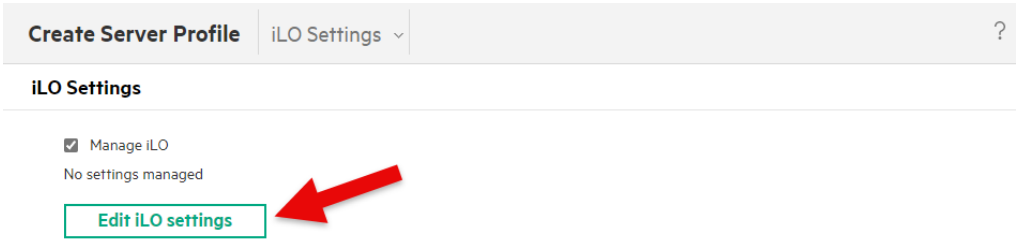
28. In the Edit BIOS settings dialog box, click *OK* after all of the desired BIOS settings are made.



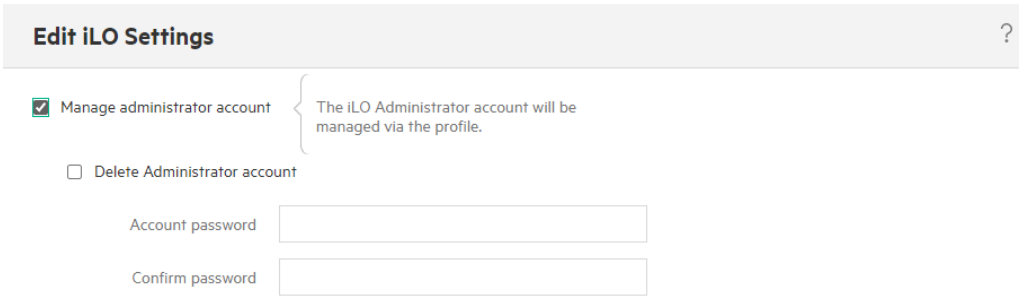
29. If desired, check the *Manage iLO* box in the iLO Settings section



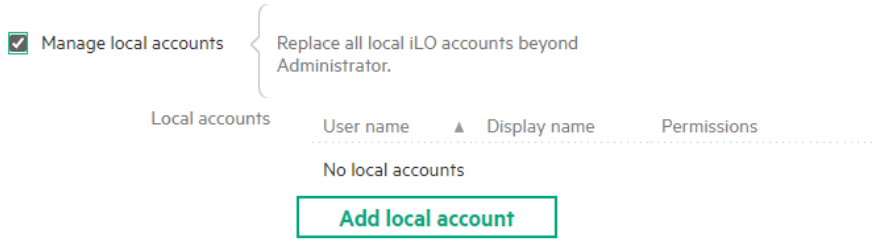
30. Click *Edit iLO settings*



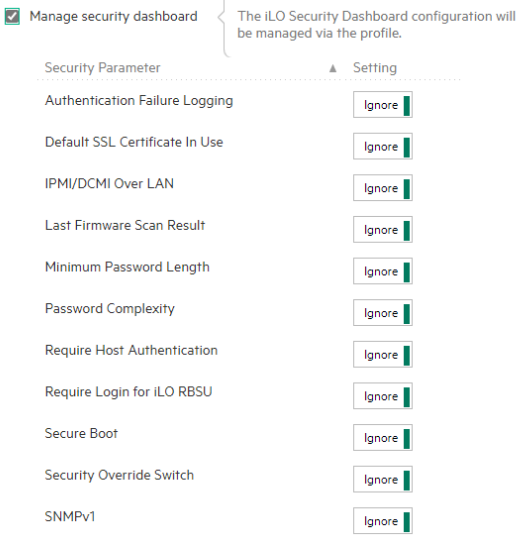
31. If desired, check the box *Manage administrator account* and edit the details as needed



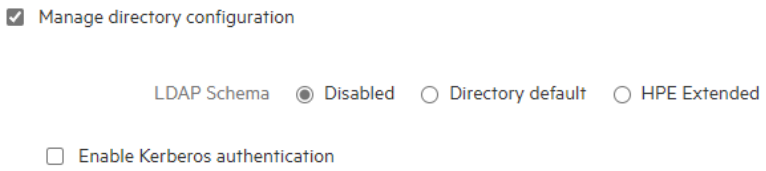
32. If desired, check the box *Manage local accounts* and edit the details as needed



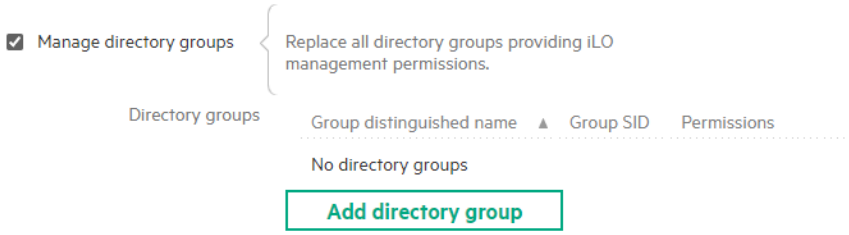
33. If desired, check the box *Manage security dashboard* and edit the details as needed



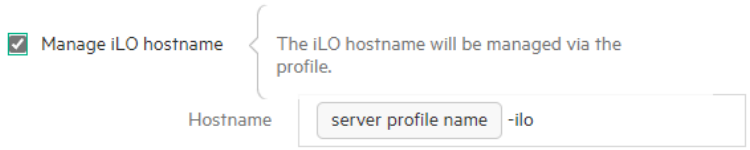
34. If desired, check the box *Manage directory configuration* and edit the details as needed



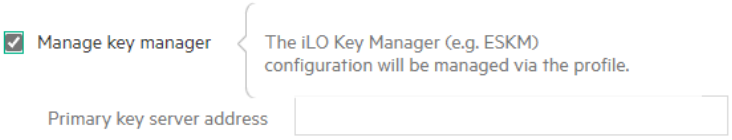
35. If desired, check the box *Manage directory groups* and edit the details as needed



36. If desired, check the box *Manage iLO hostname* and edit the details as needed



37. If desired, check the box *Manage key manager* and enter the Primary key server address

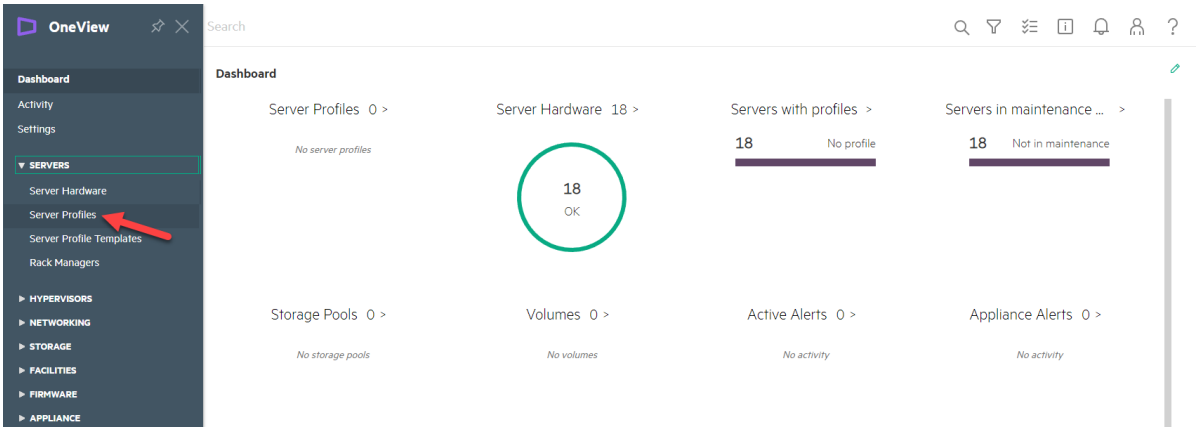


38. Once finished click *OK* to save the iLO settings and then Click *Create* or the *Create* + button to create the Server Profile

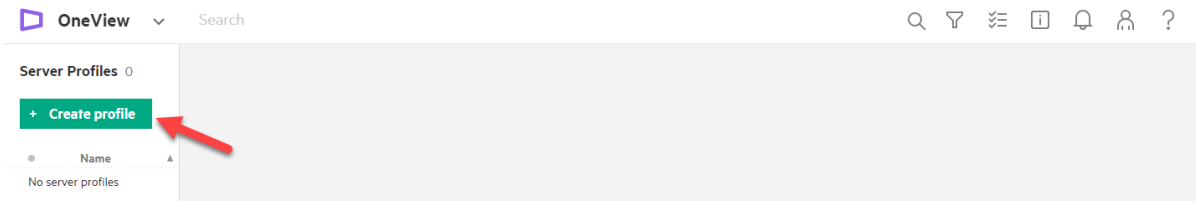
Create a Server Profile for Gen8 / Gen9 Servers

HPE OneView has basic Server Profile support for Gen8 / Gen9 platforms. Only BIOS, FC connections and Firmware management are supported with these platforms.

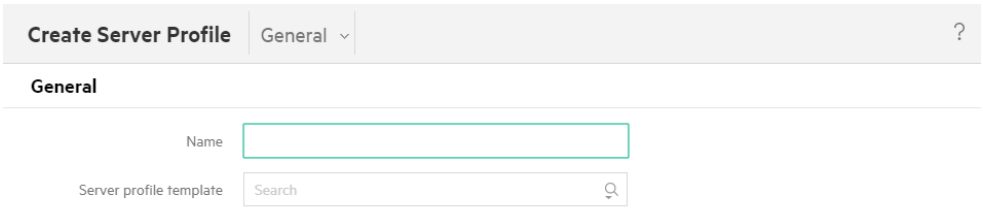
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



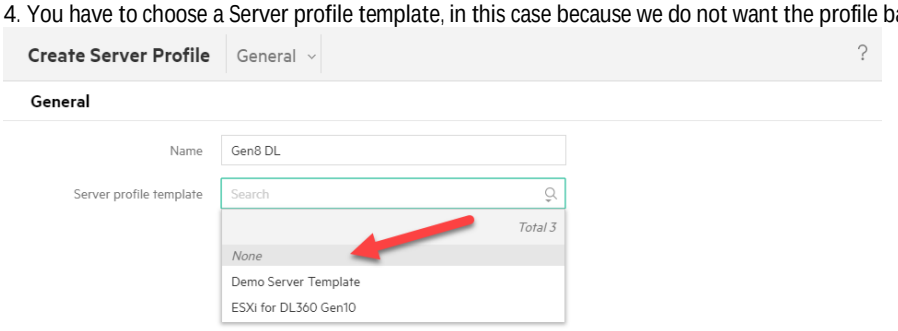
2. Click the + *Create profile* button.



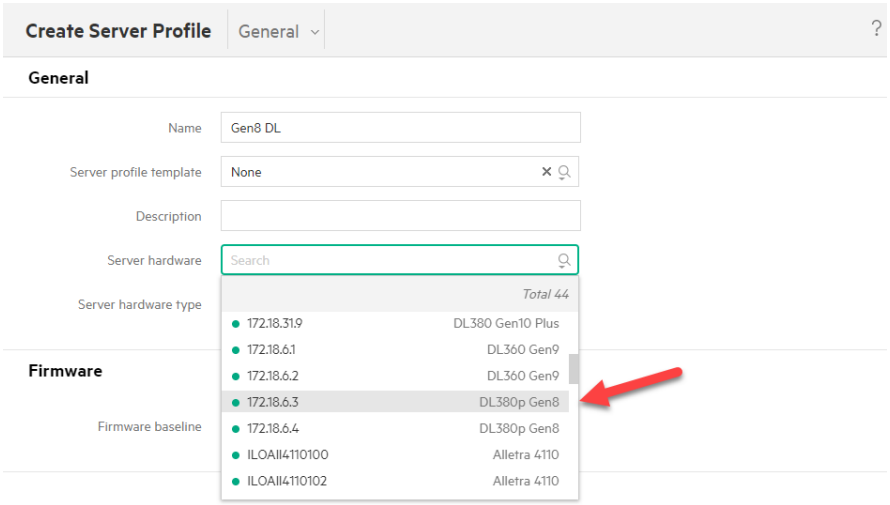
3. In the General section of the server profile creation page, provide a *Name* for the Server Profile.



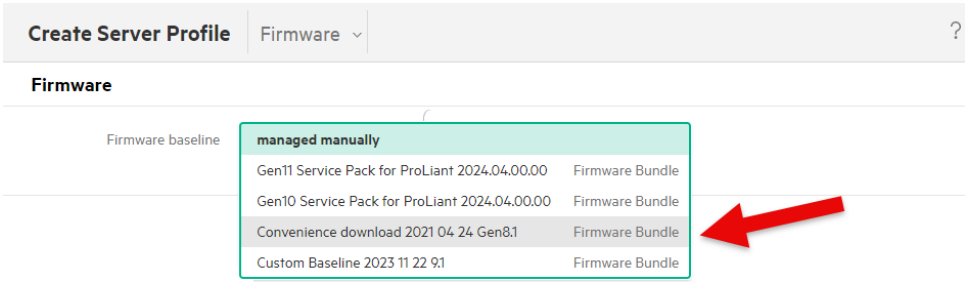
4. You have to choose a Server profile template, in this case because we do not want the profile based on one, you have to select *None*.



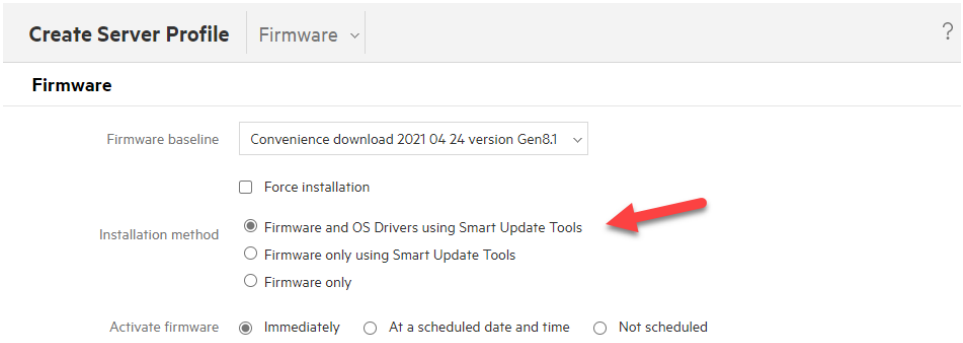
5. Select the *Server hardware* that the profile will be applied to using the dropdown menu.



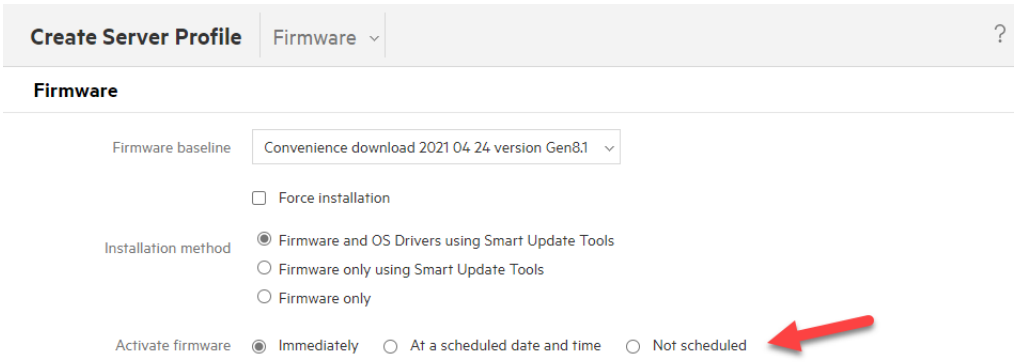
6. In the firmware section, select a *Firmware baseline* from the dropdown menu.



7. Once a baseline is selected, choose how the baseline will be applied to the servers used within this server profile template. If either of the options using the HPE Smart Update Tools is selected then the firmware or driver updates will be done while the systems are online. If the firmware *only* option is selected then the firmware will be updated offline using Intelligent Provisioning.

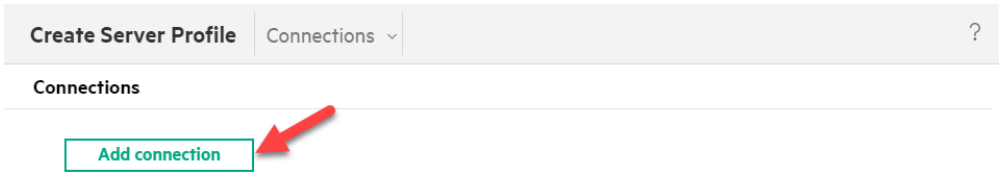


8. Select when the firmware updates will be deployed for this server profile template

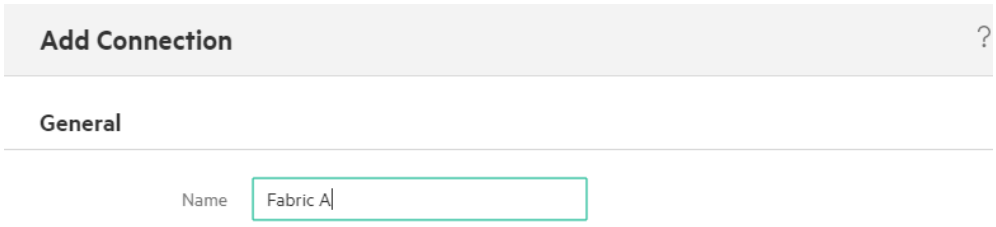


9. (Optional) You can set the SAN Fabric connection information

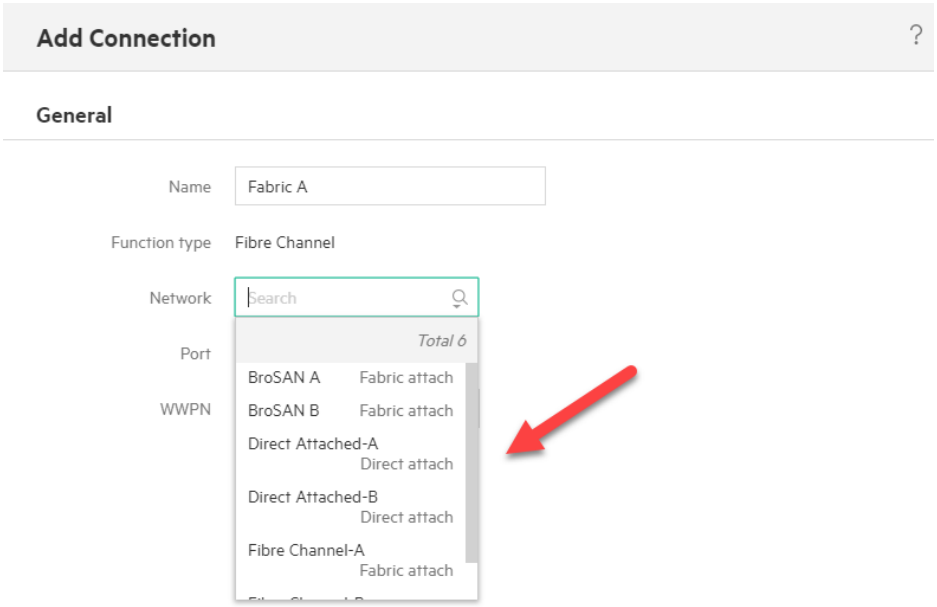
A. Choose *Add connection*.



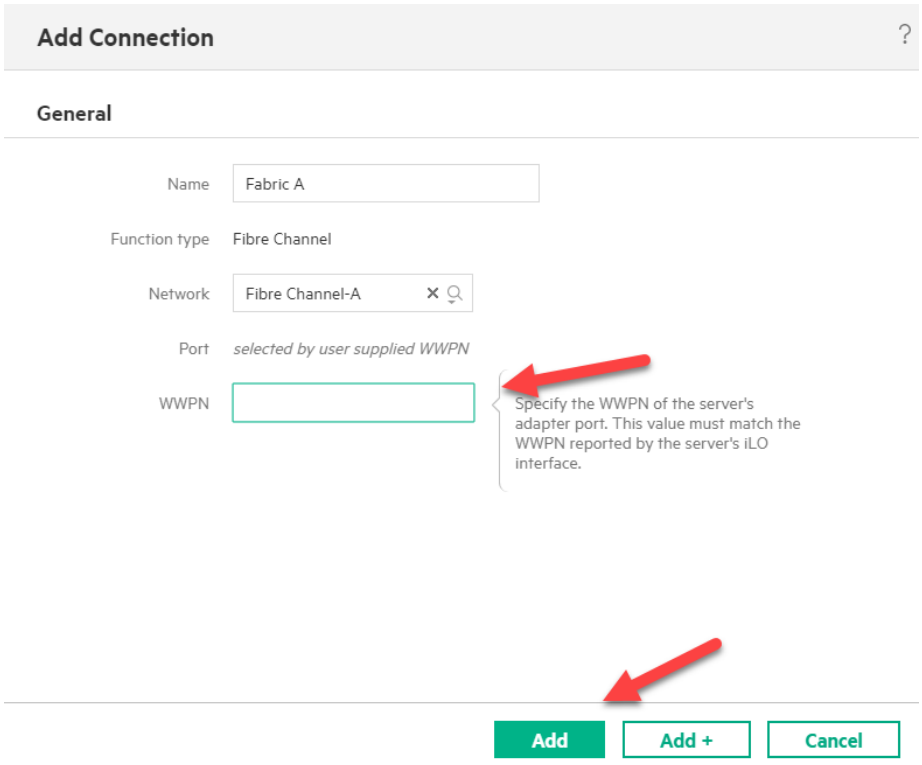
B. Type in a *Name* for the connection



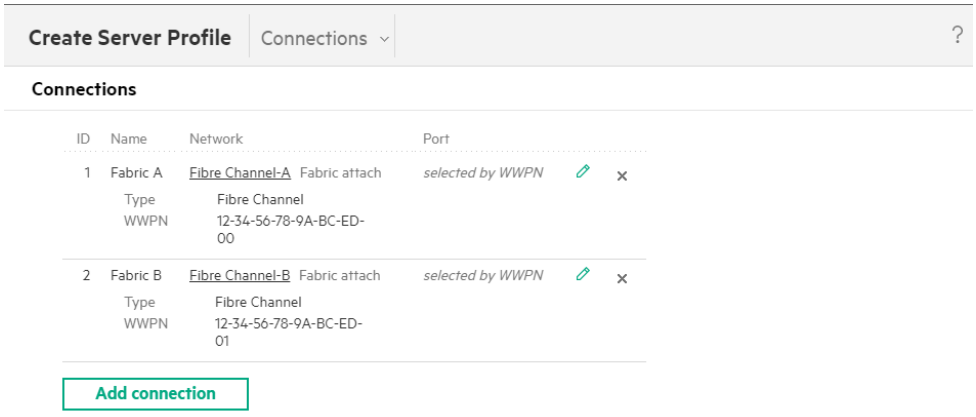
C. Select a *Network* to attach this connection to.



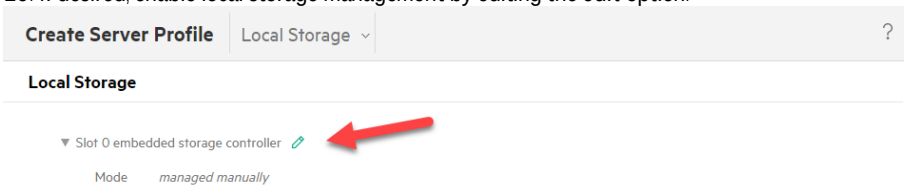
D. Input the WWPN from the information that can be found in the iLO settings of the server you are creating the profile for. Once entered click *Add* to save the connection information.



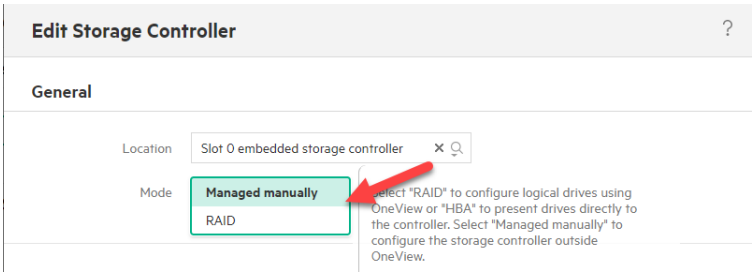
E. Once complete do the same for the second port assuming that you have either two single port cards or a single dual port FC card.



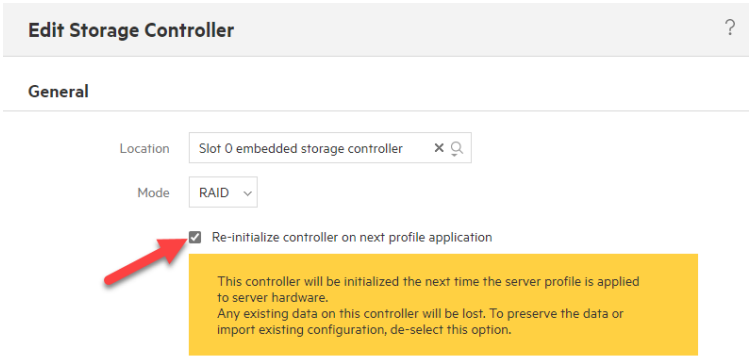
10. If desired, enable local storage management by editing the *edit* option.



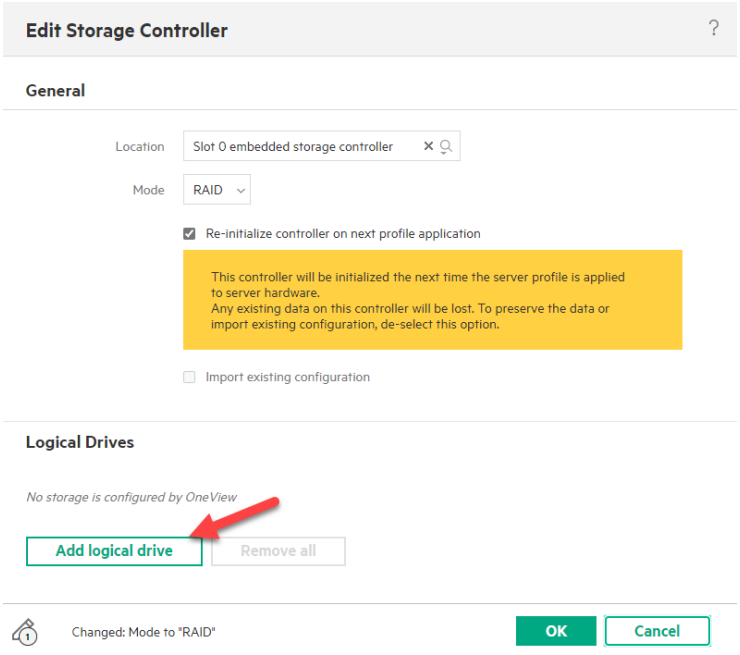
11. In the Edit Slot 0 embedded storage controller dialog box, select the *Mode* of the storage controller using the dropdown list



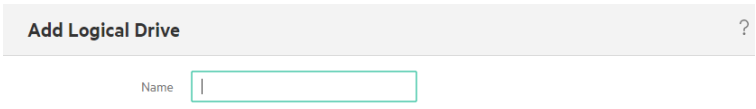
12. Enable or disable the option to Re-initialize controller on next profile application. A warning will be shown about this option



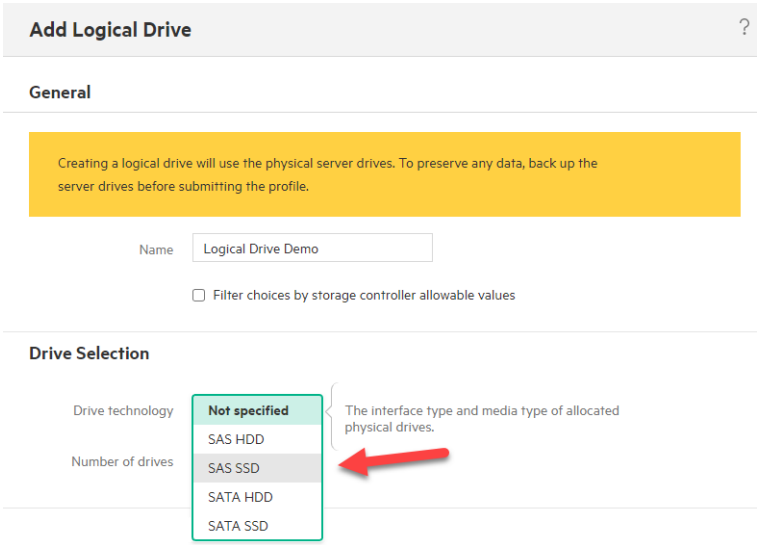
13. Click *Add logical drive*



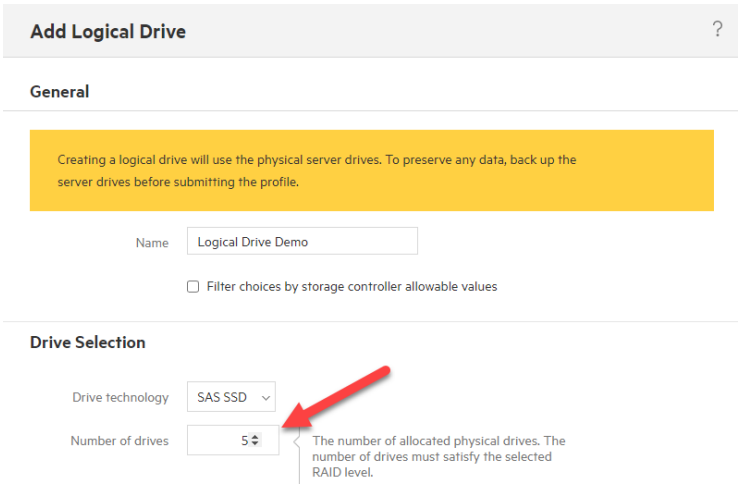
14. In the Add Logical Drive dialog window, enter a *Name* for the logical drive



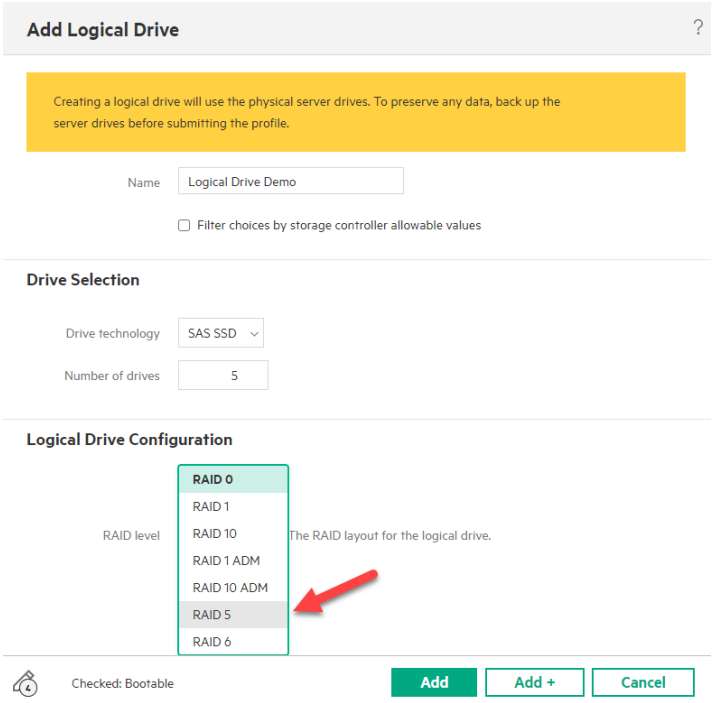
15. Select the *Drive Technology* for the logical drive



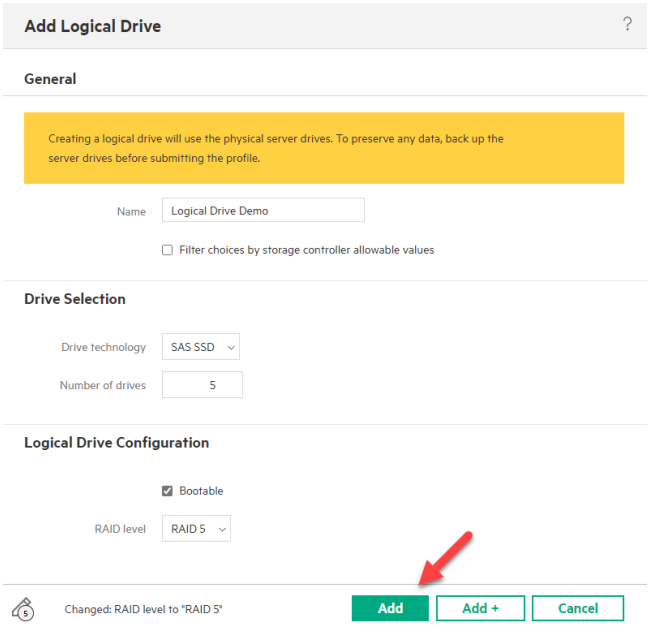
16. Select the *Number of physical drives*



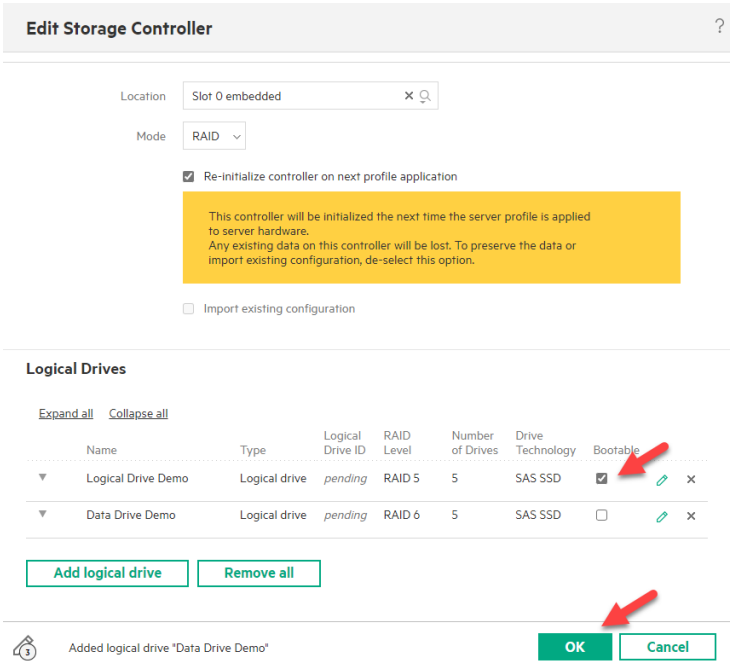
17. Select the *RAID level* and whether the drive is *Bootable*.



18. Click *Add or Add +* to create the logical drive for the server profile.



19. Once all of your logical drives are created, you can still select which one is the boot drive. Click *OK* to finish configuring the Embedded Storage Controller.



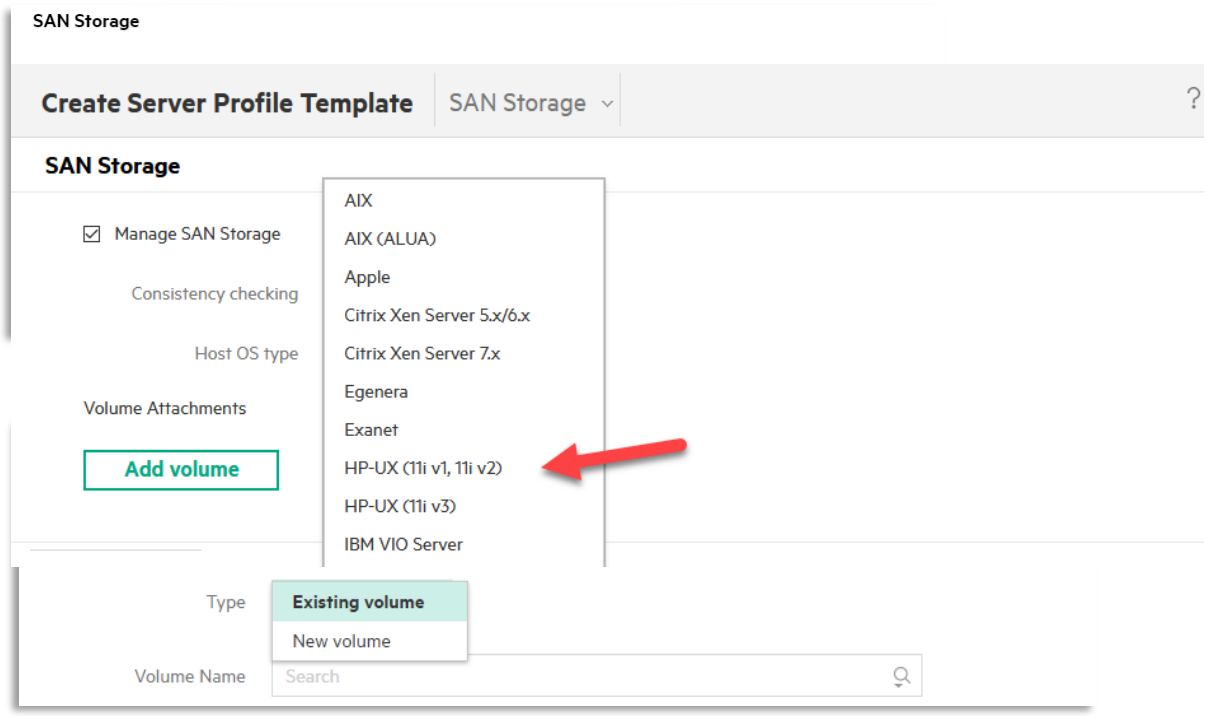
20. Enable Manage SAN Storage if necessary.

A. Check the box for *Manage SAN Storage*



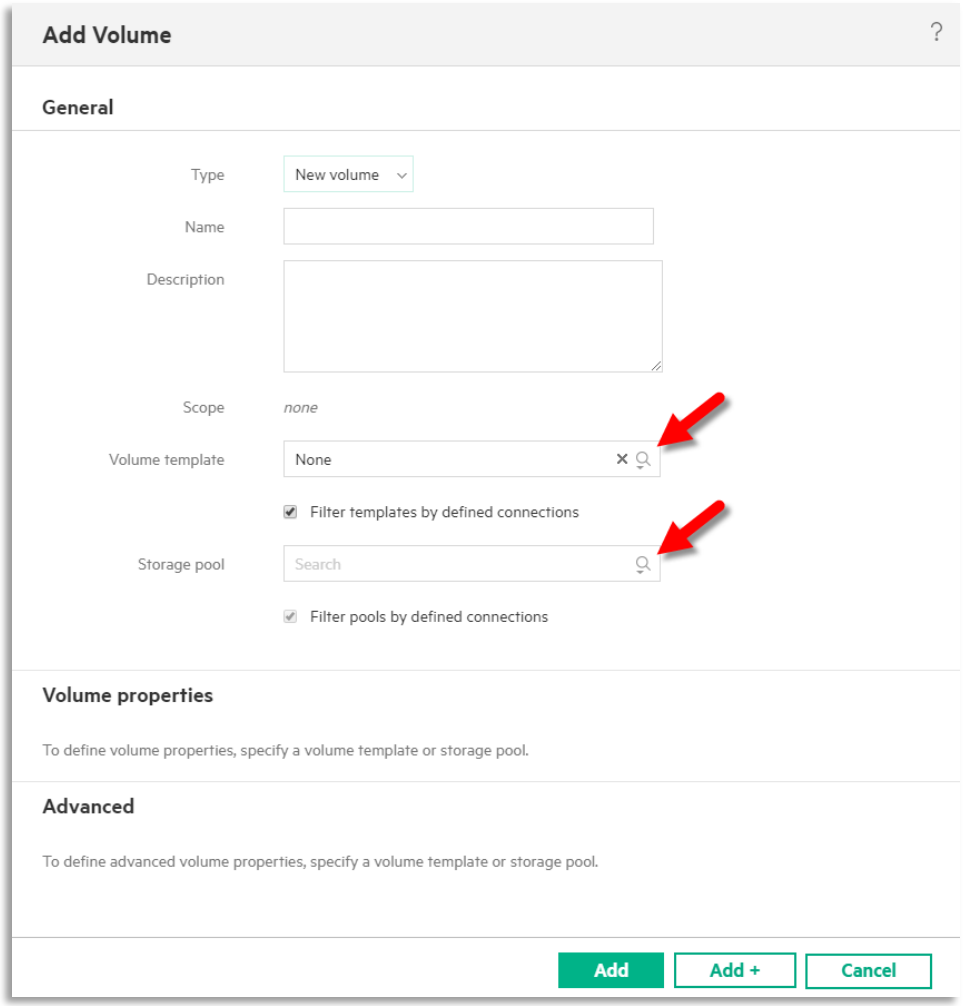
B. Specify the *Host OS type*, which controls the Host's OS / personna created on the HPE 3PAR StoreServ storage system.

C. Click the *Add Volume* button to display the list of volumes available for assignment.

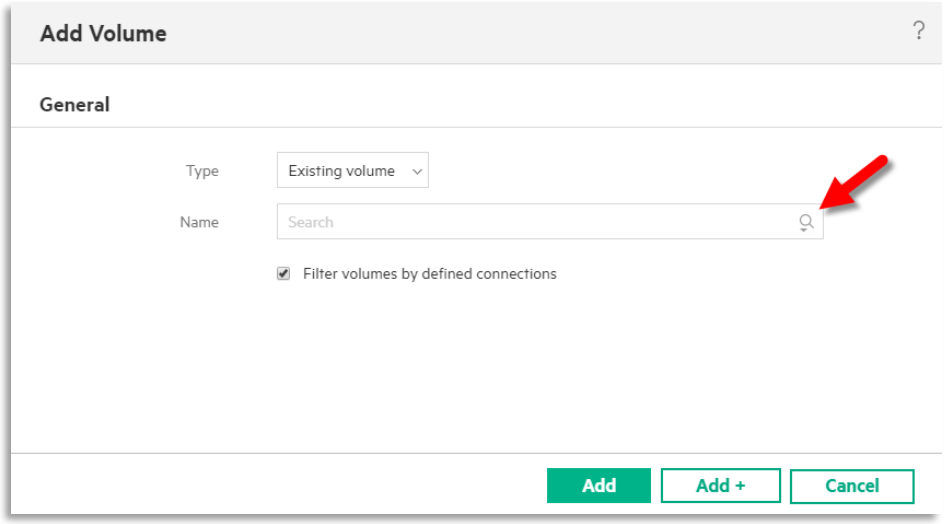


D. In the Add Volume dialog window, select volume *Type* from the drop down list

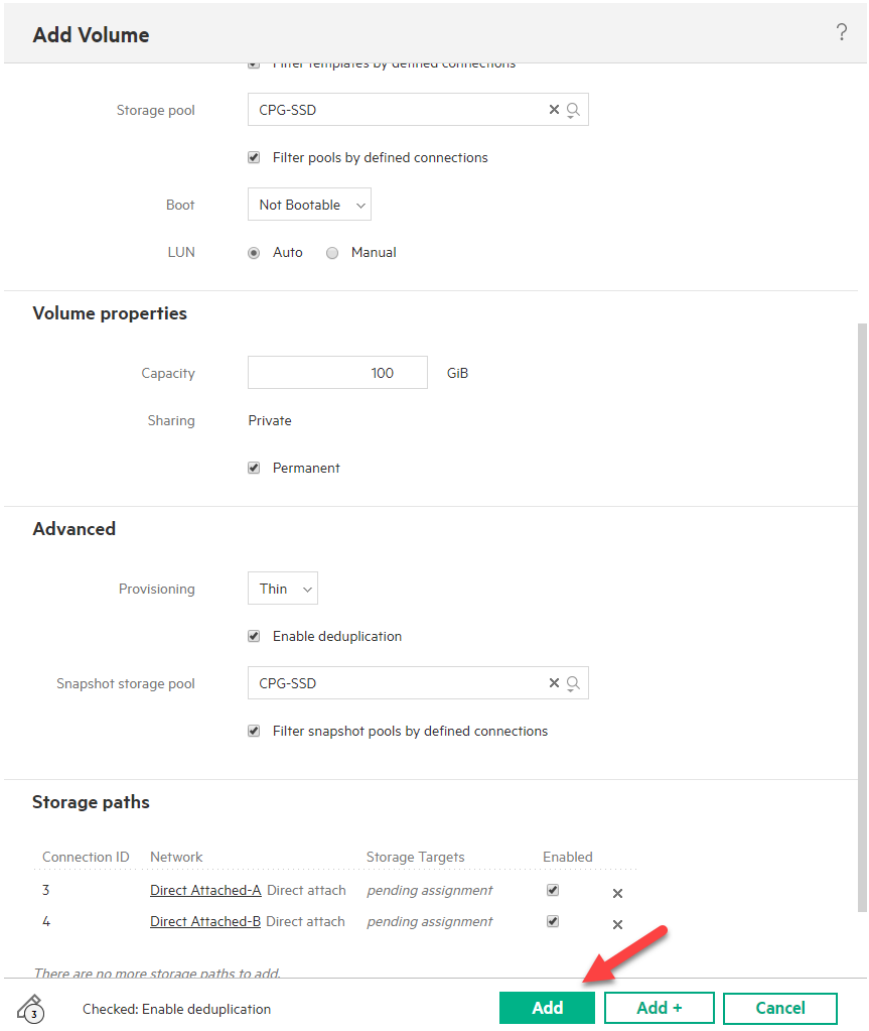
E. If creating a new volume, select a volume template or storage pool to create from and select the desired volume settings.



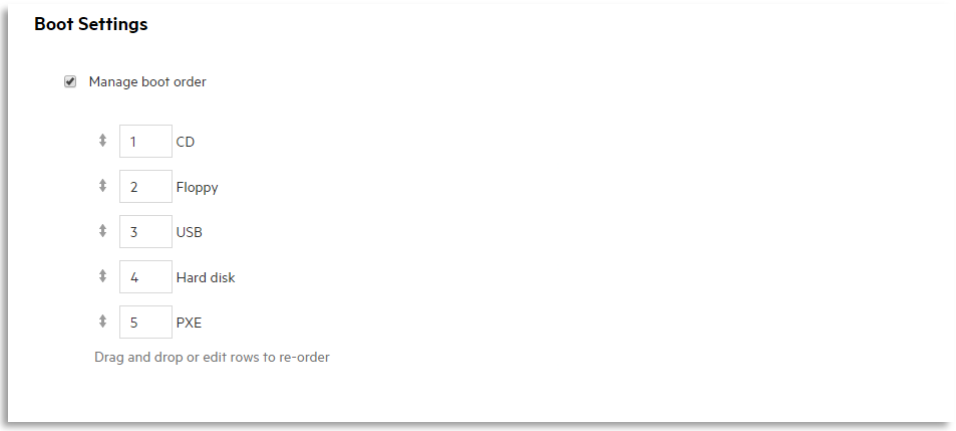
F. If using an existing volume, select the Volume using the dropdown list or the SmartSearch feature.



G. Once the *Volume* has been selected or configured, the default Storage Paths will be displayed. You can disable, remove or add Storage Paths. Click *Add or Add+* to add the volume.



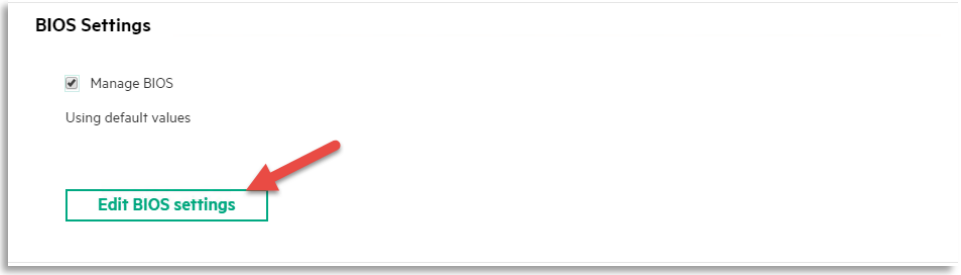
21. Adjust the boot order if desired



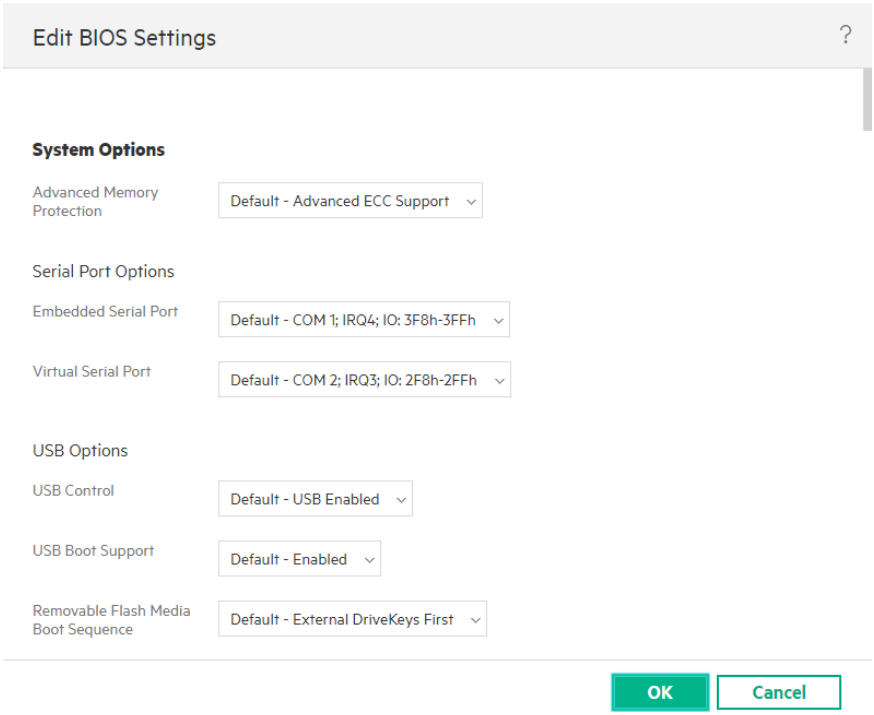
22. In the BIOS Settings section, if desired, check the box to *Manage BIOS*.



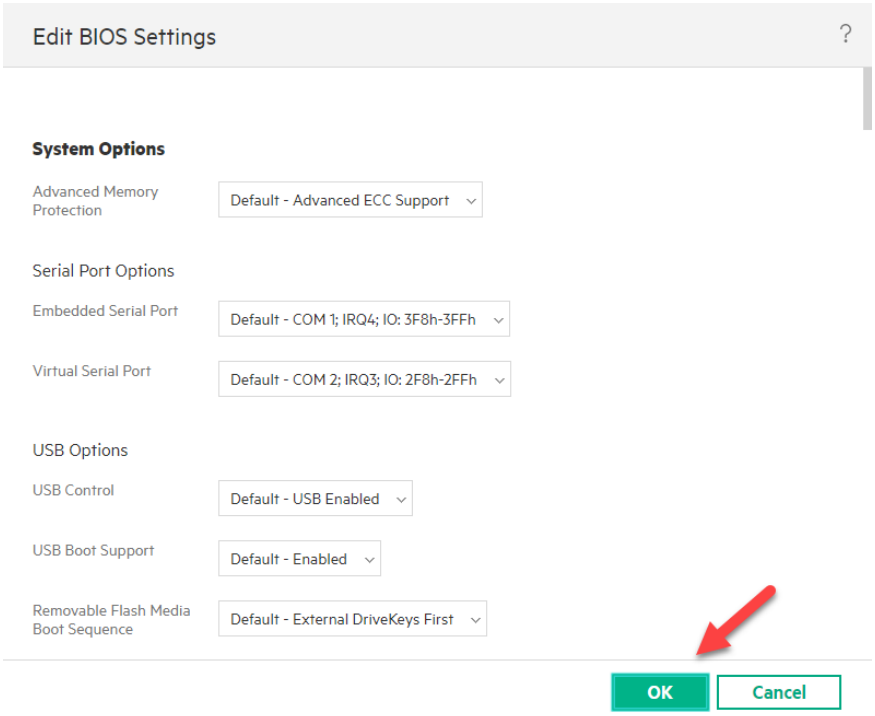
23. Click *Edit BIOS settings*



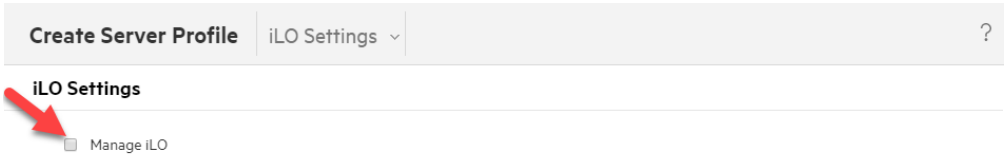
24. In the Edit BIOS settings dialog window, *edit* any desired BIOS settings.



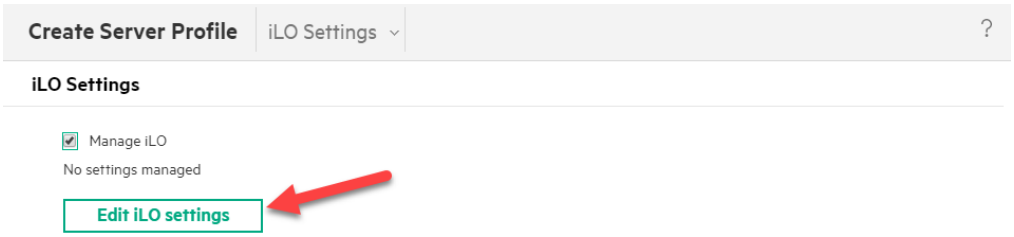
25. In the Edit BIOS settings dialog box, click *OK* after all of the desired BIOS settings are made.



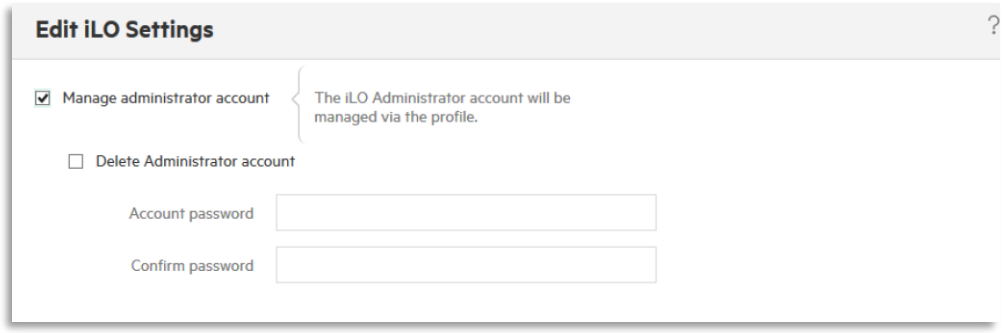
26. If desired, check the *Manage iLO* box in the iLO Settings section



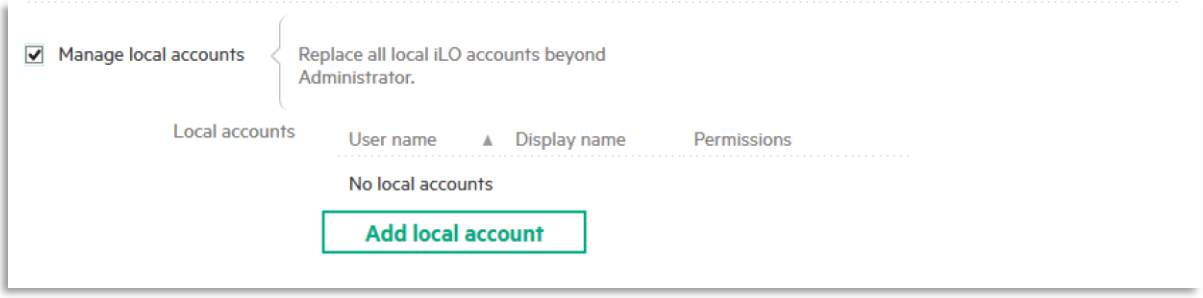
27. Click *Edit iLO settings*



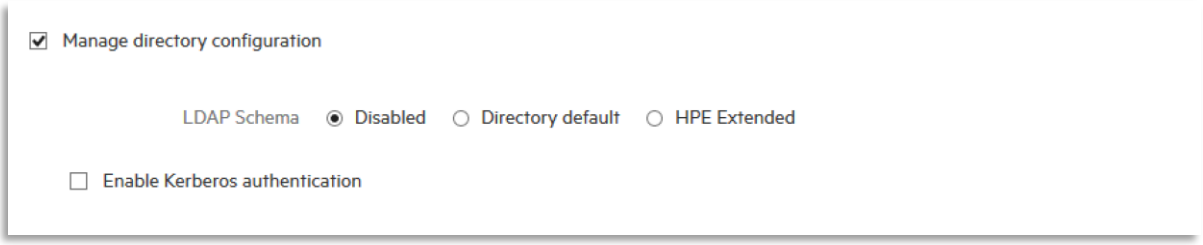
28. If desired, check the box *Manage administrator account* and edit the details as needed



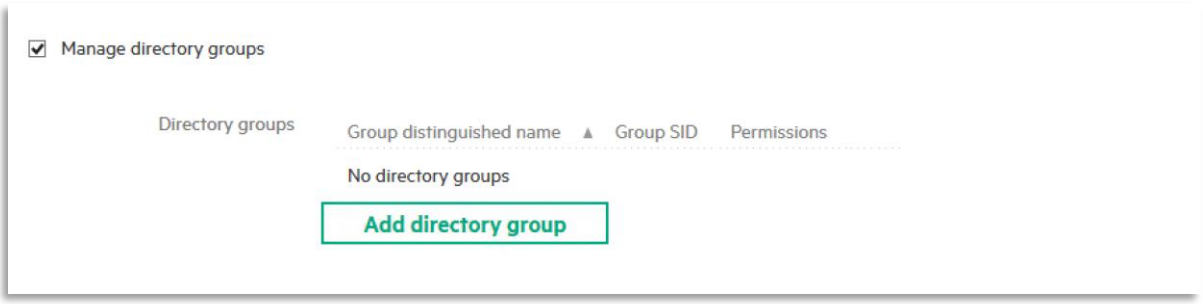
29. If desired, check the box *Manage local accounts* and edit the details as needed



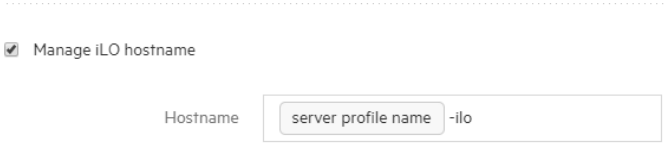
30. If desired, check the box *Manage directory configuration* and edit the details as needed



31. If desired, check the box *Manage directory groups* and edit the details as needed



32. If desired, check the box *Manage iLO hostname* and edit the details as needed



33. If desired, check the box *Manage key manager* and enter the Primary key server address



34. Once finished click *OK* to save the iLO settings and then Click *Create* or the *Create+* button to create the Server Profile

Environment Management



With HPE OneView, you can optimize the power and cooling requirements of your data center efficiently. While each individual system or PDUs in your data center can provide its power requirements and sometimes even a limited amount of power consumption history, it is still difficult to understand the power and cooling requirements for your data center in a holistic way.

In this section, you will go through how to configure your HPE OneView so you can start investigating more about the overall systems in your data center and their power & cooling capacities and consumption.

Physical data center configuration

In order to take advantage of analysis and management features for your environment, you first want your physical data center environment to be accurately represented. You have the ability to match the physical placement of systems, enclosures, racks and other unmanaged devices through HPE OneView.

Add racks based on Location Discovery Services (LDS)

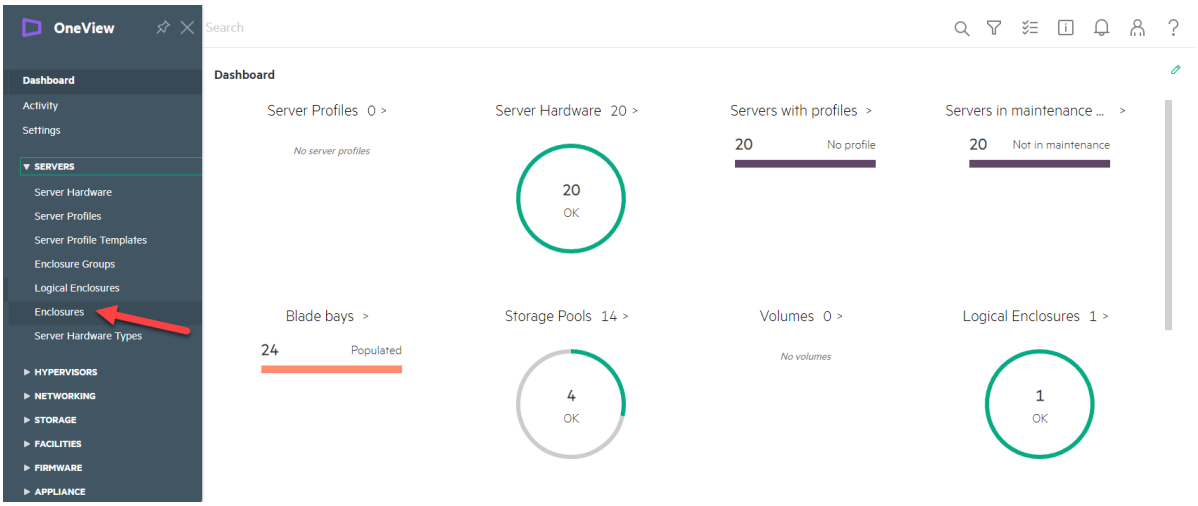
Racks are automatically created based on LDS. HPE ProLiant Servers mounted in HPE Intelligent Series Racks are automatically grouped in racks in the proper positions. The initial rack names are provided by the Rack Serial Number. The height of a created rack is displayed as 42U unless the top-most device managed by HPE OneView is in a higher position. If a managed device is later added to a position above 42U, the rack height will be automatically adjusted.

Add Synergy Frames to racks without LDS

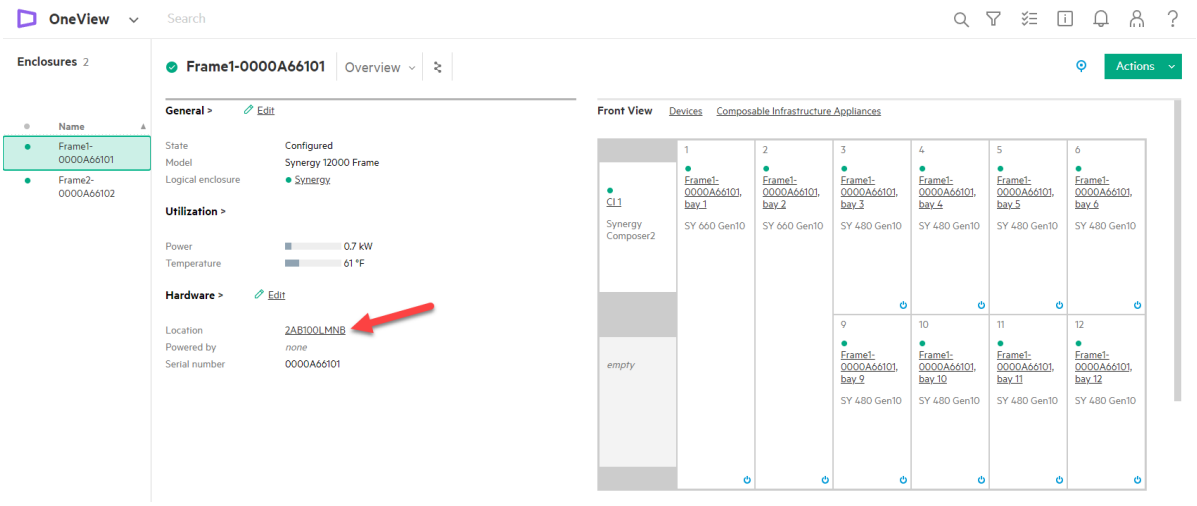
If no LDS is present, HPE Synergy Frames automatically create an enclosing rack in HPE OneView during the discovery process.

HPE Synergy Composer powered by OneView places into the rack all enclosures connected by management link cables. It causes a single rack to be created per set of enclosures. Specific slot positioning must be provided by adjusting the positioning in the UI or via REST.

1. From the Top-Level Menu, expand the *SERVERS* option and then select *Enclosures*.



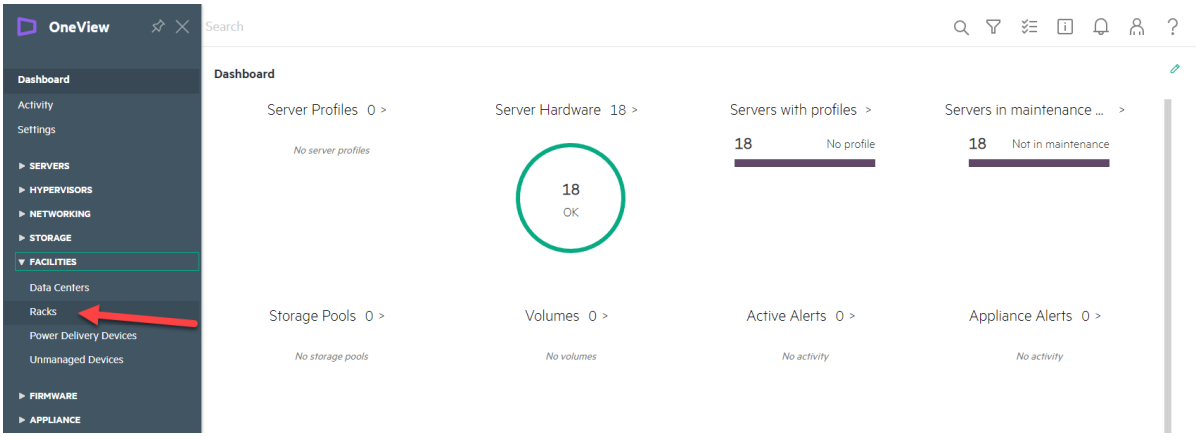
2. After selecting the correct enclosure from the main pane, the information in the Hardware section of the details pane allows you to see the rack automatically created to house the enclosure.



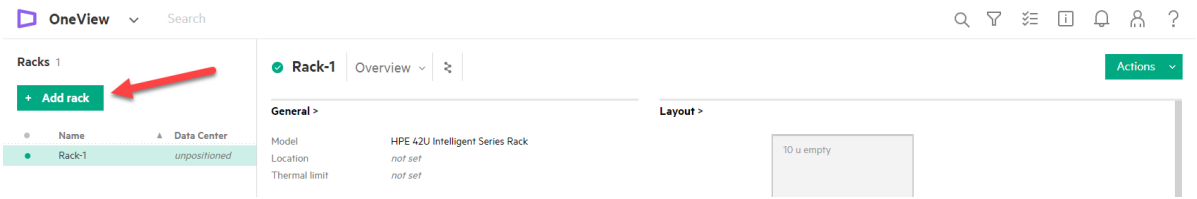
Adding DLs to rack without LDS

If LDS is not present, racks are not automatically created for DL servers. DL servers may be added to racks previously created via enclosure discovery or racks may be created manually and have servers added to them. For either option, begin by navigating to the Racks screen.

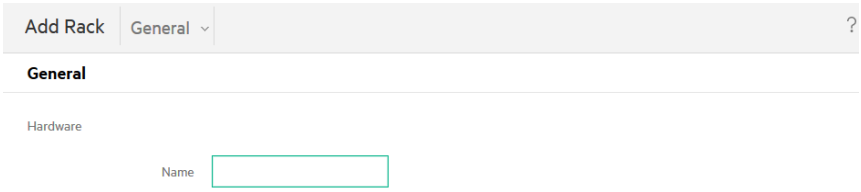
1. From the top-level menu, expand the *FACILITIES* option and then select *Racks*.



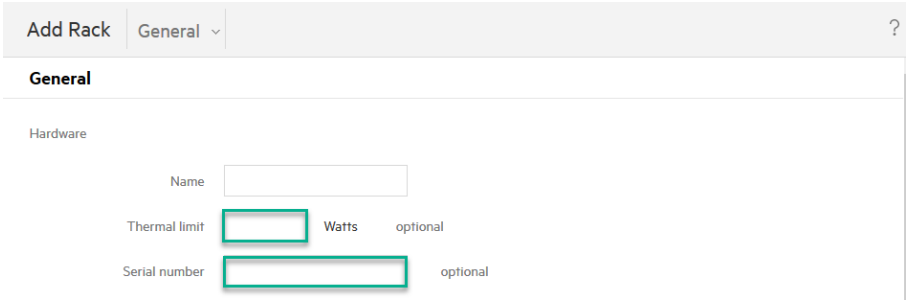
2. On the Racks screen, to create a rack either select +Add rack button in the left panel.



3. In the General section of the Add Rack dialog window, enter the *Name* for the rack



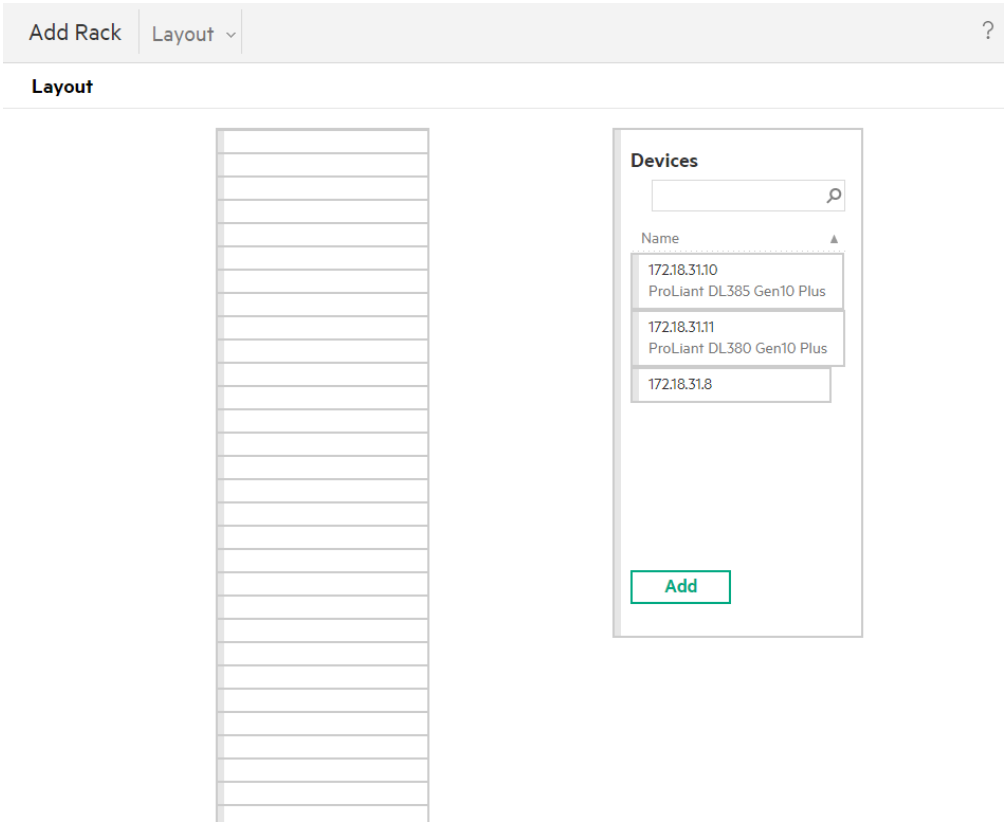
4. There are two optional settings in the General section, Thermal Limit and Serial Number. Enter these if desired



5. Enter the dimensions for the rack



6. The Layout panel consists of a visual representation of the rack and its slots, a list of available devices and a search box to find the desire systems and enclosures. From this panel, you can add, remove, and rearrange devices within the rack and edit the device details. To place a device, drag and drop it in the desired location.

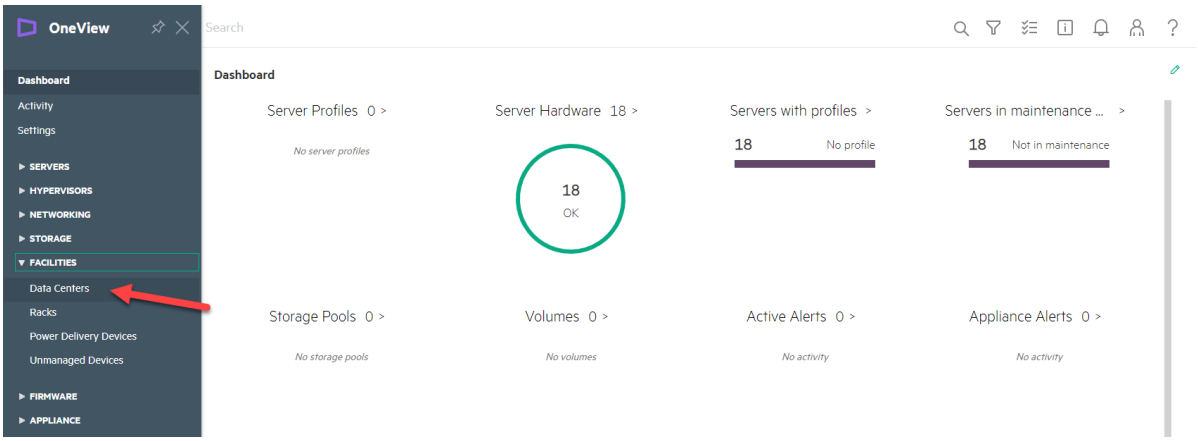


7. Once the rack has been configured, select *Add* to complete the setup or *Add +* if additional racks need to be created.

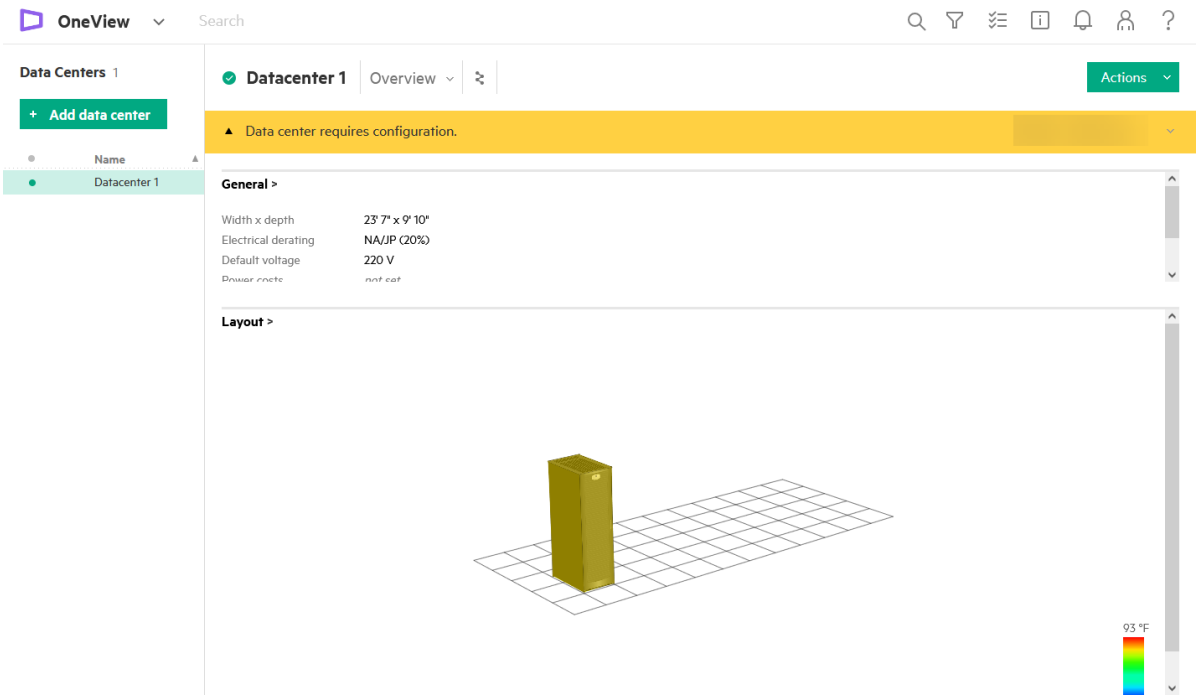
Creating a Data Center

HPE OneView allows you to describe the physical locations of your racks and systems within your data center. After placing systems in the racks, 3D data center maps can be created to accurately describe the racks location on the data center floor.

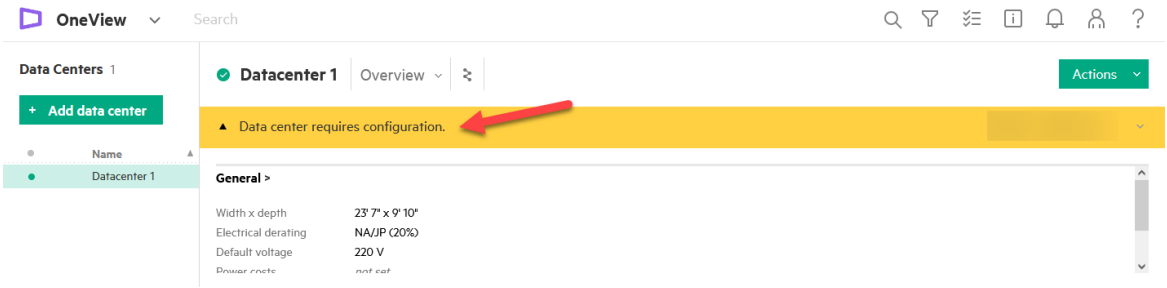
1. From the Top-Level Menu, expand the *FACILITIES* option and then select *Data Centers*.



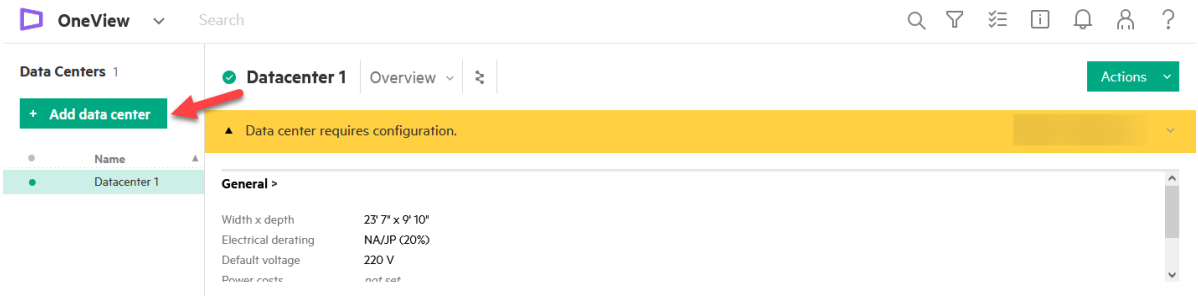
2. HPE OneView automatically creates a default data center (Datacenter 1) during setup which serves as a holding place for racks once created. All racks are listed under Datacenter 1 in the order they were created. A message is shown until the default data center indicating it has not been configured.



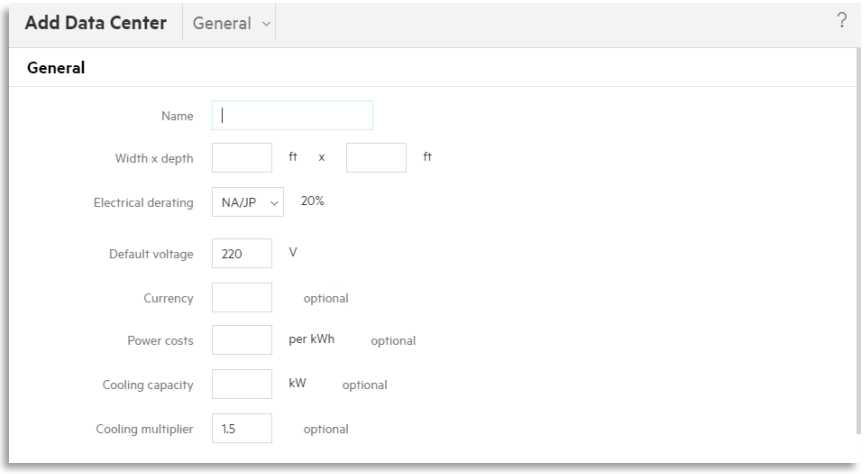
3. If you wish to use the default Datacenter 1 for your actual data center, resolve the warning message by editing Datacenter 1 and renaming / resizing it to match the data center floor (or portion thereof) you are going to be managing with HPE OneView. This process is described in subsequent steps. Alternately, you can remove Datacenter 1 and Add one or more data centers as described next.



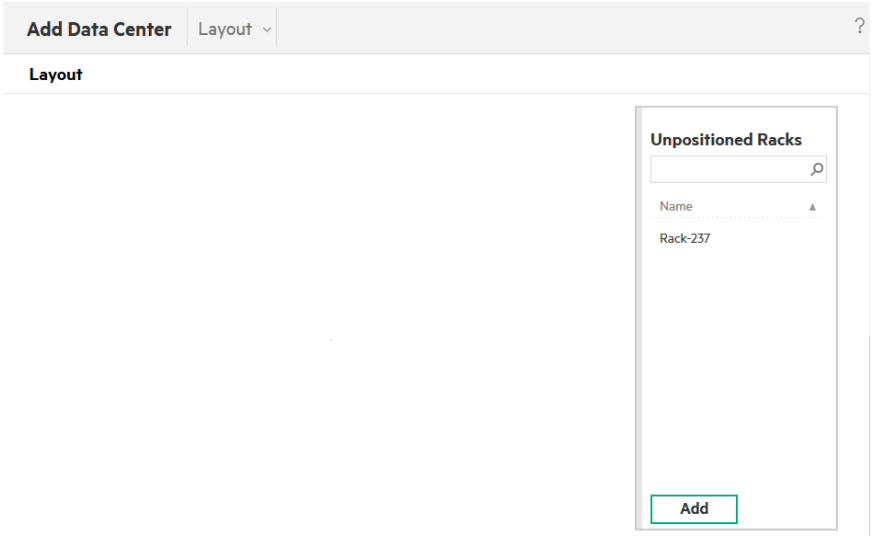
4. To add new data centers, use the *+Add data center* link on the Data Centers screen.



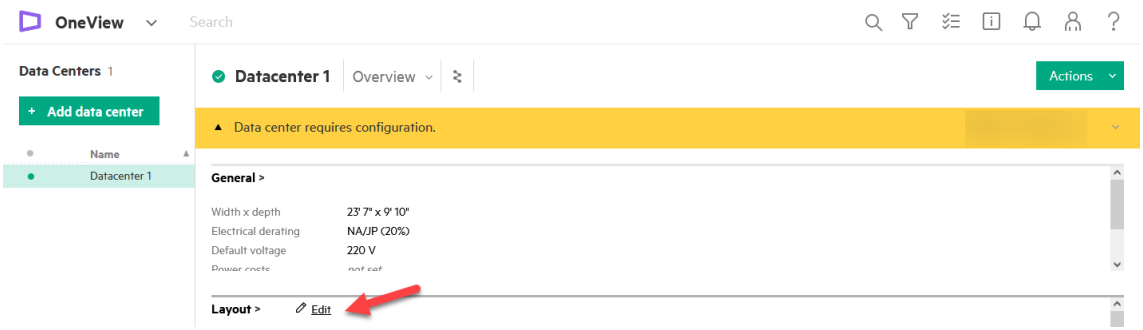
5. In the General section of the Add Data Center Window, enter the details about the new data center.



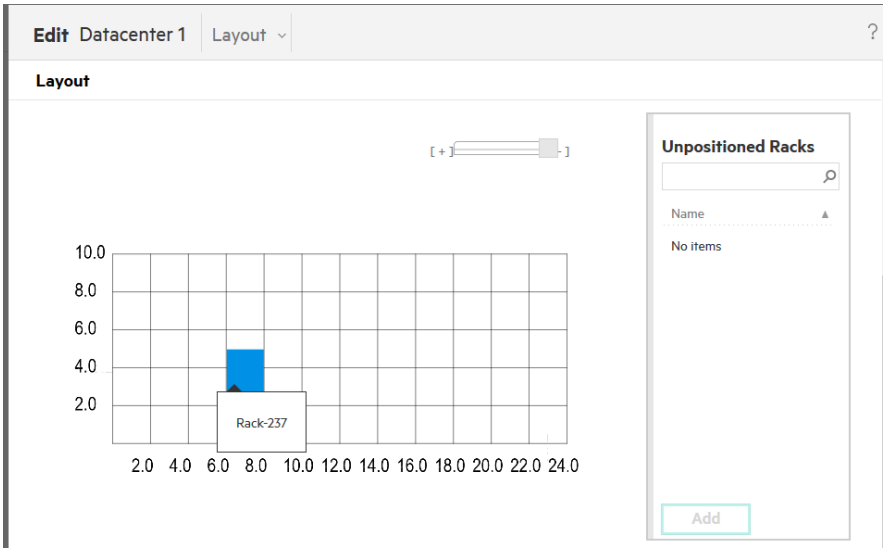
6. In the Layout section of the Add Data Center dialog box, arrange the physical location of the unpositioned racks.



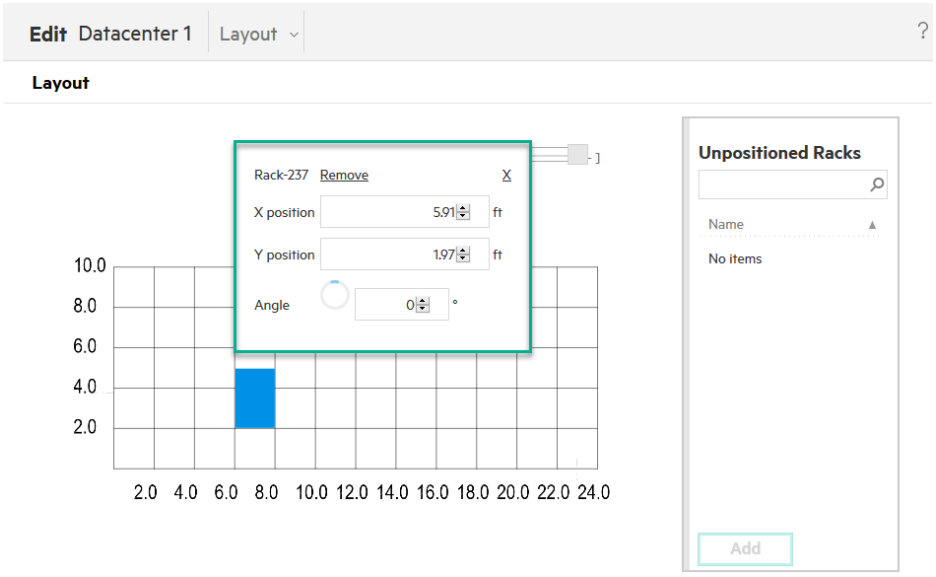
7. To edit an existing data center, select *Edit* in the Layout section of data center page.



8. The Layout panel of the Edit screen allows you to drag & drop racks on the grid from an overhead view.



9. For physically accurate positioning not aligned with the grid lines, enter the position and angle in the rack positioning popup.



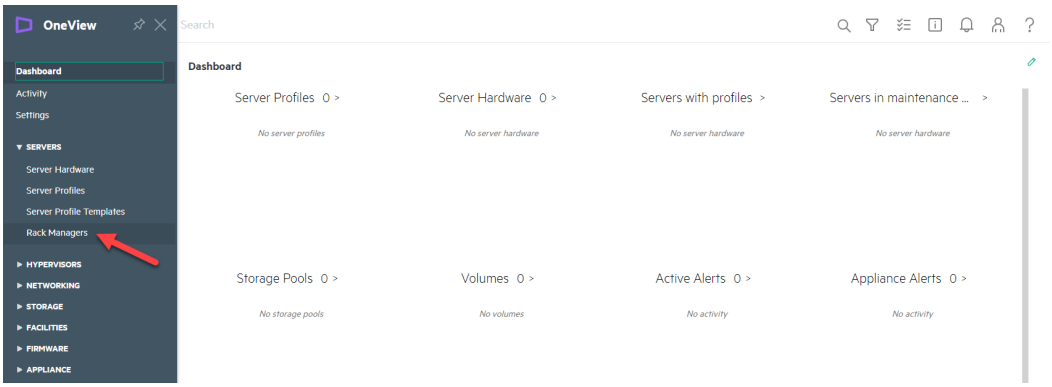
10. Once editing of the data center is complete, select the *OK* button to return to the data center screen to view the 3D model of the data center.

HPE Superdome Flex

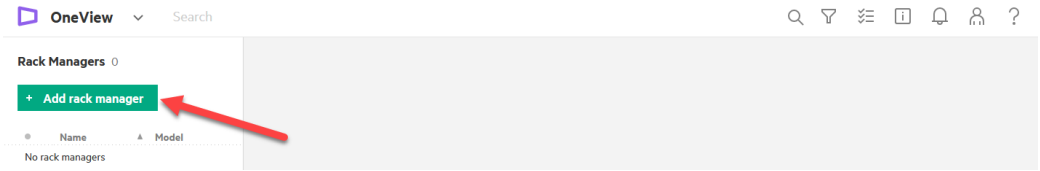
HPE OneView supports adding an HPE Superdome Flex complex for hardware monitoring or managing as long as the Superdome Flex is on 3.x or newer firmware. In this section you will import a Superdome Flex server by adding the IP address or FQDN of its Rack Manager Controller (RMC).

Import the Rack Management Controller

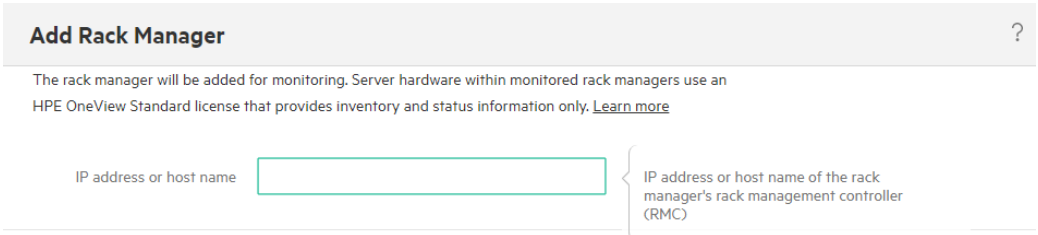
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Rack Managers*.



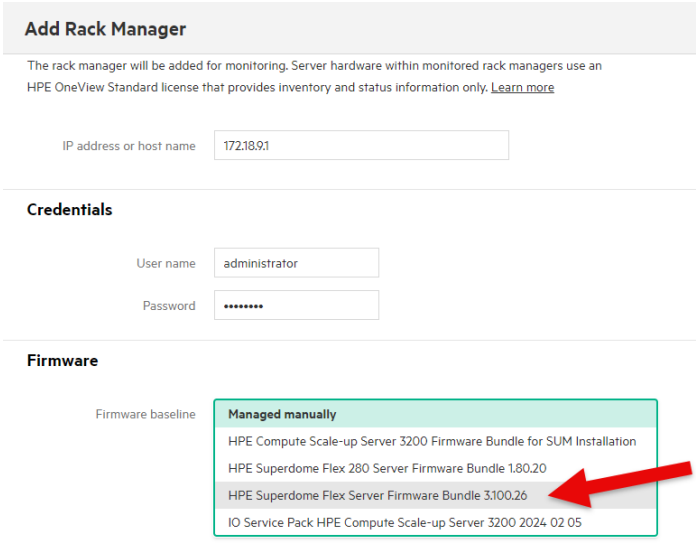
2. From the menu, select Add rack manager



3. Enter the IP address or host name of the Rack Manager

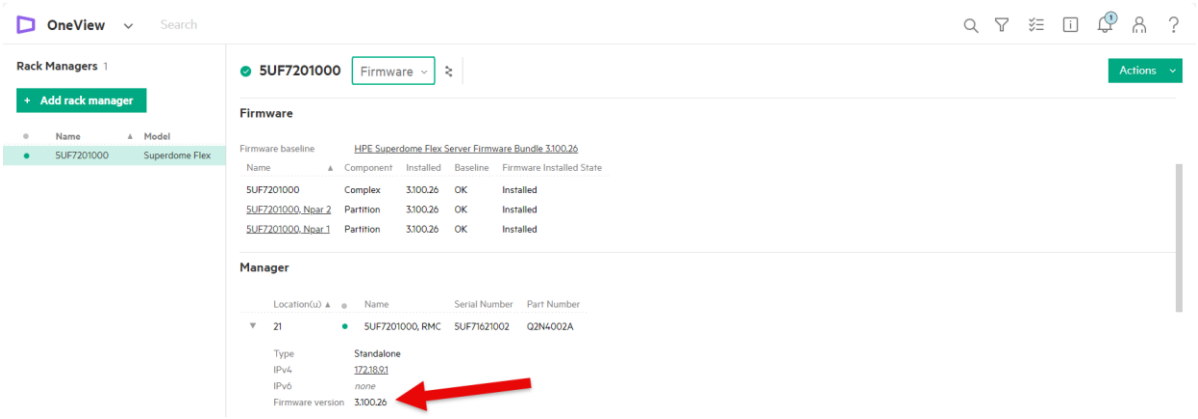


4. Enter the *Credentials* of the rack manager, choose the *Firmware baseline* and then click *Add.*

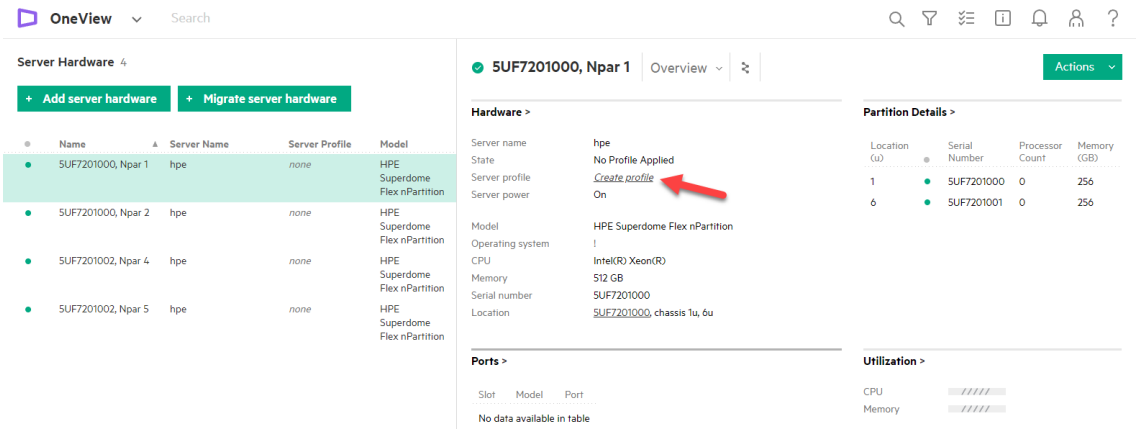


When you import a Superdome Flex server if the firmware is below v3.x then the Superdome Flex Server will only be monitored in OneView. In order for it to be managed (have the ability to create Server Profiles) then you will need to update the Firmware to v3.x or later.

5. Check the Firmware version by looking at the Firmware from the Menu

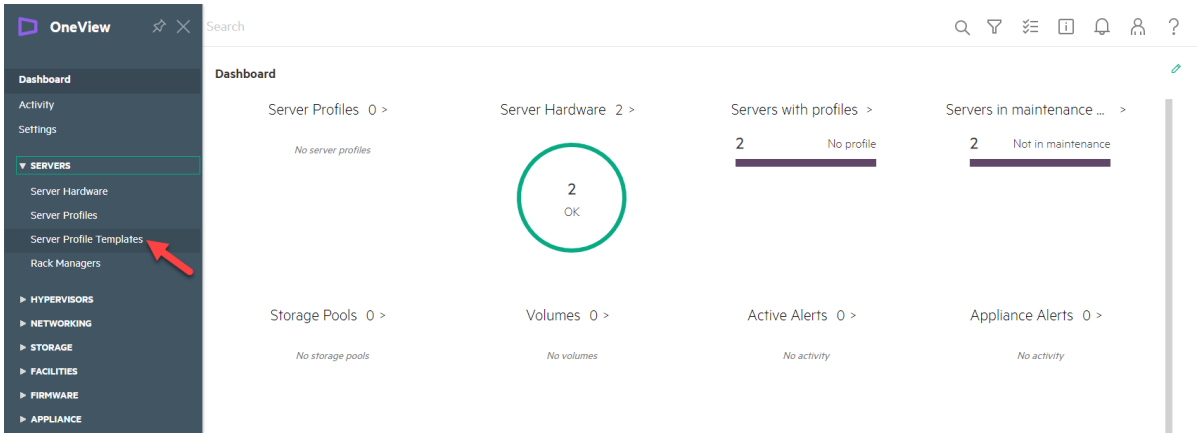


6. Go into the Server Hardware you will now be able to create a Server Profile for the Superdome Flex Server.

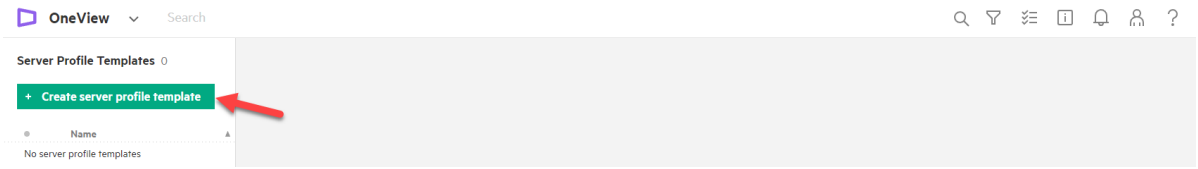


Create Superdome Flex Server Profile Template

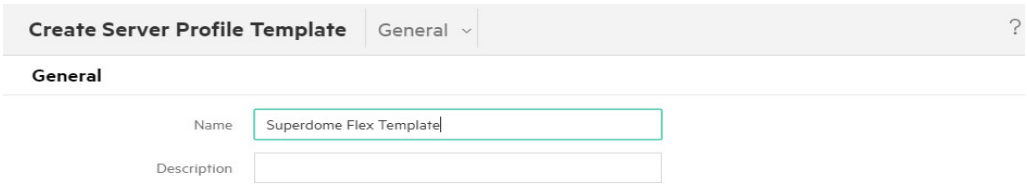
1. You can create a Server Profile Template for Superdome Flex the same as any other Server Hardware Type managed by OneView. From the main menu, expand the *Servers* option and then select *Server Profile Templates.*



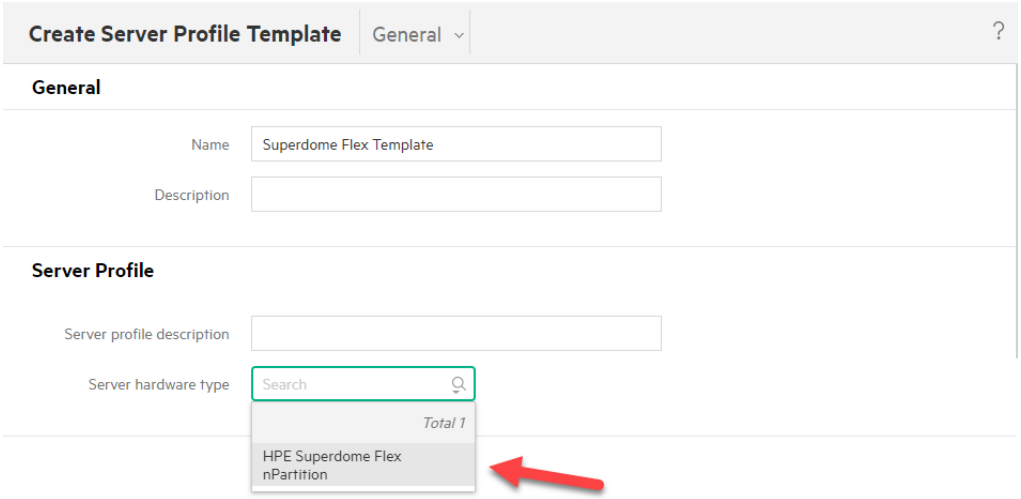
2. Once on the Server Profile Template screen, select the + *Create server profile template* button



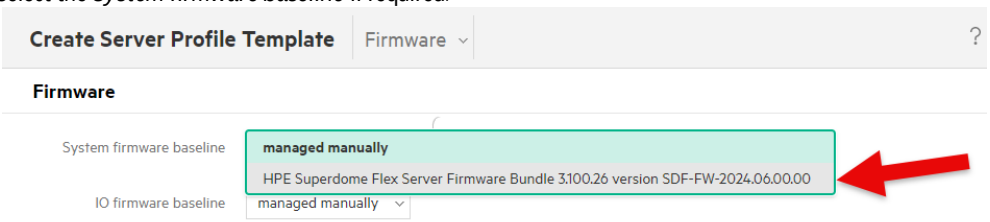
3. In the Server Profile section of the server profile template creation page, enter a *Name* and optionally a *Description* for the server profile template



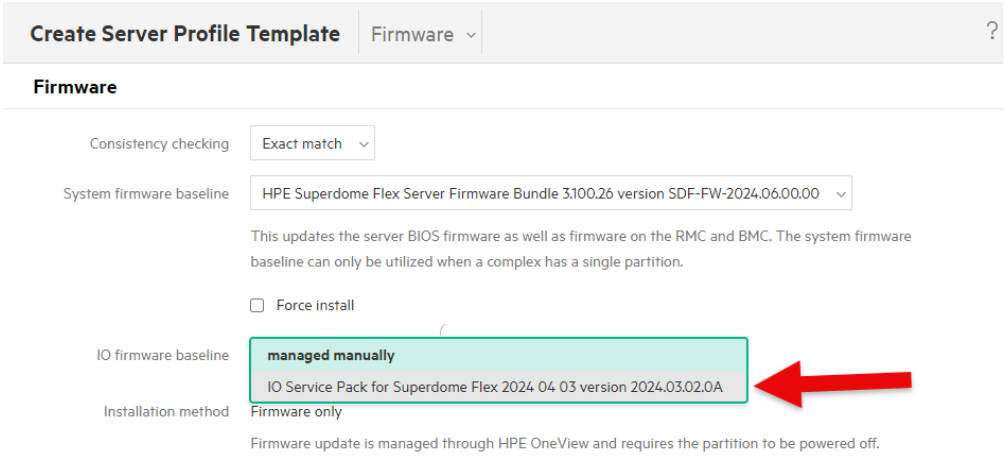
4. Choose the *Server hardware type*.



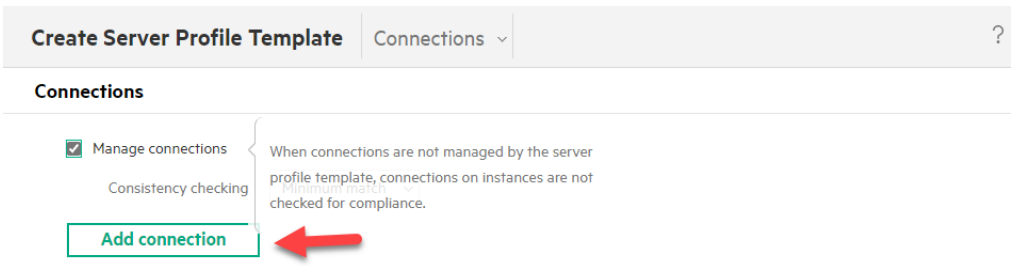
5. Select the *System firmware baseline* if required.



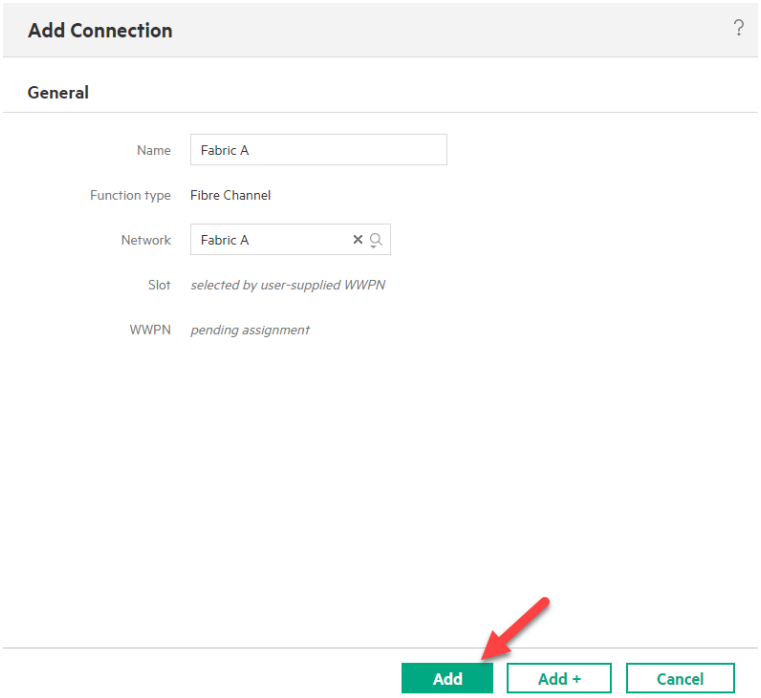
6. Select the *IO firmware baseline* if required.



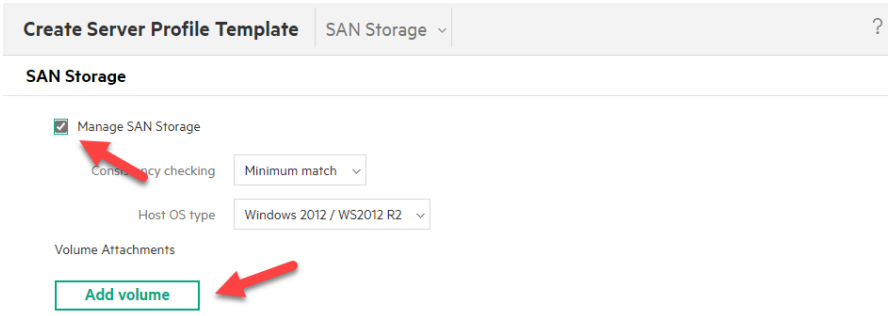
7. Fibre Channel Connections can be added which allows SAN Fabric Zoning and HPE Storage to be provisioned as part of applying the Server Profile. Click on *Manage connections* and then you can click on *Add connection*.



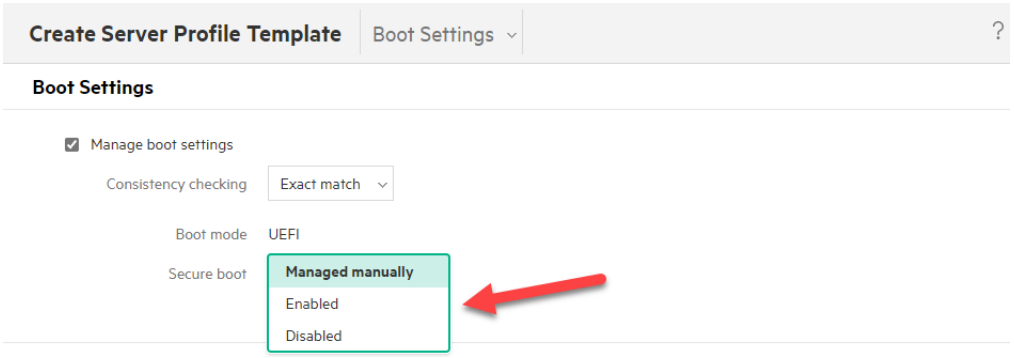
8. Now you can add the name of the Fabric and the Fabric Network that you want the Server connected to, once you have made your selections and click *Add* / *Add* + to add the connection.



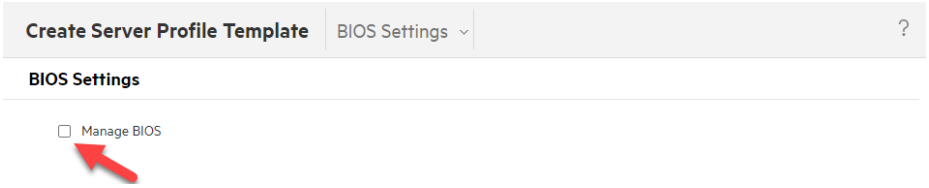
9. You now have the option to attach HPE SAN Storage LUNs by selecting *Manage SAN Storage* and then you can click *Add volume*. To attach a HPE SAN LUN.



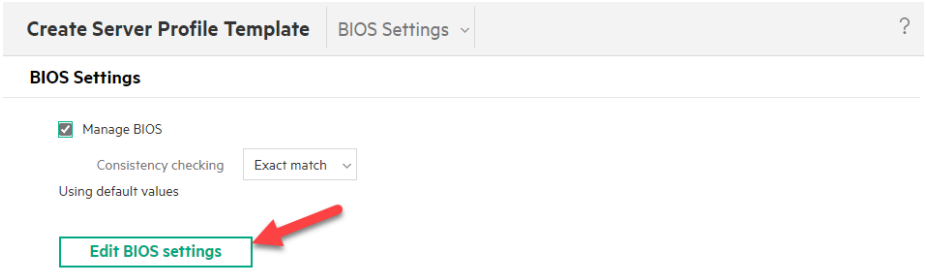
10. You can manage the boot settings (Secure Boot).



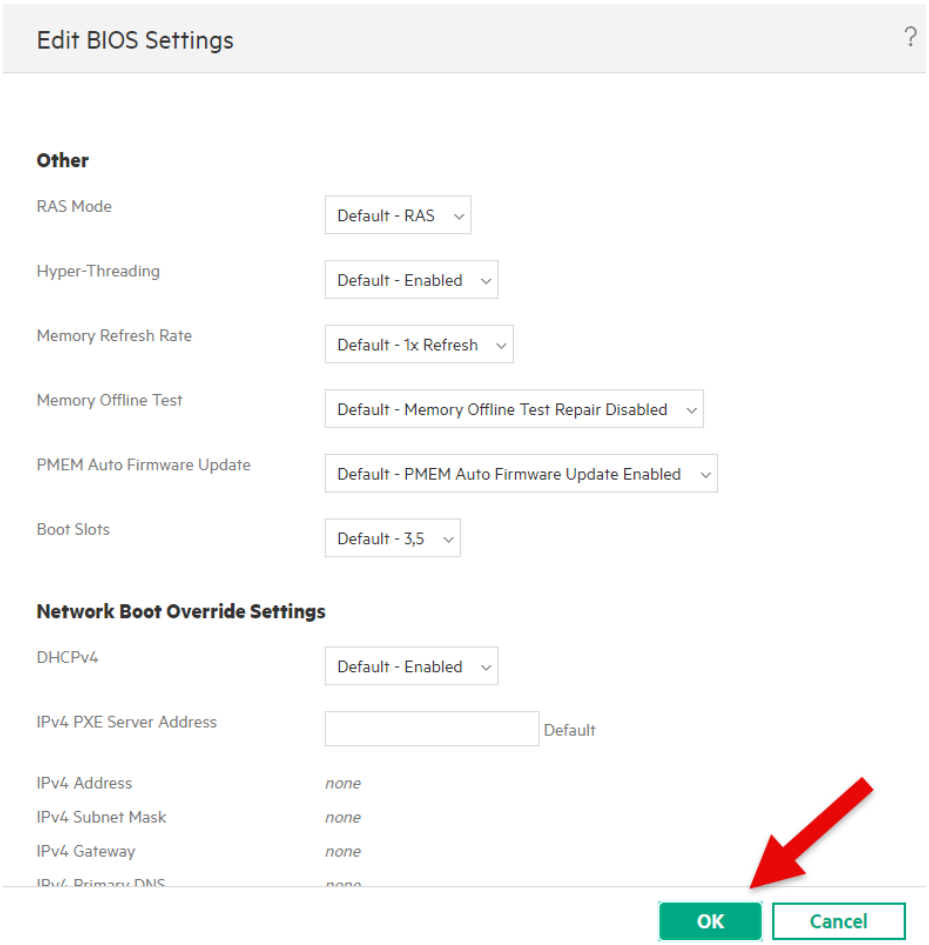
11. You can manage the BIOS Settings by clicking on *Manage BIOS*.



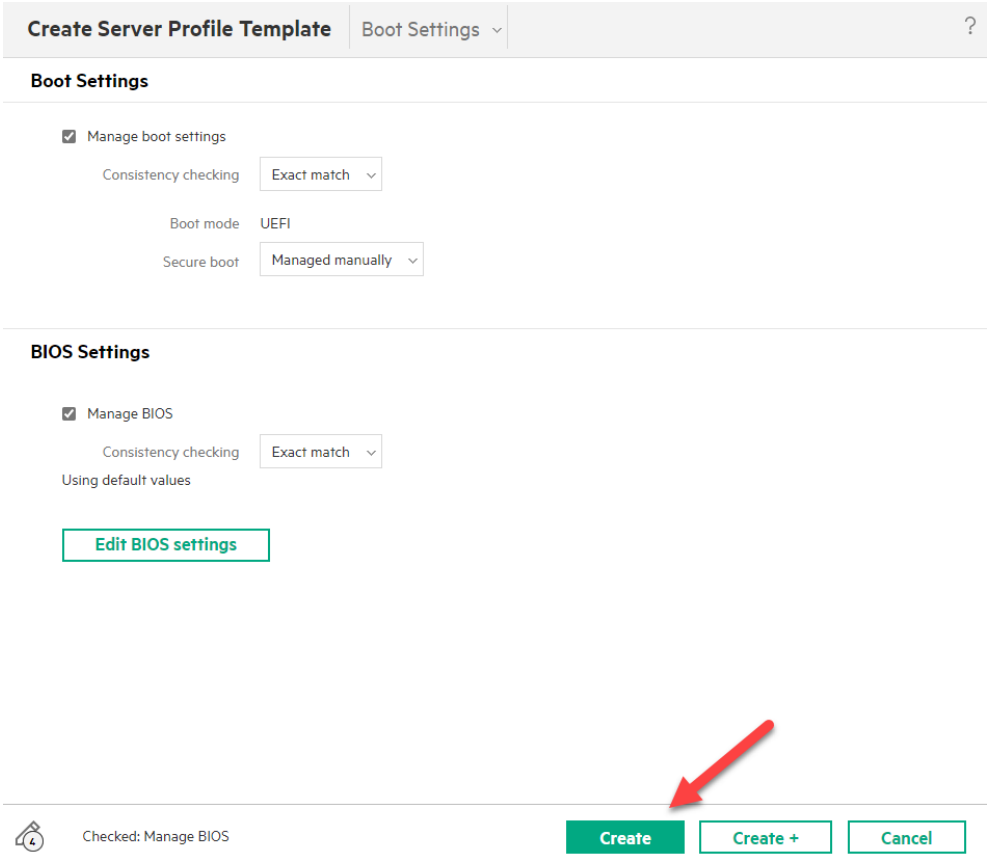
12. Then select *Edit BIOS settings*.



13. Make the required changes to the BIOS Settings and click *OK* to save them to the Server Profile Template.

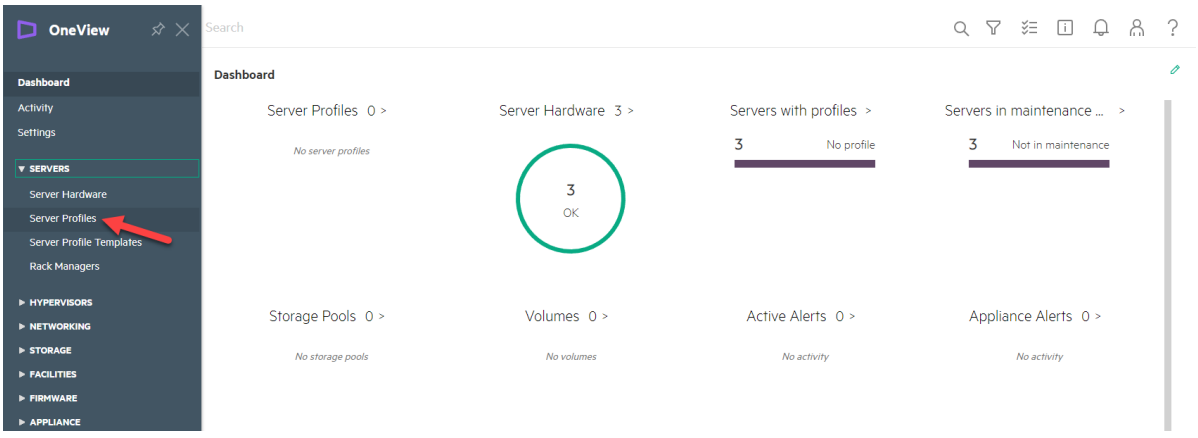


14. Click on the *Create* button to create the Server Profile Template

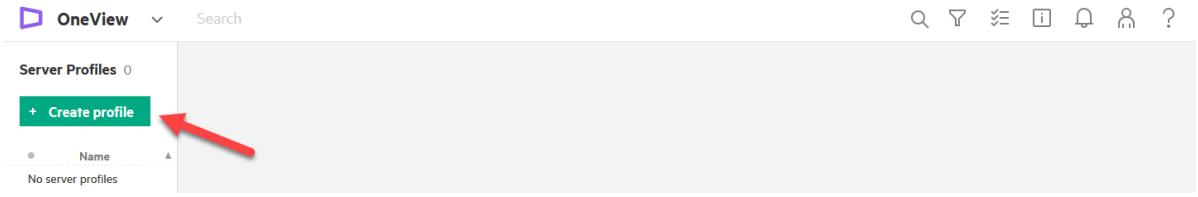


Create Superdome Flex Server Profile

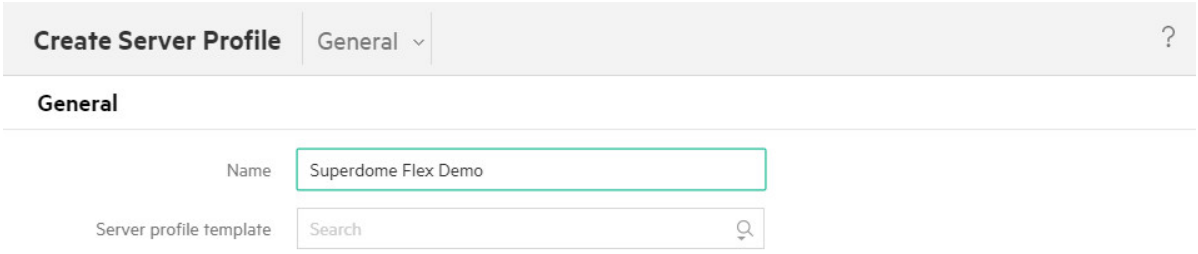
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



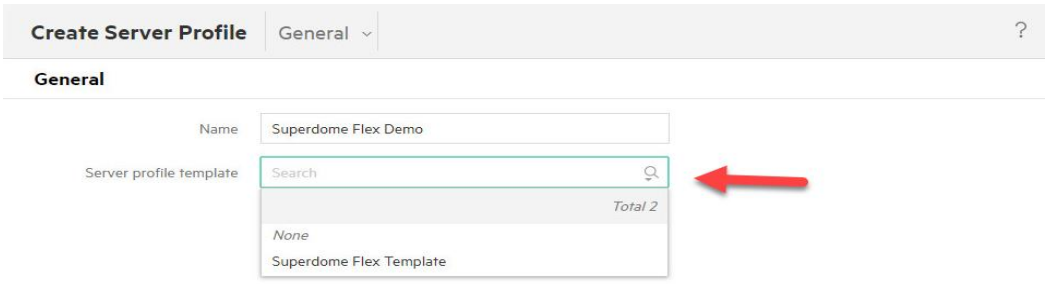
2. Choose + *Create profile*



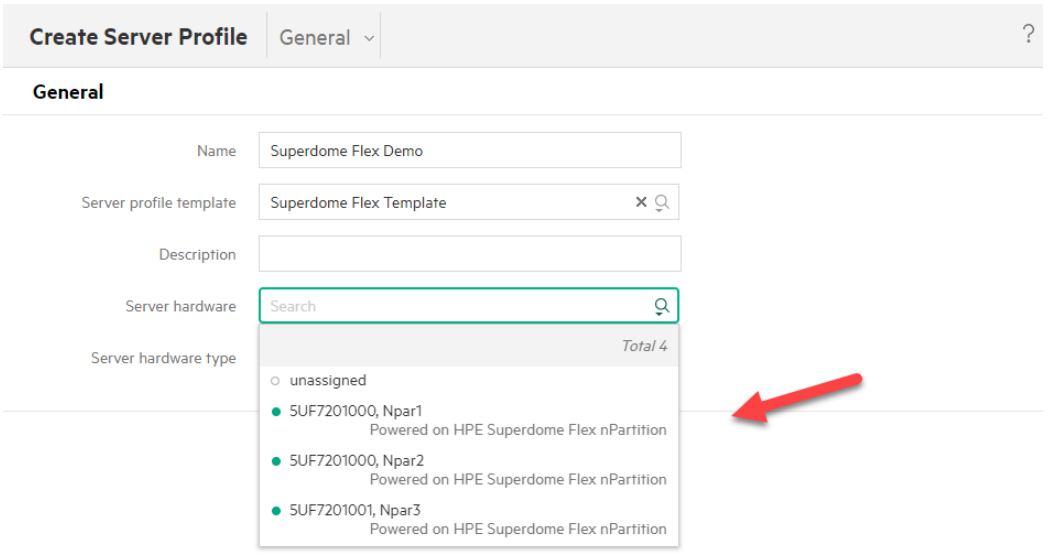
3. Type in Server *Name.*



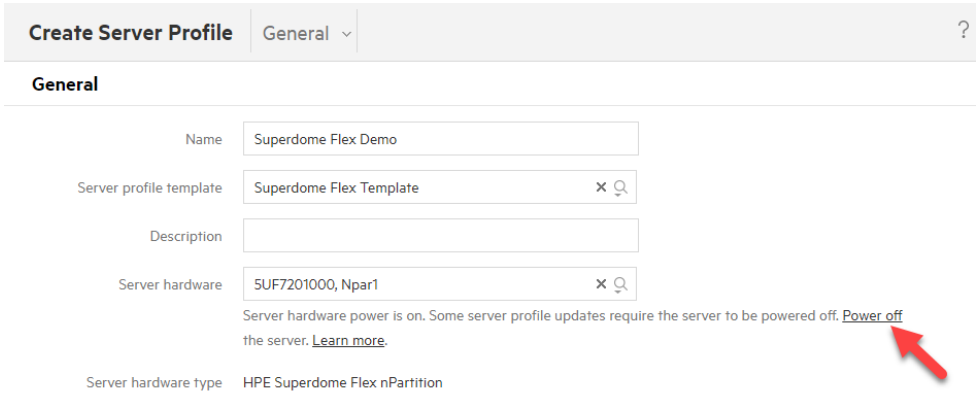
4. You can base it on an existing *Server profile template* if one has been created or select *None.*



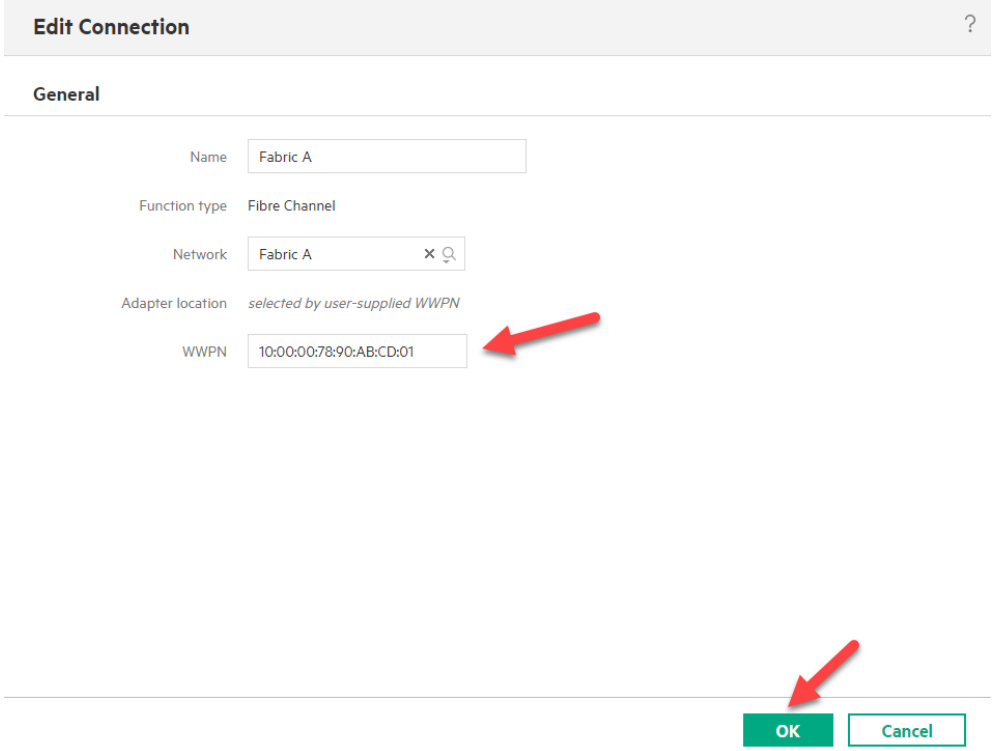
5. Choose the Superdome *NPar* in *Server hardware* that you wish the Server Profile to be assigned to



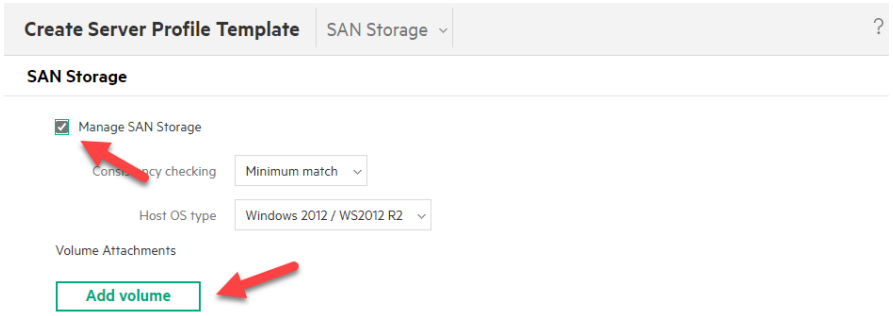
6. A Server Profile can only be applied to a Server that is “Powered Off” and as you can see this server is still Powered on.



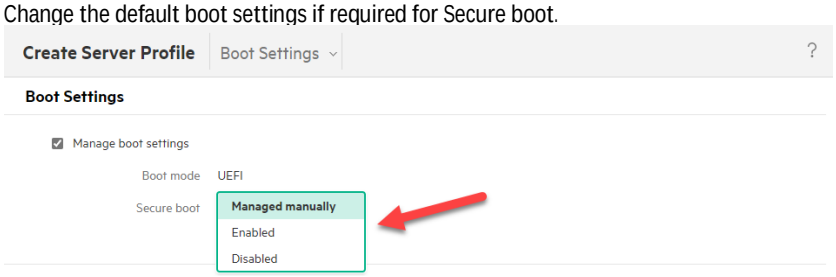
7. Enter the WWPN from the FC SAN Adapter that is to be connected to the SAN Fabric (do the same for the secondary fabric)



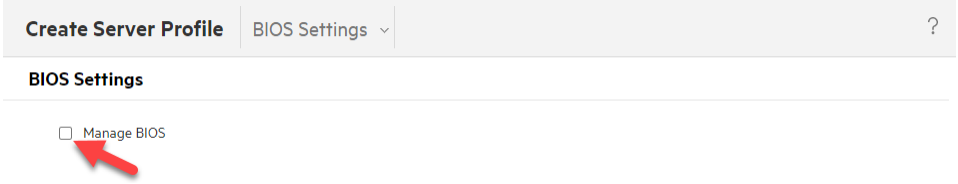
8. To attach HPE SAN Storage LUNs, select *Manage SAN Storage* and then you can click *Add volume*. To attach a HPE SAN LUN.



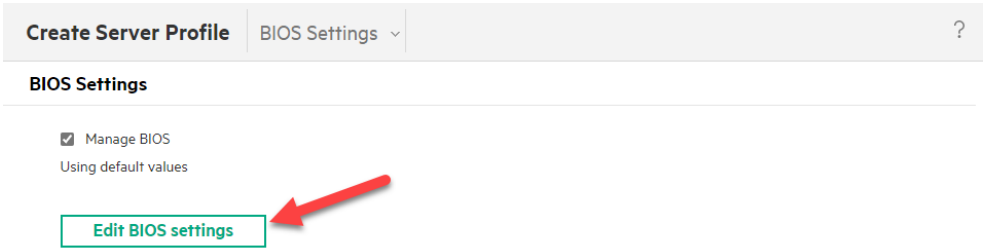
9. Change the default boot settings if required for Secure boot.



10. BIOS Settings can be managed by clicking on *Manage BIOS.*

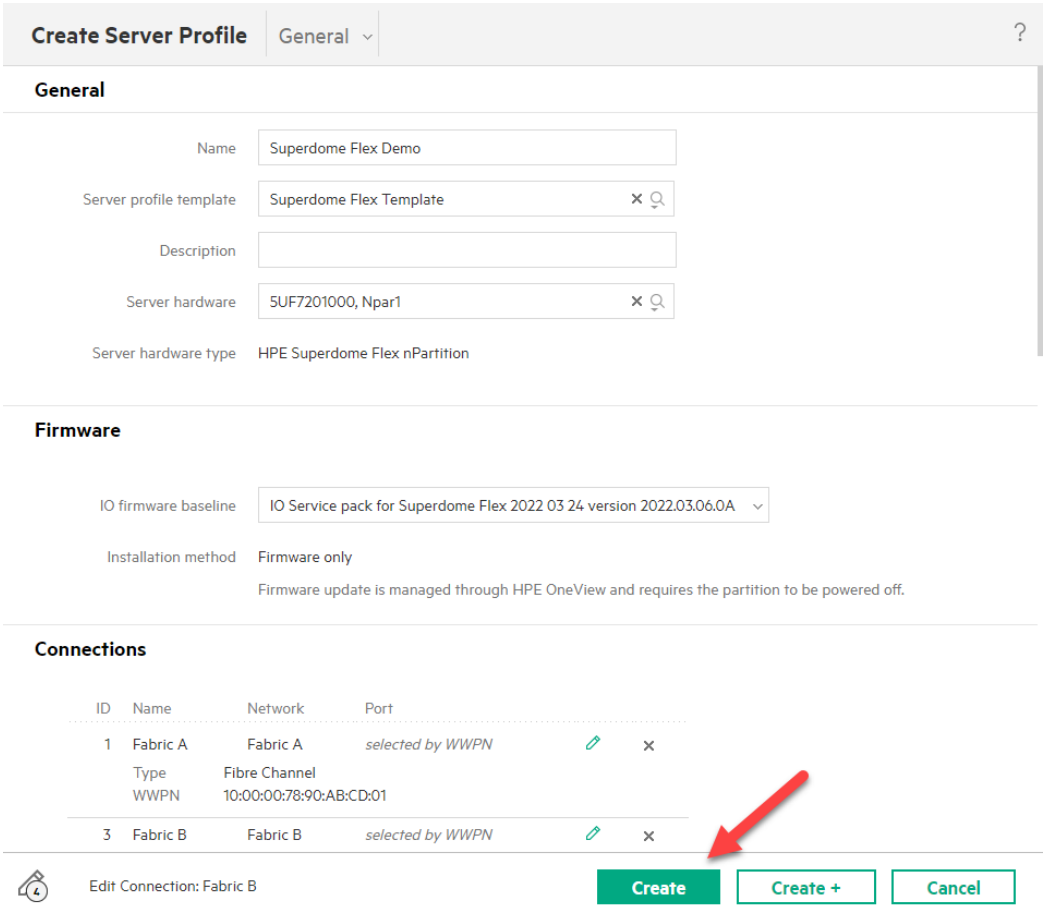


11. Now click on *Edit BIOS Settings.*



12. Change any of the BIOS Settings as required and click *OK* to save the changes.

13. Click *Create* to create the Server Profile for the Superdome Flex



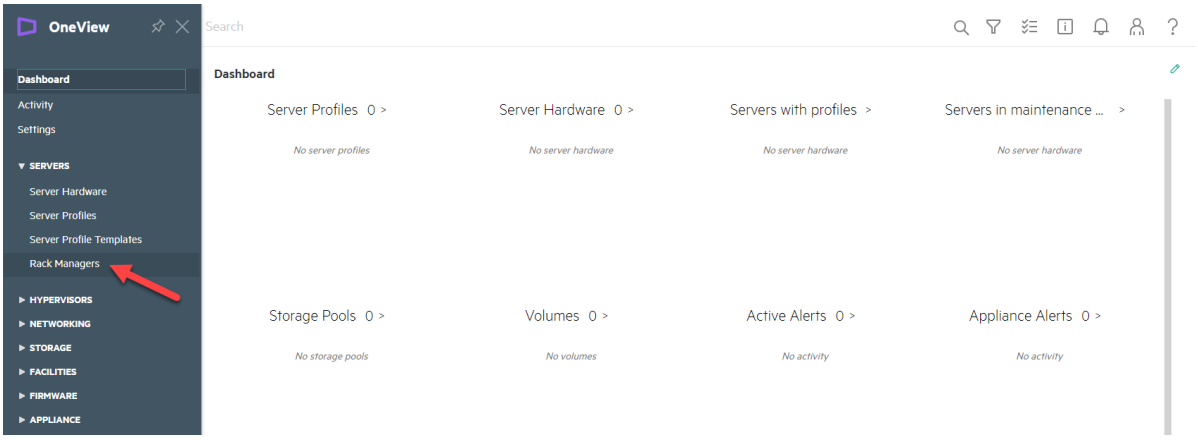
14. The Server Profile is then applied.

HPE Superdome Flex 280

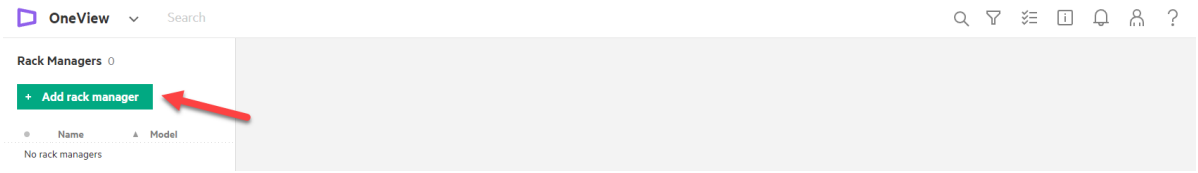
HPE OneView supports adding an HPE Superdome Flex 280 for hardware monitoring or managing. In this section you will import a Superdome Flex 280 server by adding the IP address or FQDN of its Rack Manager Controller (eRMC).

Import the Rack Management Controller

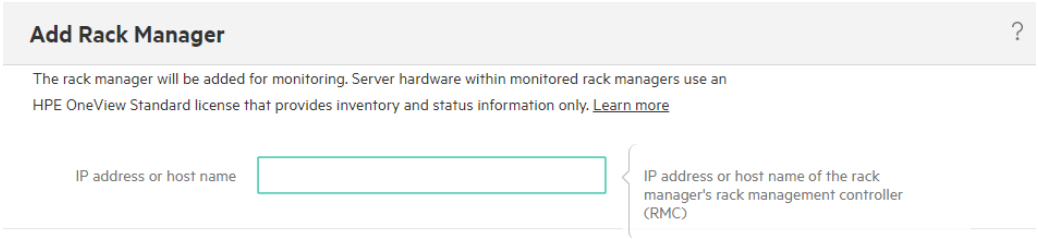
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Rack Managers*.



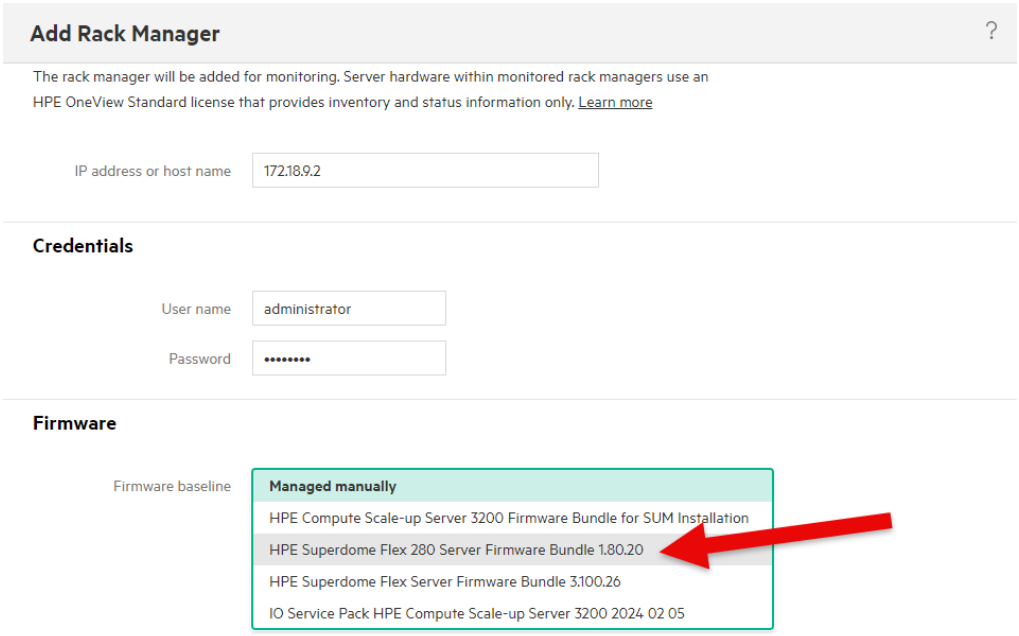
2. From the menu, select Add rack manager



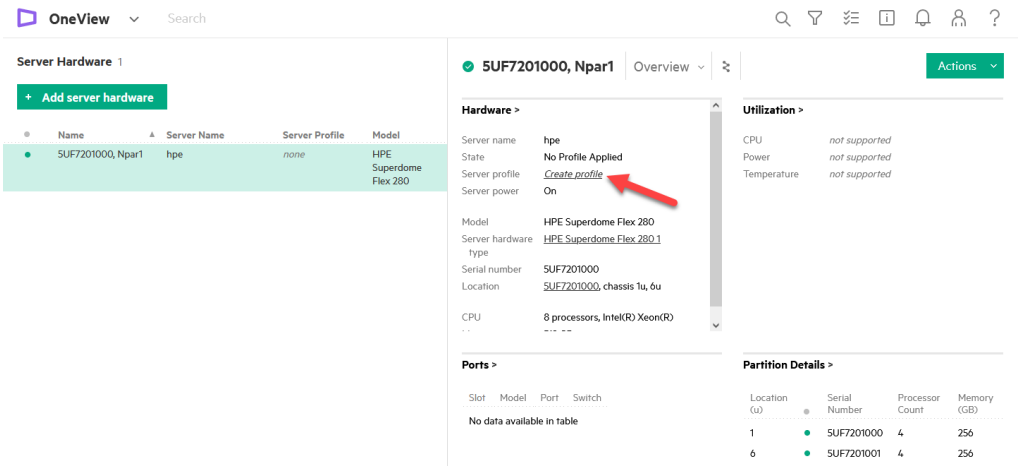
3. Enter the IP address or host name of the rack manager



4. Enter the *Credentials* of the rack manager, choose the *Firmware baseline* and then click *Add*.

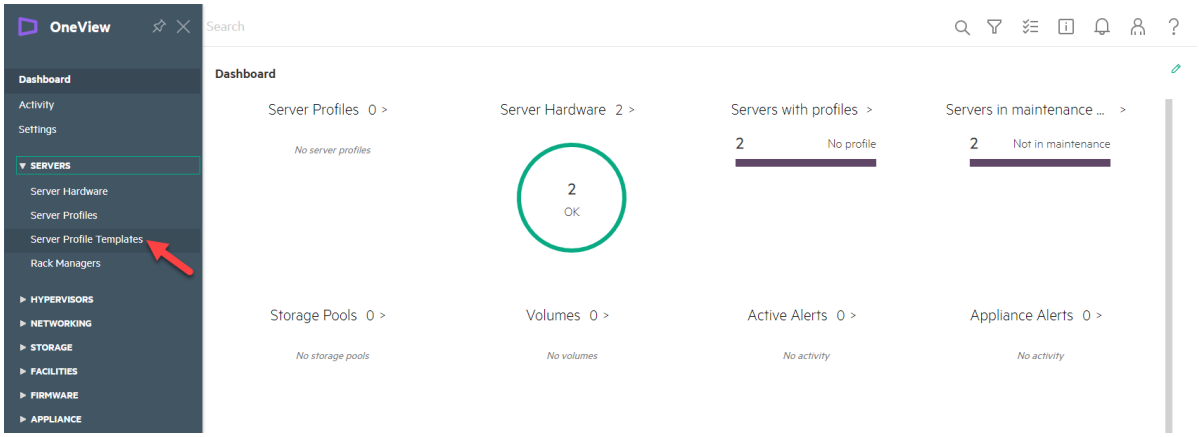


5. Go into the Server Hardware you will now be able to create a Server Profile for the Superdome Flex 280 Server.

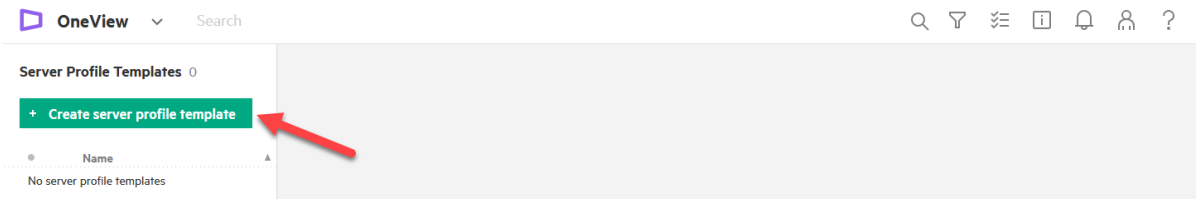


Create Superdome Flex 280 Server Profile Template

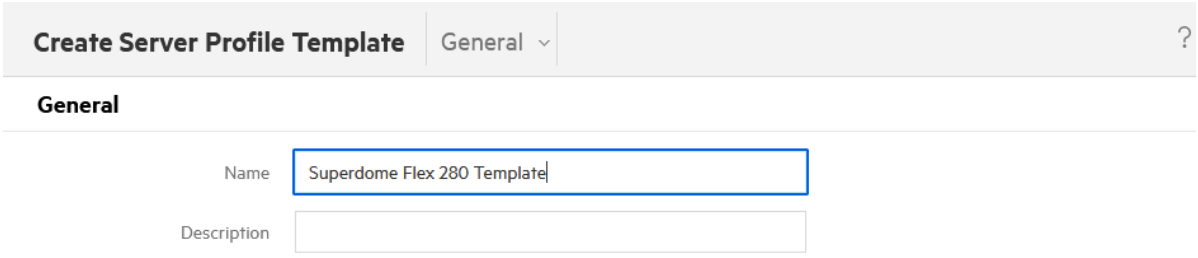
1. You can create a Server Profile Template for Superdome Flex the same as any other Server Hardware Type managed by OneView. From the main menu, expand the *Servers* option and then select *Server Profile Templates*.



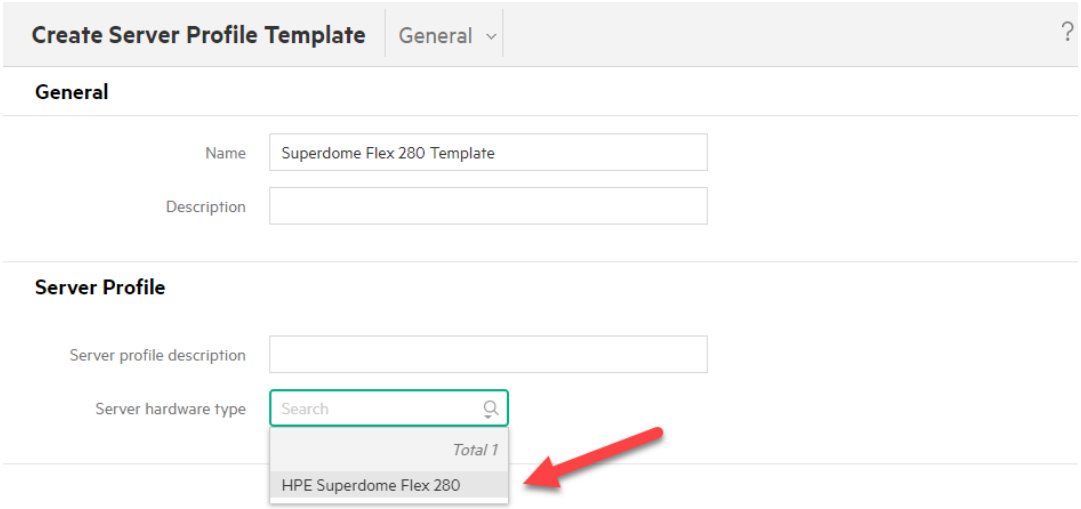
2. Once on the Server Profile Template screen, select the + *Create server profile template* button



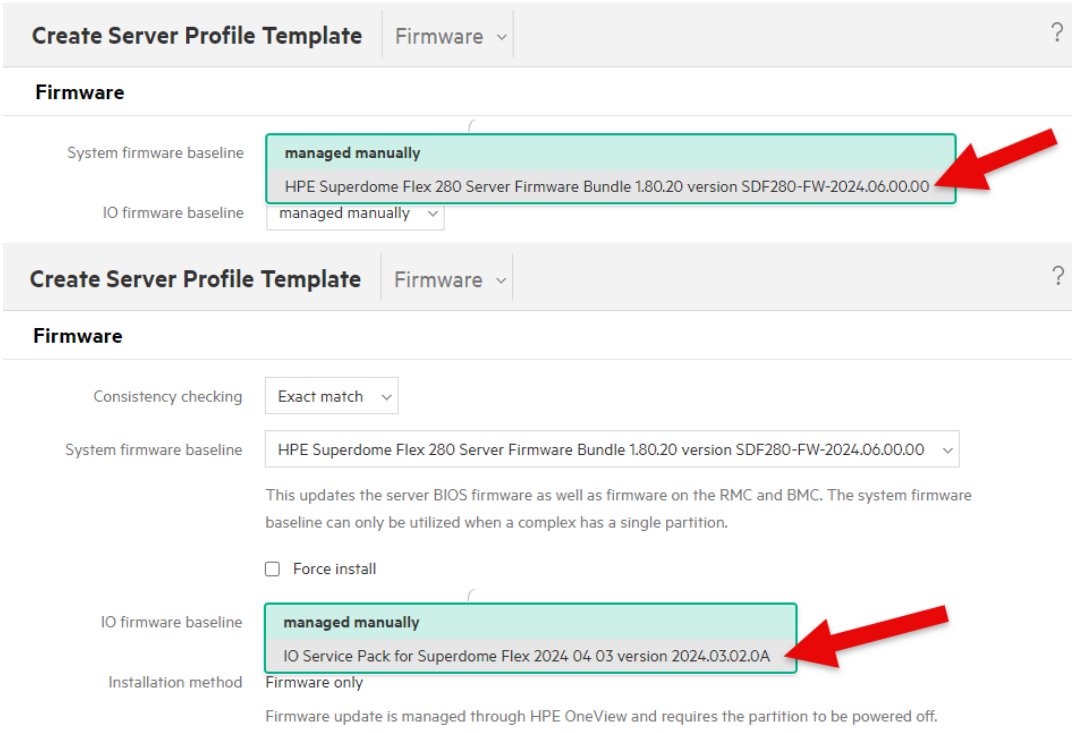
3. In the Server Profile section of the server profile template creation page, enter a *Name* and optionally a *Description* for the server profile template



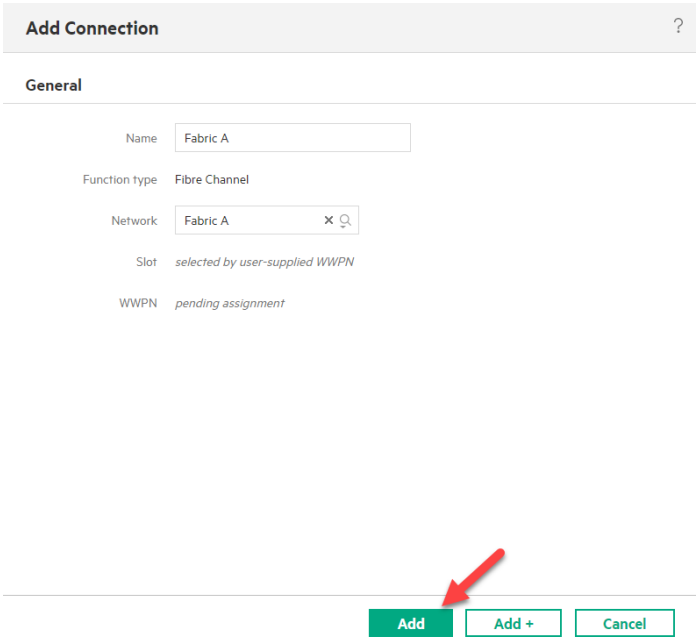
4. Choose the *Server hardware type*.



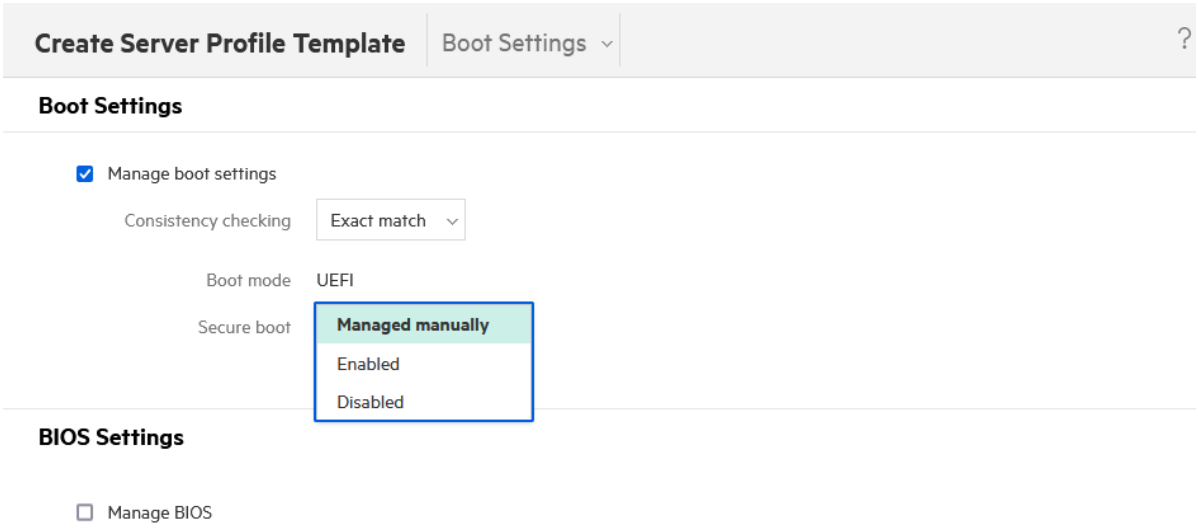
5. You can set a *Firmware Baseline* that the Hardware will be upgraded to when the Superdome Flex 280 has a Server Profile created



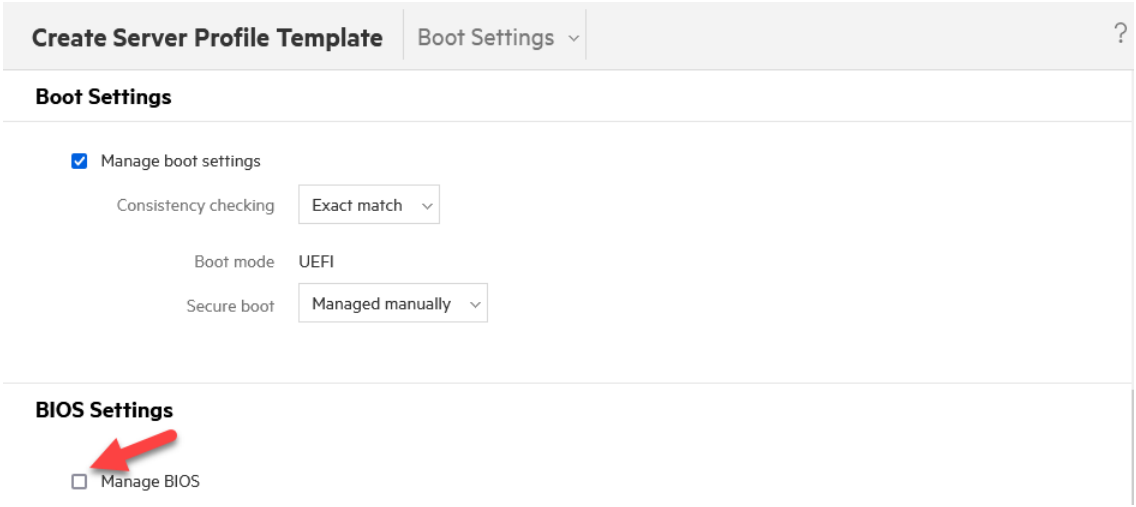
6. Now you can add the name of the Fabric and the Fabric Network that you want the Server connected to, once you have made your selections and click Add / Add + to add the connection.



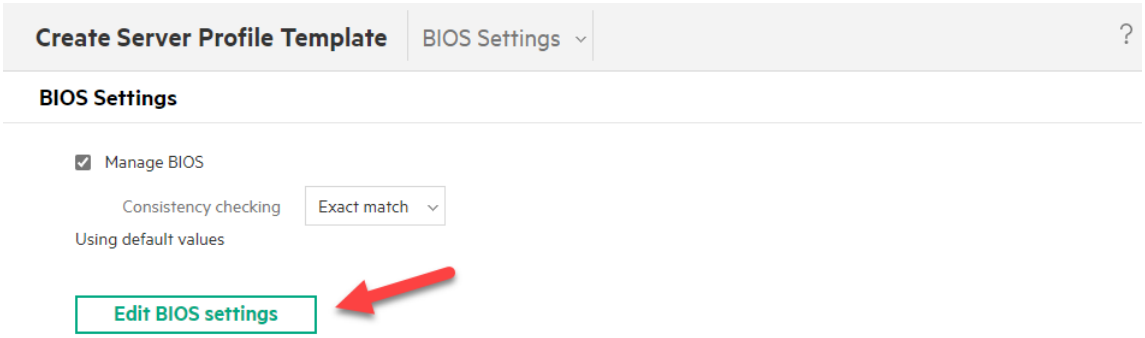
7. You can manage the boot settings (Secure Boot).



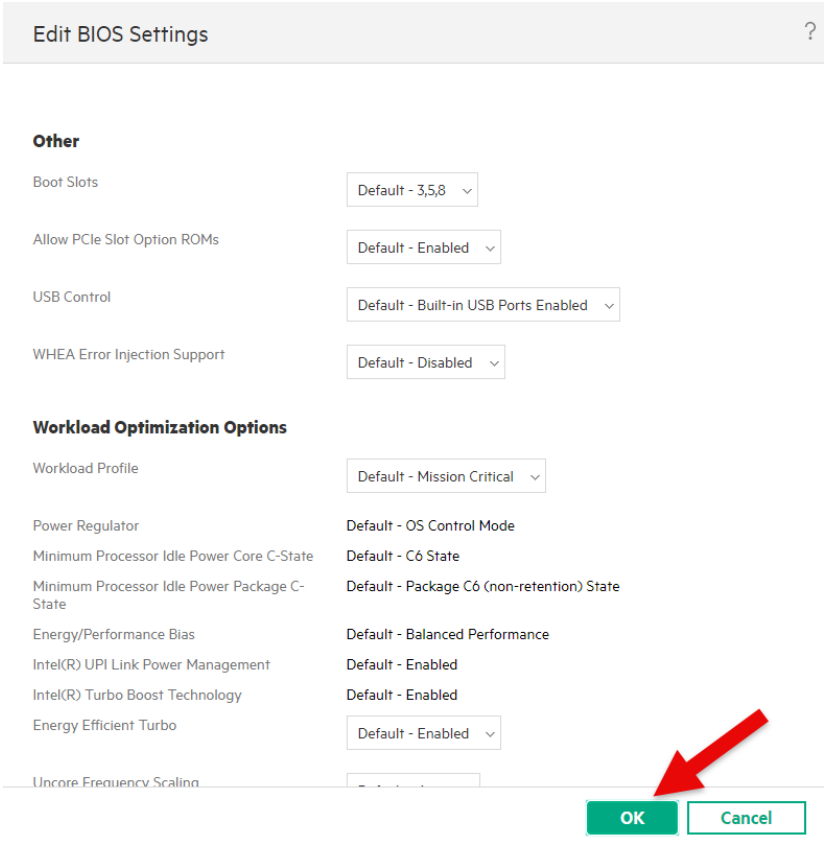
8. You can manage the BIOS Settings by clicking on *Manage BIOS*.



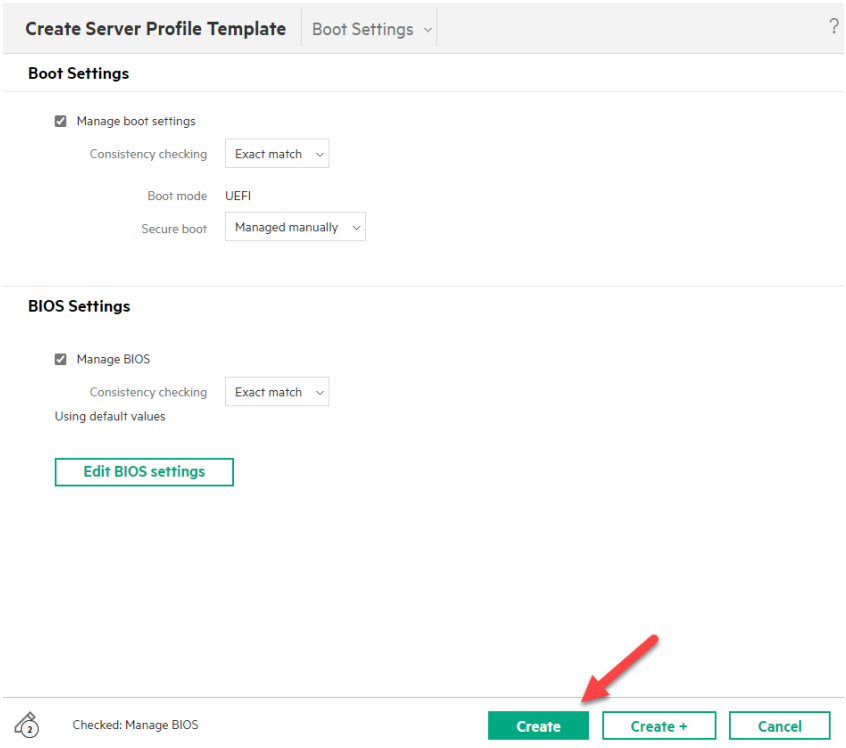
9. Then select *Edit BIOS settings*.



10. Make the required changes to the BIOS Settings and click *OK* to save them to the Server Profile Template.

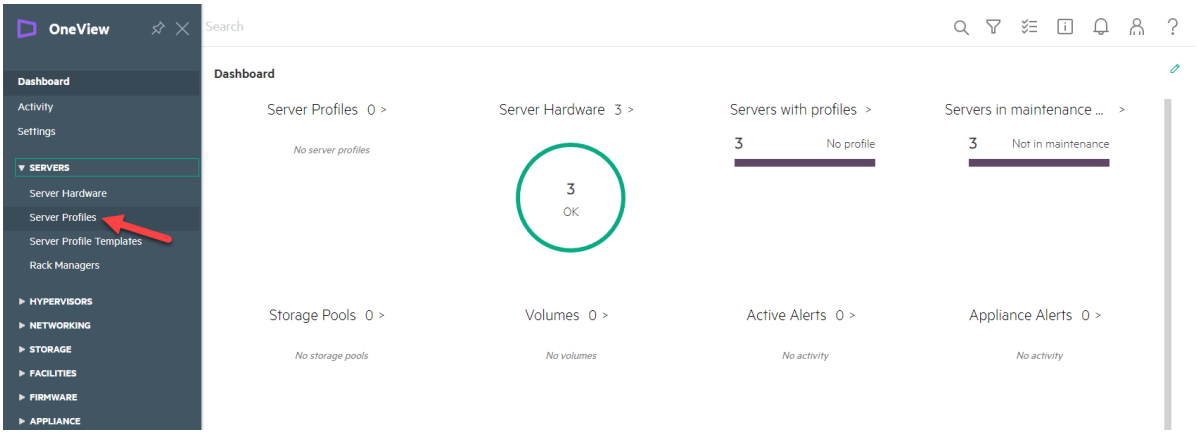


11. Click on the *Create* button to create the Server Profile Template

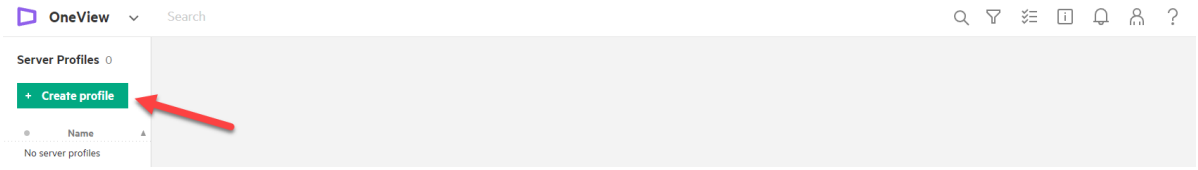


Create Superdome Flex 280 Server Profile

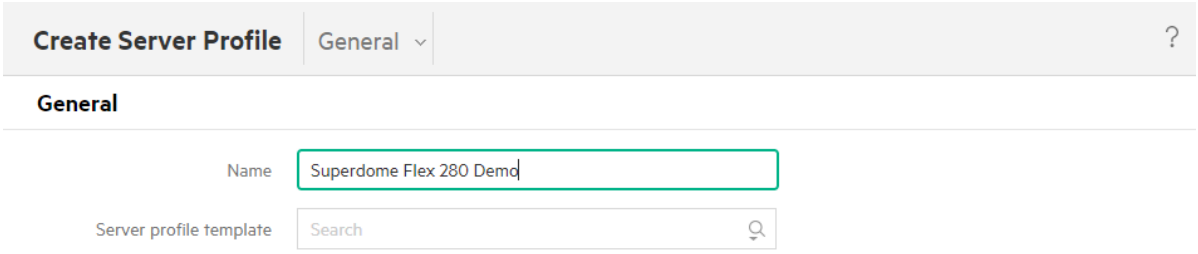
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



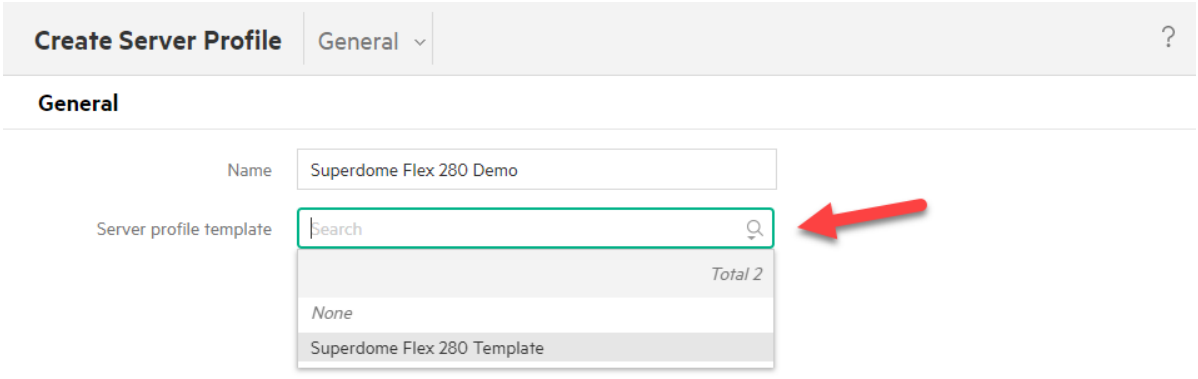
2. Choose + *Create profile*



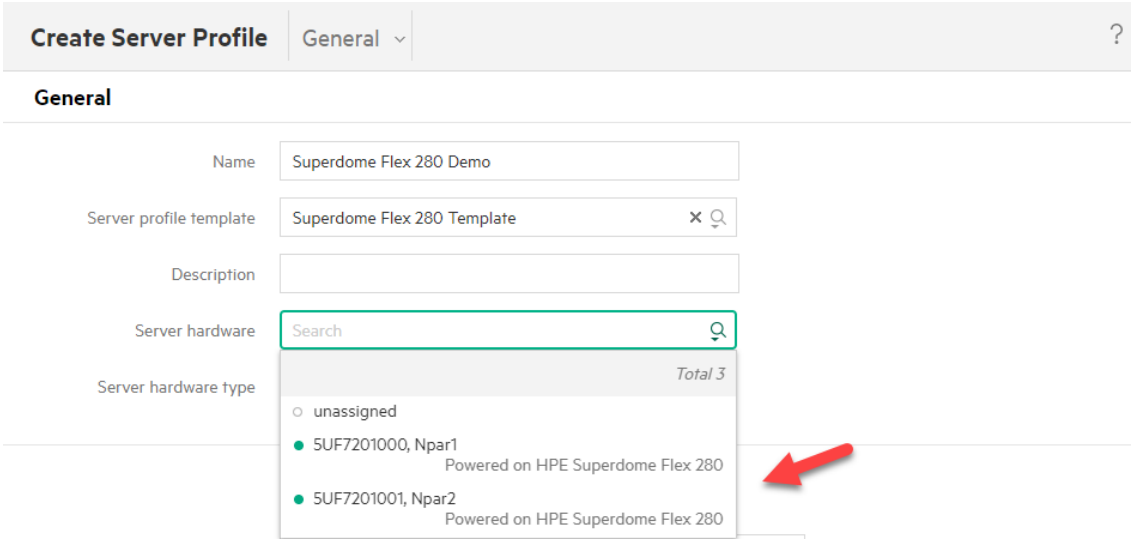
3. Type in Server *Name*.



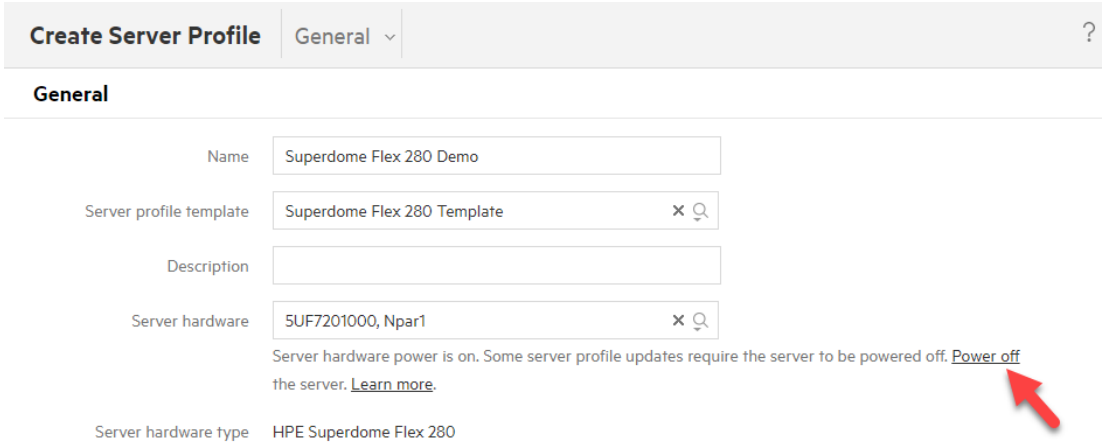
4. You can base it on an existing *Server profile template* if one has been created or select *None*.



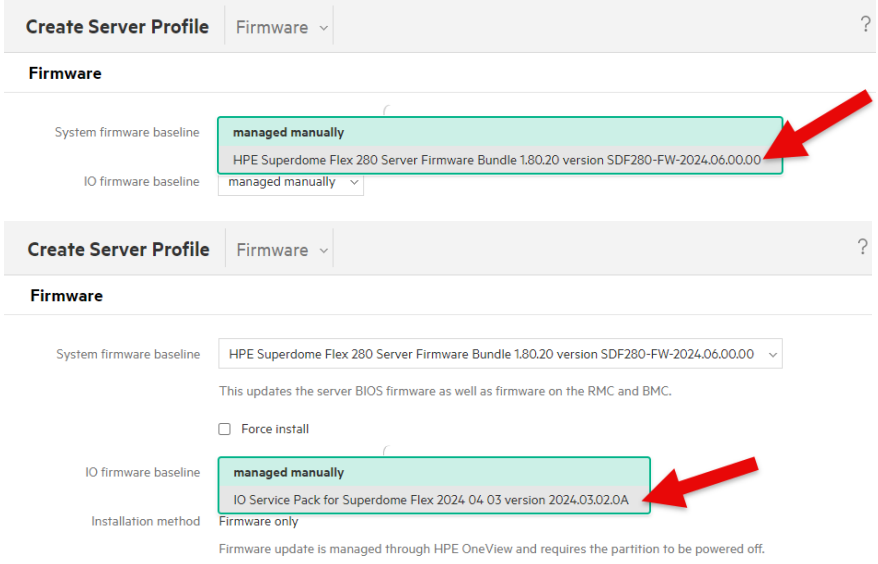
5. Choose the Superdome Flex 280 *NPar* in *Server hardware* that you wish the Server Profile to be assigned to



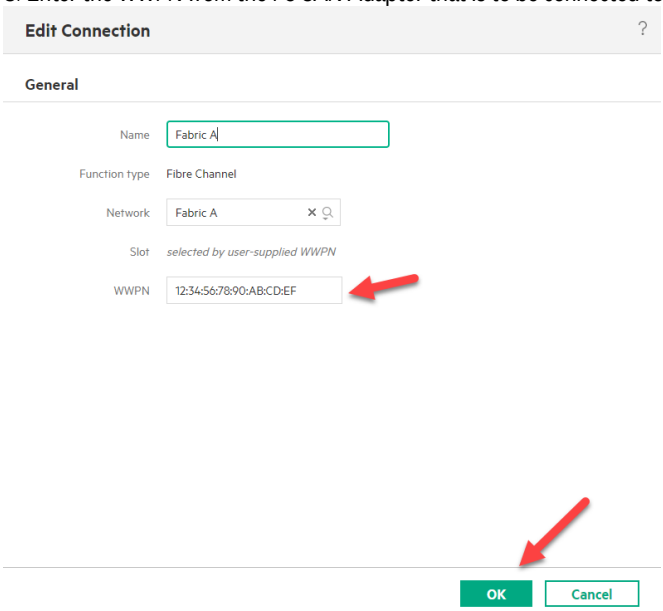
6. You can only apply a Server Profile to a Server that is "Powered Off" and as you can see this server is still Powered on.



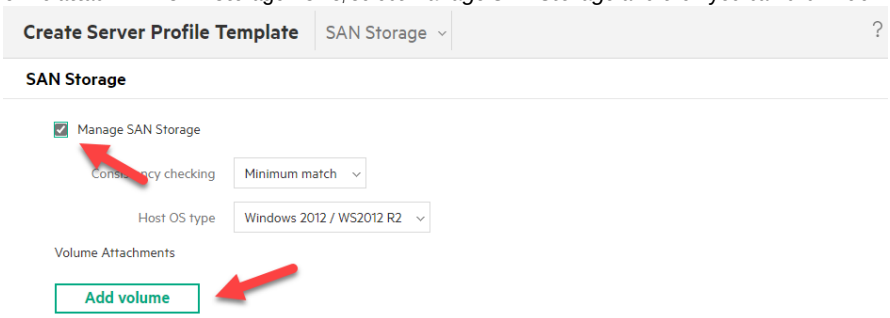
7. You can now set if you want the Superdome Flex 280 to have its firmware changed to support a different *Firmware baseline*



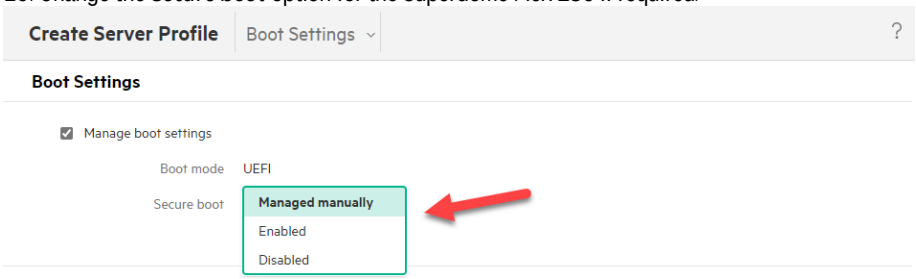
8. Enter the WWPN from the FC SAN Adapter that is to be connected to the SAN Fabric (do the same for the second Fabric)



9. To attach HPE SAN Storage LUNs, select *Manage SAN Storage* and then you can click *Add volume*. To attach a HPE SAN LUN.



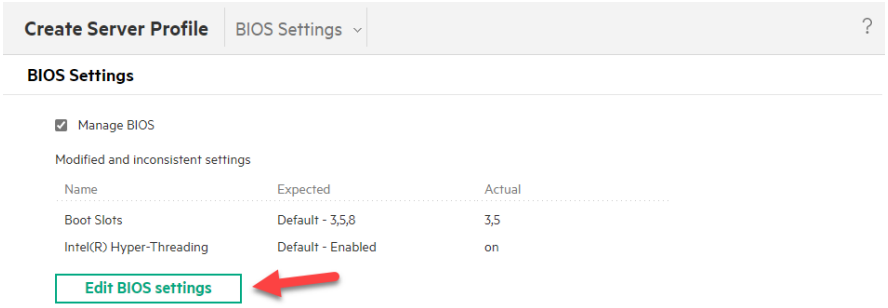
10. Change the *Secure boot* option for the Superdome Flex 280 if required.



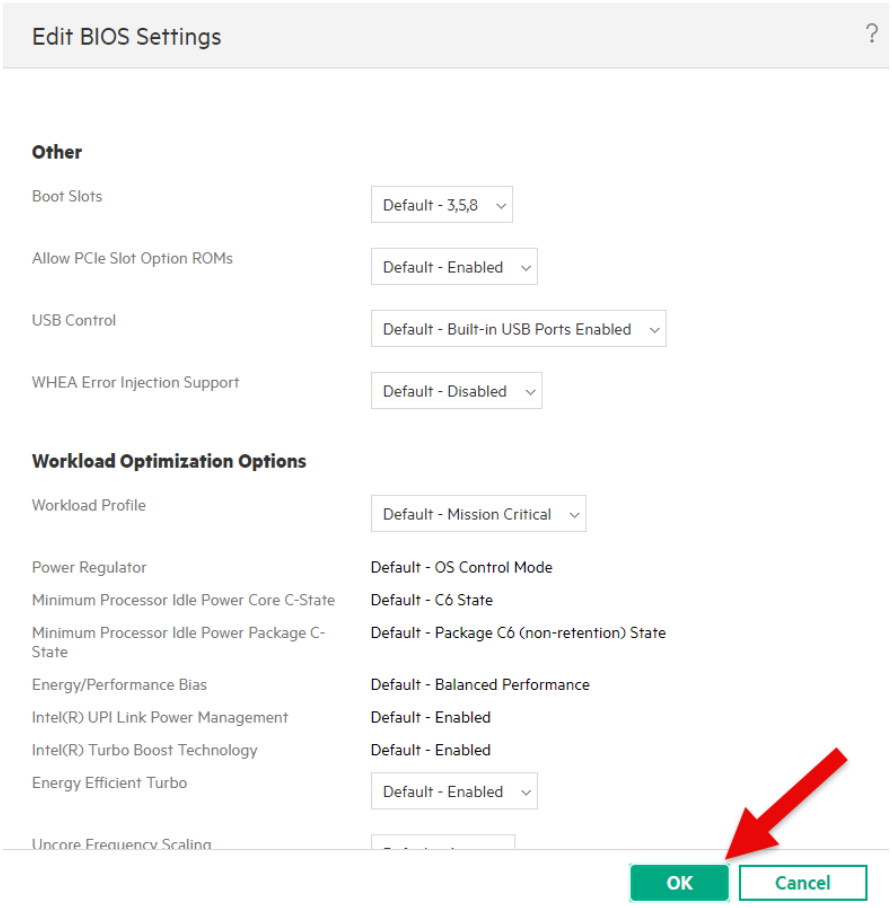
11. BIOS Settings can be managed by clicking on *Manage BIOS*.



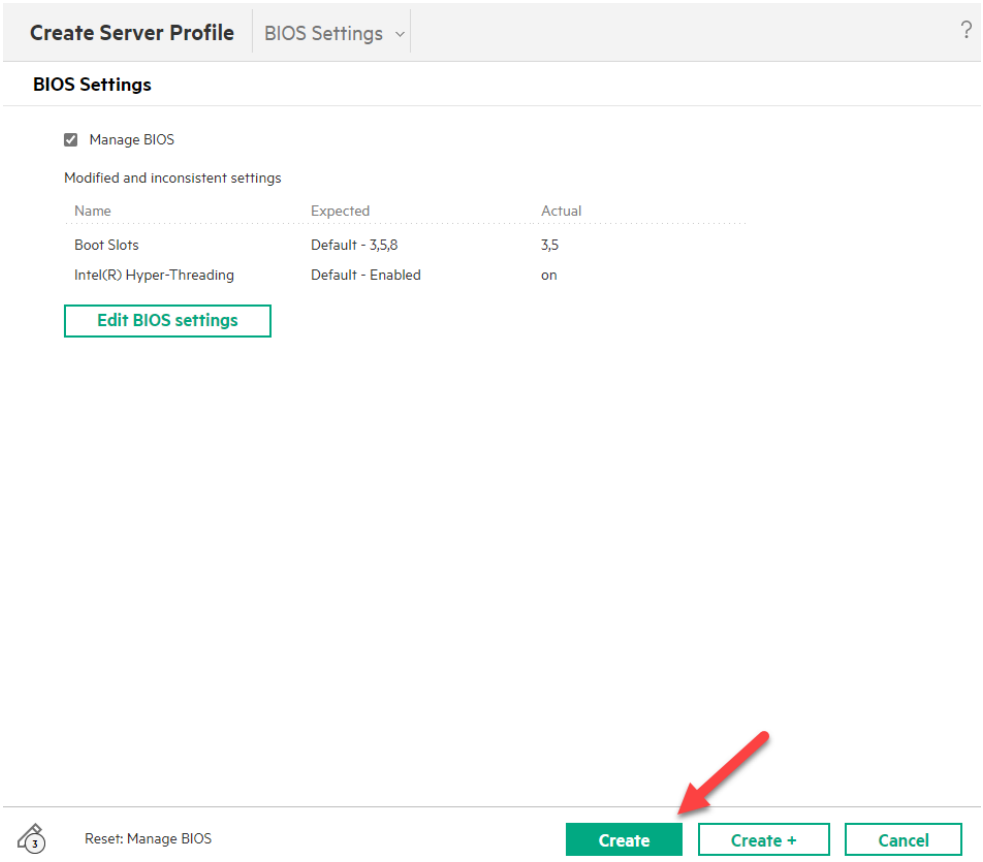
12. Now click on *Edit BIOS settings*.



13. Change any of the BIOS Settings as required and click *OK* to save the changes.



14. Click *Create* to create the Server Profile for the Superdome Flex 280.



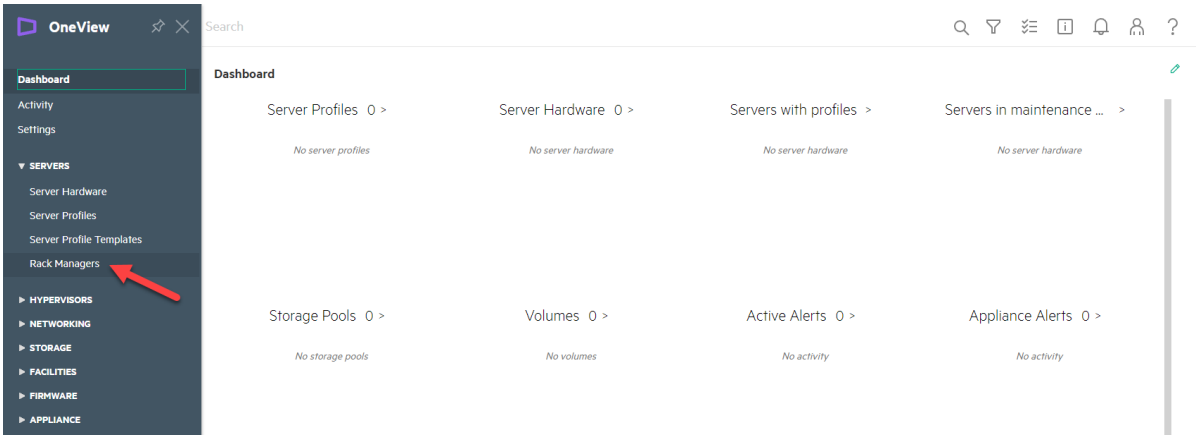
15. The Server Profile is then applied.

HPE Compute Scale-up Server 3200

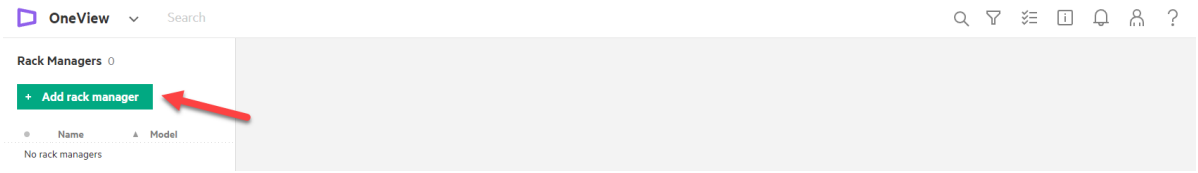
HPE OneView supports adding an HPE Compute Scale-up for hardware monitoring or managing. In this section you will import a HPE Compute Scale-up Server 3200 server by adding the IP address or FQDN of its Rack Manager Controller (eRMC).

Import the Rack Management Controller

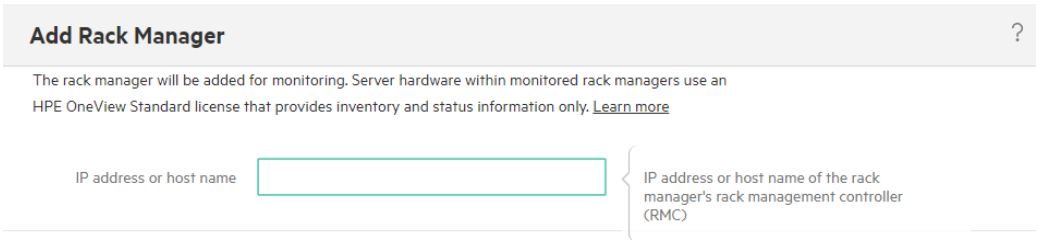
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Rack Managers*.



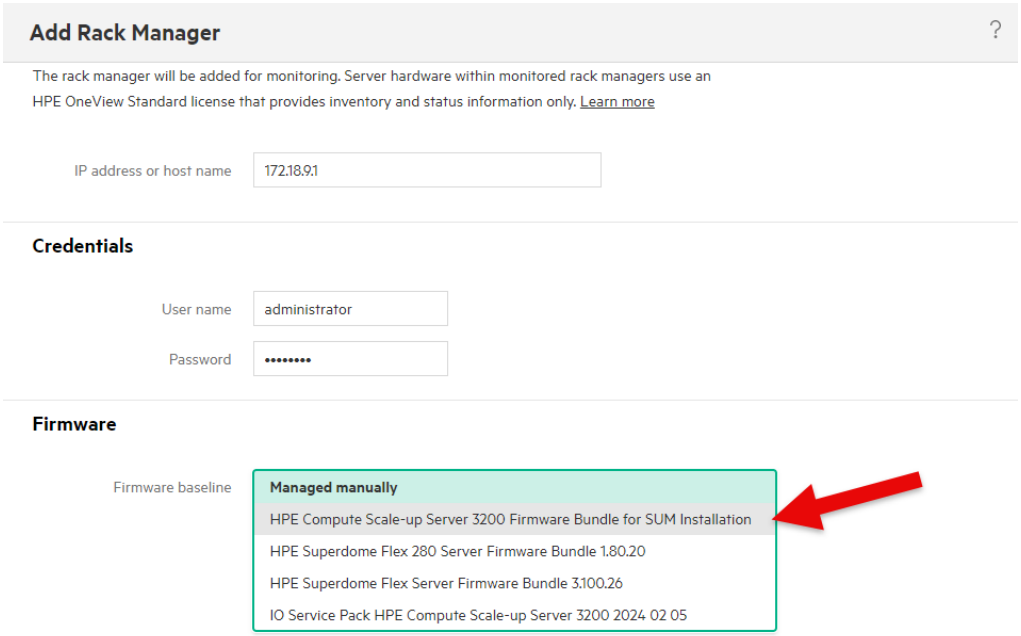
2. From the menu, select Add rack manager



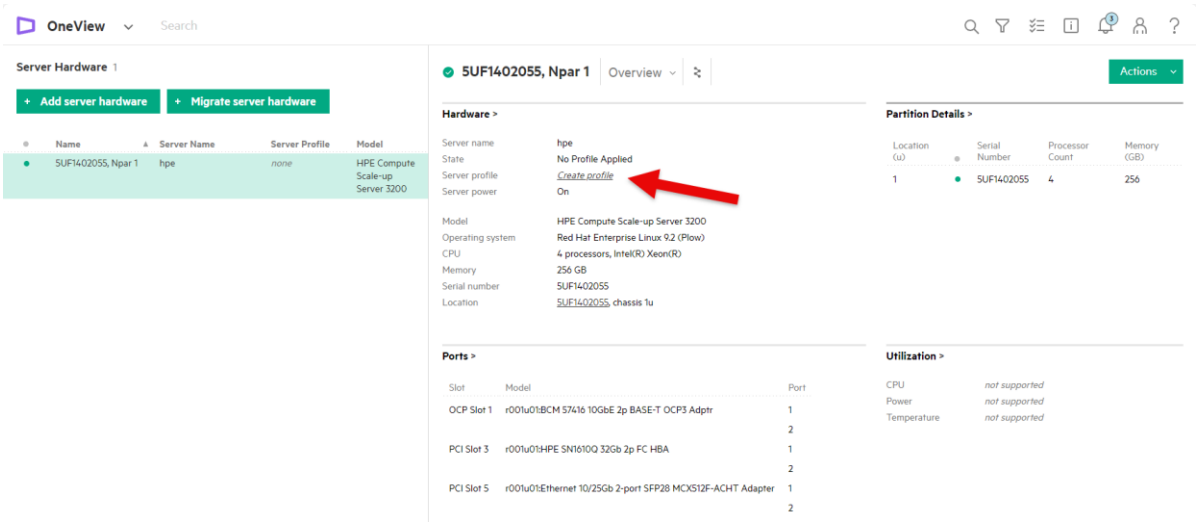
3. Enter the IP address or host name of the rack manager



4. Enter the *Credentials* of the rack manager, choose the *Firmware baseline* and then click *Add*.

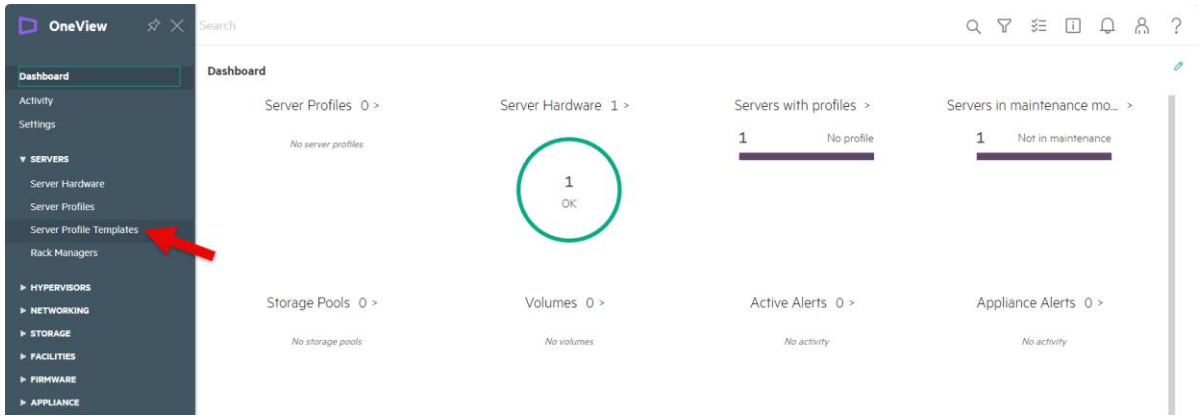


5. Go into the Server Hardware you will now be able to create a Server Profile for the HPE Compute Scale-up Server 3200.

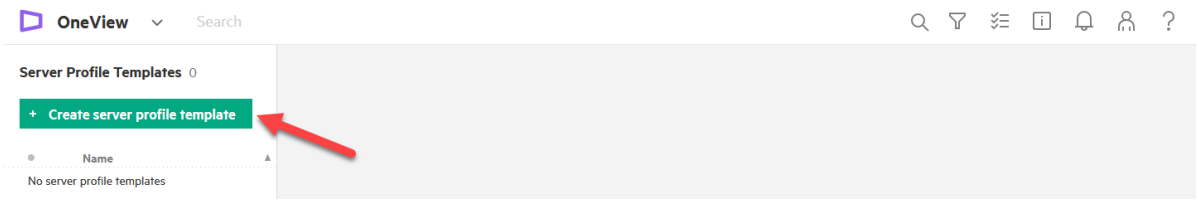


Create HPE Compute Scale-up Server 3200 Profile Template

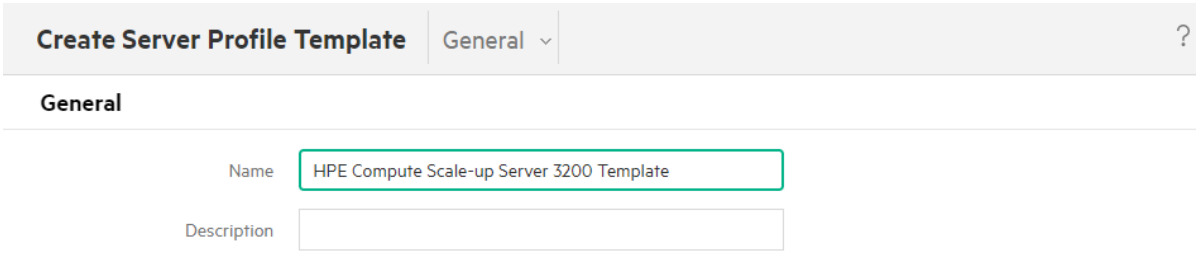
1. You can create a Server Profile Template for HPE Compute Scale-up Server 3200 the same as any other Server Hardware Type managed by OneView. From the main menu, expand the *Servers* option and then select *Server Profile Templates*.



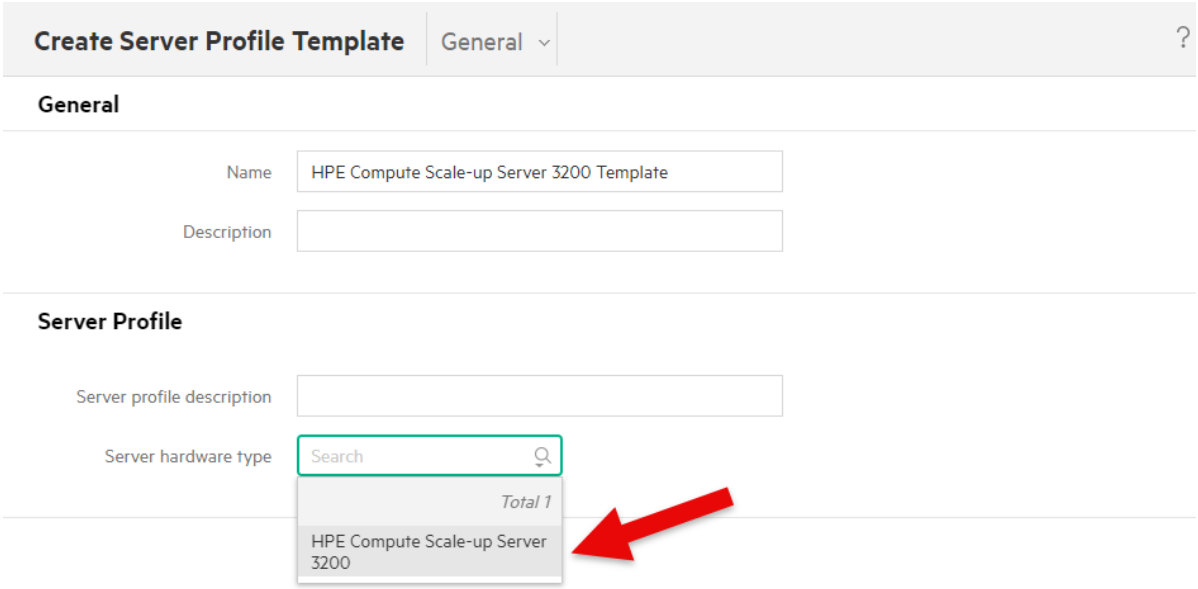
2. Once on the Server Profile Template screen, select the + *Create server profile template* button



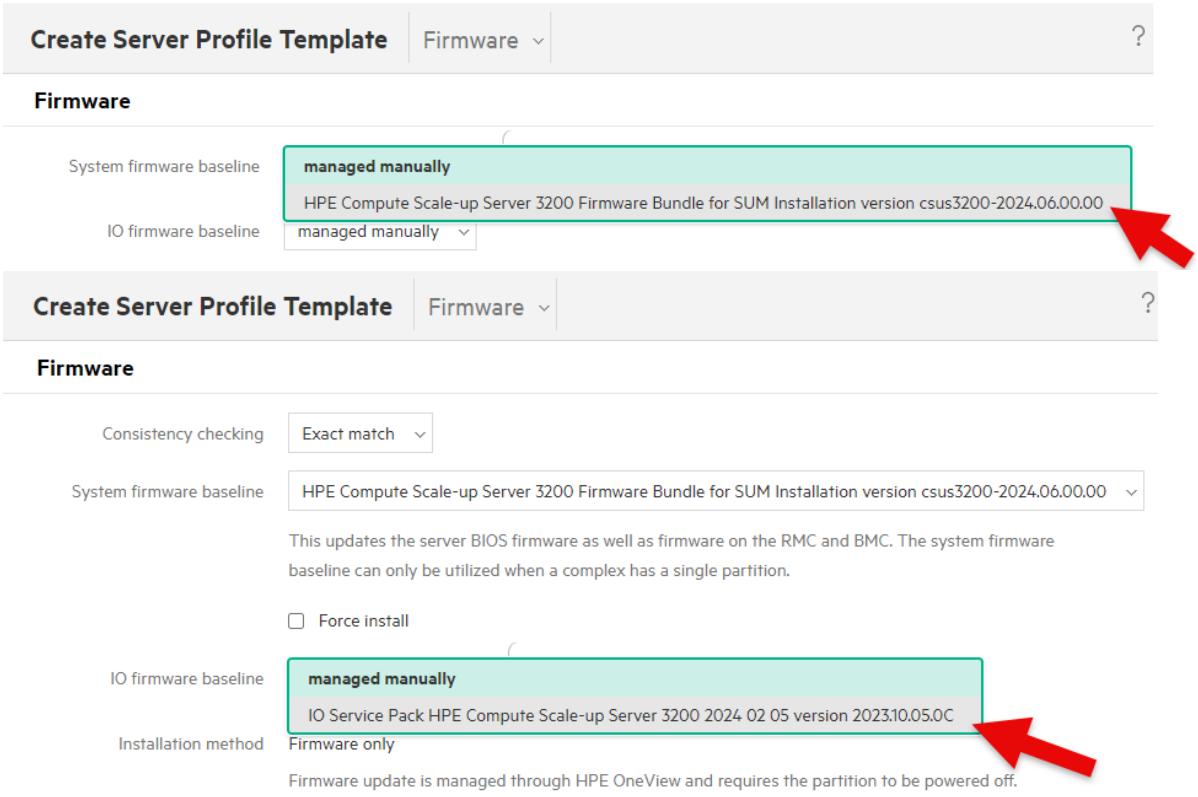
3. In the Server Profile section of the server profile template creation page, enter a *Name* and optionally a *Description* for the server profile template



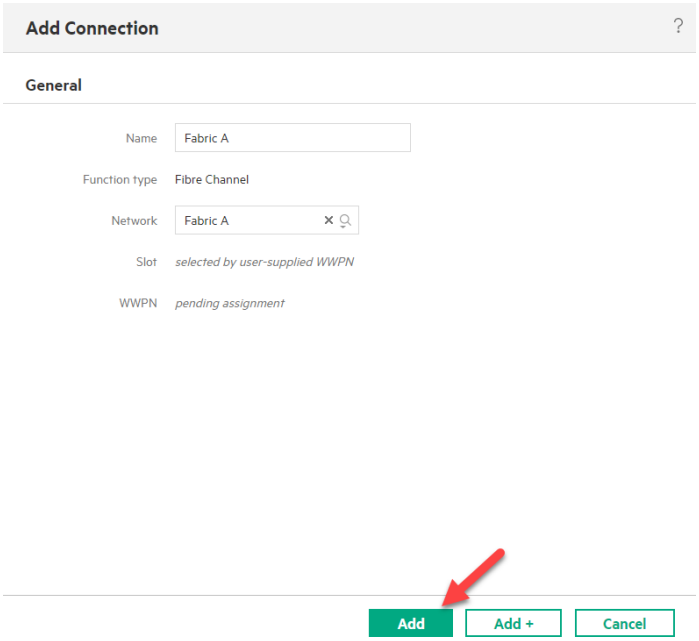
4. Choose the *Server hardware type*.



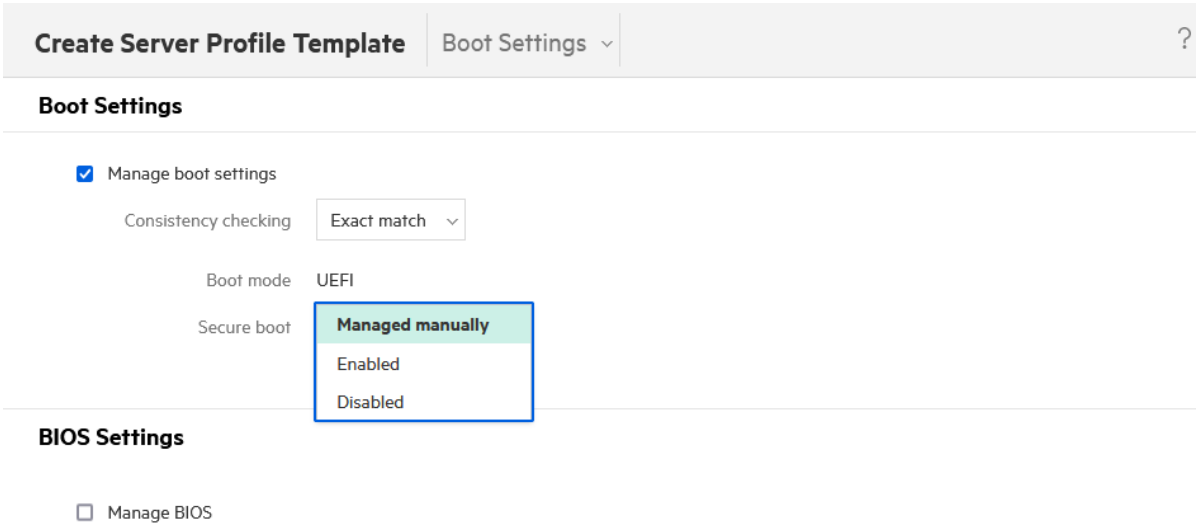
5. You can set a *Firmware Baseline* that the Hardware will be upgraded to when the HPE Compute Scale-up Server 3200 has a Server Profile created



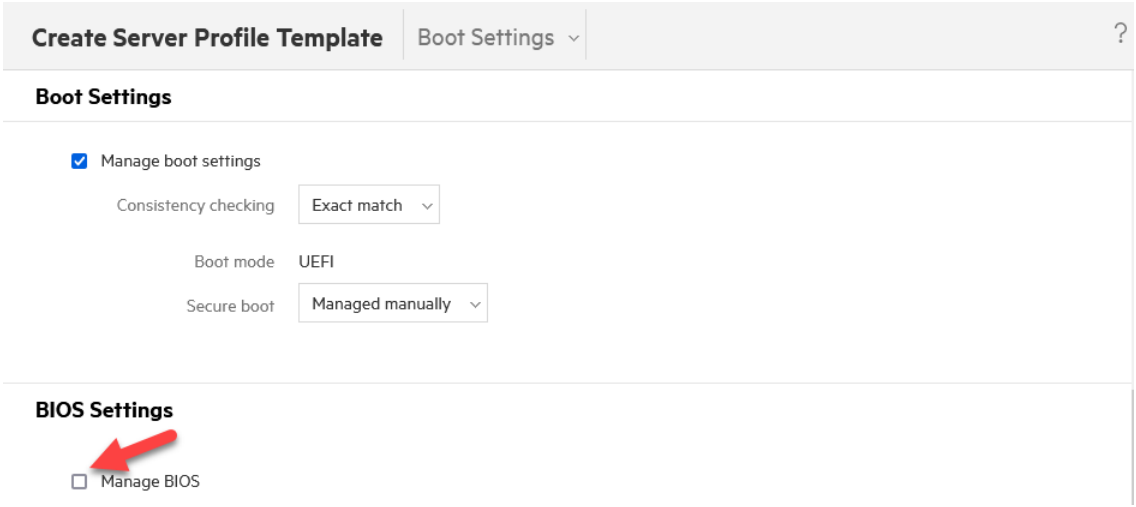
6. Now you can add the name of the Fabric and the Fabric Network that you want the Server connected to, once you have made your selections and click Add / Add + to add the connection.



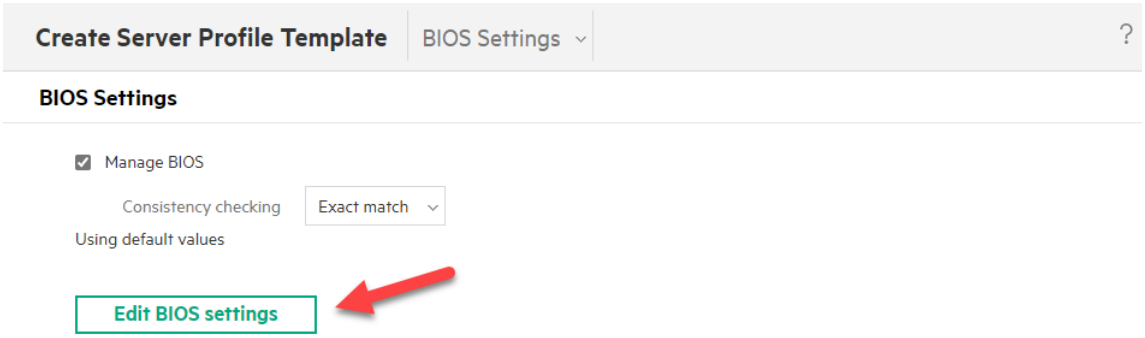
7. You can manage the boot settings (Secure Boot).



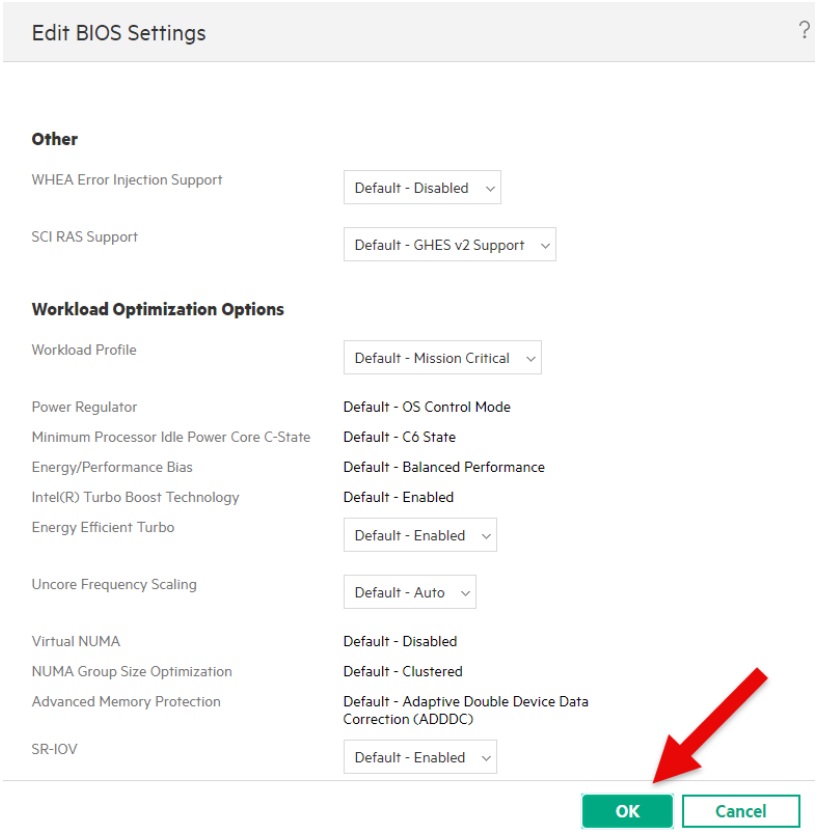
8. You can manage the BIOS Settings by clicking on *Manage BIOS*.



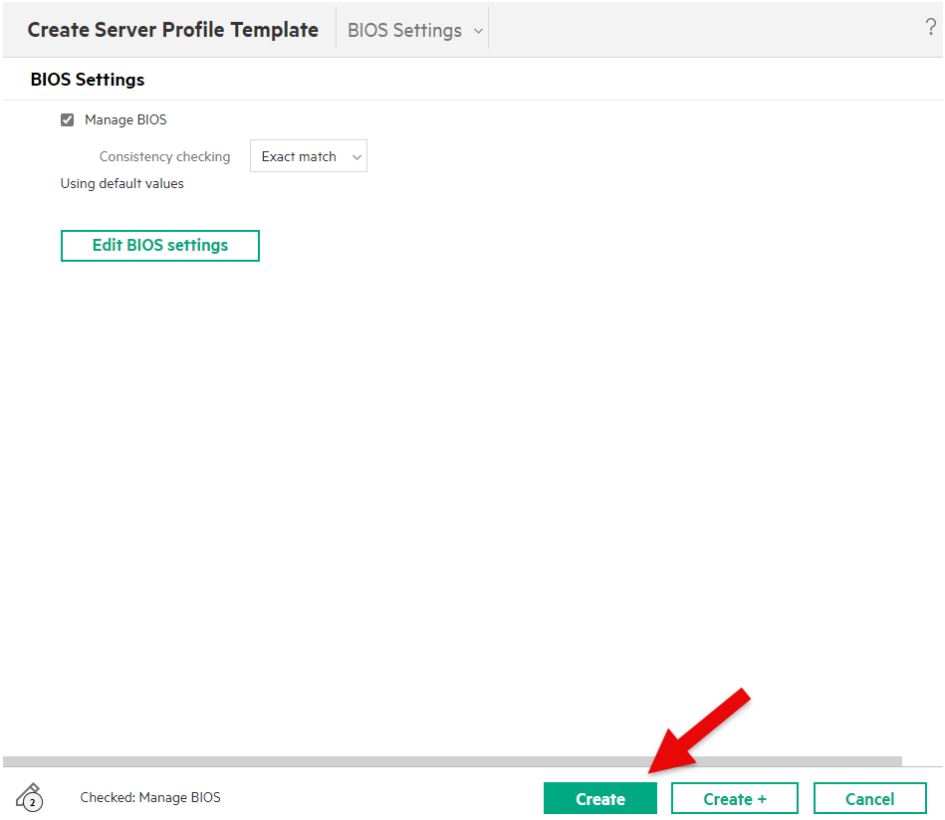
9. Then select *Edit BIOS settings*.



10. Make the required changes to the BIOS Settings and click *OK* to save them to the Server Profile Template.

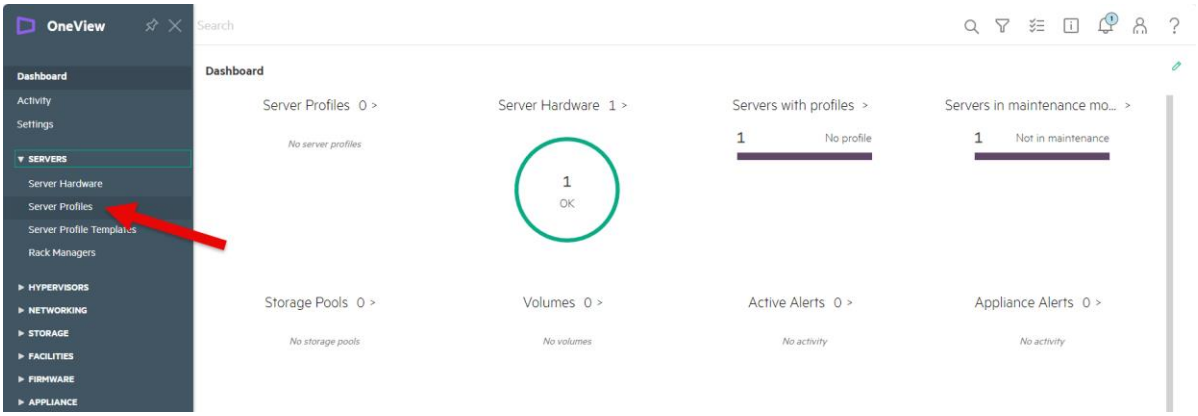


11. Click on the *Create* button to create the Server Profile Template

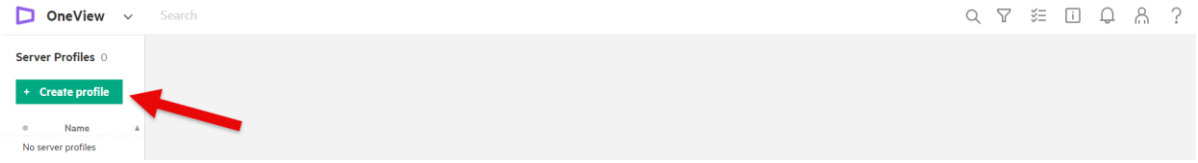


Create HPE Compute Scale-up Server 3200 Server Profile

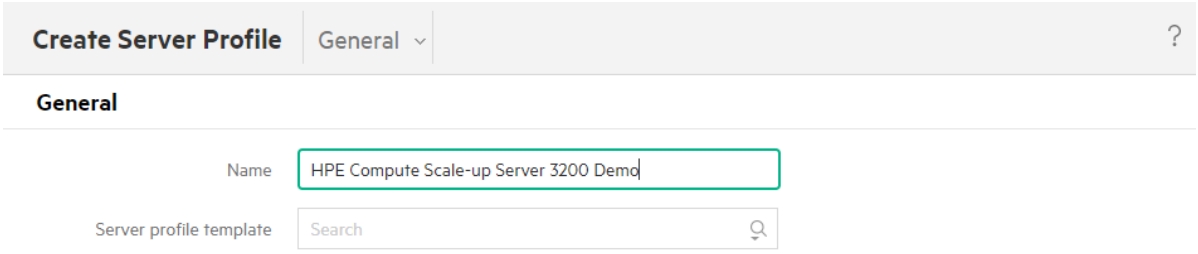
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



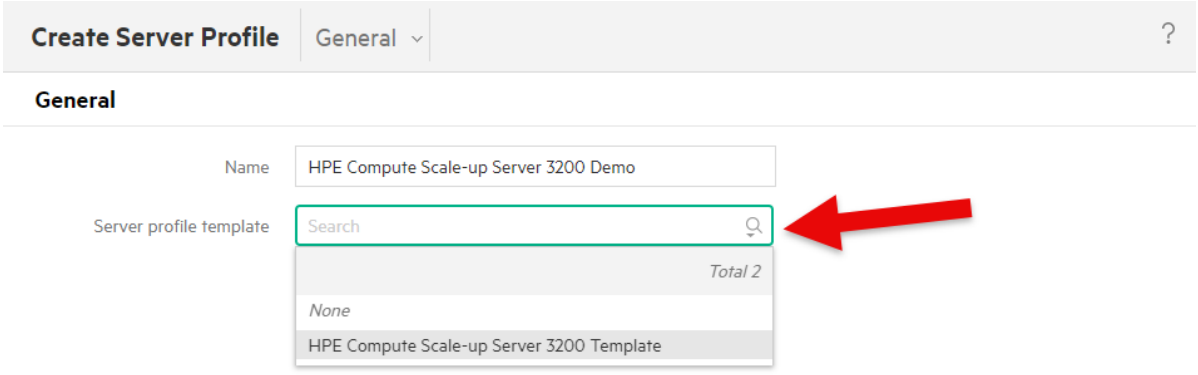
2. Choose + *Create profile*



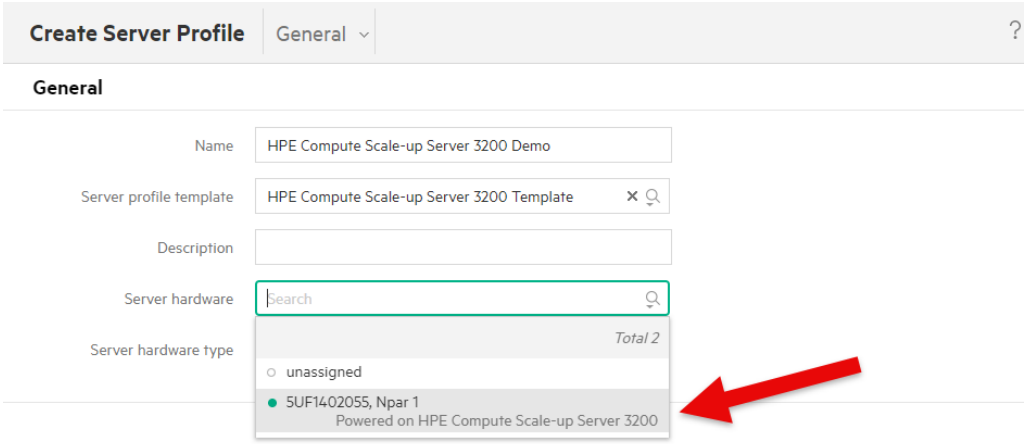
3. Type in Server *Name.*



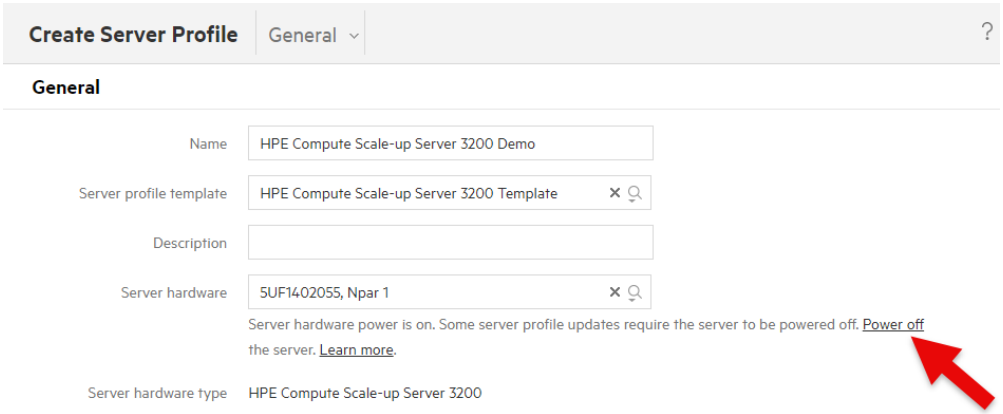
4. You can base it on an existing *Server profile template* if one has been created or select *None.*



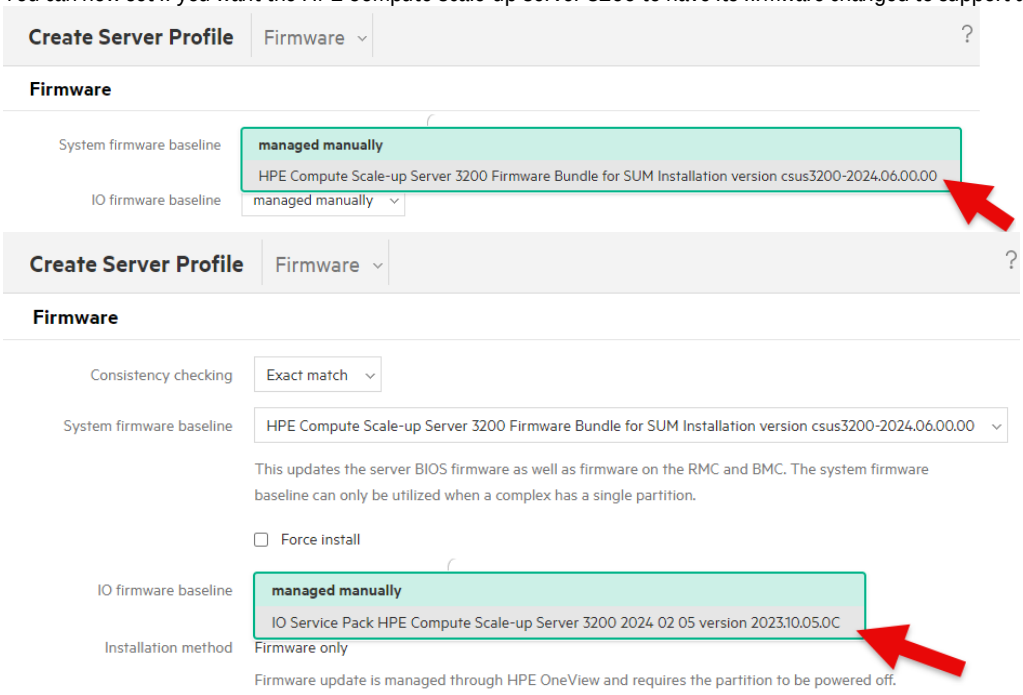
5. Choose the HPE Compute Scale-up Server 3200 *NPar* in *Server hardware* that you wish the Server Profile to be assigned to



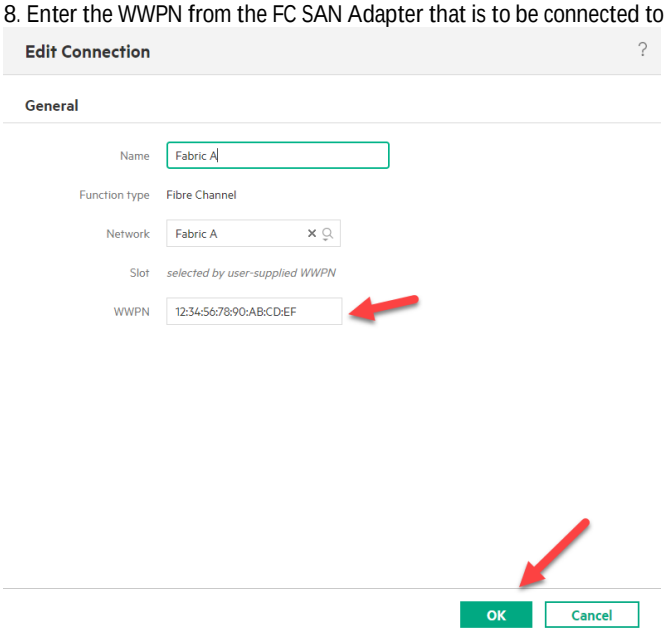
6. You can only apply a Server Profile to a Server that is "Powered Off" and as you can see this server is still Powered on.



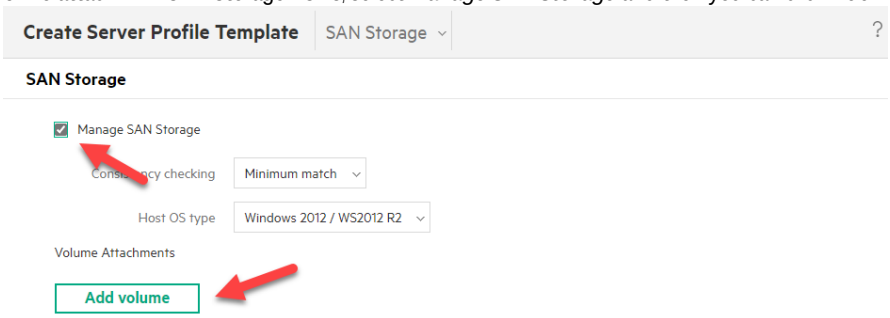
7. You can now set if you want the HPE Compute Scale-up Server 3200 to have its firmware changed to support a different *Firmware baseline*



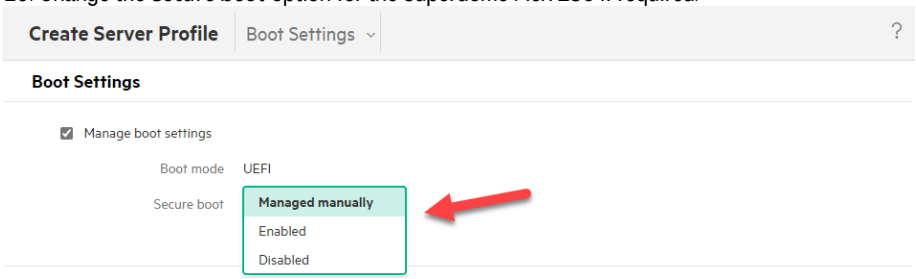
8. Enter the WWPN from the FC SAN Adapter that is to be connected to the SAN Fabric (do the same for the second Fabric)



9. To attach HPE SAN Storage LUNs, select *Manage SAN Storage* and then you can click *Add volume*. To attach a HPE SAN LUN.



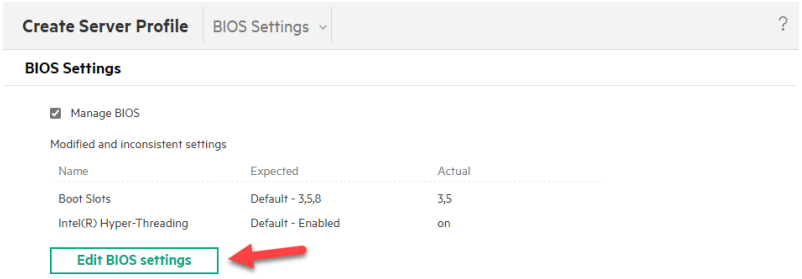
10. Change the *Secure boot* option for the Superdome Flex 280 if required.



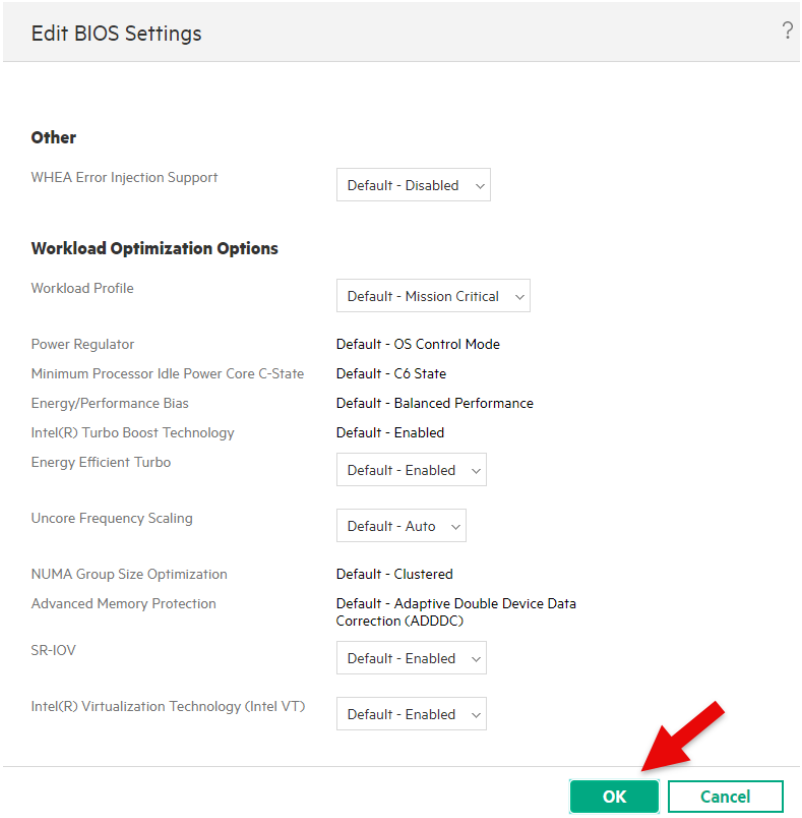
11. BIOS Settings can be managed by clicking on *Manage BIOS*.



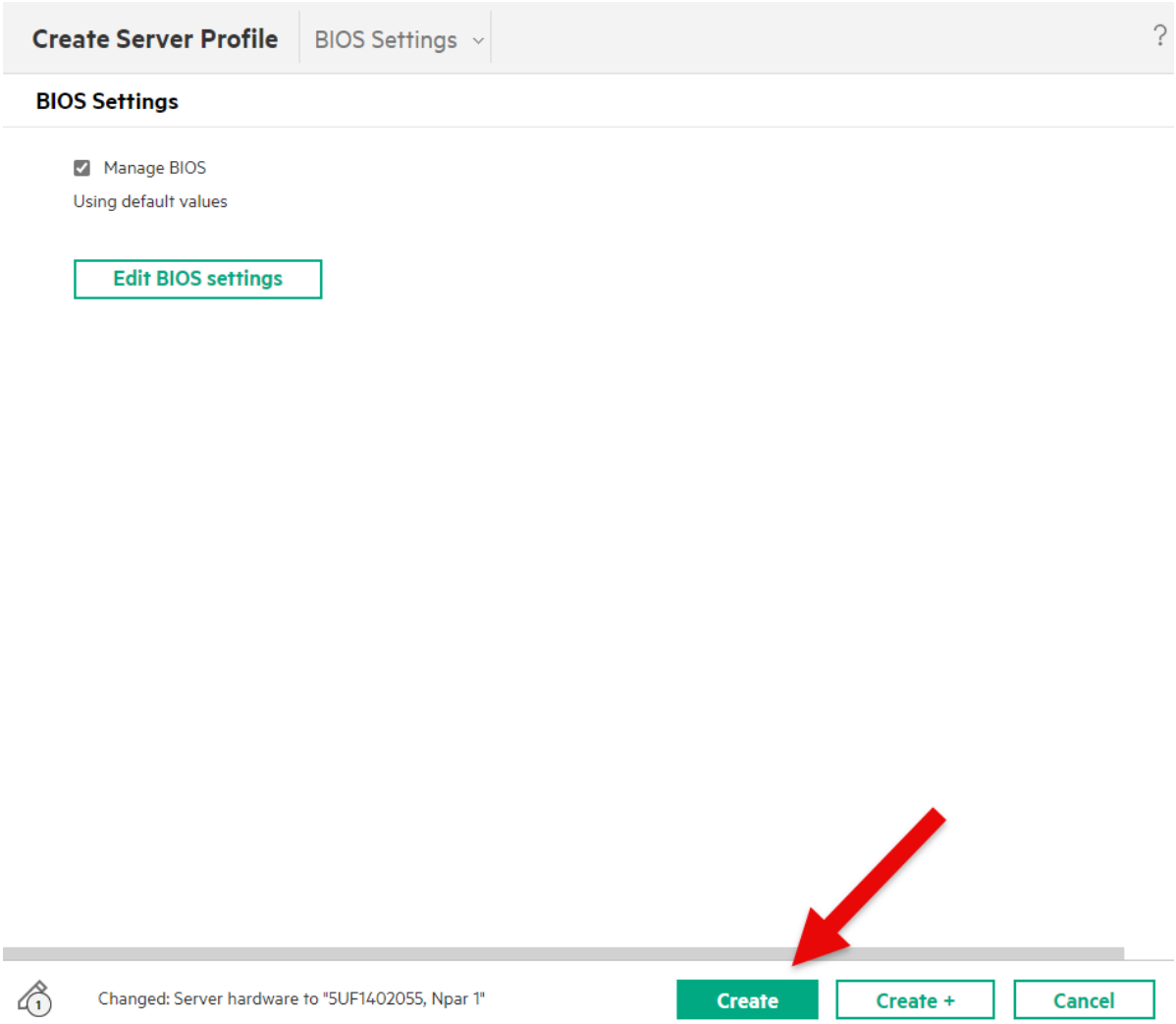
12. Now click on *Edit BIOS settings*.



13. Change any of the BIOS Settings as required and click *OK* to save the changes.



14. Click *Create* to create the Server Profile for the HPE Compute Scale-up Server 3200.



15. The Server Profile is then applied.

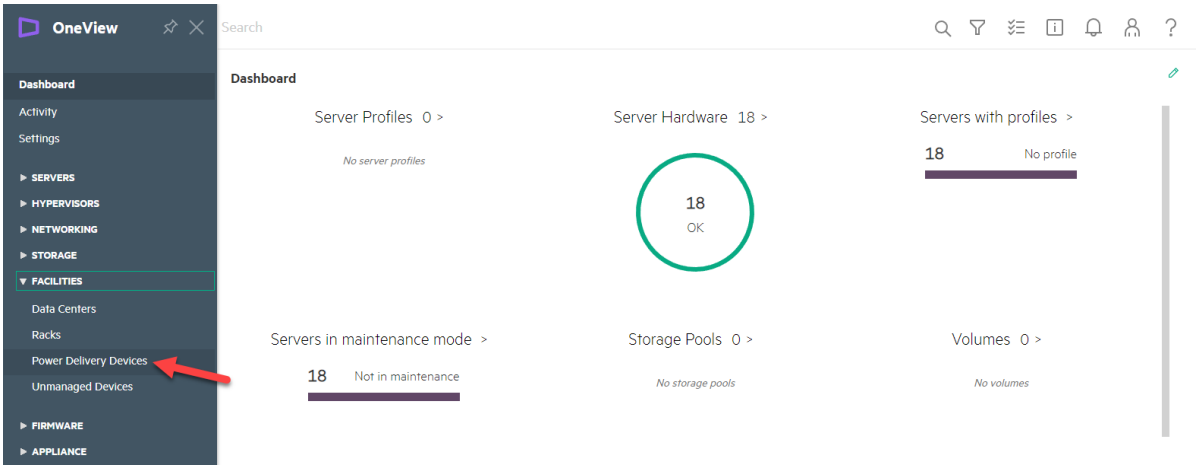
Configuring power delivery topology for the Data Center

Configuring the physical setup for your data center is only half the picture. To get a complete understanding of your environment, you can also configure its power delivery hierarchy. Building out your environment's power topology helps reduce downtime by eliminating wiring errors and identifying potential overloads. HPE OneView enables you to create power distribution device objects and describe the power source for one or more components in the rack. Below, configures the rack-level power distribution for each rack.

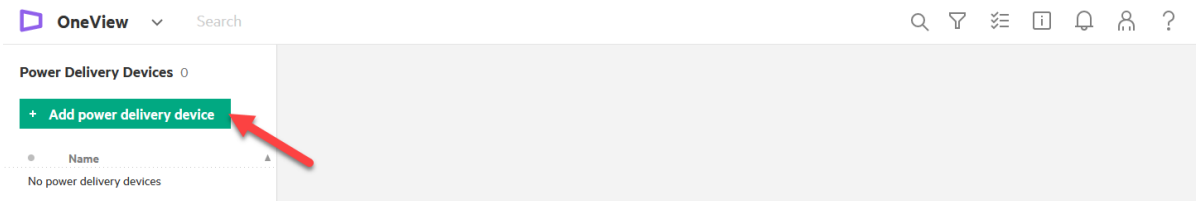
Note: *Starting with OneView 5.2 with a newly deployed environment, TLS 1.0 is disabled by default. If your OneView Appliance was upgraded from a previous version with TLS 1.0 enabled then it will remain so after the upgrade to OneView 5.2 or later. If you need to enable TLS 1.0 (not recommended) then please consult OneView Help to enable TLS 1.0 using the OneView REST API.*

Adding HPE **iPDU's**

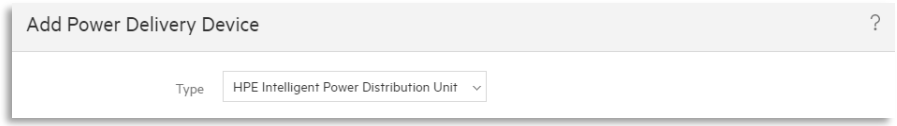
1. From the Top-Level Menu, expand the *FACILITIES* option and then select *Power Delivery Devices*.



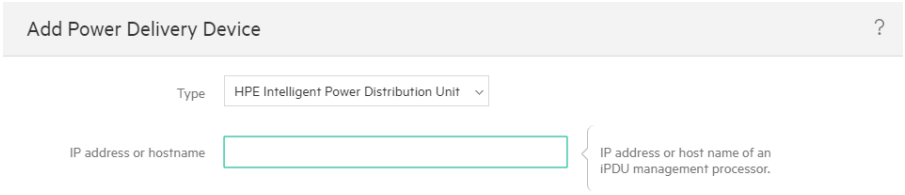
2. To add HPE iPDU's that power your previously discovered equipment, select *+ Add power delivery device*.



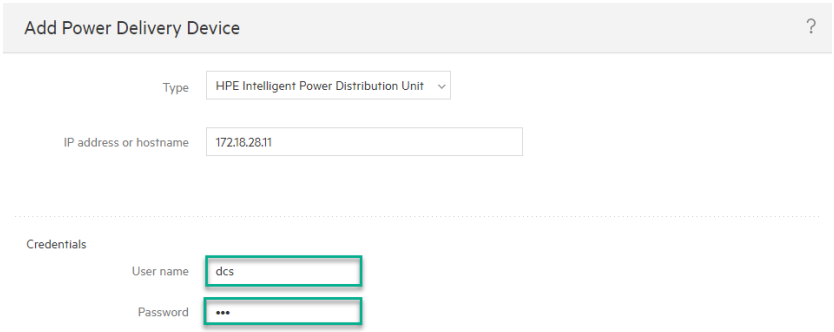
3. Select the type of PDU from the dropdown list



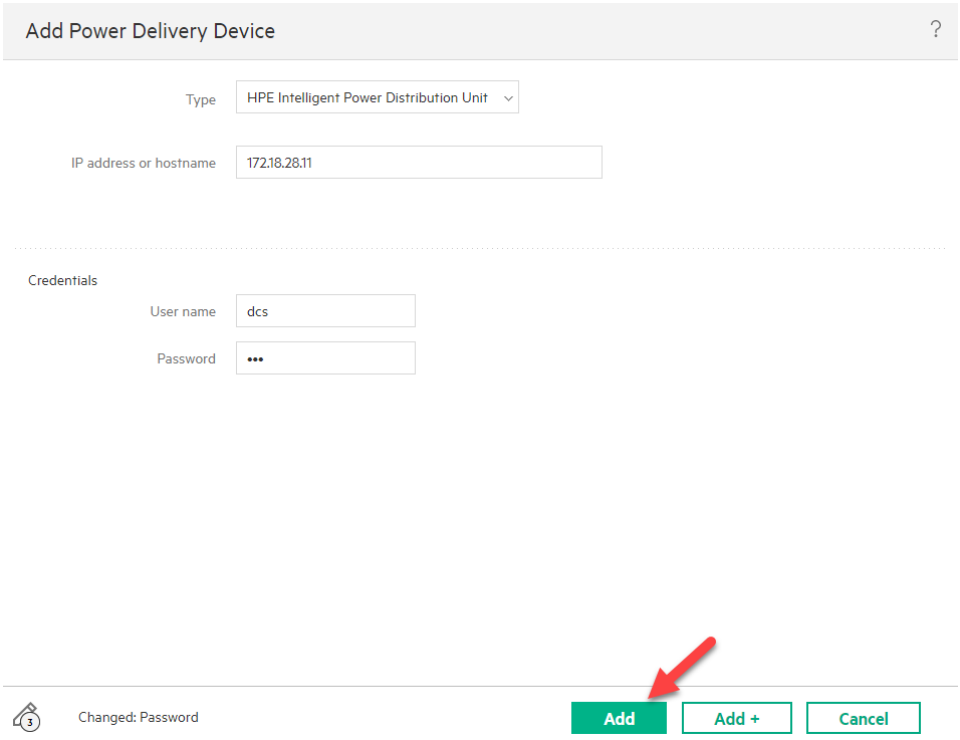
4. Enter the *FQDN or IP address* of the iPDU to be imported



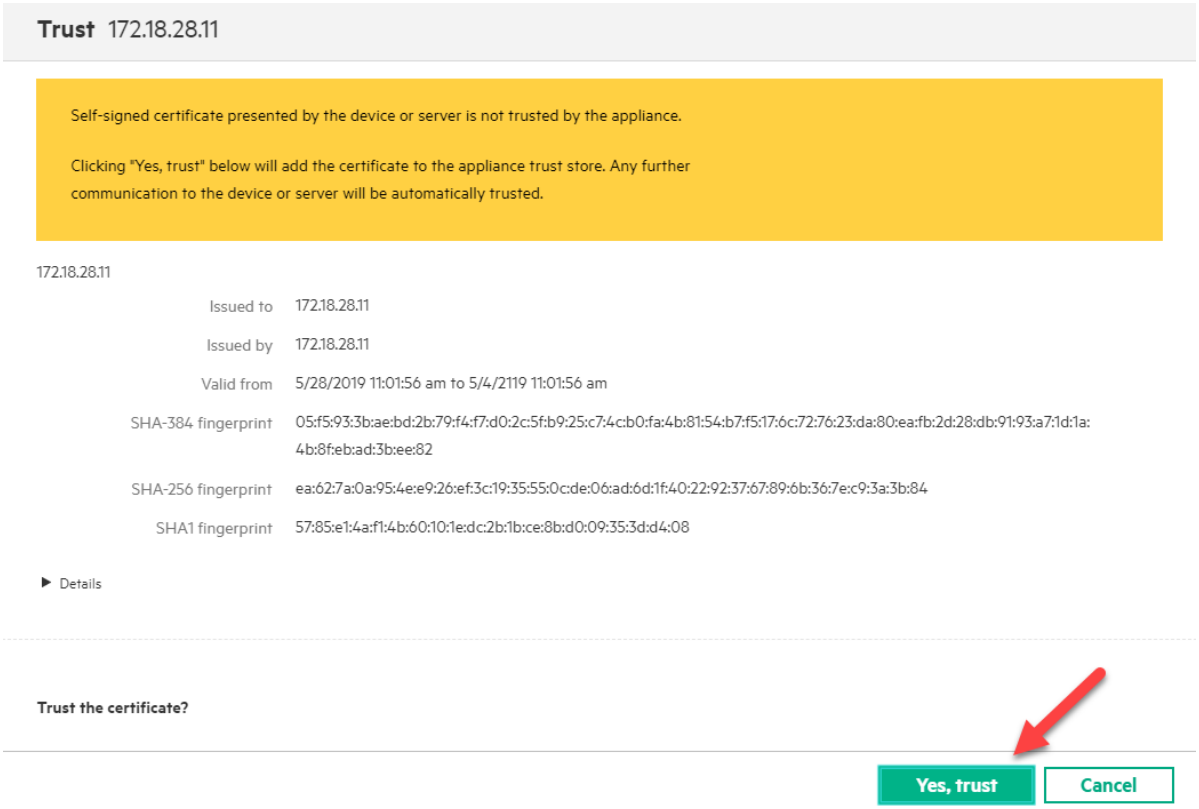
5. Enter the *Credentials* for the iPDU.



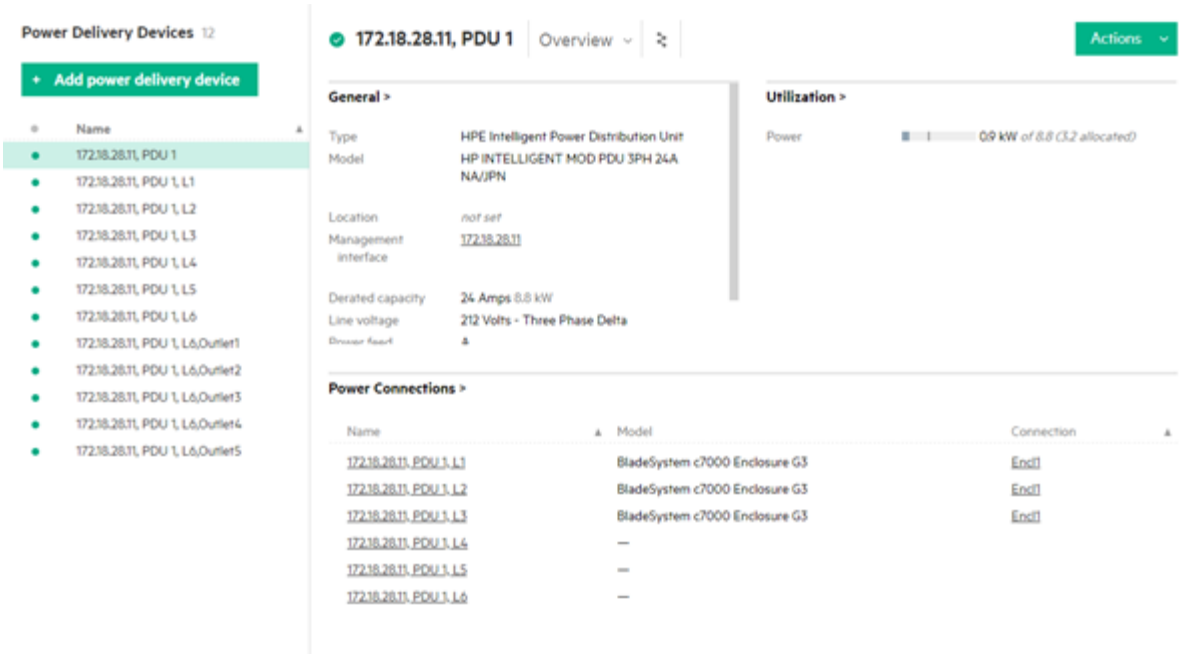
6. Click *Add or Add+* to import the iPDU



7. Click *Yes, trust* regarding the server certificate for the iPDU



Note: *The import process will take a few minutes as it discovers the iPDU with all extension bars attached to it. It will also discover any other HPE equipment that is attached to the iPDU and extension bars.*

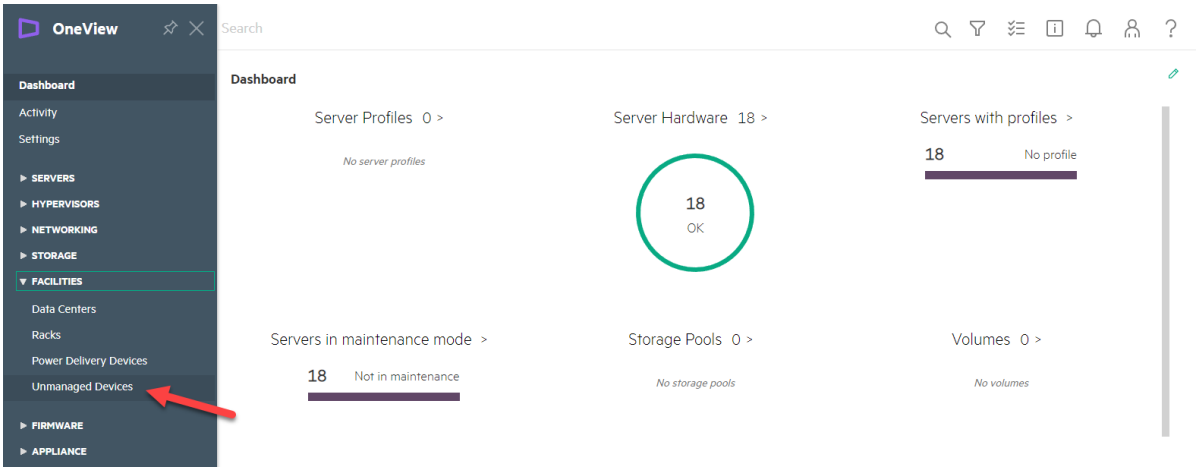


Note: *After importing the iPDU it is recommended that you edit the rack associated with the iPDU to set the iPDU core position properly. This is accomplished by dragging the iPDU to the upper or lower 0U space drop zones on the A / B side of the rack as appropriate. Or specify the position via the device configuration popup accessible via the gear icon on the device.*

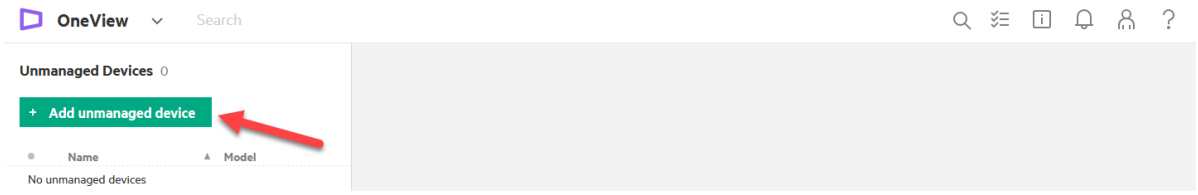
Adding Unmanaged Devices

Unmanaged devices can be created for any devices that cannot be discovered by HPE OneView that consume power or slots in the rack.

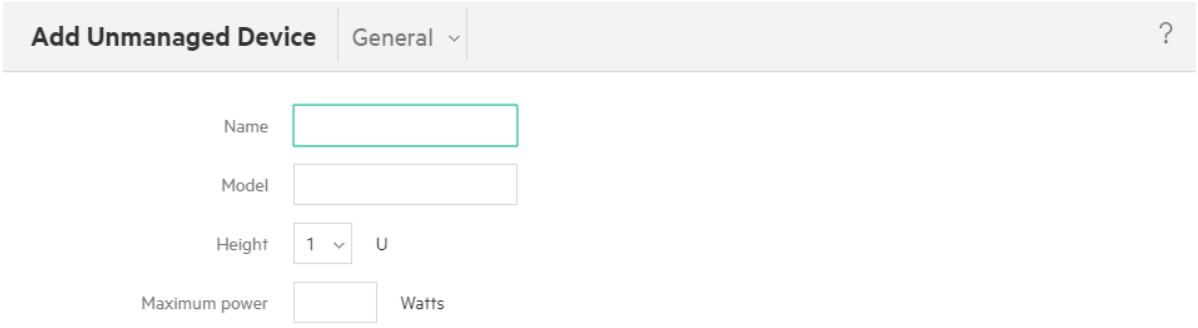
1. From the Top-Level Menu, expand the *FACILITIES* option and then select *Unmanaged Devices*.



2. Once on the Unmanaged Devices screen, select the *+Add unmanaged device* button.



3. Enter the specified information to represent the unmanaged device. Specify the maximum power value for the device to enable capacity and consumption analysis of your power delivery system. Once all information is completed, click the *Add* or *Add+* button.



4. The device can then be added to any rack layout and associated with any power delivery device.

Securing the Appliance



- Create Local User Accounts
- (Optional) Configure Active Directory or OpenLDAP
- (Optional) Configure Directory Groups
- (Optional) Configure Two-Factor Authentication

HPE OneView supports Role-based Access to the appliance with either local User Accounts, or it can be integrated with Microsoft Active Directory or other LDAP directories, such as OpenLDAP. HPE OneView also supports Scope Based Access Control. This section will cover how to create local user accounts, as well as optional configurations such as Active Directory authentication within the appliance or Two Factor Authentication.

(Optional) Integrating Active Directory / LDAP Security

You will need the following prior to configuring Active Directory settings within the appliance:

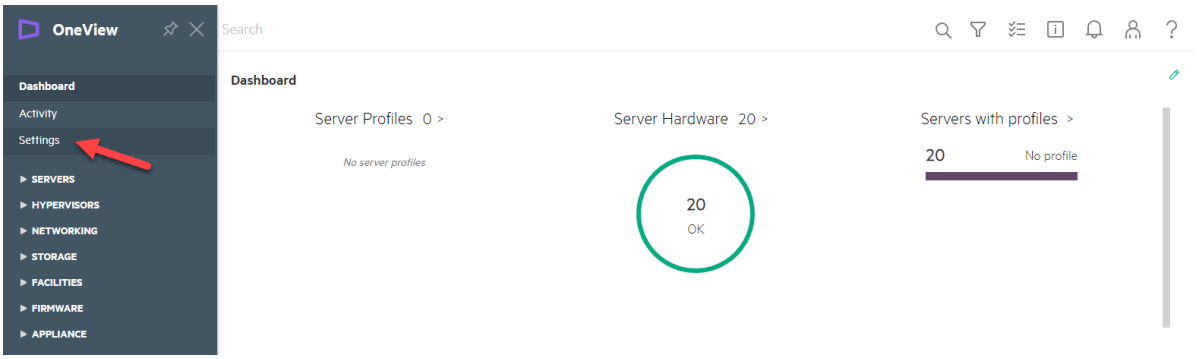
Active Directory or OpenLDAP Checklist

Table 13. Active Directory or OpenLDAP Checklist

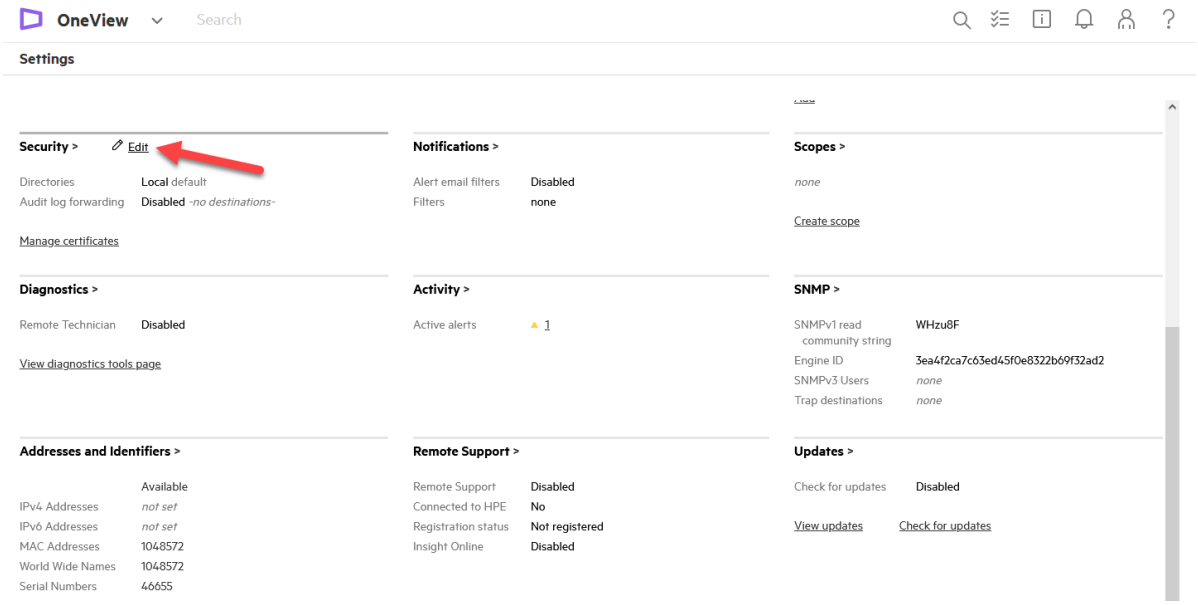
Task	Completed? (Y|N)
SSL certificates installed on your Domain Controllers	
FQDN of available Domain Controllers or LDAP Servers	
Domain Security Groups for Server Admins (will map to *Specialized Server Administrator* role)	
Network Admins (map to *Specialized Network Administrator* role)	
Infrastructure Admins (map to *Full Administrator* role.)	
Read-Only Users	

(Optional) Integrating with Active Directory / OpenLDAP

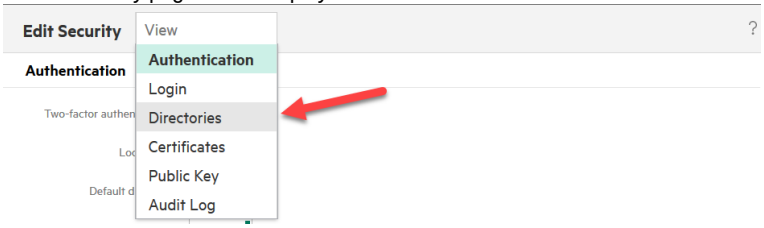
1. From the Top-Level Menu, select *Settings*.



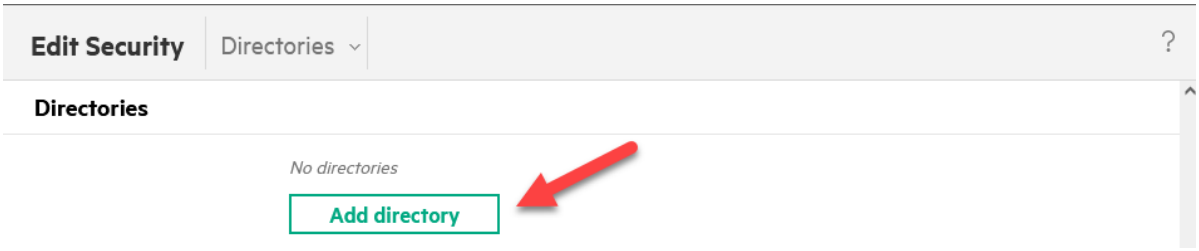
2. Select *Security* by clicking on *Edit*



3. The Security page will be displayed. Click on *View* and select *Directories*



4. Select *Add directory*



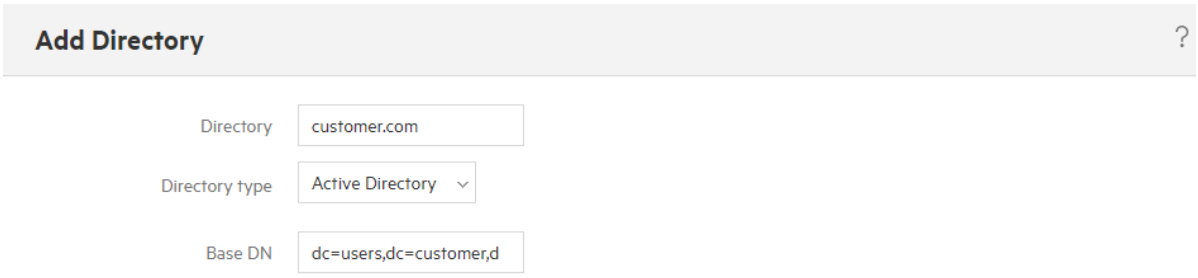
5. In the *Add directory* window, you will need to specify the following:

- Directory Name
- Directory Type
- Base DN
- Click the *Add directory server* button to add your Domain Controller FQDN and Base-64 Public Key Certificate used for Server Authentication.
- The Username and Password fields are to validate the Directory configuration. A valid user account must exist.

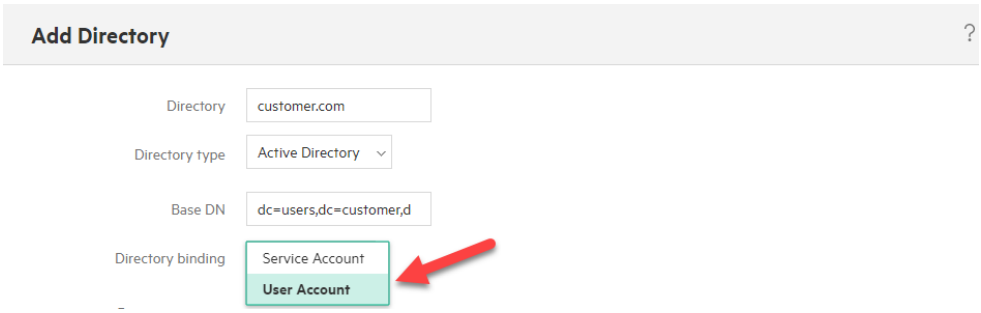
Note:

If the Active Directory Server Service configured in HPE OneView has a user lock-out policy (defined, for example, on "n" number of successive failed login attempts), Hewlett Packard Enterprise recommends that you use the email or the domain\user name format to log into HPE OneView. If email or domain\user name format is not used (instead, just the user name is used, even if you chose the correct directory on the login page), HPE OneView internally tries different login formats. This may result in locking out the user from the GUI on a single failed login attempt (e.g. wrong password). To minimize login attempts, configure the directory display name to be the same as the first component of the directories fully qualified domain name. For example, assign the HPE OneView name customer *for the directory* customer.com.

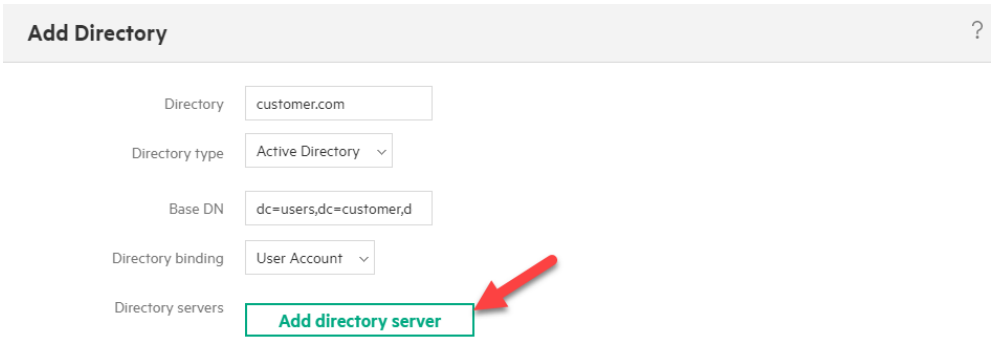
6. Enter the directory information



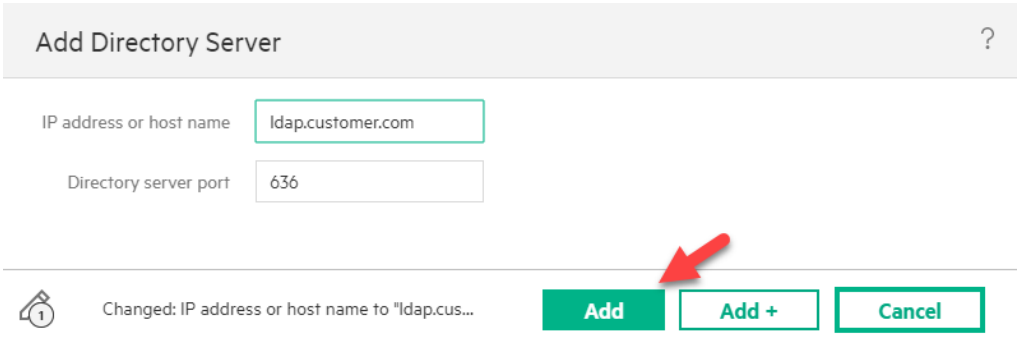
7. Select the *Directory binding* that will be used



8. Click *Add directory server*

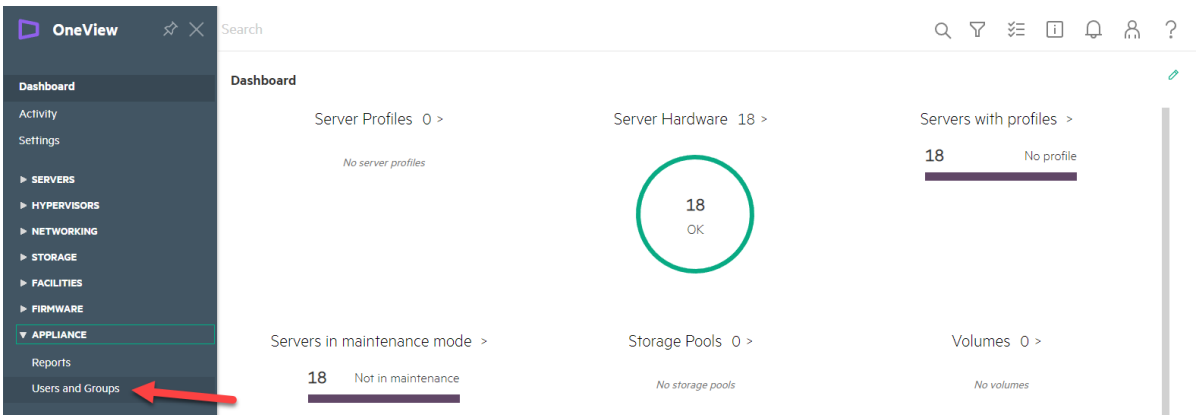


9. Enter the IP address or host name and server port for the Directory server and click *Add*

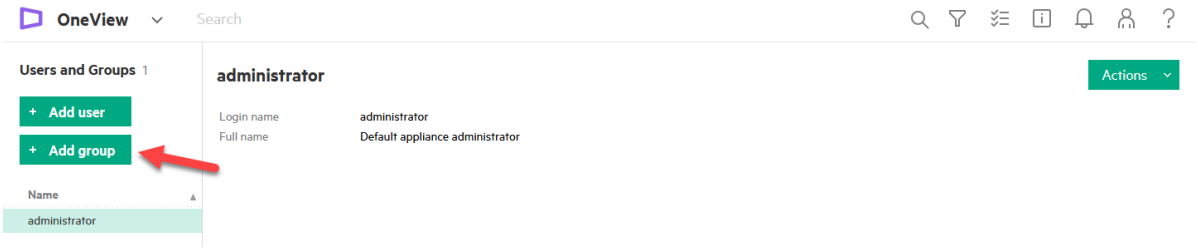


Note: *Depending on whether the correct certificate is installed in your OneView Appliance you may get a message about having to accept the certificate from the Active Directory server.*

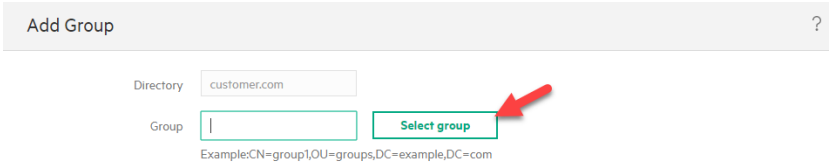
10. From the Top-Level Menu, expand the *APPLIANCE* option and then select *Users and Groups*.



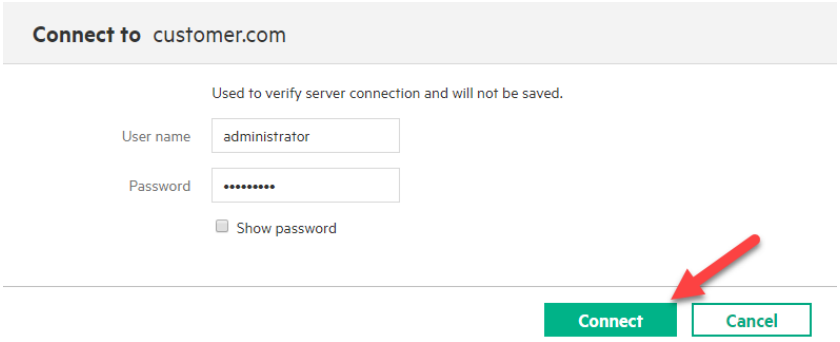
11. In the Users and Groups view, select the *Actions* menu and choose *Add group*



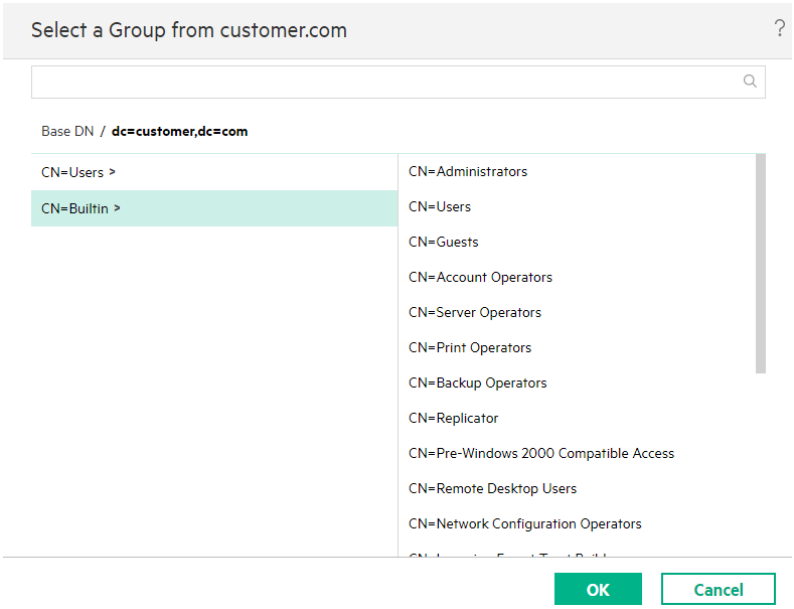
12. Select the *Select group* button



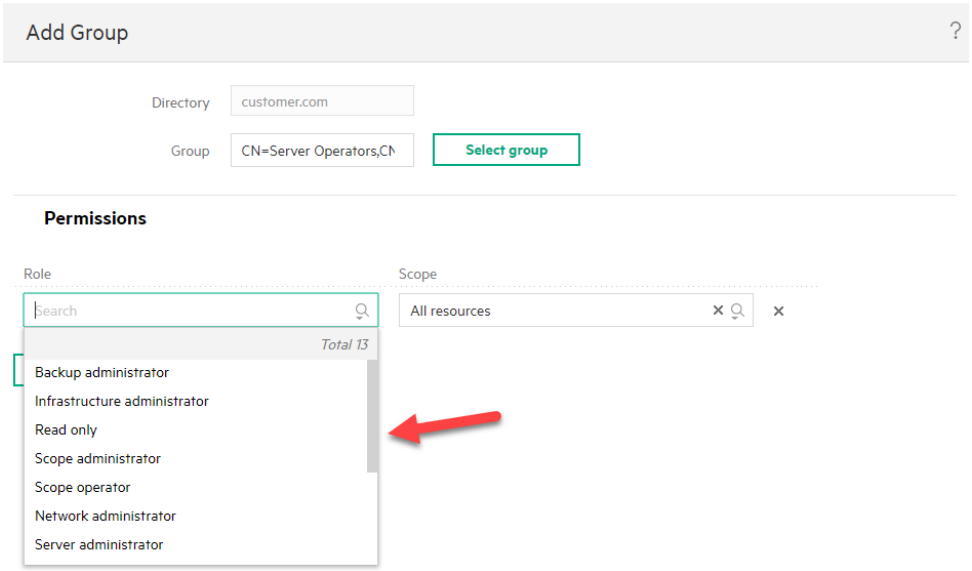
13. Provide the credentials to authenticate and click *Connect*.



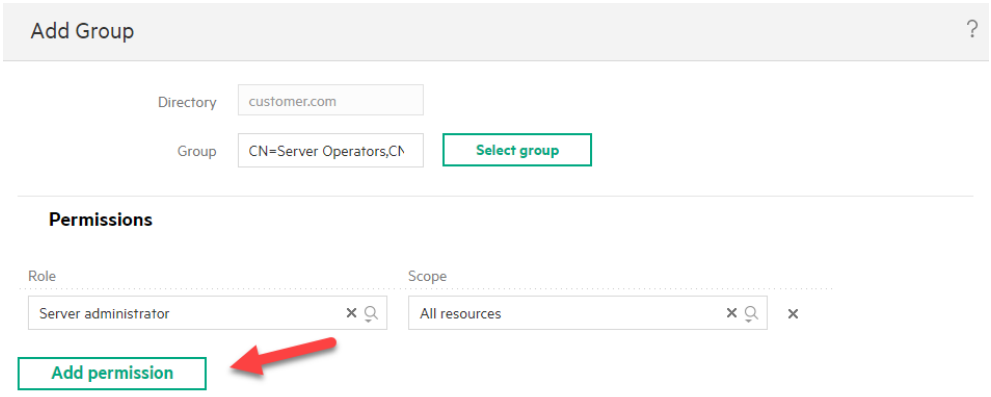
14. Once authenticated, select a group from the groups dialog window and click *OK*.



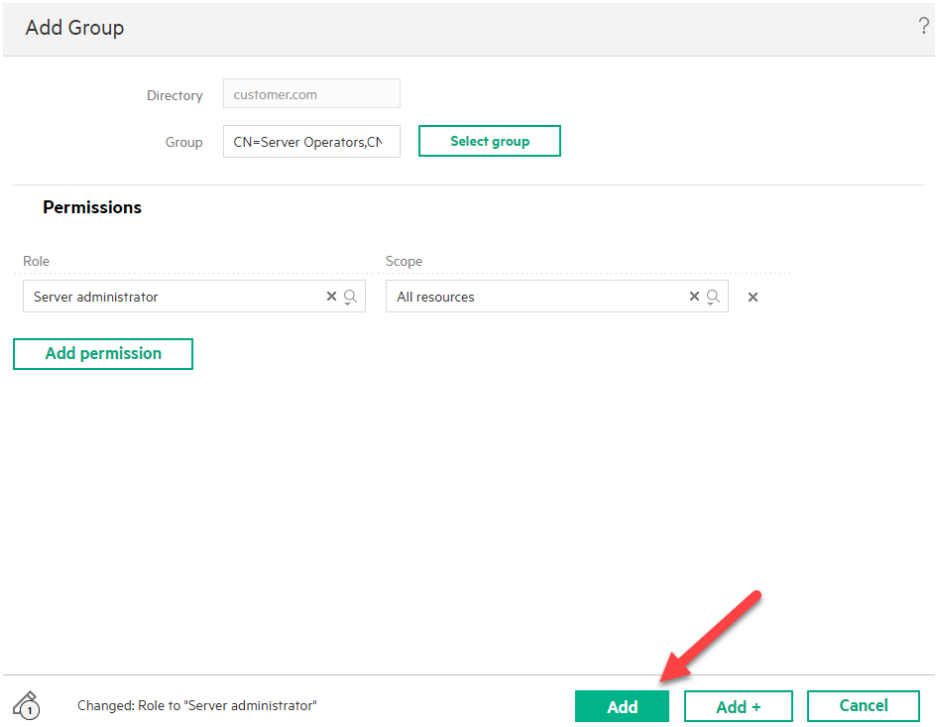
15. Assign the role that is needed for that directory group



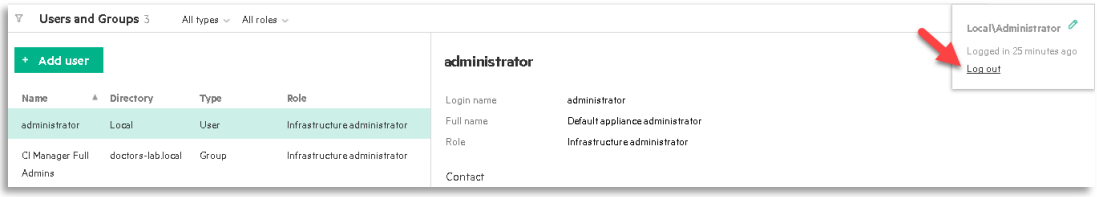
16. If the Group needs more than one permission then click on the *Add permission* to add additional permissions



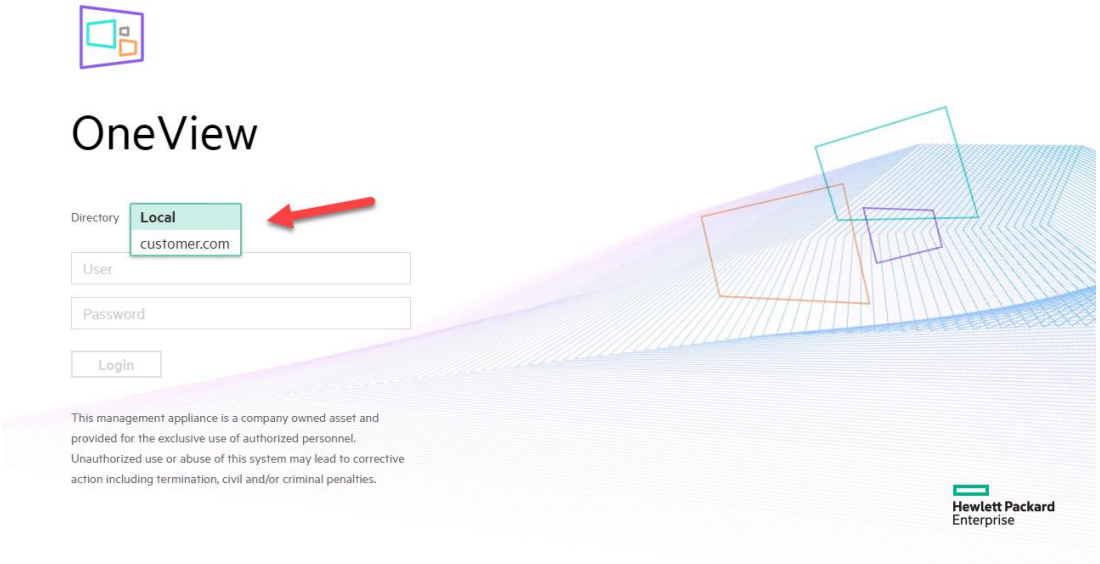
17. Click *Add* to close the Add Group Dialog window



18. Repeat the same steps to add any other *Directory Groups*.
19. After you have configured your Directory Groups, you should log out by clicking the User button in the upper right of the UI and select *Logout*.



20. On the logon page, you will notice a new field to choose. This is the Directory chooser. You can select from the configured Directories and Local (if Local was not disabled in your Directory configuration.) Verify that you have setup the various groups correctly by logging in with different users and ensure the permissions are set correctly.

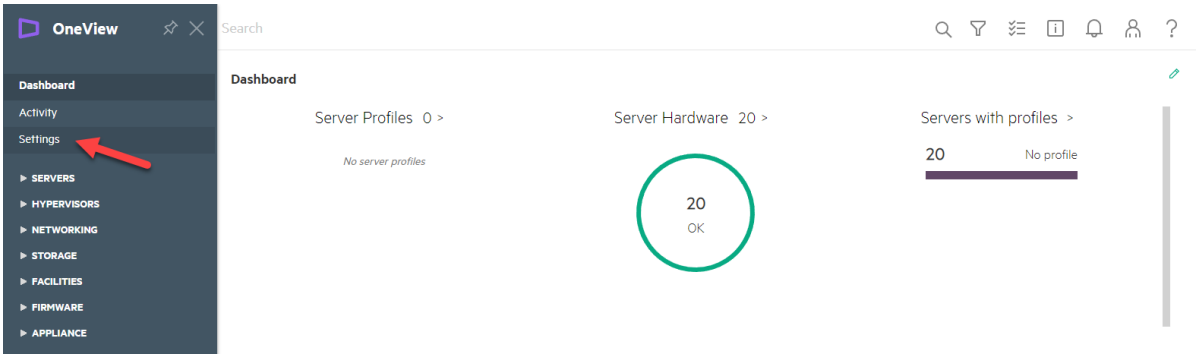


(Optional) Integrating with Two-Factor Authentication

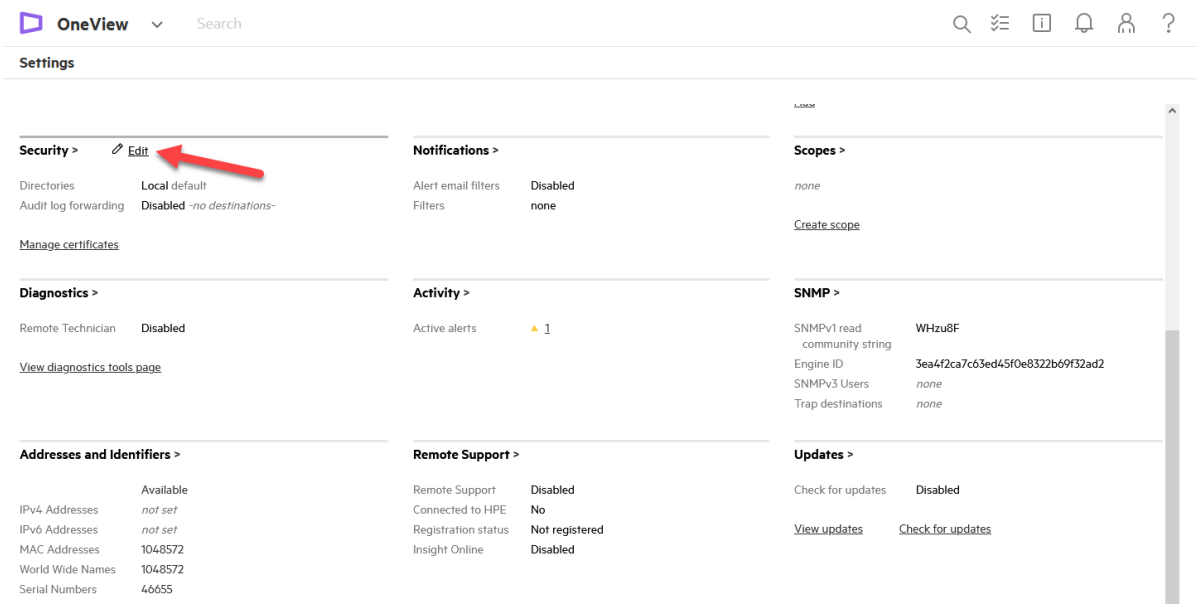
Enabling two-factor authentication allows you to use smart cards — for example, Common Access Cards (CAC), or Personal Identity Verification (PIV) cards — to authenticate within HPE OneView. The smart card reader plugin in the browser reads the smart card and accesses the certificate in the card using the PIN specified by the user. The client certificate embedded in the smart card is presented to HPE OneView by the browser. The client certificate must be signed by a root or intermediate Certificate Authority (CA) that has been previously imported into HPE OneView. The appliance authenticates the client certificate to validate that the user name specified in the certificate is that of a valid user recognized by the directory server configuration in HPE OneView.

Active Directory or OpenLDAP is required for two-factor authentication

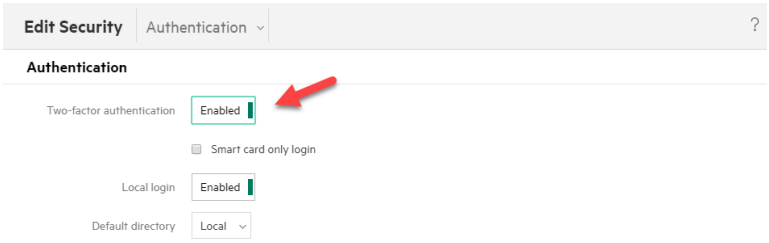
1. From the Top-Level Menu, select *Settings*.



2. Select *Security* and click on *Edit*

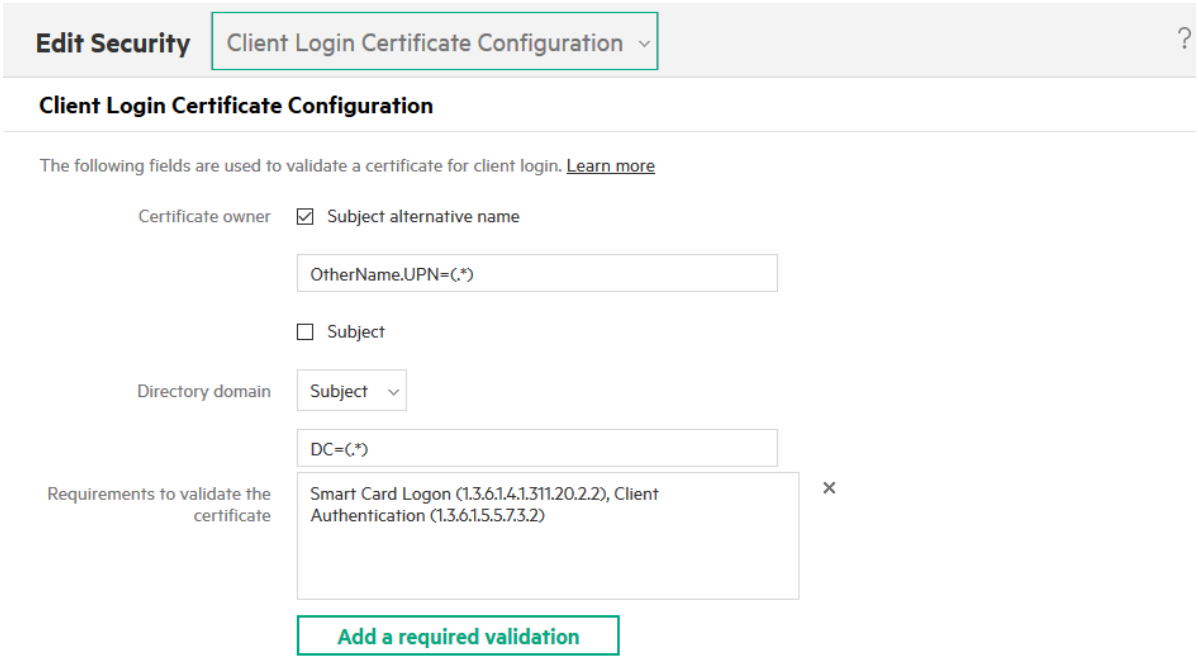


3. Enable Two-factor authentication



Note:

The certificates stored on CAC / PIV cards are X.509 security certificates. They contain fields of information used to identify the certificate owner, the certificate issuer, and other certificate identification elements. When you enable two-factor authentication, you can specify which certificate fields HPE OneView must use to validate a user in the "Client Login Certificate Configuration Screen", see below



Note:

Certificate owner, displays options to configure from where in the smart card certificate HPE OneView must extract the user name for querying the enterprise directories to validate the user.

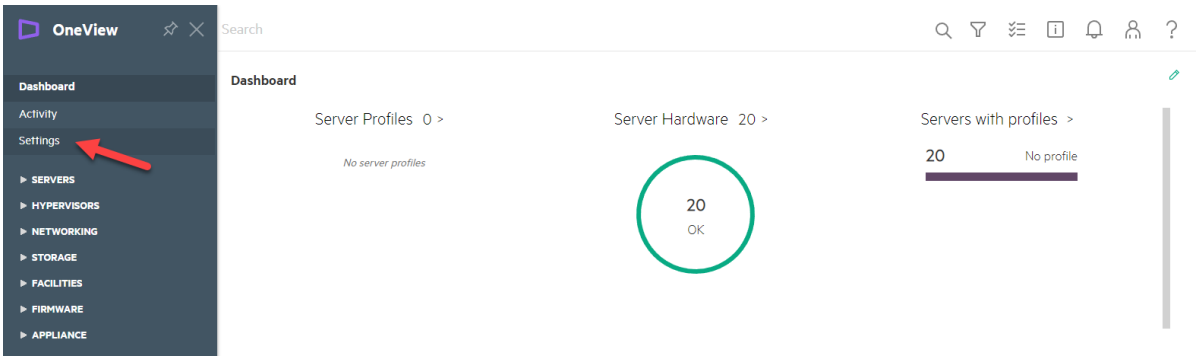
By default, HPE OneView uses the "Subject alternative name" field to retrieve the user name to query the enterprise directory. You can instruct HPE OneView to search attributes within the "Subject attributes" field in the certificate by selecting the "Subject" check box.

Directory domain, displays options to configure from where in the certificate HPE OneView must extract domain information for the user. HPE OneView uses the extracted domain information when querying the enterprise directory to authenticate the user. Directory domain provides details.

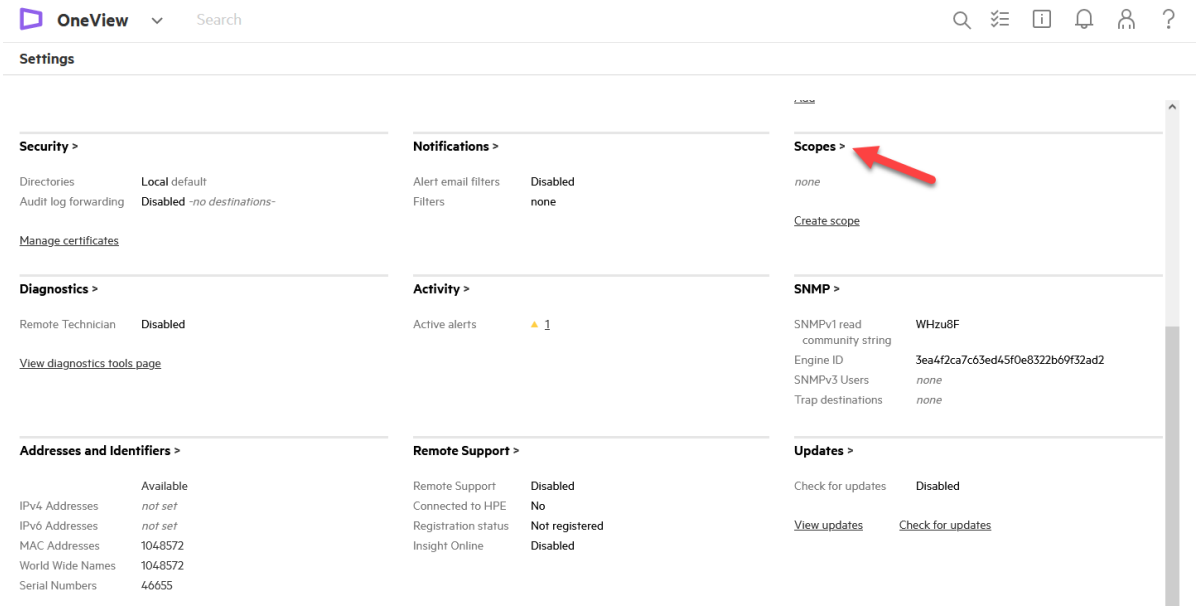
Requirements to validate the certificate allows you to specify the requirements to validate the certificate for key usage and policy identifiers for two-factor login.

Creating a Scope

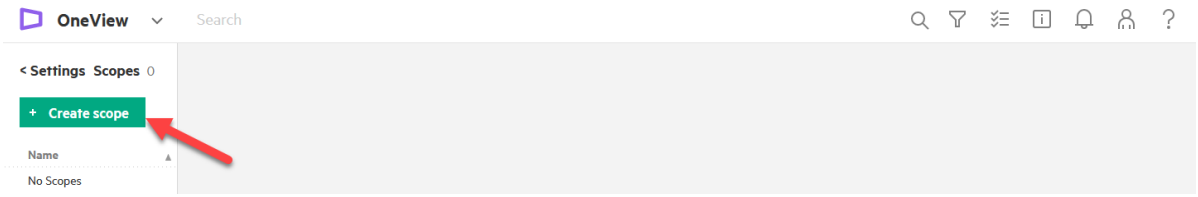
1. From the Top-Level Menu, select *Settings*.



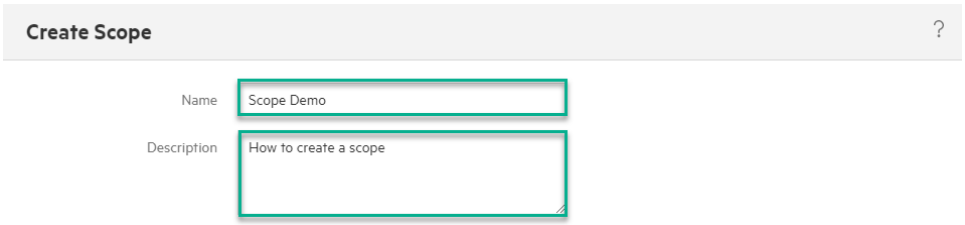
2. Select *Scopes*



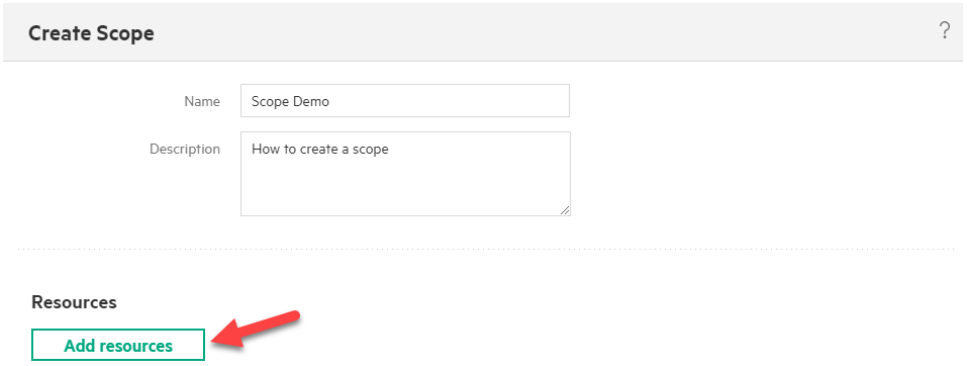
3. The Scopes page will be displayed. Select *Create scope*



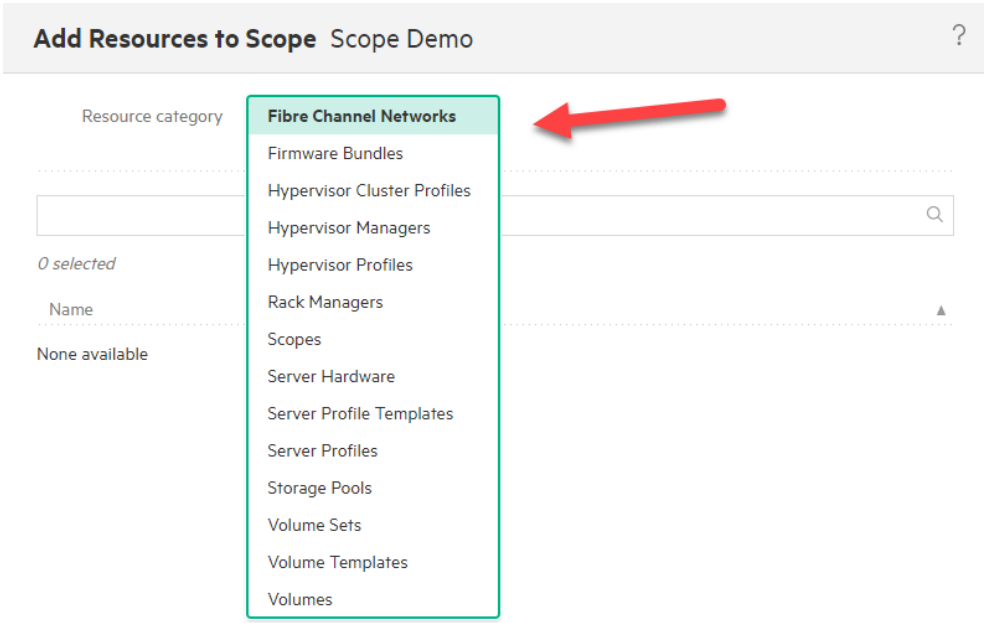
4. In the Create Scope dialog window add a *Name* and *Description* for the Scope



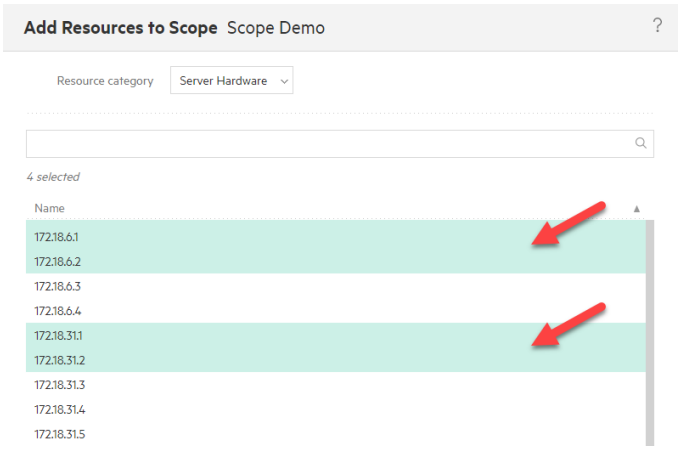
5. Click *Add resources*



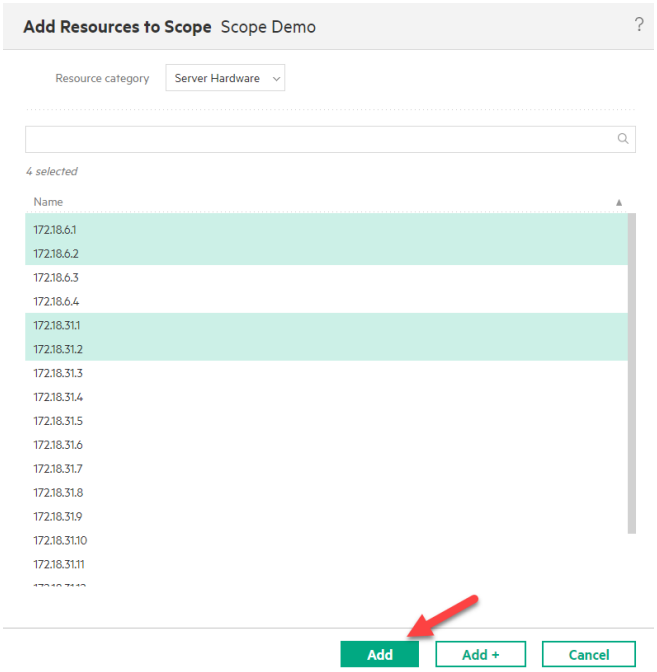
6. In the Add Resources to Scope dialog window, use the dropdown box to find the resources to be added to the scope (note that the following is from a OneView VM, Synergy has more Categories)



7. Select the resources to be added to the scope



8. Click *Add* or *Add+* to close the Add Resources to Scope dialog window



9. Click *Create* or *Create+* to create the scope

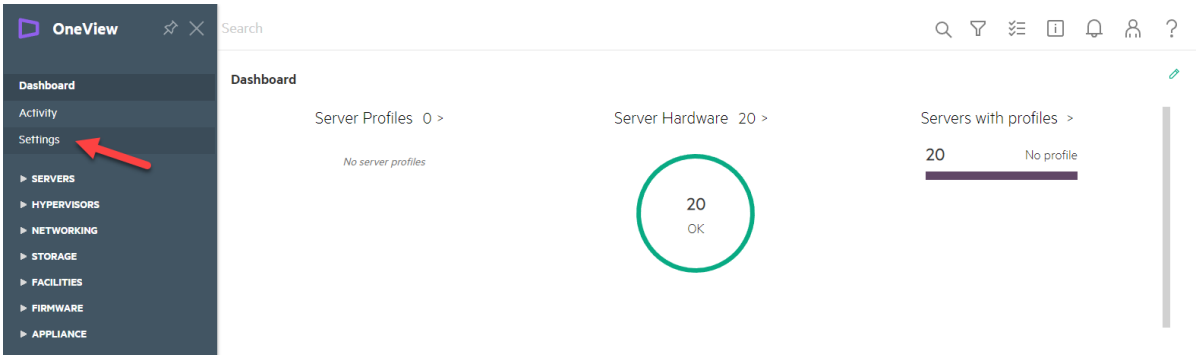
Maintaining Your Appliance

This section will guide you through the maintenance tasks you may encounter when using the HPE OneView appliance. It will cover maintaining user groups and accounts, alerts and monitoring as well as other tasks you may experience when using HPE OneView to manage your Composable Infrastructure.

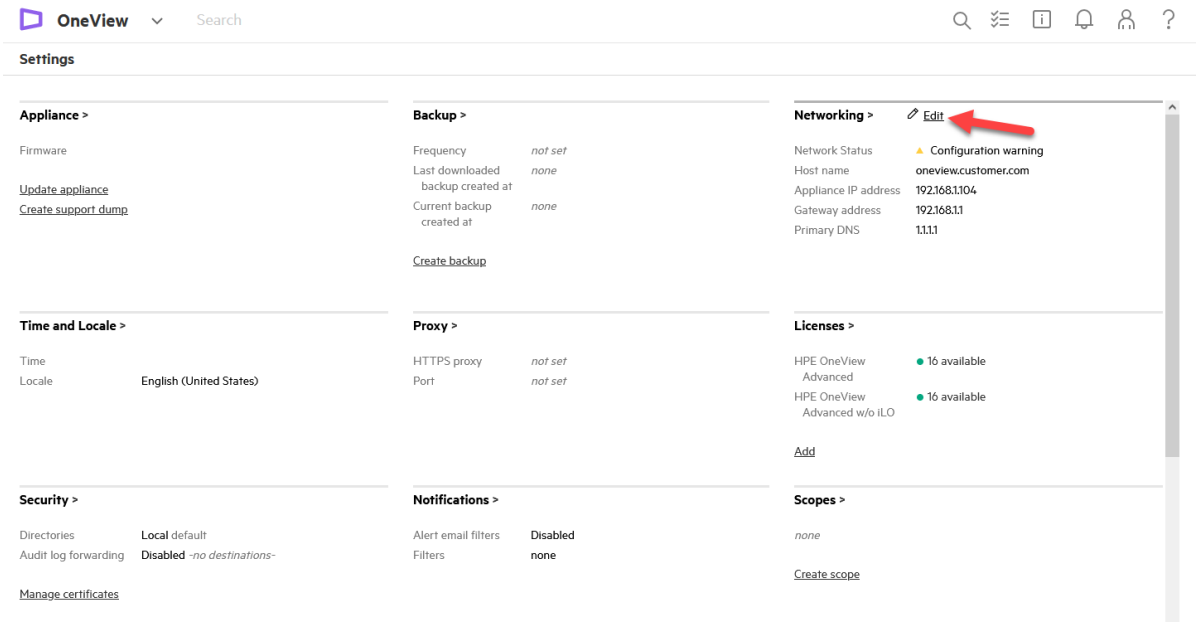
Changing the IP address of the HPE OneView Appliance

There may come a time when the IP address of the HPE OneView Appliance needs to be changed. Please follow these steps to ensure a smooth and easy transition for your Composable Infrastructure.

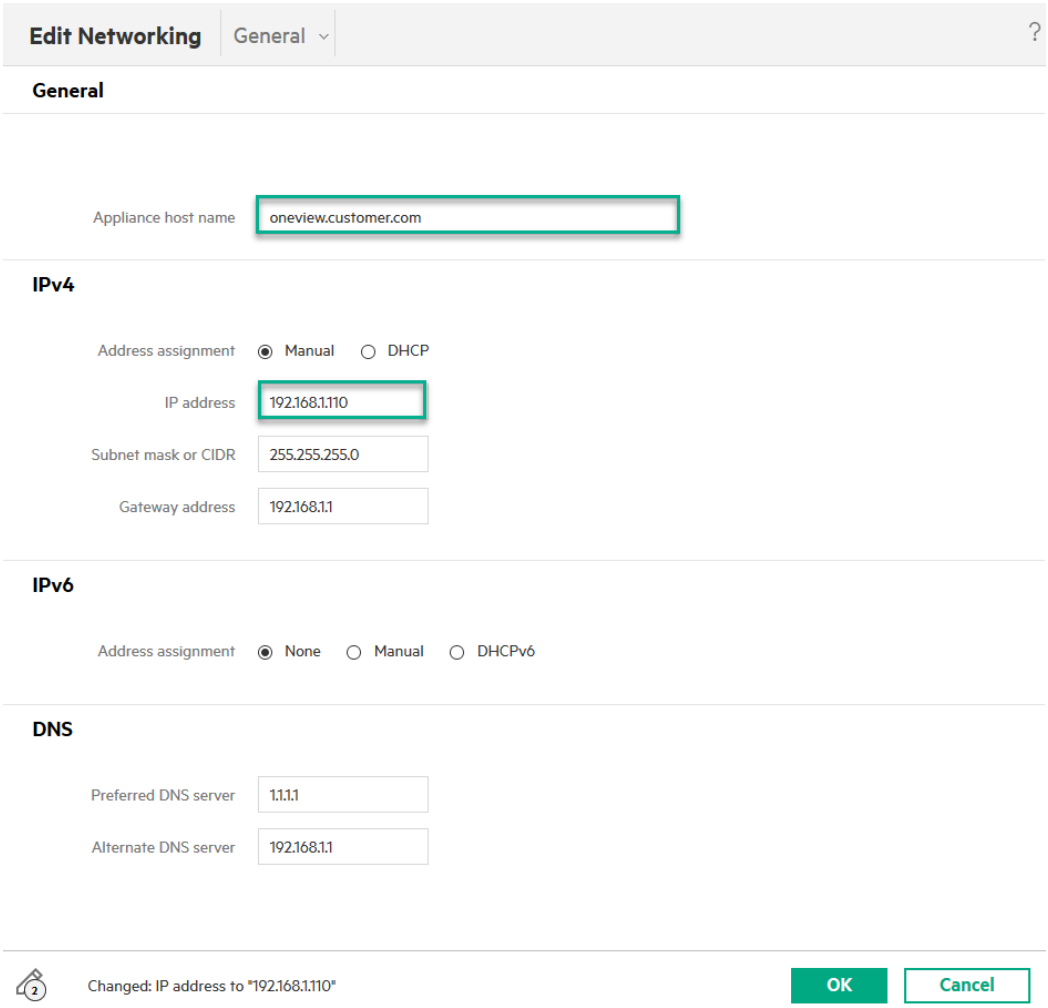
1. From the Top-Level Menu, select *Settings*.



2. On the settings page, select *Networking* and click on *Edit*



3. Enter the new *IP address or FQDN* (Appliance host name) for the HPE OneView Appliance.



4. Click *OK*.

Note:
After clicking OK, the appliance will be configured using the new parameters. If you selected Static for the IP Address Assignment, you should be redirected to the new IP address. As this change is being applied the HPE OneView appliance will push the changes to the managed resources (storage devices, enclosures, etc.)

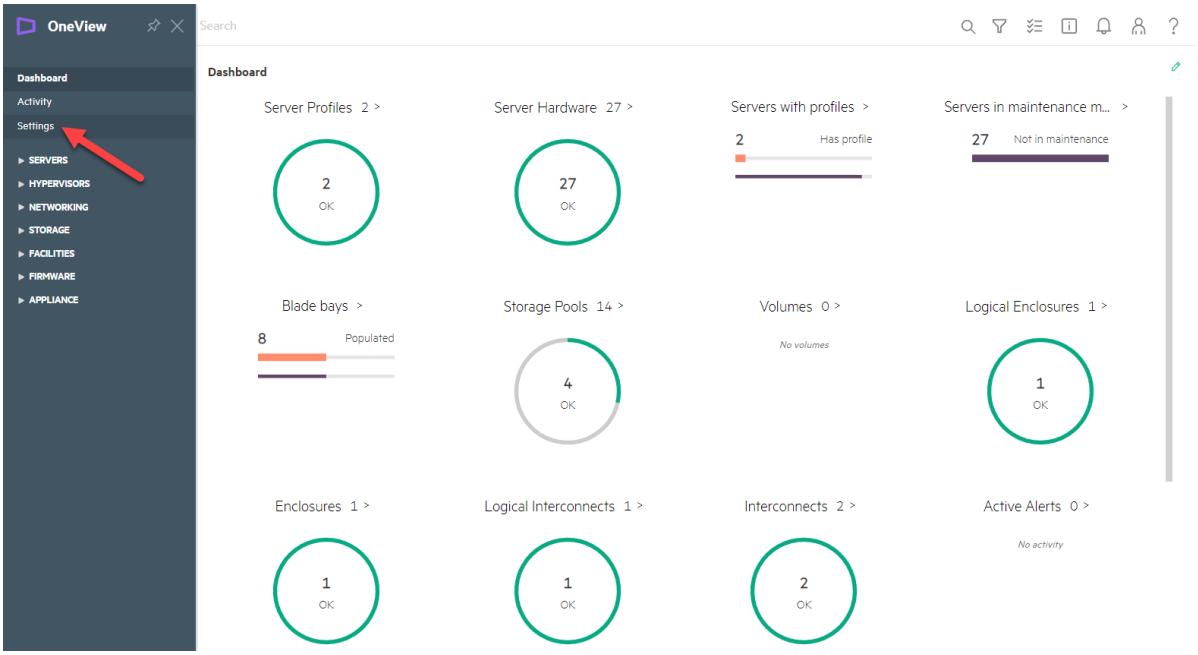
Upgrading the OneView Appliance / Synergy Composer

With the release of OneView 7.0, some older hardware is no longer supported. If the OneView Appliance is managing any of this older hardware, then you will need to migrate the supported server hardware to a new OneView 7.0 or later OneView Appliance. Migration of Servers from a HPE OneView 6.6 Appliance to HPE OneView 7.x / 8.x is covered elsewhere in this guide.

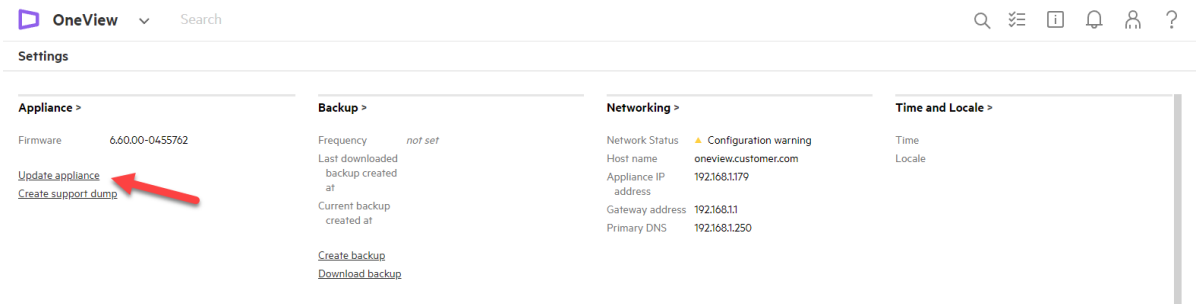
In the case of Synergy, the Original Synergy Composer 1 is no longer supported, and you will not be able to upgrade to HPE OneView 7.0 or later. You will need to upgrade the Synergy Composer 1's to Synergy Composer 2's. It is possible to do a backup of the Synergy Composer 1's and restore the backup to a new pair of HPE Synergy Composer 2's with exactly the same version of OneView installed on the HPE Synergy Composer 2's. We will not be covering how to do this in this document, for details please go to https://support.hpe.com.

Upgrading the HPE OneView Appliance

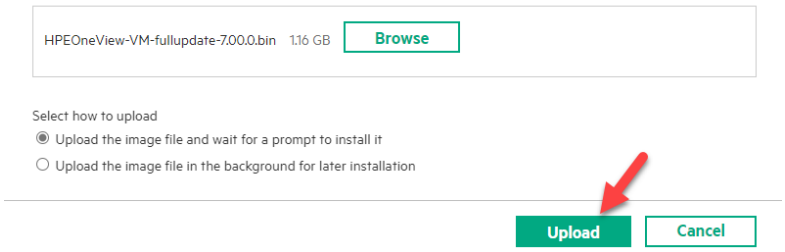
1. From the Top-Level Menu, select *Settings*.



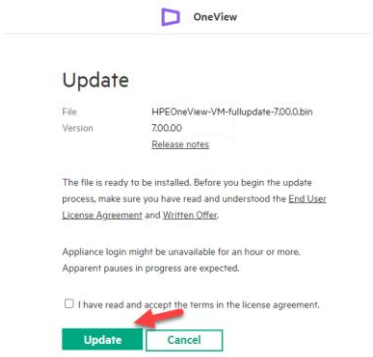
2. On the settings page, click on *Update appliance* in the Appliance section.



3. Ensure you have a recent backup of the as a best practice and then click on *Browse* in order to select an HPE OneView upgrade ".bin" file. Once selected you can click on *Upload* in order to upload the file to the HPE OneView Appliance.



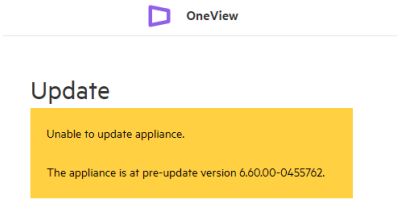
4. The upload of the update file will commence and once completed you can then start the upgrade process.



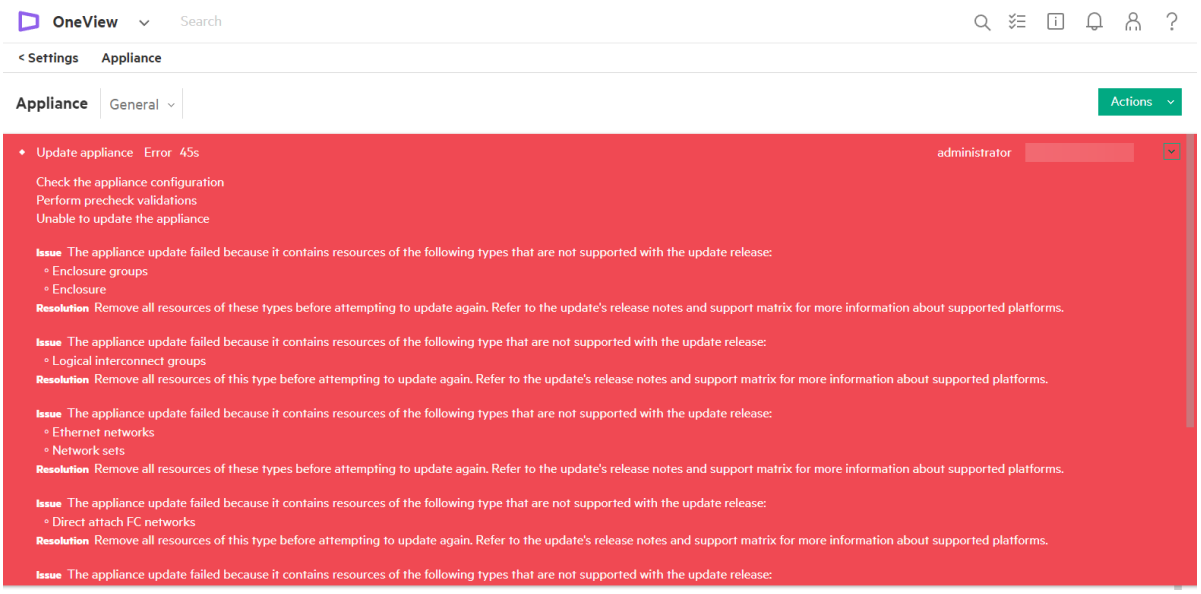
5. If your HPE OneView Appliance has any unsupported hardware then the update will fail. If there is no unsupported hardware in the HPE OneView Appliance then the upgrade will complete and the HPE OneView Appliance will reboot as part of the upgrade process.

   The following is an error from a failed upgrade of a HPE OneView Appliance because it is still managing c7000 Chassis. Any Apollo / ProLiant / Superdome Flex / Superdome Flex 280 Server need to be migrated to another HPE OneView 7.0 or later HPE OneView Appliance using the new Migrate feature that is available in the later versions. This will move the Server hardware and relevant HPE OneView license that each Server is using to the new HPE OneView Appliance.

   You will first see the following screen



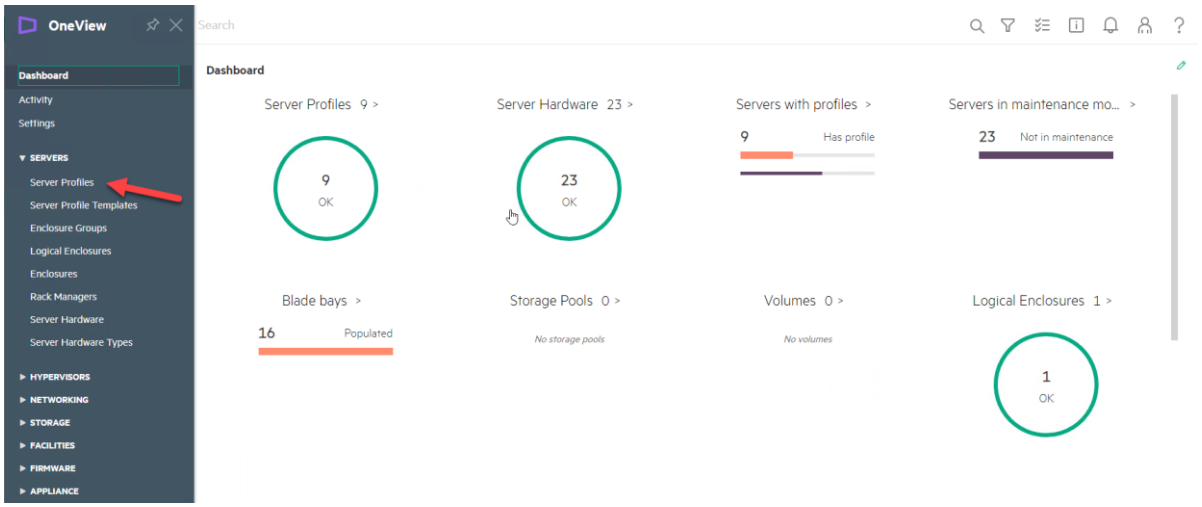
   When you click on the error that comes up and see the details the screen will show the hardware that is managed that is blocking the update from taking place. As mentioned previously you will either need to remove the old hardware or deploy a new HPE OneView 7.0 or later Appliance and use the Migrate feature in the Server profile section of the newly deployed HPE OneView Appliance.



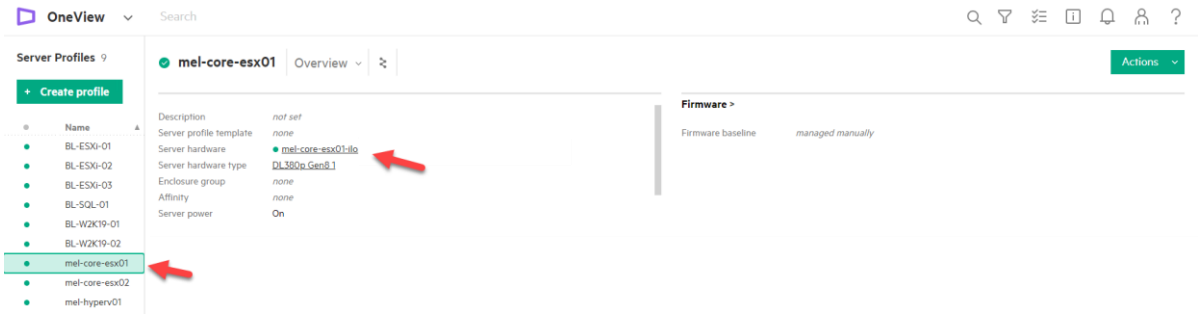
Migrating a Server from OneView 6.6 to OneView 7.0, 7.1, 7.2 or 8.0

With the release of OneView 7.0 or later there is hardware that is no longer supported by HPE OneView 7.0 or later. You can now migrate hardware that is still support out of an existing HPE OneView 6.6 Appliance to HPE OneView 7.0, 7.1, 7.2 or 8.0. This will allow you to migrate for example Rack Mount, Apollo or Superdome Flex / Superdome Flex 280 Servers to the new HPE OneView 7.0, 7.1, 7.2 or 8.0 Appliance without having to power off the Server. This process will also copy any SAN configuration to the new HPE OneView instance along with the OneView License that is managing the device. With OneView 8.1 or later you can only migrate hardware between the same versions ie 8.1->8.1 or 8.2->8.2 etc.

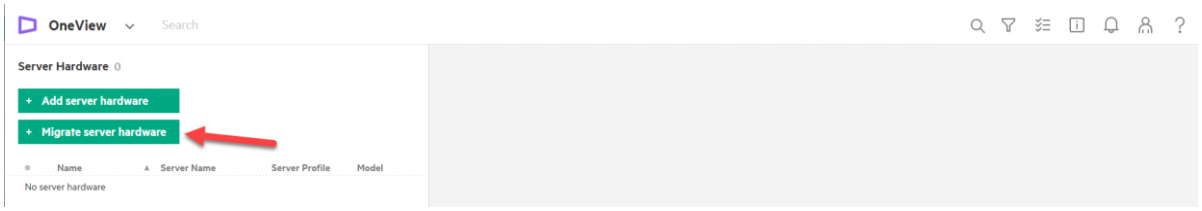
1. From the Top-Level Menu of the HPE OneView 6.6 Appliance, expand the *SERVERS* option and select *Server Profiles* to identify the Server Profile and Hardware that you wish to migrate.



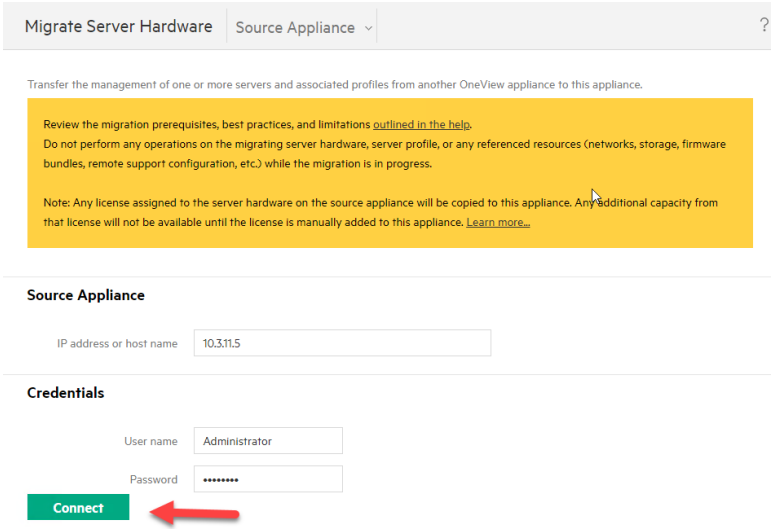
2. Select the Server hardware that you wish to migrate and note the Server hardware information (which is the iLO address) of the Server



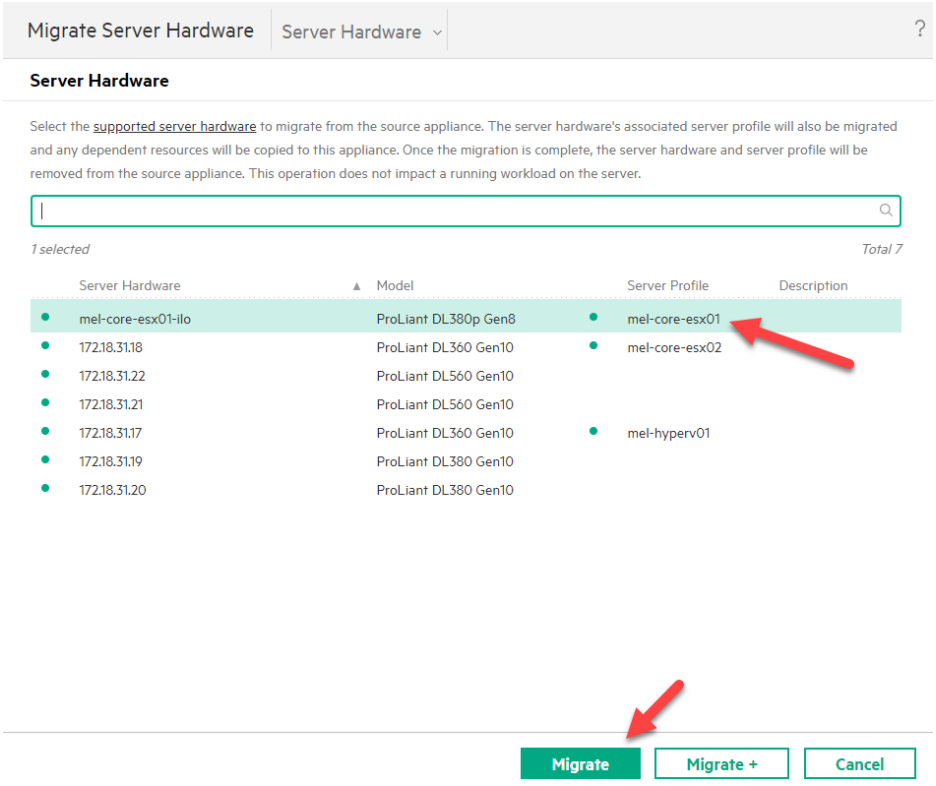
3. Now go to your new HPE OneView 7.0, 7.1, 7.2 or 8.0 Appliance into the Server Profiles and click on *Migrate server hardware*.



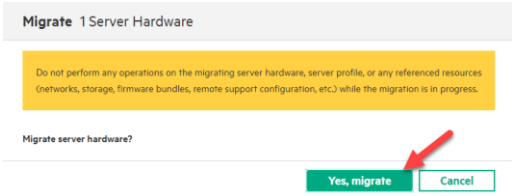
4. You enter the Source HPE OneView Appliance and relevant Administrator level credentials to login into it and click *Connect*.



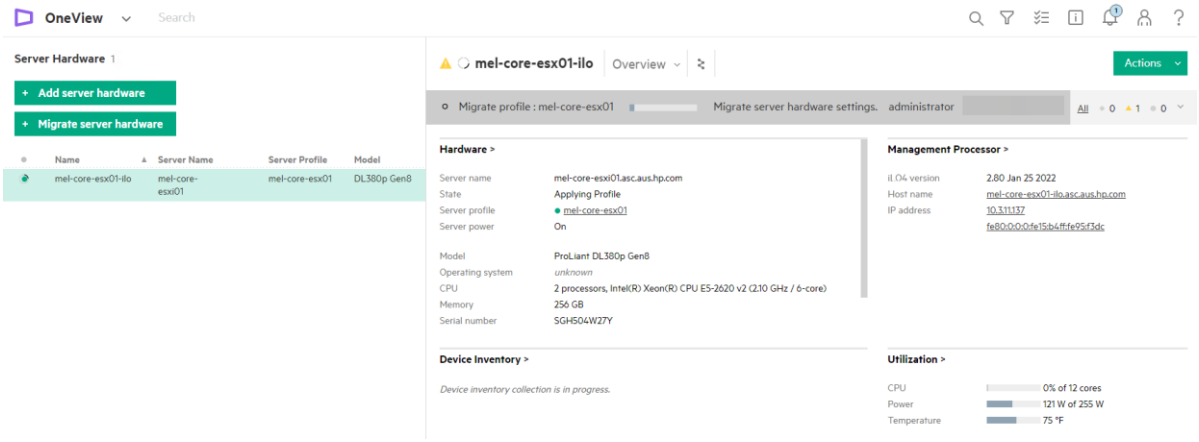
5. The supported Server hardware that is available to be migrated from the old HPE OneView 6.6 Appliance will be shown, select the Server hardware that you wish to be migrated and click on *Migrate*.



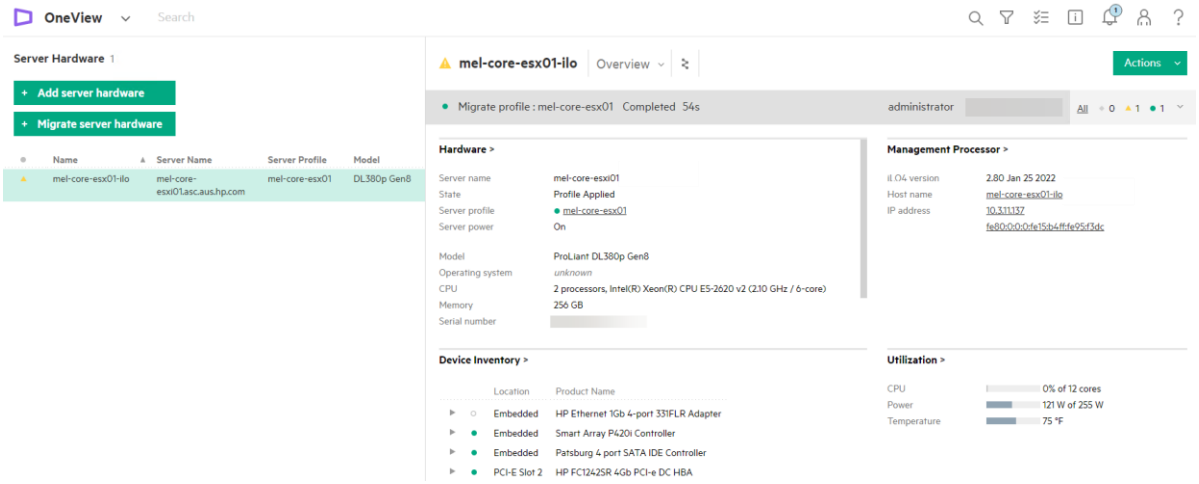
6. Ensure that no other changes occur with the Server Hardware or related items while it is being migrated and then click on *Yes, migrate*



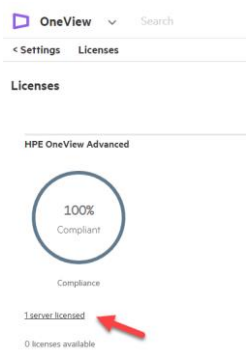
7. The Server hardware is now migrated over to the new HPE OneView 7.0 or later Appliance.



8. The Server is migrated and the Server Profile and HPE OneView License are brought over to the new HPE OneView Appliance.



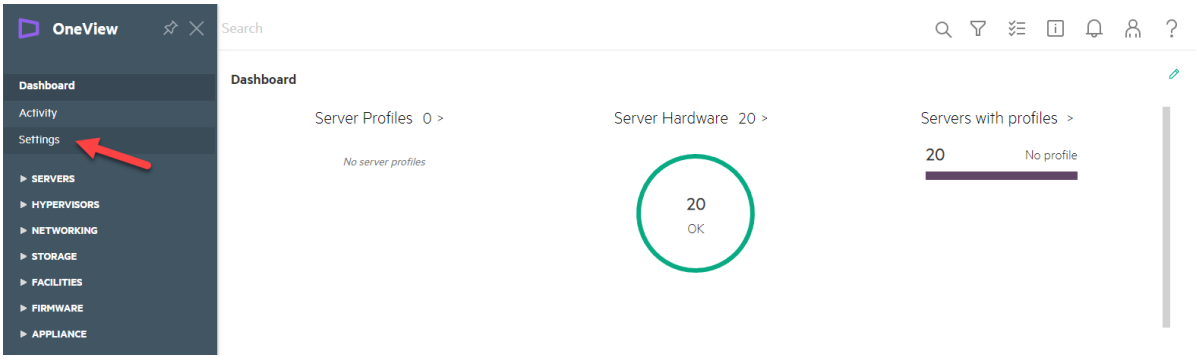
9. The HPE OneView License has been migrated from the old HPE OneView Applaince to the new Appliance



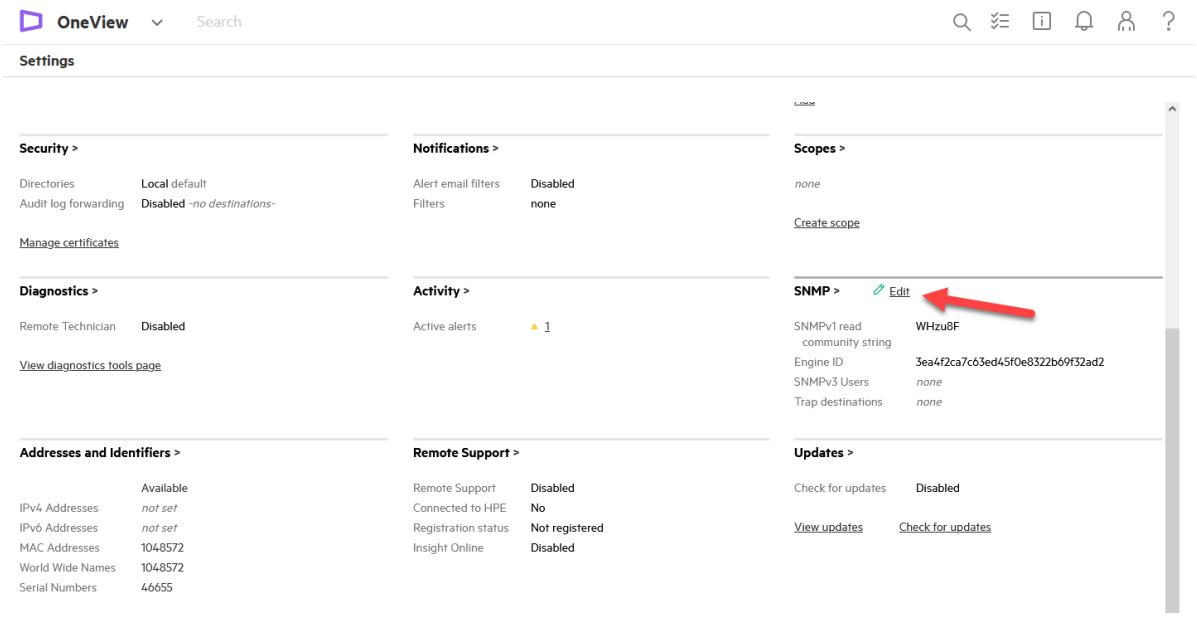
Changing the SNMP Read String of the HPE OneView Appliance

There may come a time when the SNMP Read string of the HPE OneView Appliance needs to be changed. Please follow these steps to ensure a smooth and easy transition for your Composable Infrastructure.

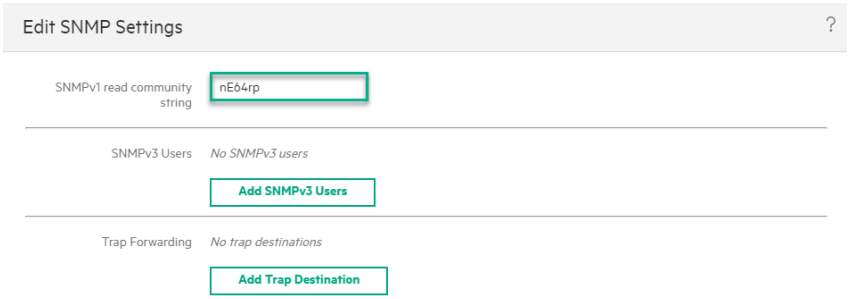
1. From the Top-Level Menu, select *Settings*.



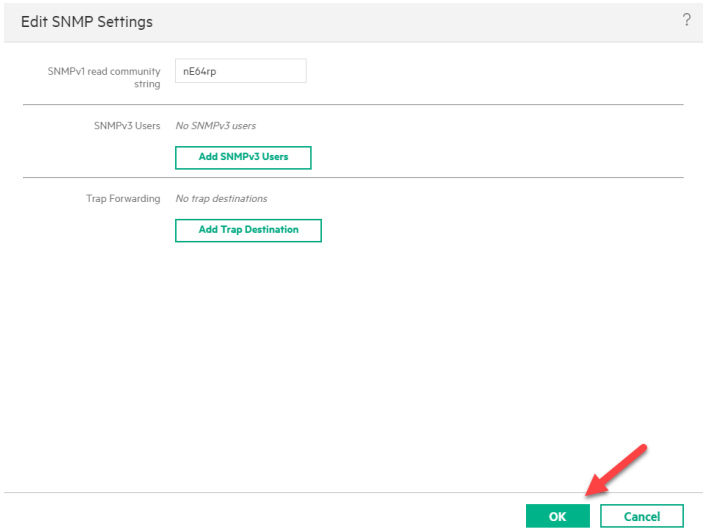
2. On the settings page, click on *Edit* in the SNMP section.



3. Enter the new *read community string*



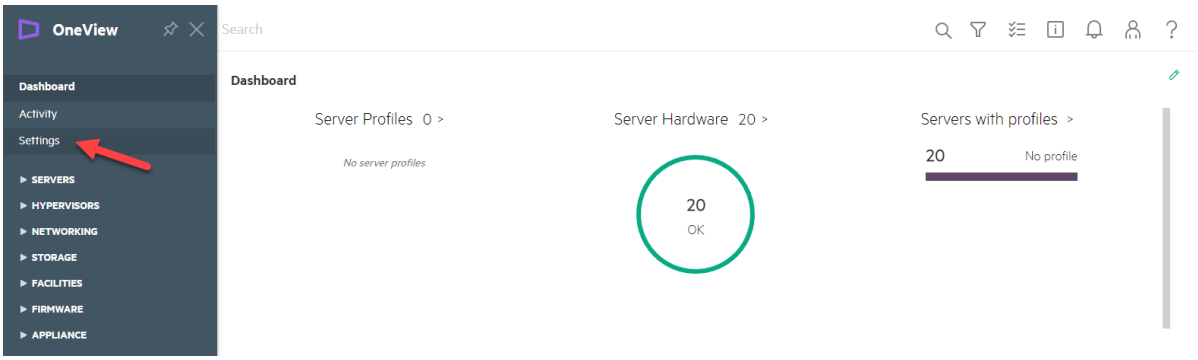
4. Click *OK* to close the Edit SNMP Settings dialog window.



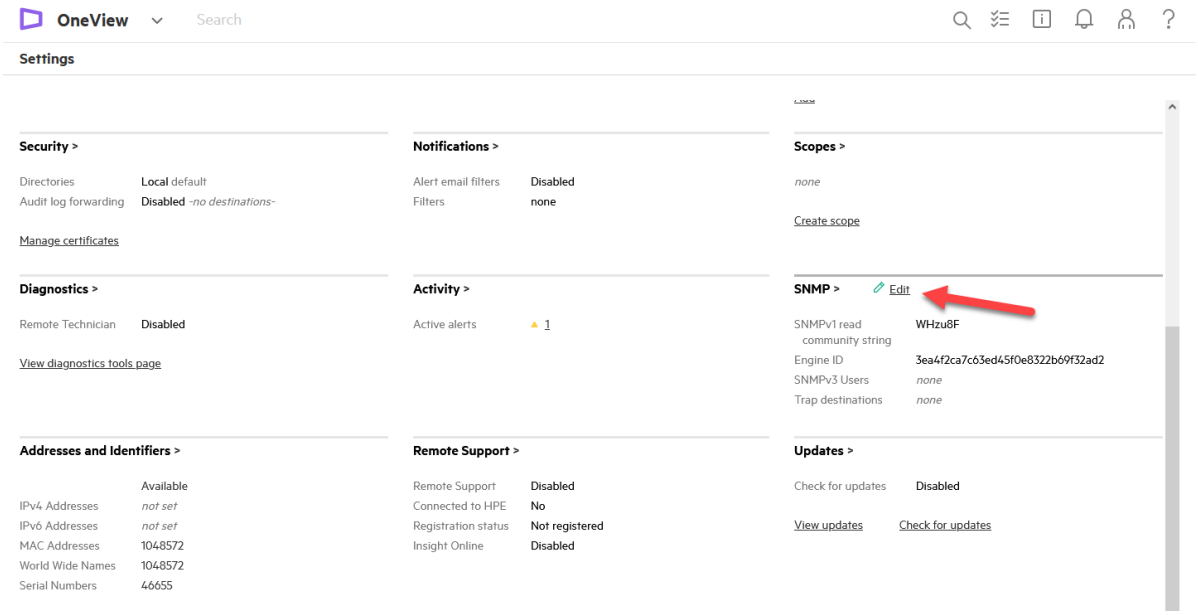
Note:
Changing the read string is recommended when running HPE System Insight Manager and HPE OneView in conjunction with each other.

Configuring SNMP v3

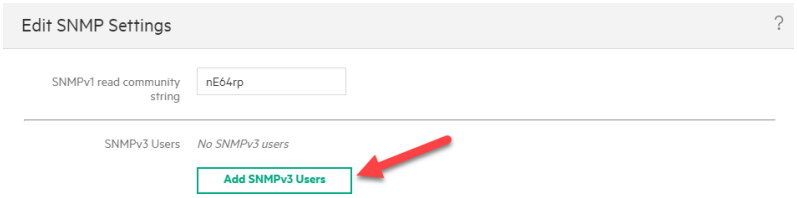
1. From the Top-Level Menu, select *Settings*.



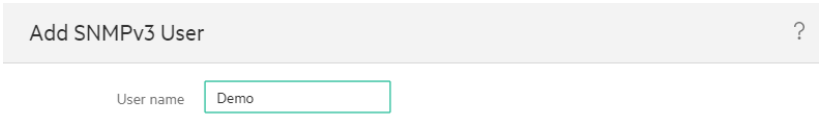
2. On the settings page, select *SNMP* and then click *Edit*.



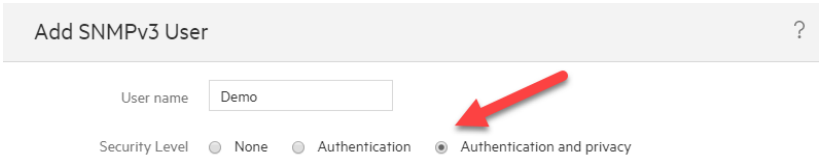
3. Click *Add SNMPv3 Users*



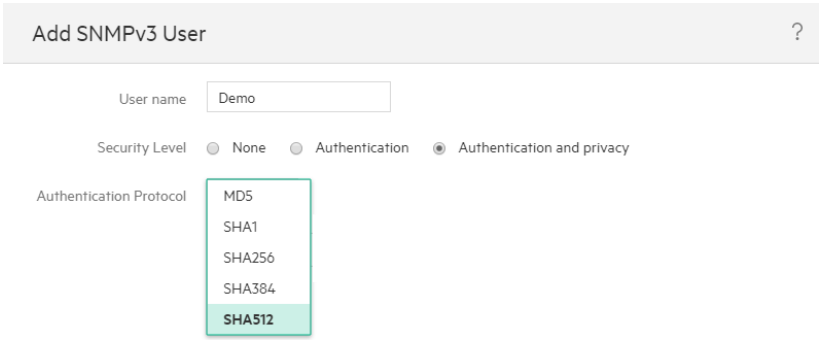
4. Enter the *User name* for the SNMPv3 User



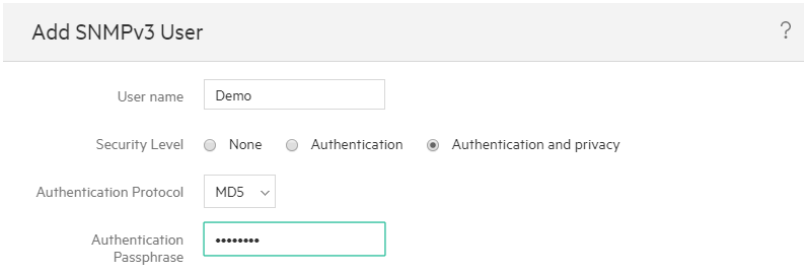
5. Select the appropriate *Security Level*



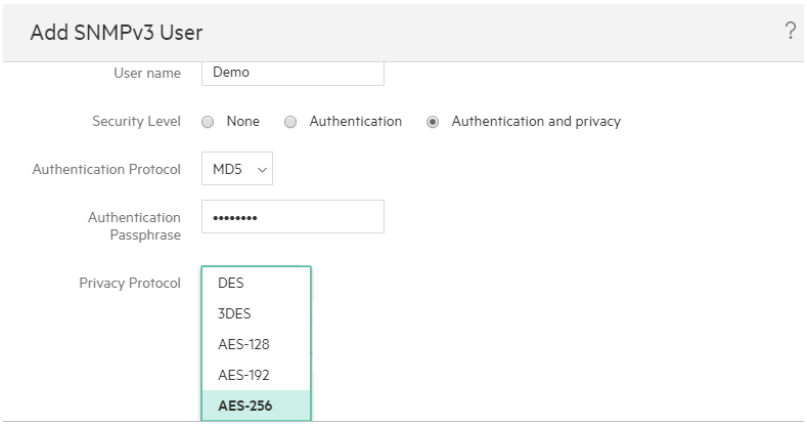
6. Select the desired *Authentication Protocol* from the drop-down list



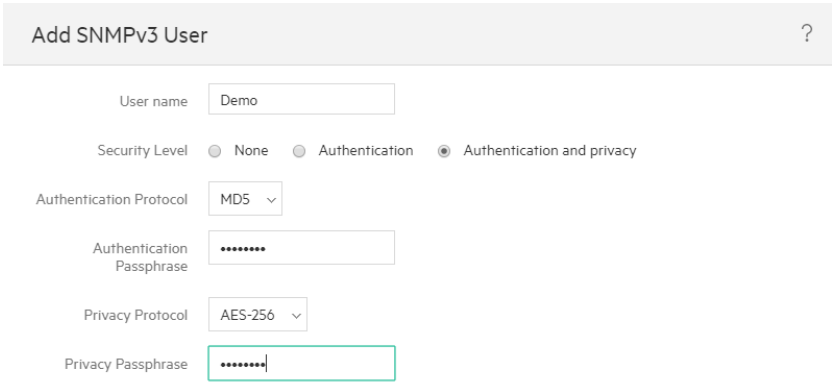
7. Enter an *Authentication Passphrase*



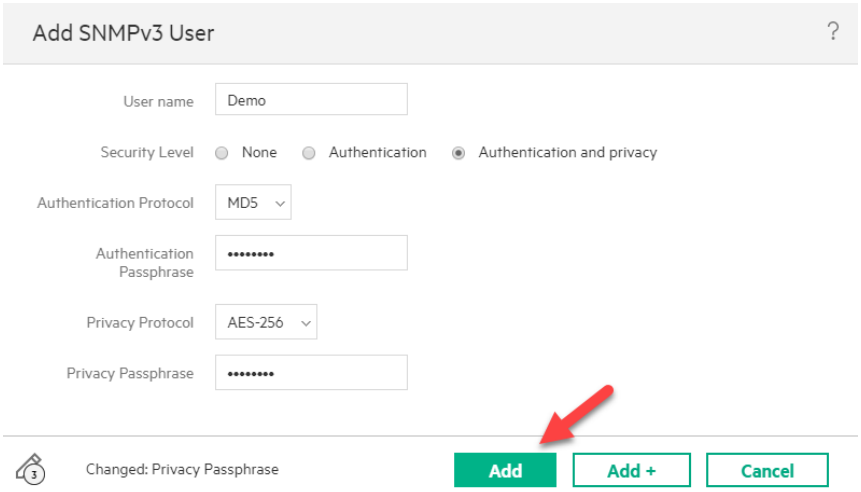
8. Select the desired *Privacy Protocol* from the drop-down list



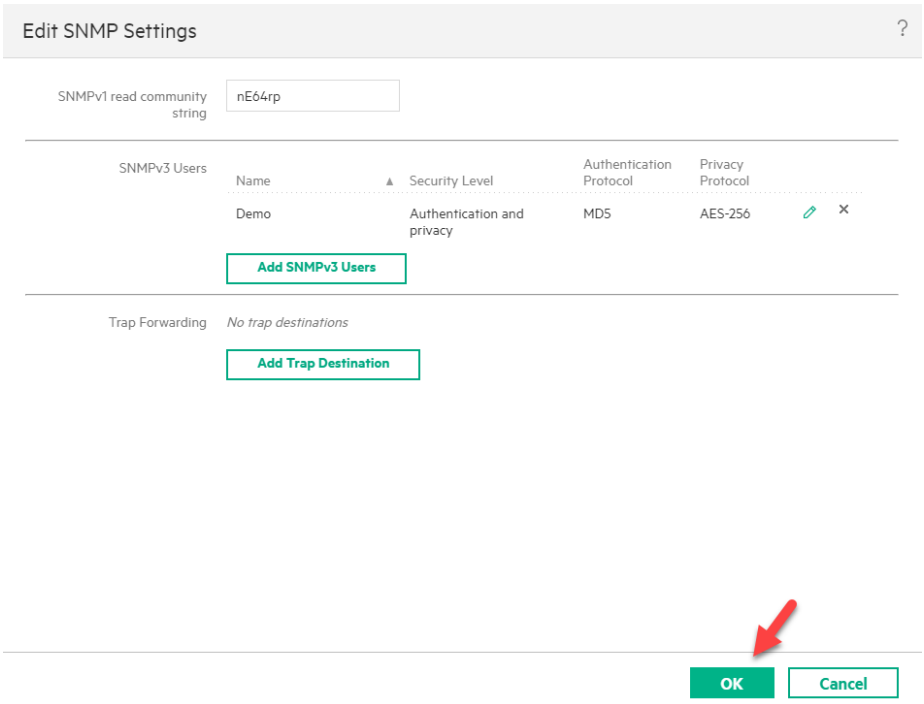
9. Enter the *Privacy Passphrase*



10. Click *Add*



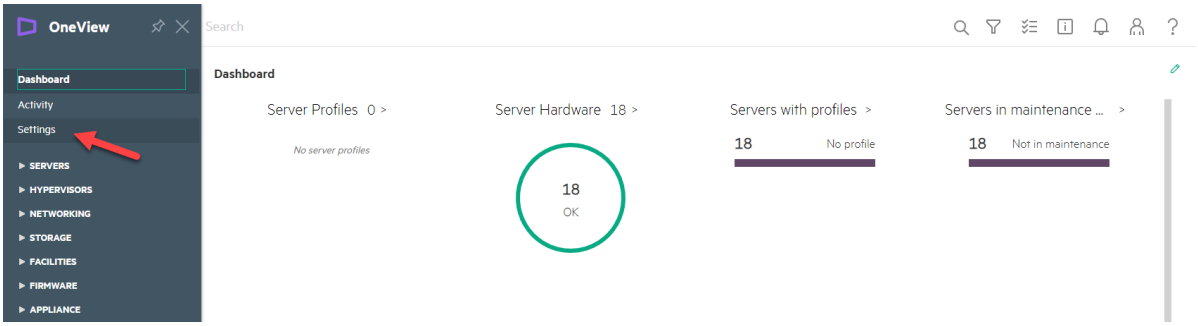
11. Click *OK*



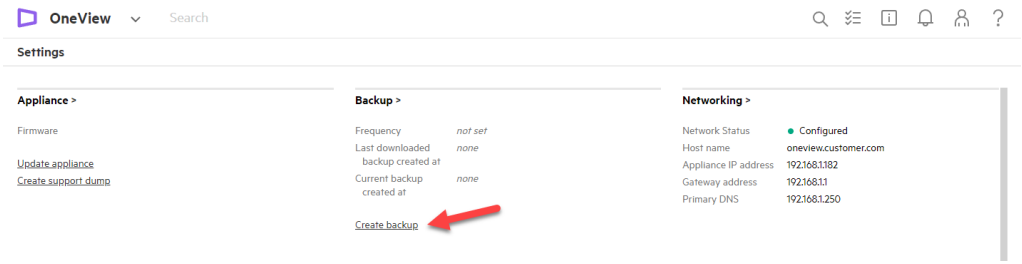
Backing up the HPE OneView Appliance – One time method

HPE OneView allows for the backing up of the configuration and imported devices. This section will describe how to create a onetime backup of the HPE OneView Appliance.

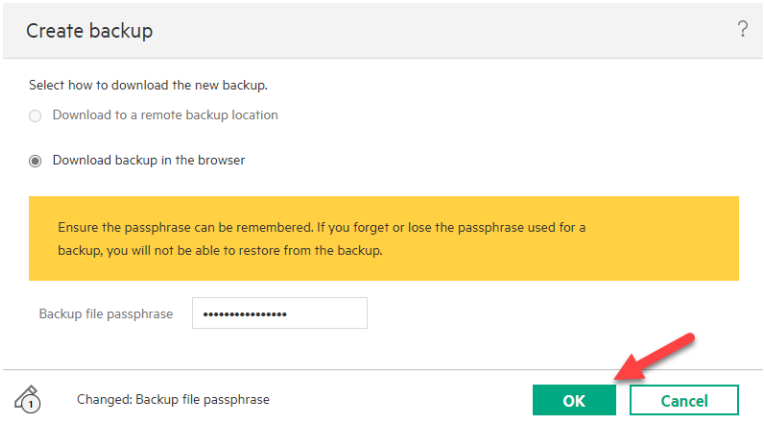
1. From the Top-Level menu, select *Settings*



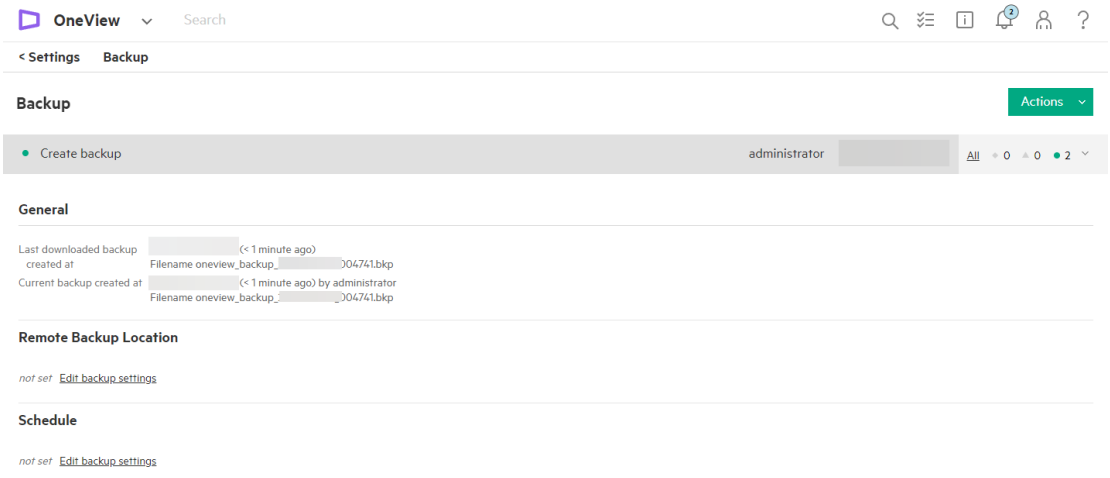
2. From the Settings page, find the Backup Section. Select *Create backup*



3. The user will be taken to the backups page, you need to type a passphrase to secure the backup and then backup will immediately begin.



4. The backup file will be saved to the users default browser Downloads folder.

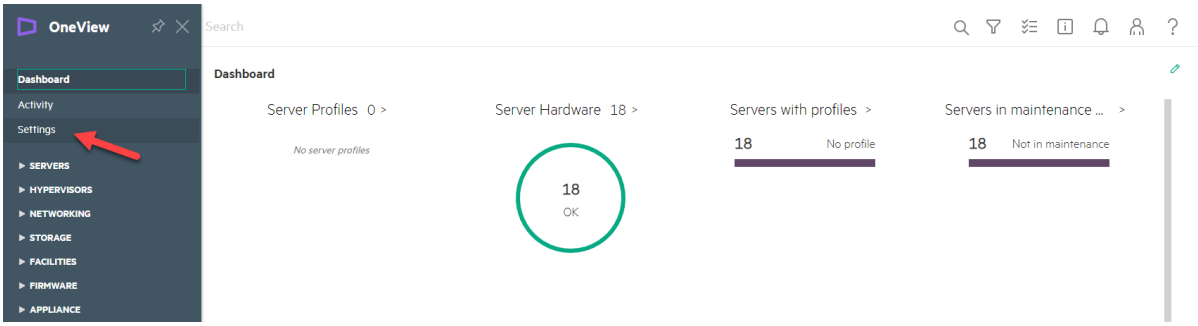


Restoring an HPE OneView Appliance from Backup

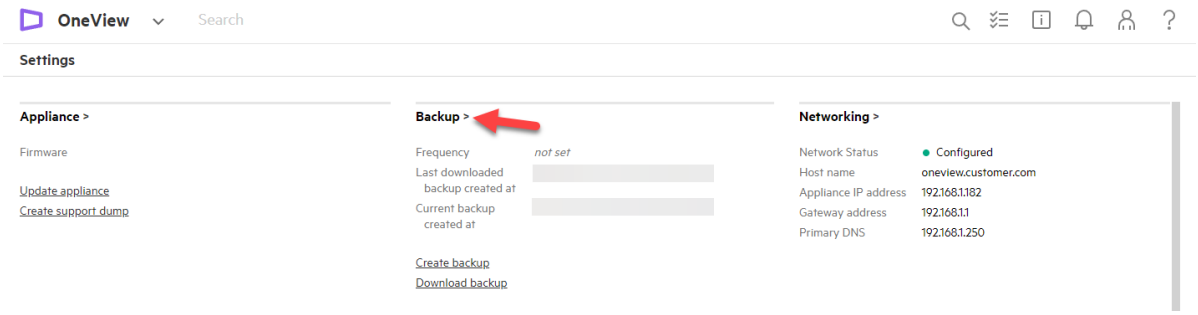
HPE OneView allows for the restoration of the configuration and imported devices from a backup file. This section will describe how to restore the HPE OneView Appliance from backup.

Note: *You can only restore a OneView backup file to the same version of OneView that it was backed up from ie a back from OneView 5.00.00.01 cannot be restored to a OneView instance running 5.00.01. This is the same whether it is a OneView Appliance or Synergy Composer.*

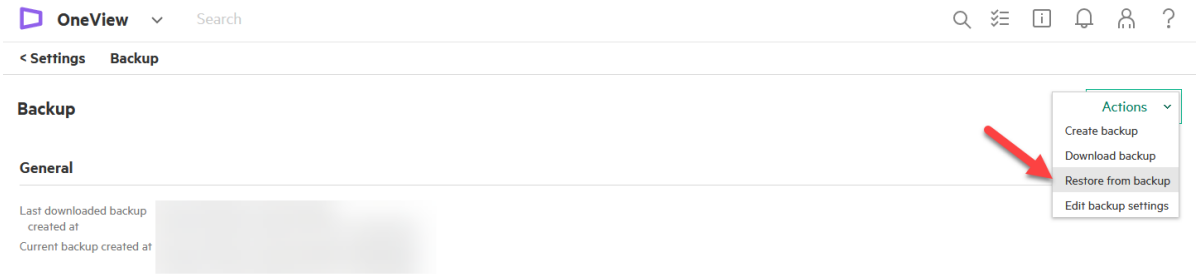
1. From the Top-Level menu, select *Settings*



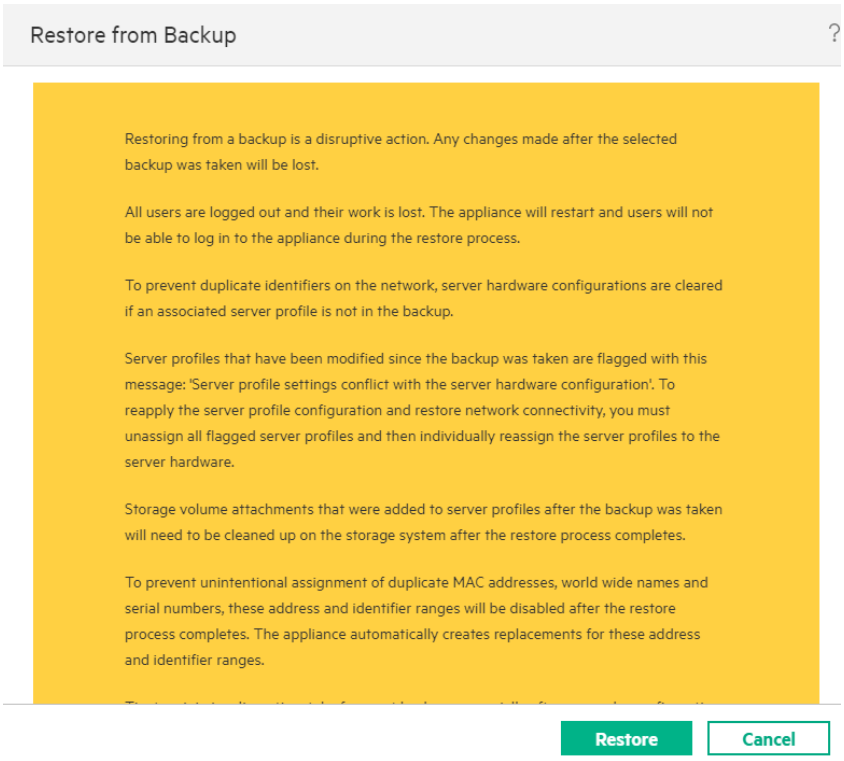
2. From the Settings page, click *Backup*



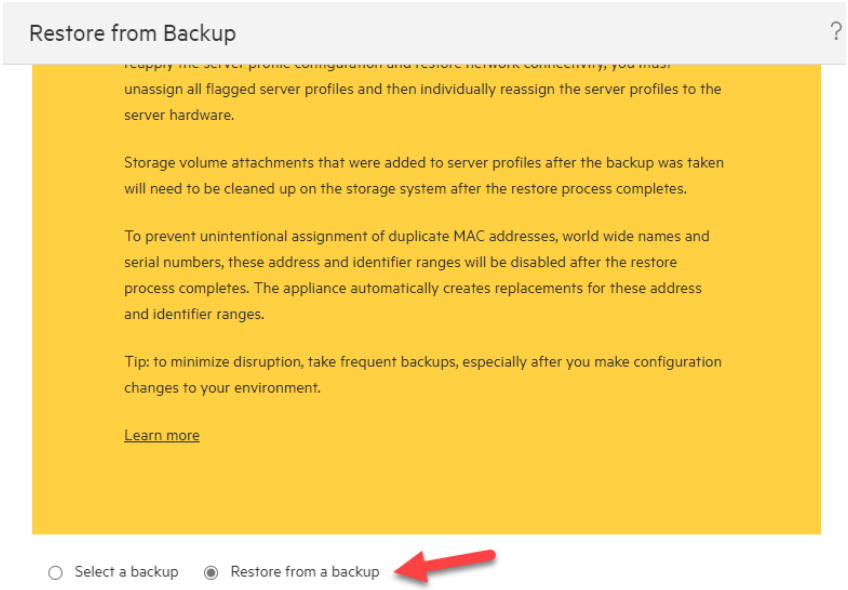
3. From the Backup section, open the Actions Menu and select *Restore from backup*.



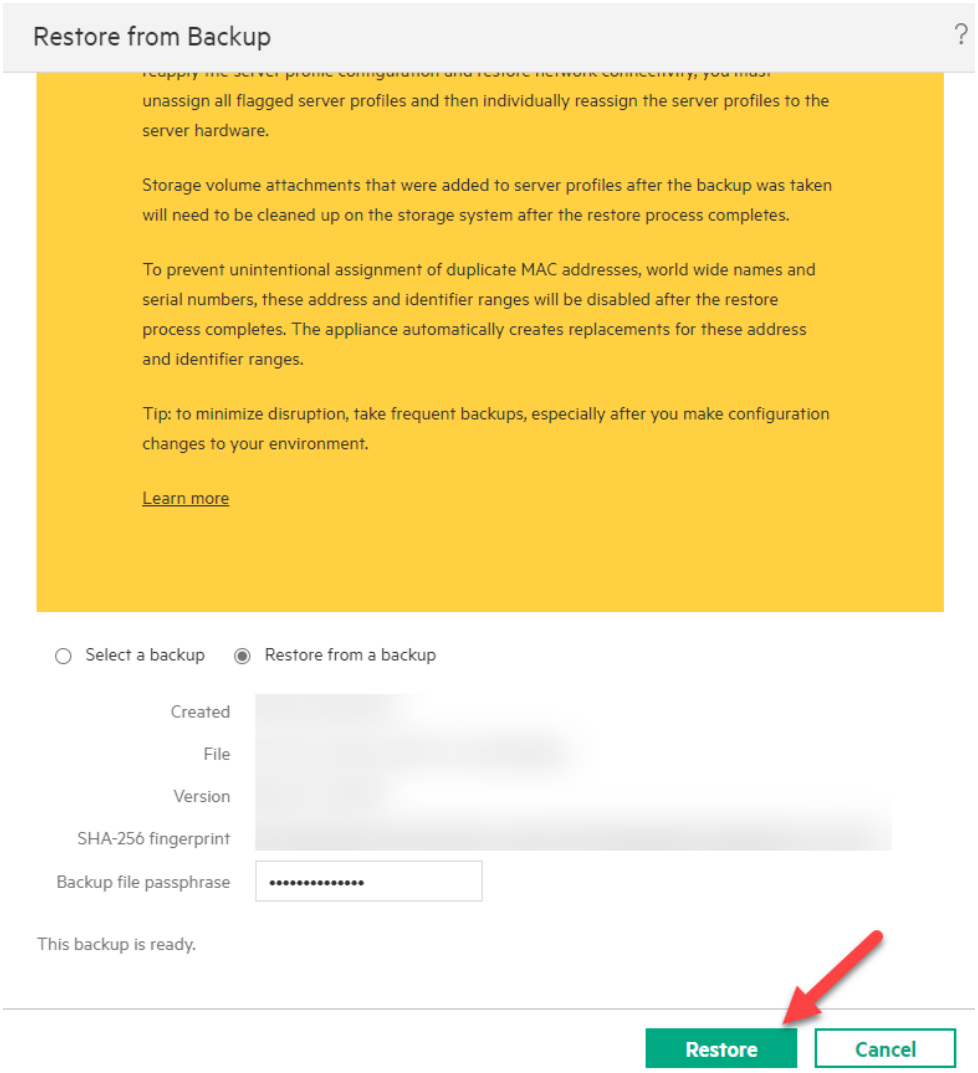
4. Scroll to the bottom of the Restore from Backup Dialog window



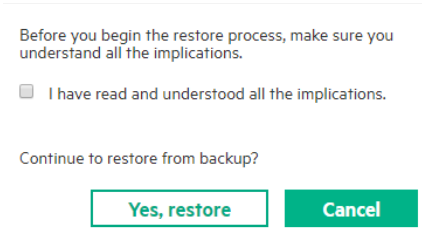
5. Select the backup file that the HPE OneView appliance will be restored to.



6. Click *Restore*



7. Confirm that you want execute the restore process, then click *Yes, Restore*



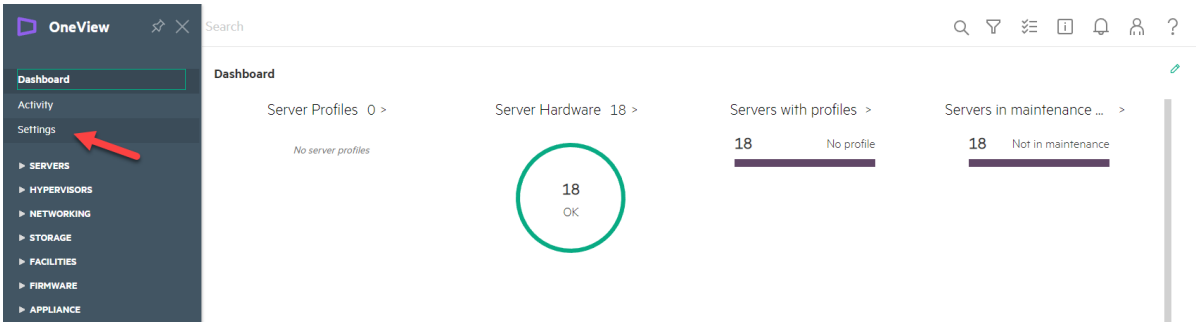
8. The restore process will begin.

Note: *Once completed you will need to re-upload any SPP / SSP to the Appliance as these are not stored in the Backup file that is being restored.*

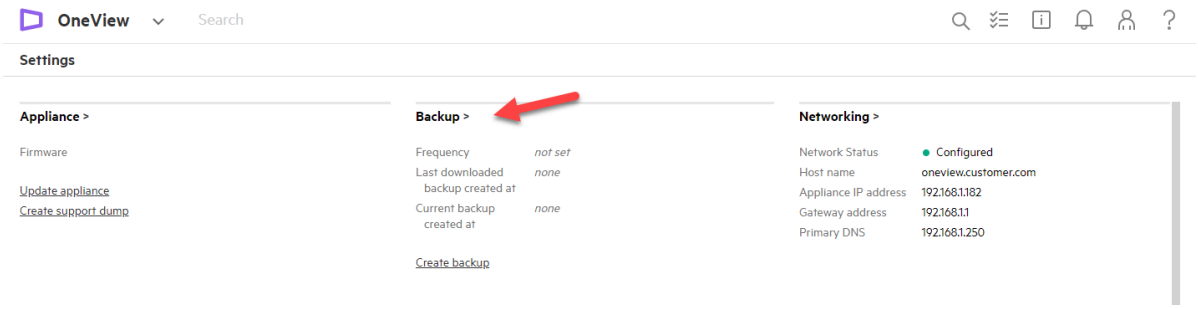
Setting a remote Backup location and Schedule for Backups

HPE OneView allows for the scheduled backing up of the configuration and imported devices to a remote file store. This section will describe how to configure the settings of the remote backup of the HPE OneView Appliance

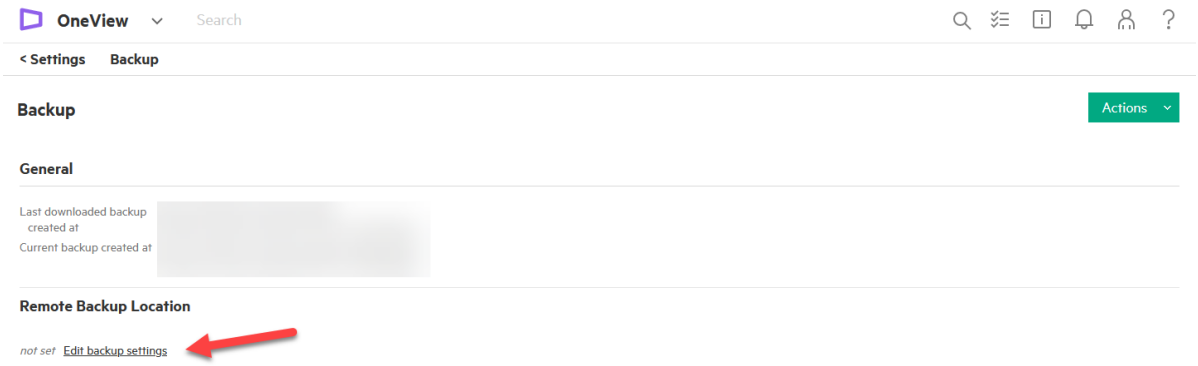
1. From the Top-Level menu, select *Settings*



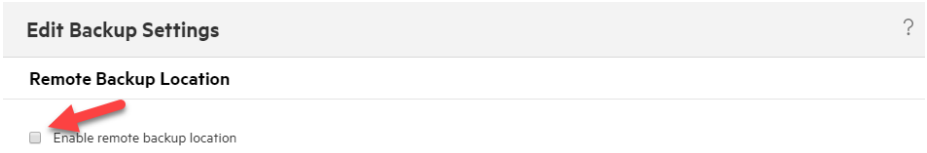
2. From the Settings page, select *Backup*



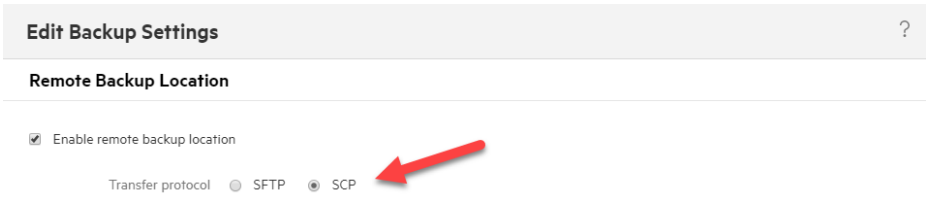
3. From the backup page, select *Edit backup settings*.



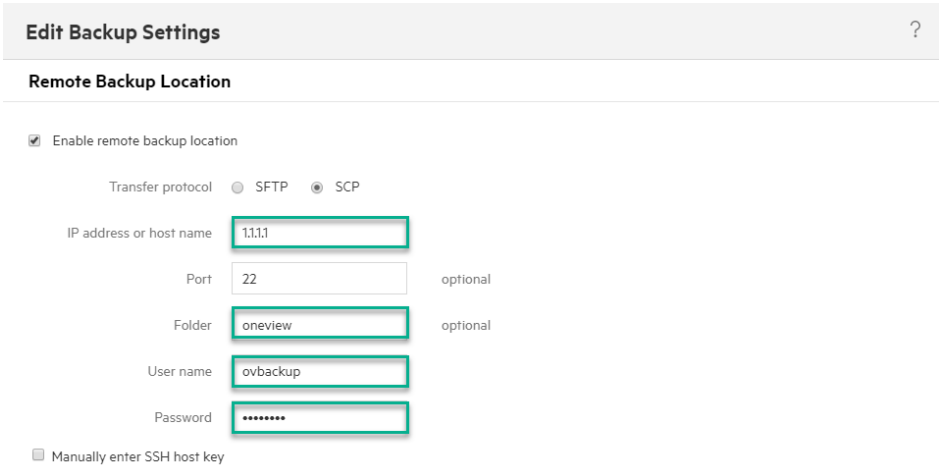
4. From the Edit Backup Settings dialog window, check the box *Enable remote backup location*



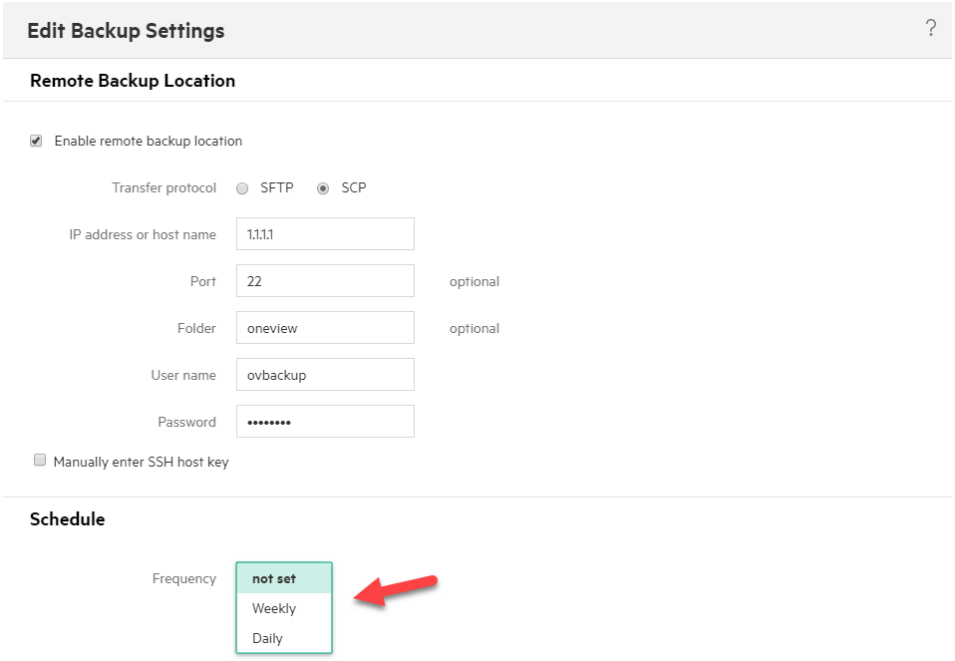
5. Select the Transfer Protocol to be used to upload your backup file to the remote location.



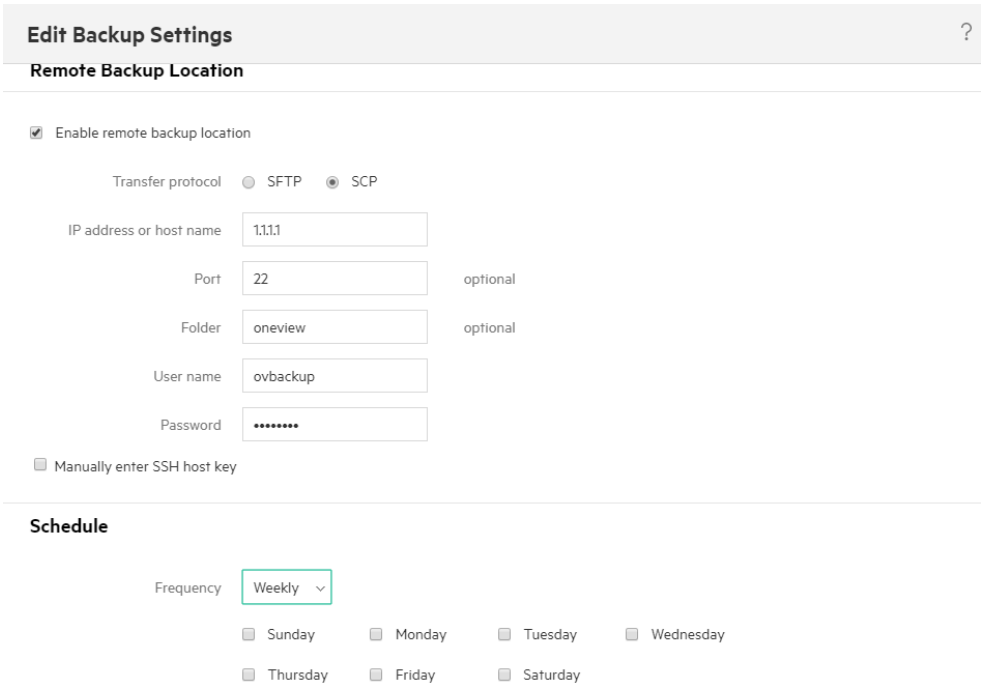
6. Enter the details for the host that the file will be uploaded to



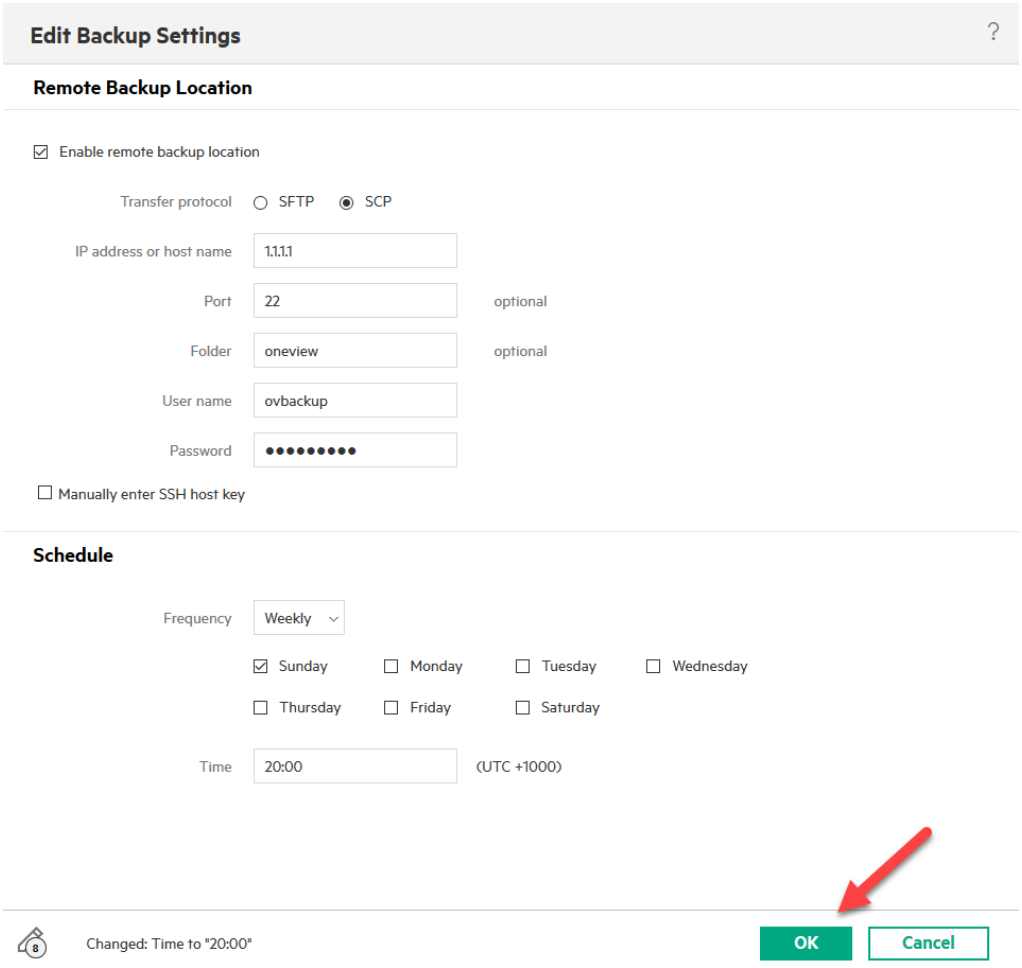
7. In the Schedule section, use the drop-down list to select the frequency of the backups



8. Select and configure the scheduled frequency of the backups



9. Select *OK* to apply the changes to the backup settings

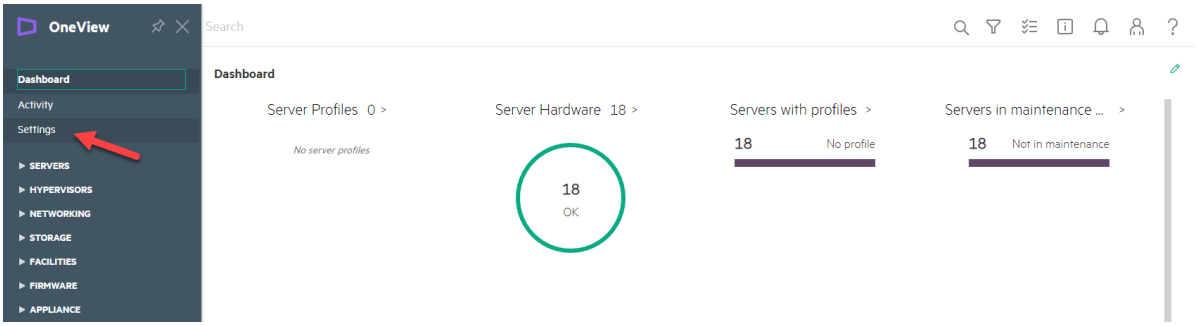


10. The new settings will be tested for accuracy and then saved.

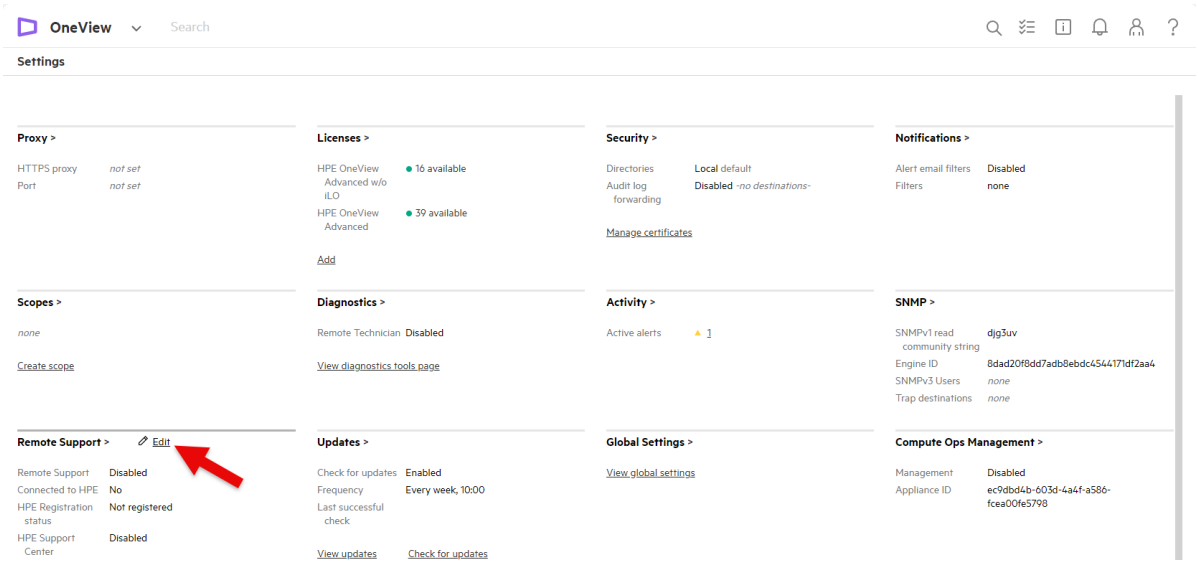
Setting up Remote Support for supported devices

HPE OneView contains support automation functionality for Gen8 and newer devices. These devices will have cases for them created automatically through the remote support functionality.

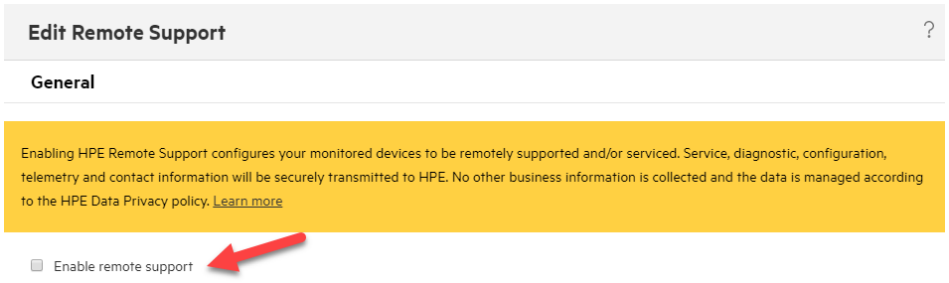
1. From the Top-Level menu, select *Settings*



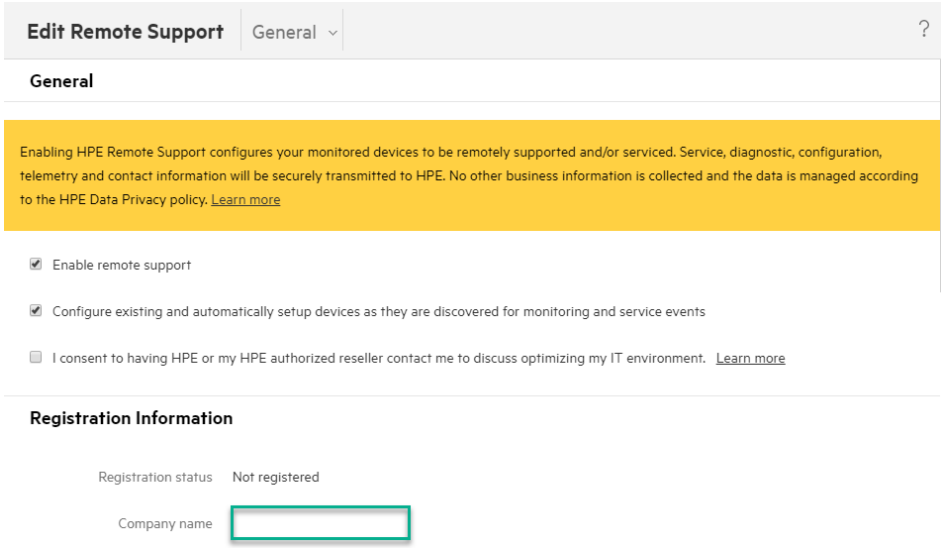
2. From the Settings page, find the Remote Support Section and select *Remote Support* and click on *Edit*.



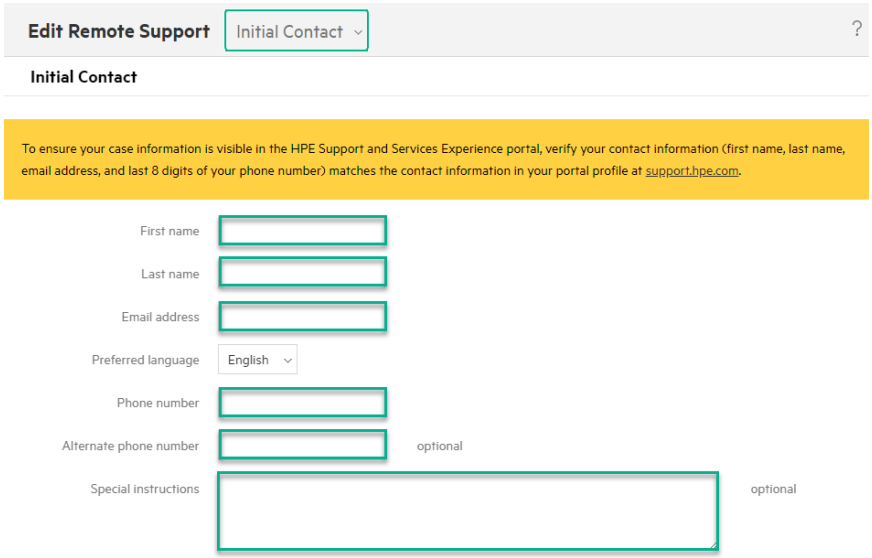
3. On the Edit Remote Support dialog window, check the box *Enable Remote Support*



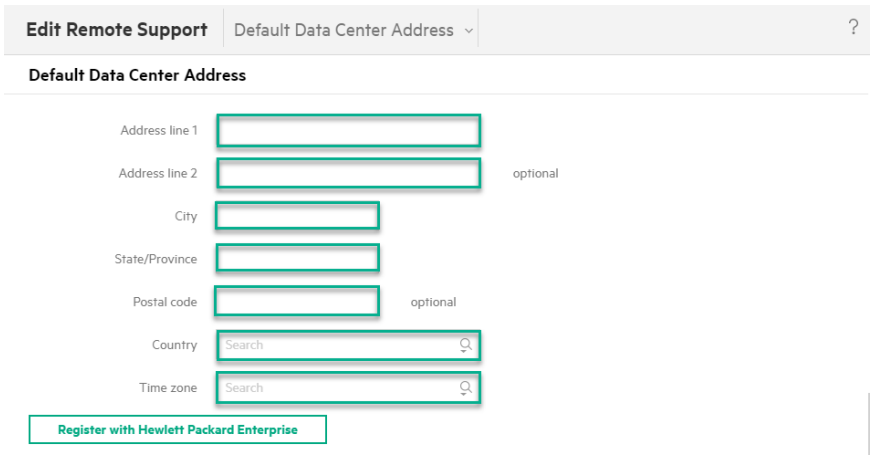
4. In the Registration Information section of the Edit Remote Support dialog window, enter the *Company Name*



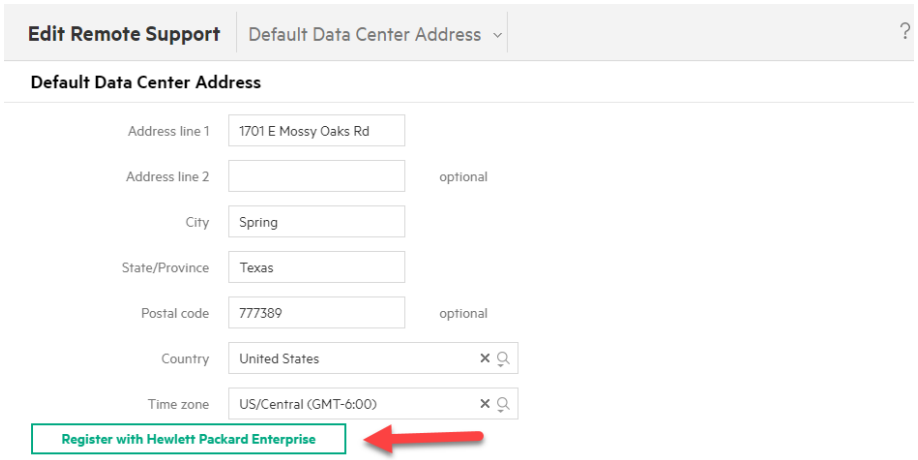
5. Enter the *Initial Contact* Information



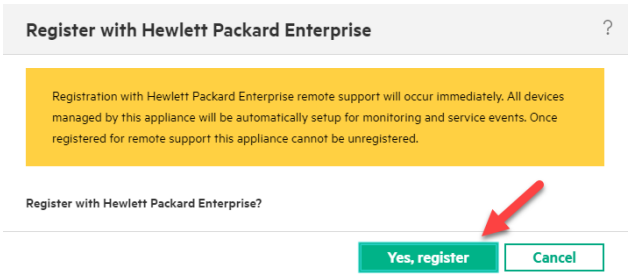
6. Enter the *Default Data Center Address*. This needs to be where the servers are physically located because this is where the parts will be sent.



7. Click *Register with Hewlett Packard Enterprise*



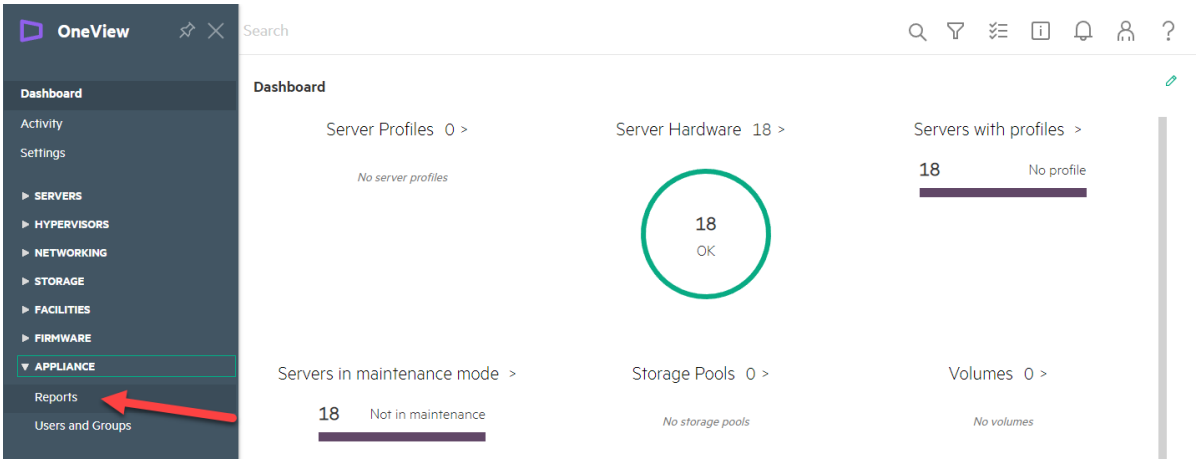
8. Click *Yes, register* to initialize the registration with Hewlett Packard Enterprise.



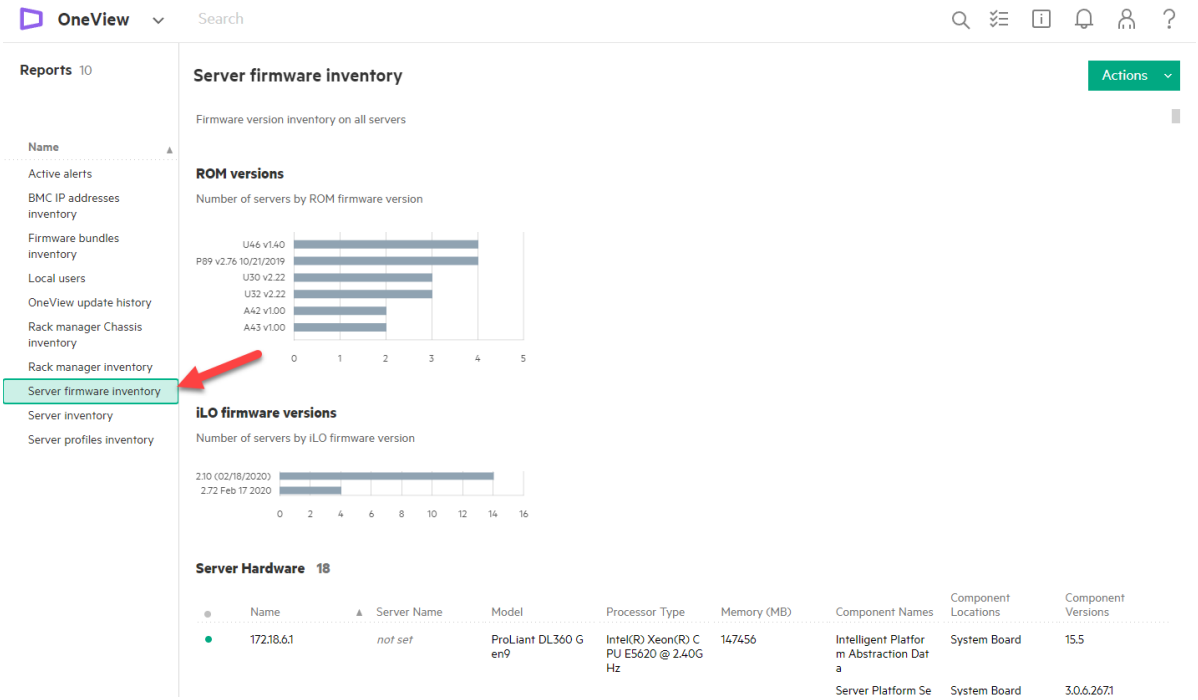
Viewing Reports

HPE OneView provides a pre-defined list of reports giving the administrators and users information based on HPE OneView inventory, configuration, health status and more. Reports can also be pulled from the HPE OneView appliance via REST API's.

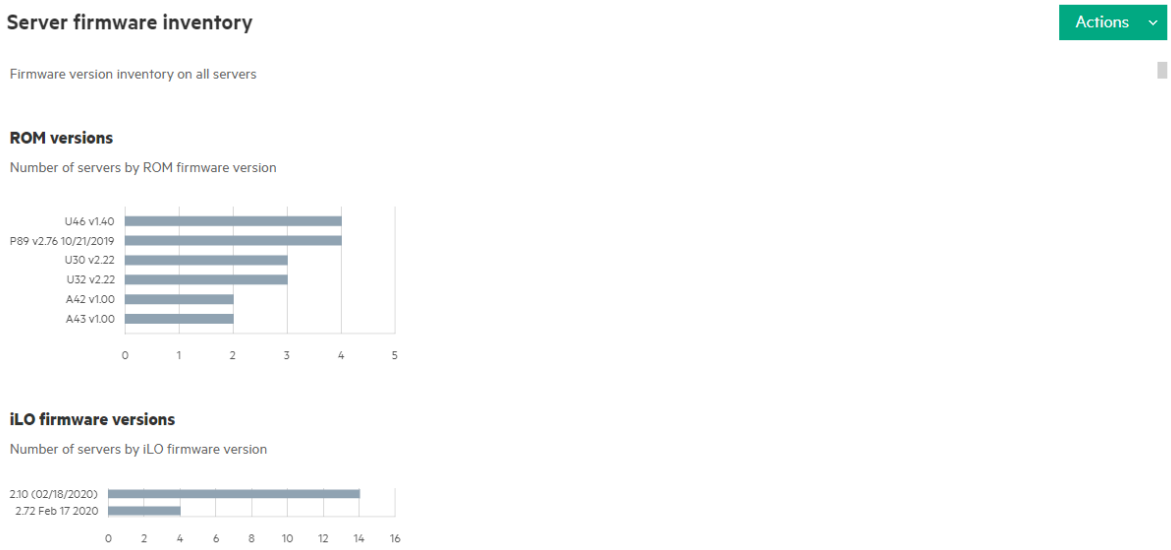
1. From the Top-Level menu, expand the *APPLIANCE* and then select *Reports*



2. From the menu, select the desired report. For this example, we will select the *Server firmware inventory* Report.



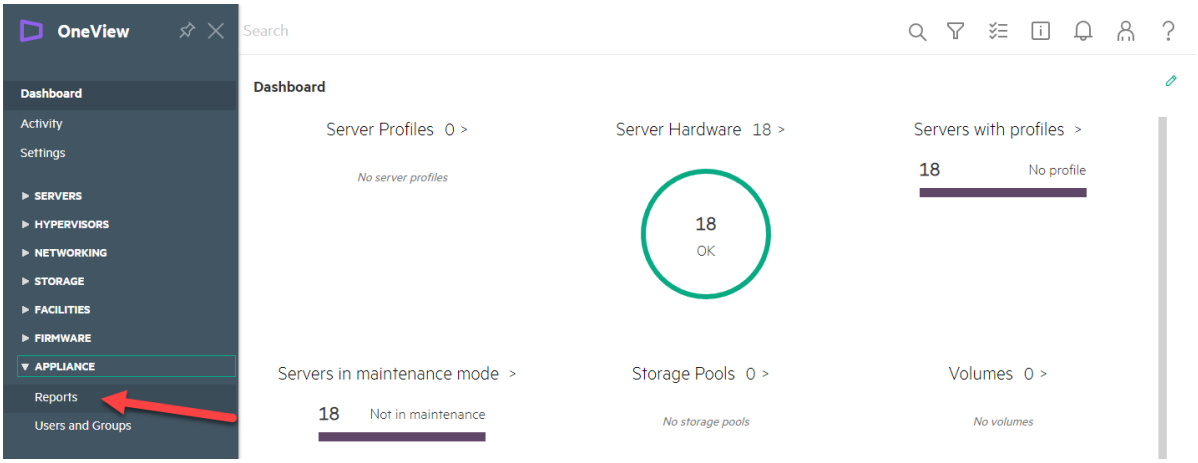
3. The selected report will be displayed



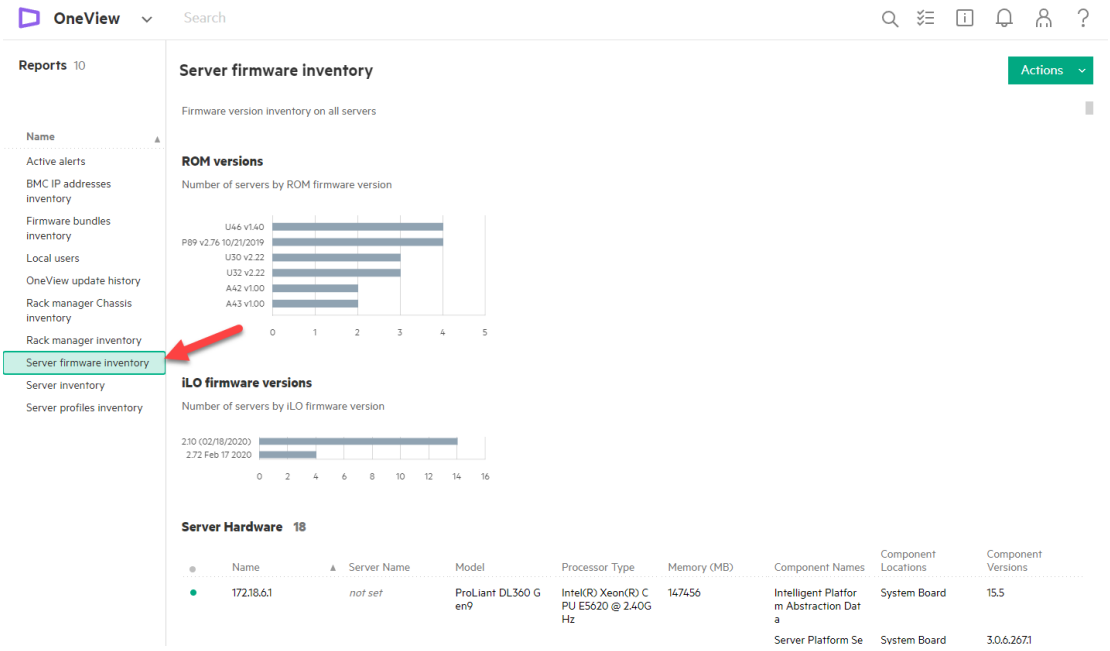
Exporting Reports

Reports within HPE OneView can be exported to Excel XLSX or CSV files for use in other applications.

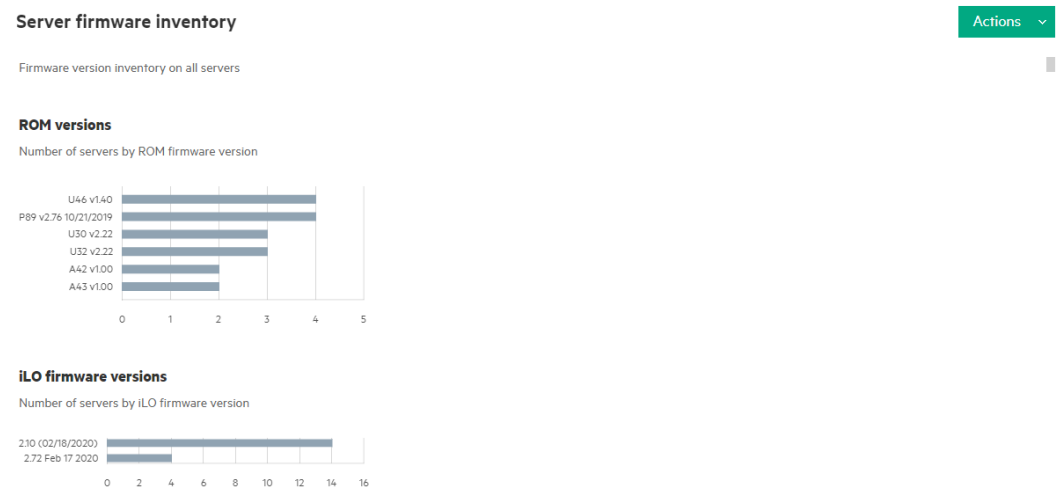
1. From the Top-Level menu, expand the *APPLIANCE* option and then select *Reports*



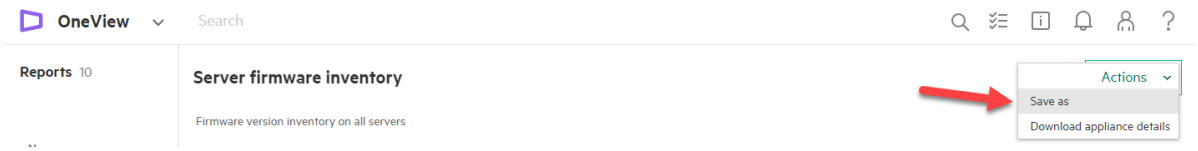
2. From the menu, select the desired report. For this example, we will select the *Server firmware inventory* Report.



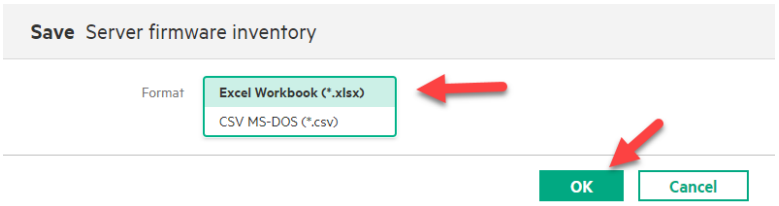
3. The selected report will be displayed



4. From the Actions menu, select *Save As*.



5. Select the desired output format – Excel Workbook (*.xlsx) or CSV MS-DOS (*.csv) using the dropdown menu and then click *OK* to save the report.

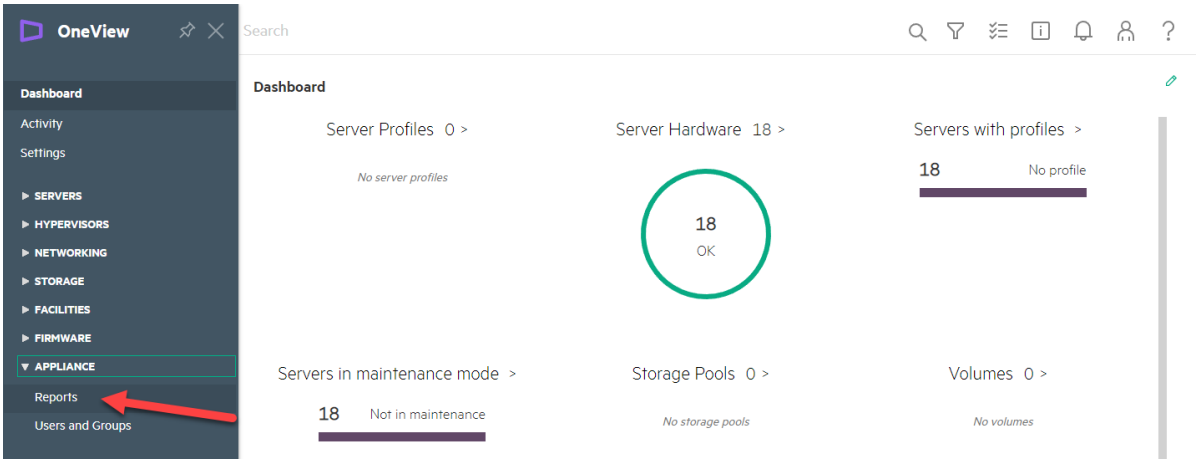


6. The file will be saved in the Downloads folder of the local user

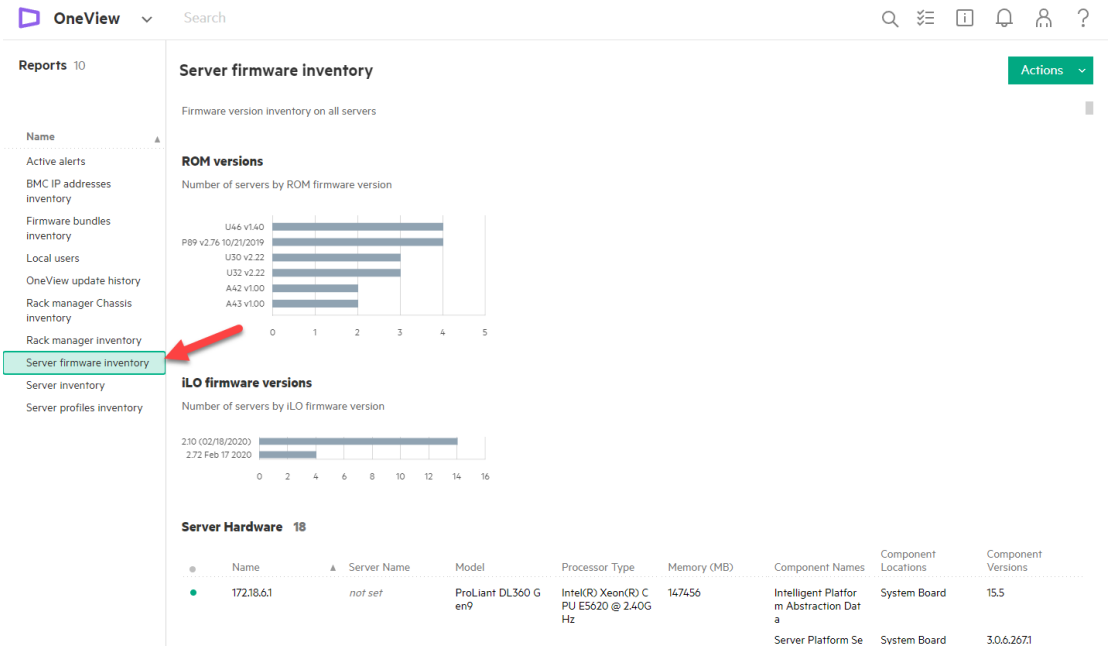
Printing Reports

Reports within HPE OneView can be printed in PDF format.

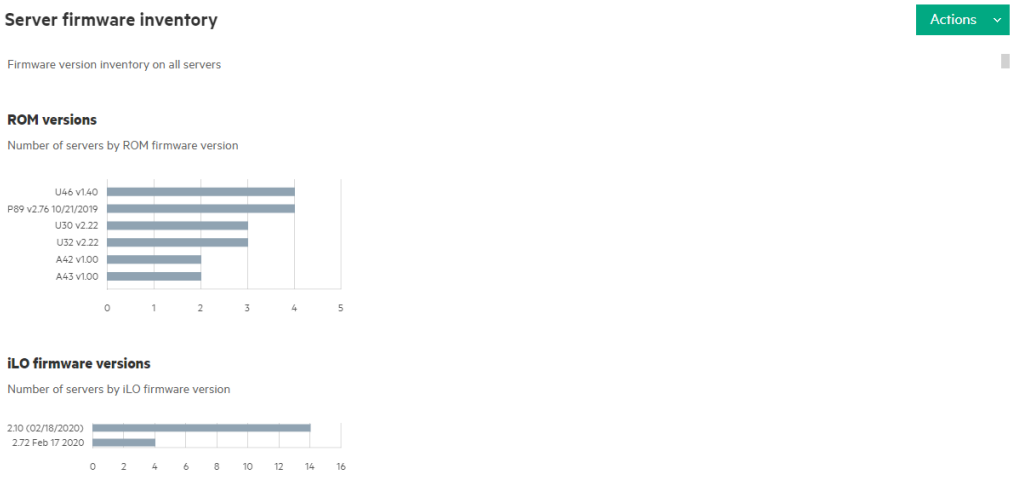
1. From the Top-Level menu, expand the *APPLIANCE* option and then select *Reports*



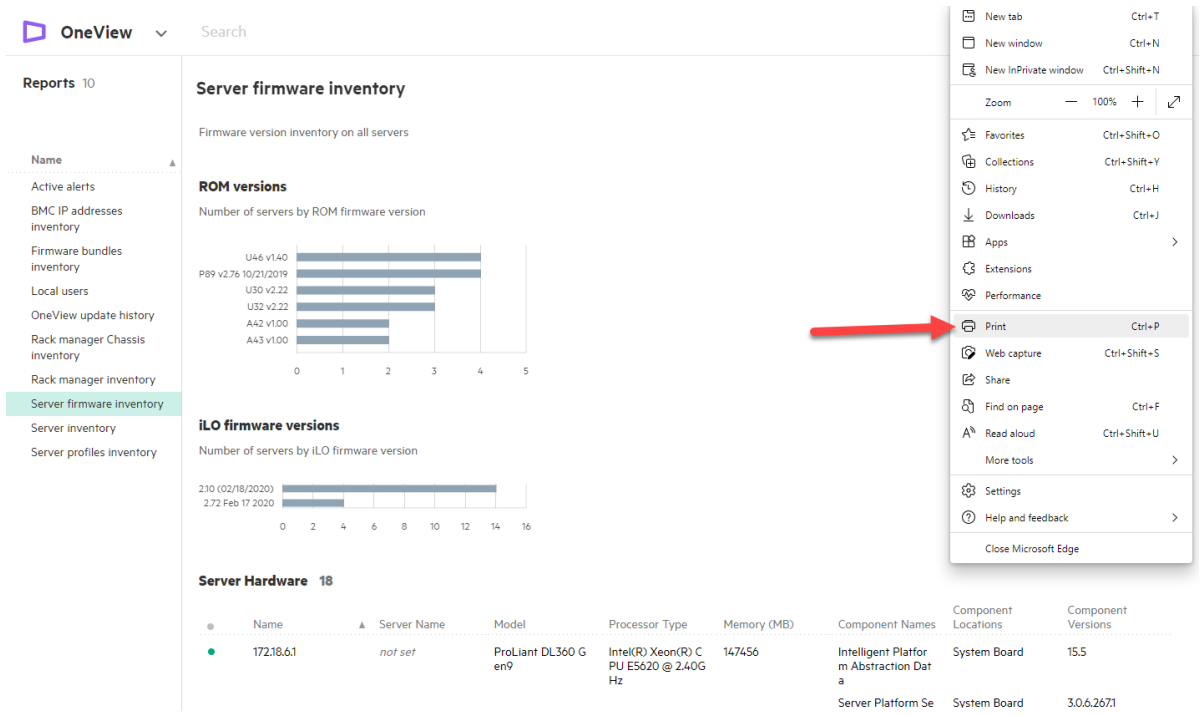
2. From the menu, select the desired report. For this example, we will select the *Server firmware inventory* Report.



3. The selected report will be displayed



4. From the browsers context menu select *Print*.

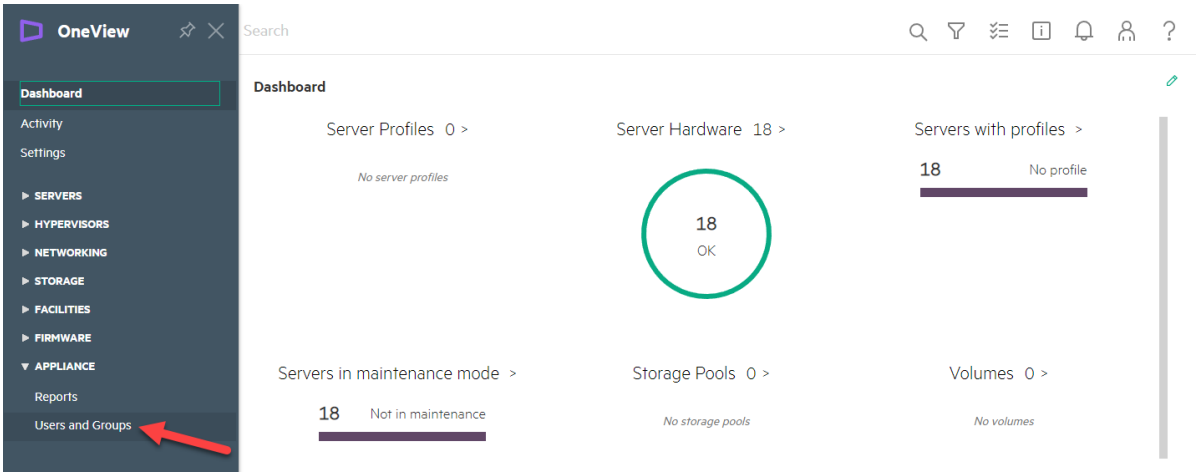


5. The file can now be printed or saved in PDF format (if you have a PDF based Printer Driver installed).

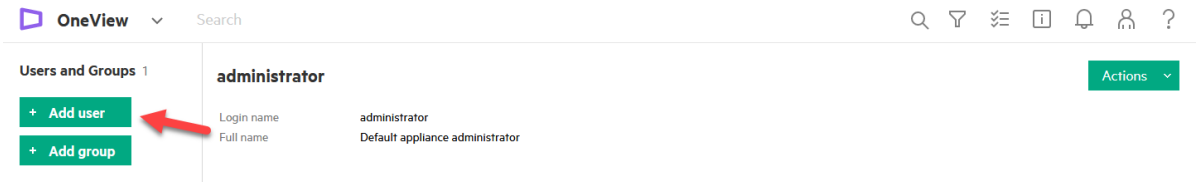
Creating New Users

HPE OneView supports the methodology of differing roles within a Composable Infrastructure. In this section we will create a new user for the HPE OneView environment.

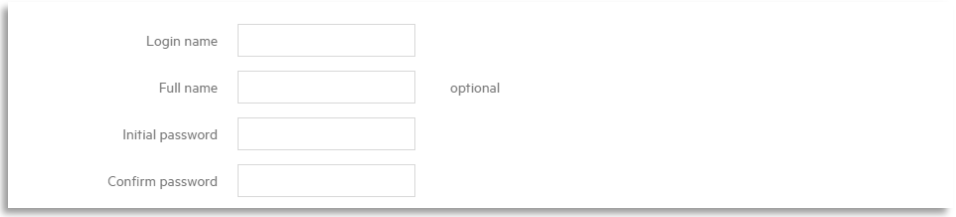
1. From the top-level menu, expand the *APPLIANCE* option and then select *Users and Groups*



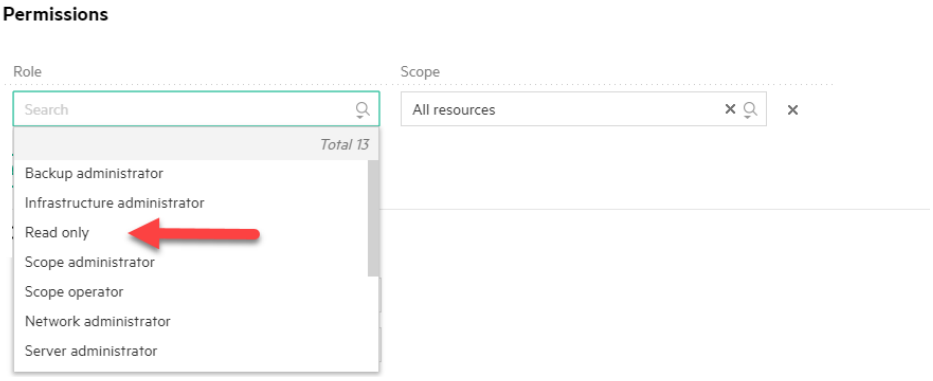
2. Select the *+Add user* button.



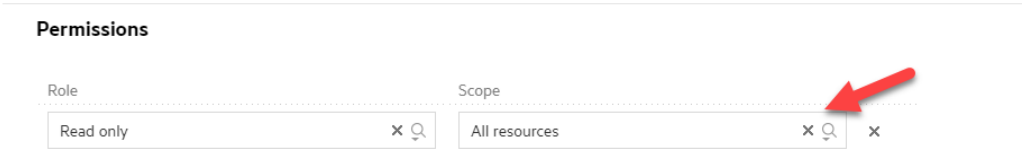
3. Provide a *login name*, *Full name* (optional), then enter and confirm the password that will be used for the account.



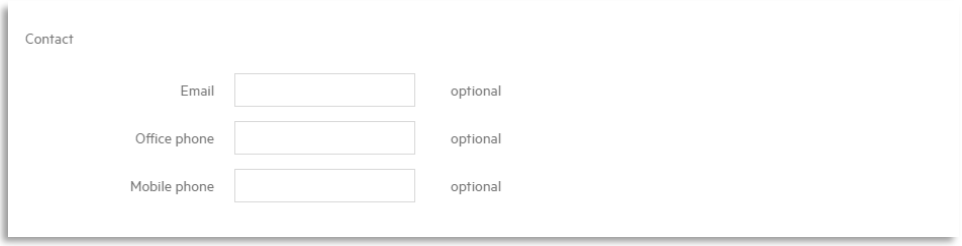
4. Select the type of Role that this user will have.
   Specialized accounts can be limited to Backup functions, Network functions or Server functions.
   Full accounts are administrators for all segments.
   Read only accounts will be able to view information within HPE OneView but not change any information.



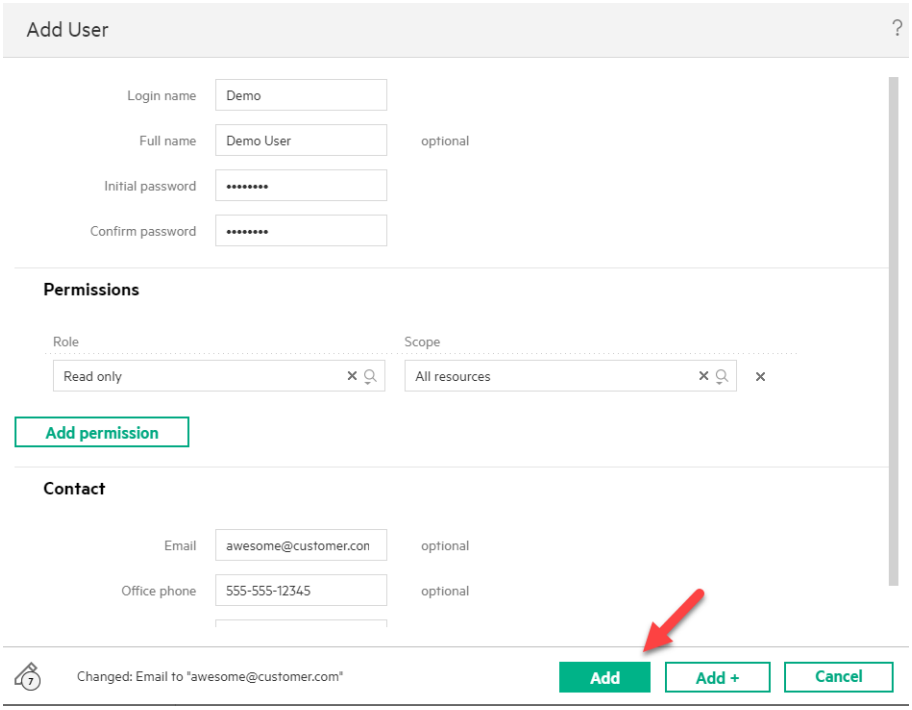
5. Select a scope if you want to restrict access to resources available to the account. if you do not have any Scopes setup then the default of "All resources" is used. See elsewhere in this document for *Creating a Scope* on how this is done.



6. Contact Email, Office and Mobile Phone numbers can be added if desired.



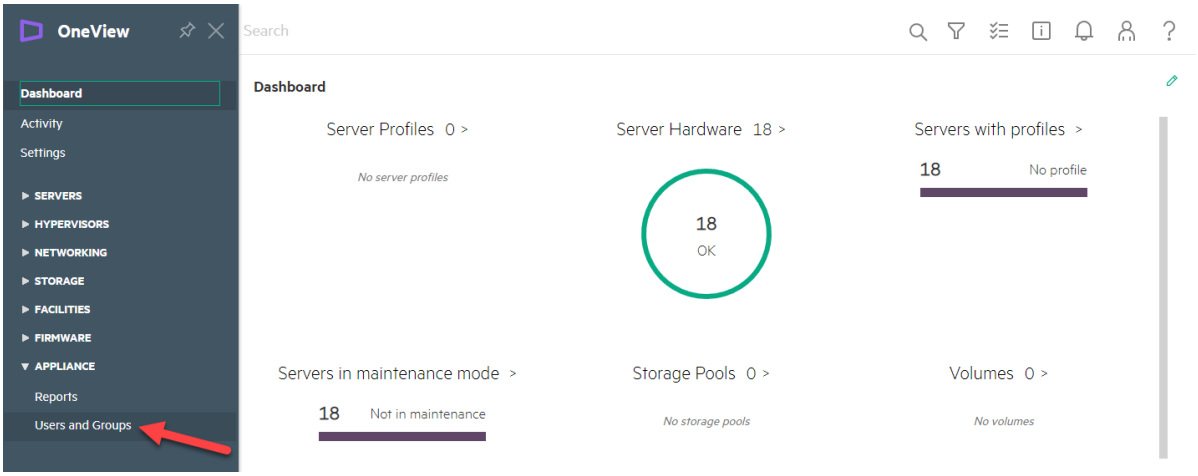
7. Select *Add or Add +* button to create the account.



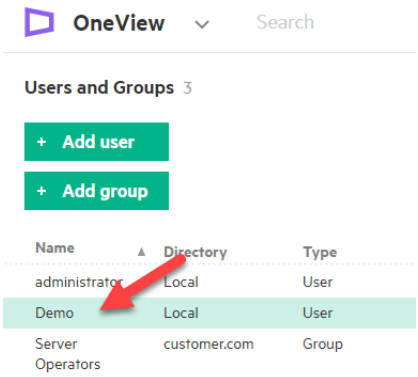
Deleting Existing Users

HPE OneView supports the methodology of differing roles within a Composable Infrastructure. In this section we will delete an existing user in the HPE OneView environment.

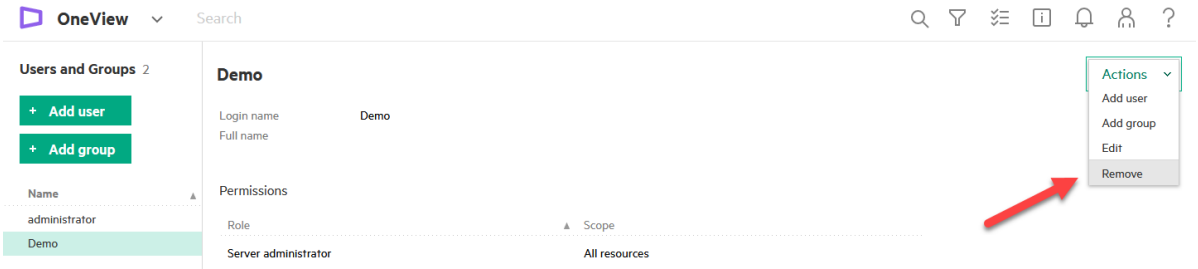
1. From the top-level menu, expand the *APPLIANCE* option and then select *Users and Groups*.



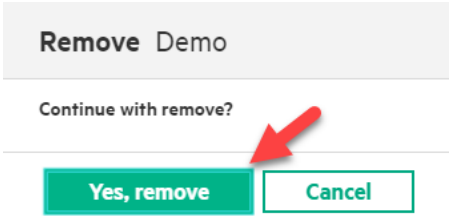
2. Select the user that needs to be deleted from the menu



3. Select *Remove* from the Actions menu



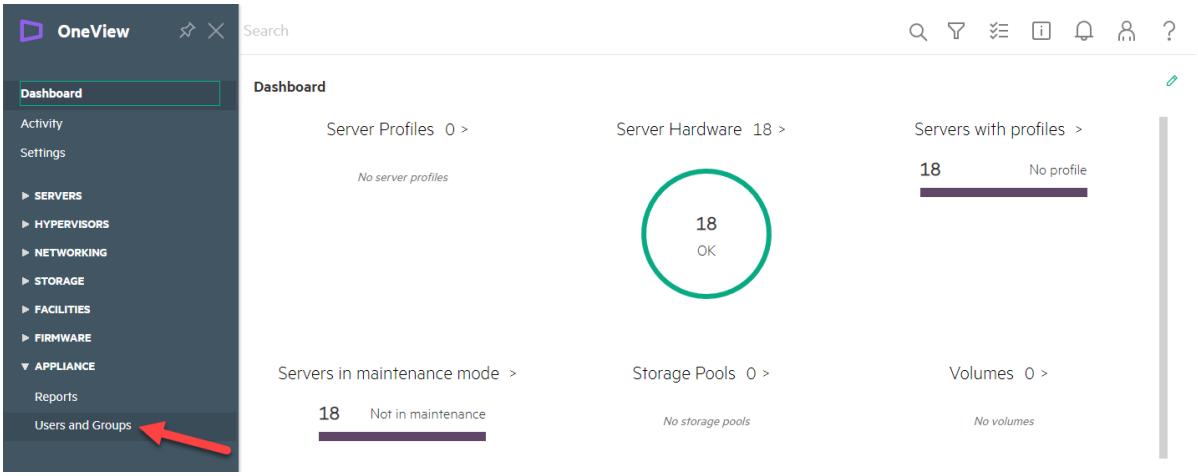
4. Confirm your selection by selecting the *Yes, remove* button to delete the account.



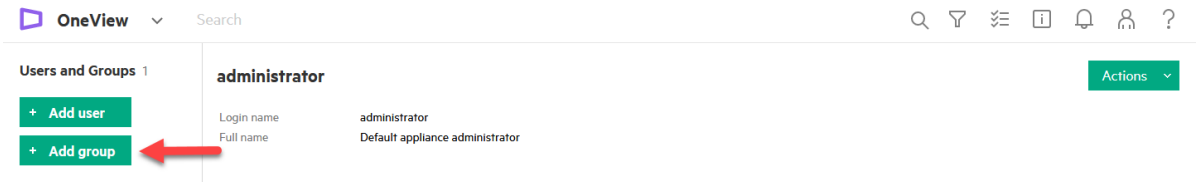
Creating Groups

HPE OneView supports the methodology of differing roles within a Composable Infrastructure. In this section we will create a new group in the HPE OneView environment.

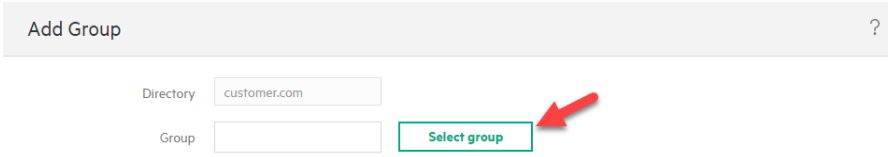
1. From the top-level menu, expand the *APPLIANCE* option and then select *Users and Groups*.



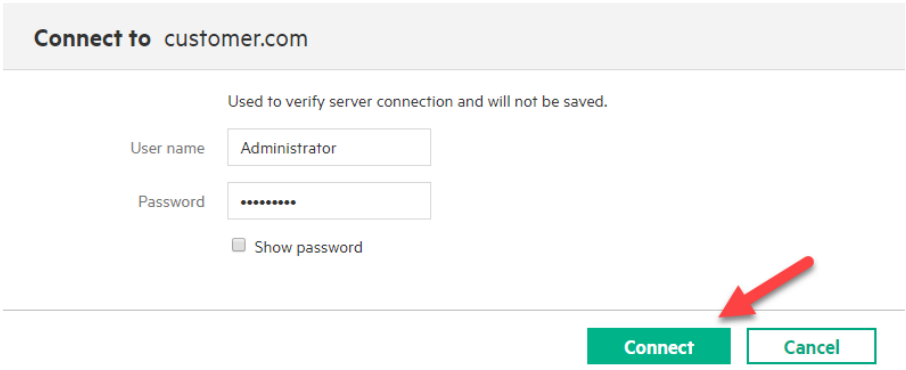
2. Click on *Add group*



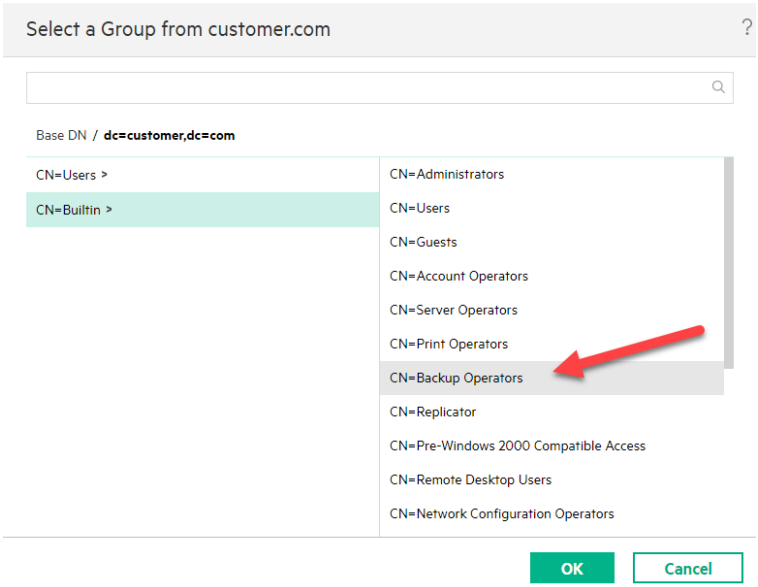
3. Select the *Select Group* button



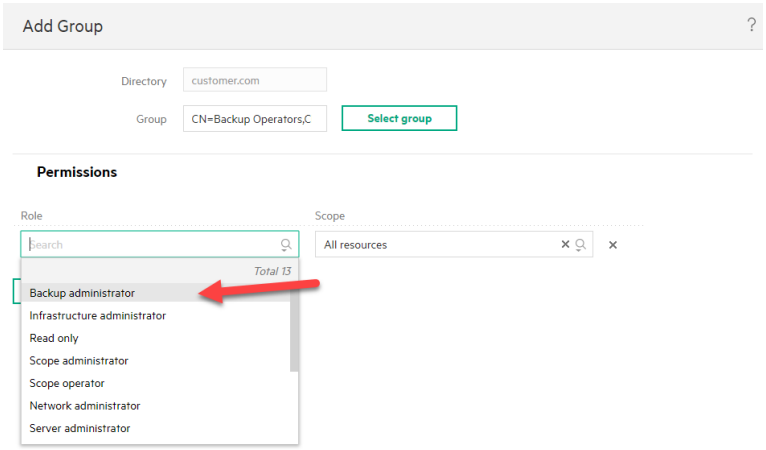
4. Provide the credentials to authenticate and click *Connect*.



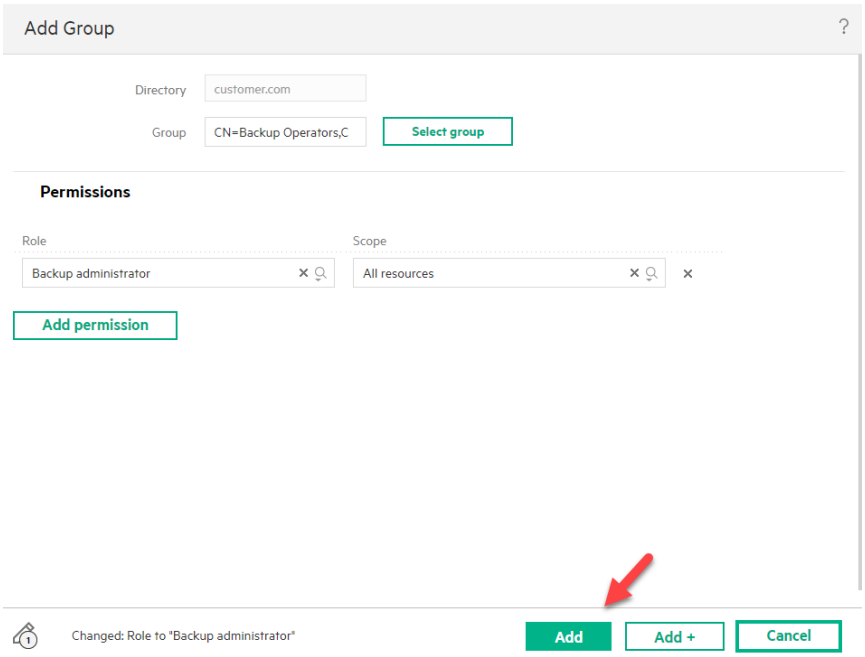
5. Once authenticated, select a group from the groups dialog window and click *OK*.



6. Assign the role that is needed for that directory group.



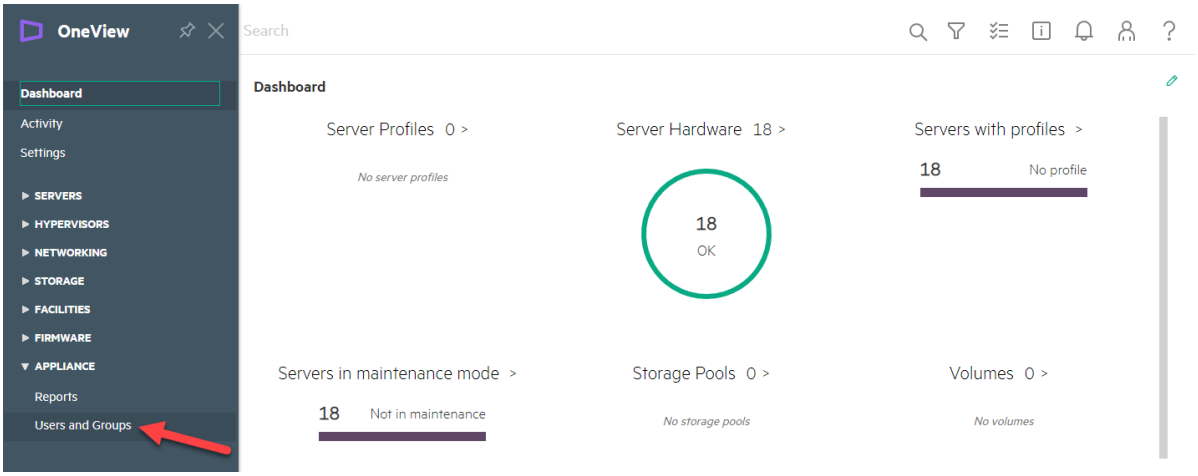
7. Click *Add* to close the Add Group Dialog window



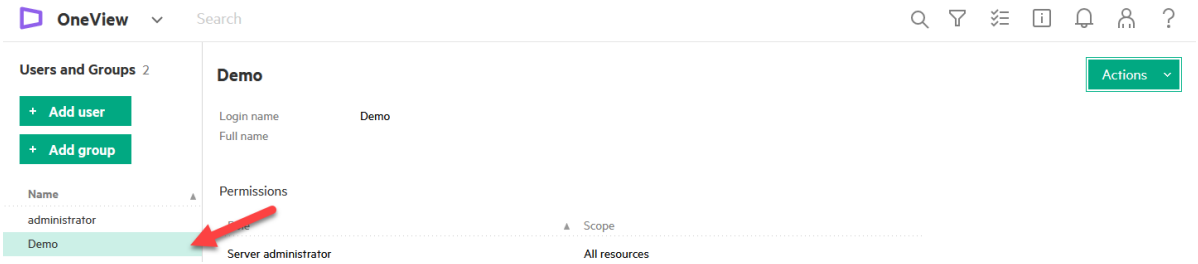
Changing User Permissions

HPE OneView supports the methodology of differing roles within a Composable Infrastructure. In this section we adjust the permissions for a user within the for the HPE OneView environment.

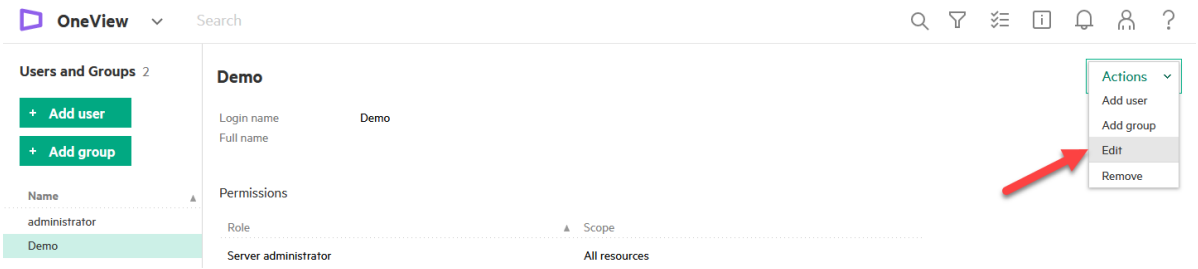
1. From the Top-Level Menu, expand the *APPLIANCE* option and then select *Users and Groups*



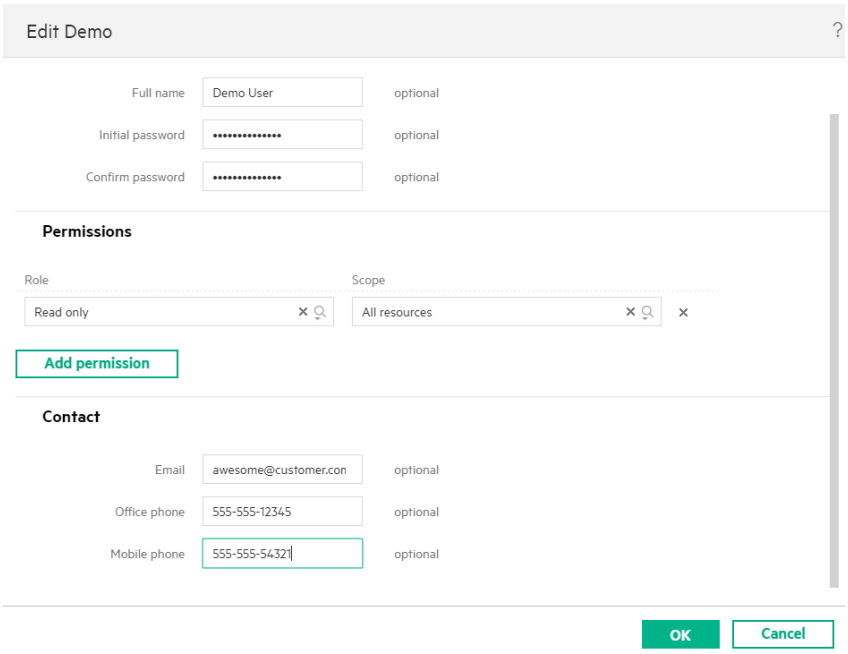
2. Select the user you want to edit from the menu



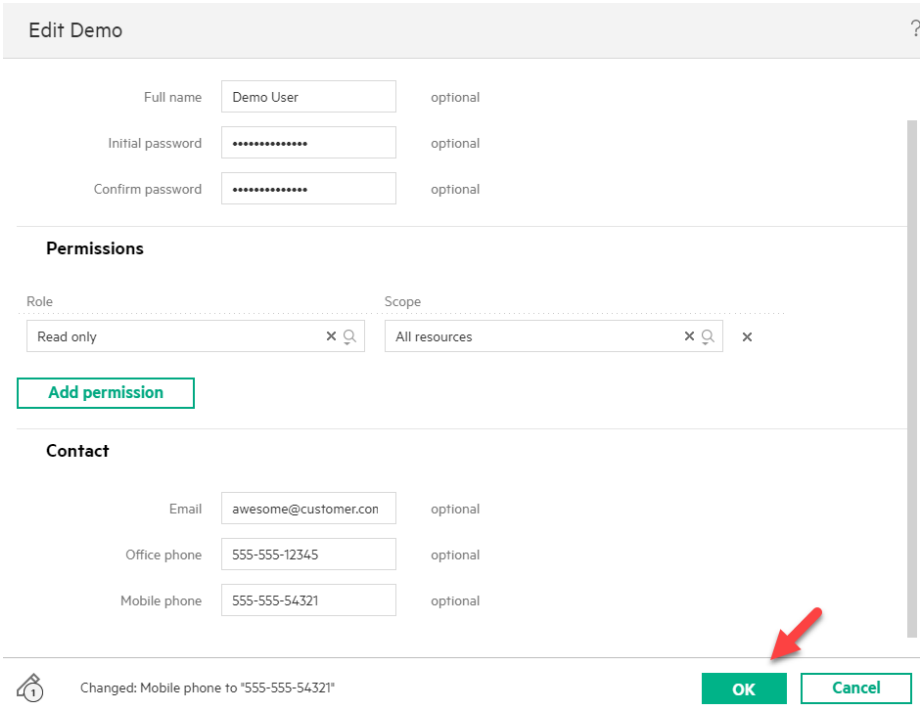
3. Select *Edit* from the Actions menu.



4. Edit the information that needs to be changed.



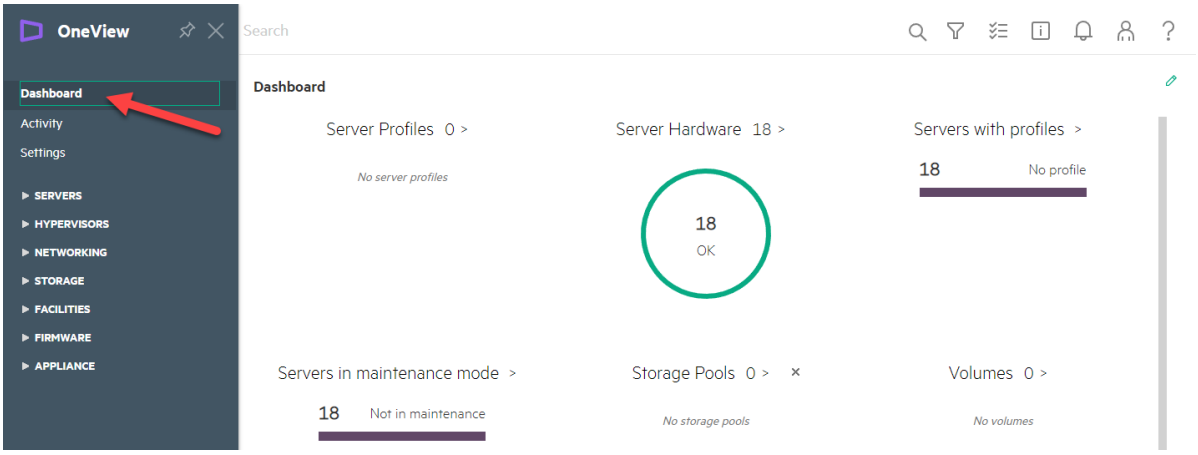
5. Click the *OK* button to save the changes that have been made.



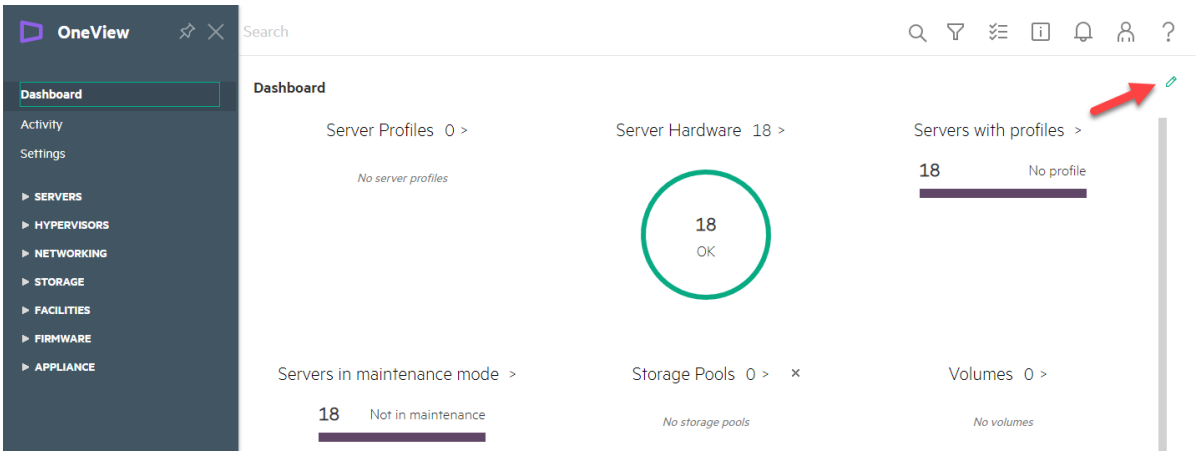
Adding a Dashboard Panel to the HPE OneView Dashboard

HPE OneView allows the user to customize the Dashboard interface. The customization allows each user to pick the categories that will be presented to the user when they log in.

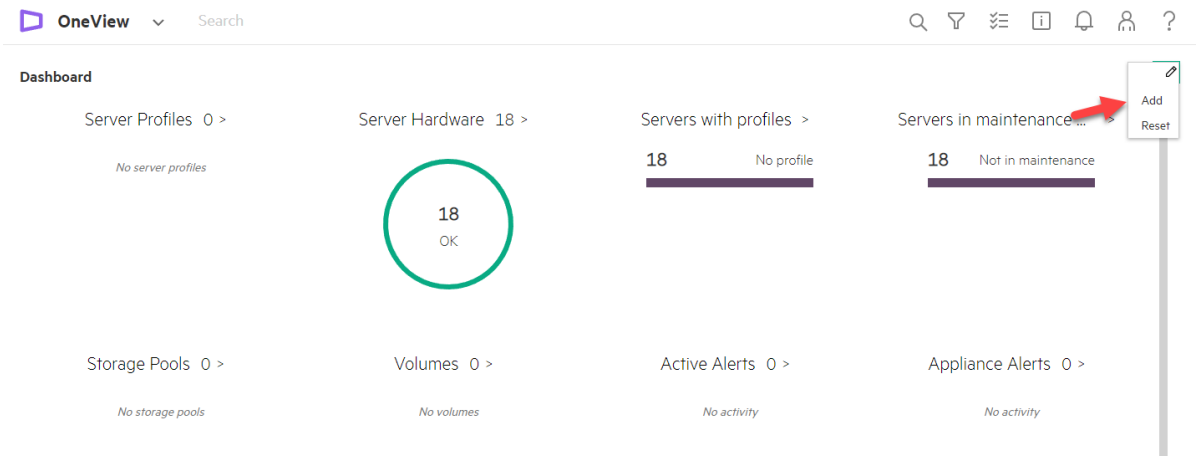
1. From the Top-Level Menu, select *Dashboard*



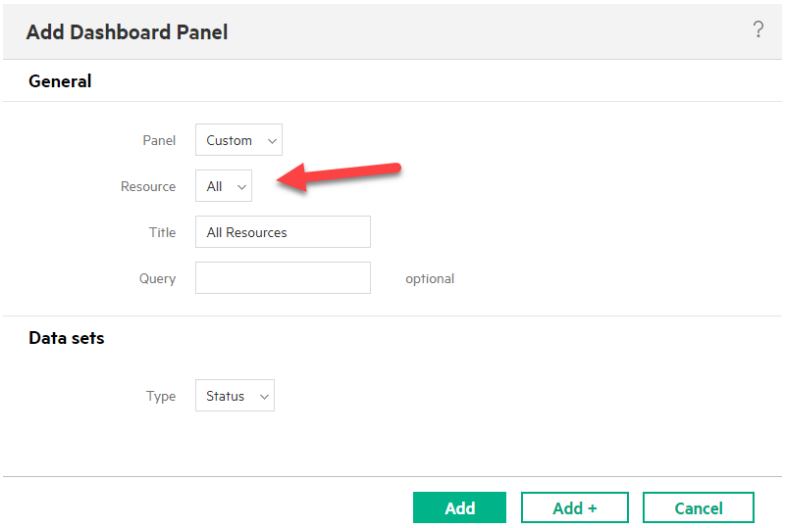
2. From the dashboard, select the *Pencil icon* to open the Dashboard Actions menu



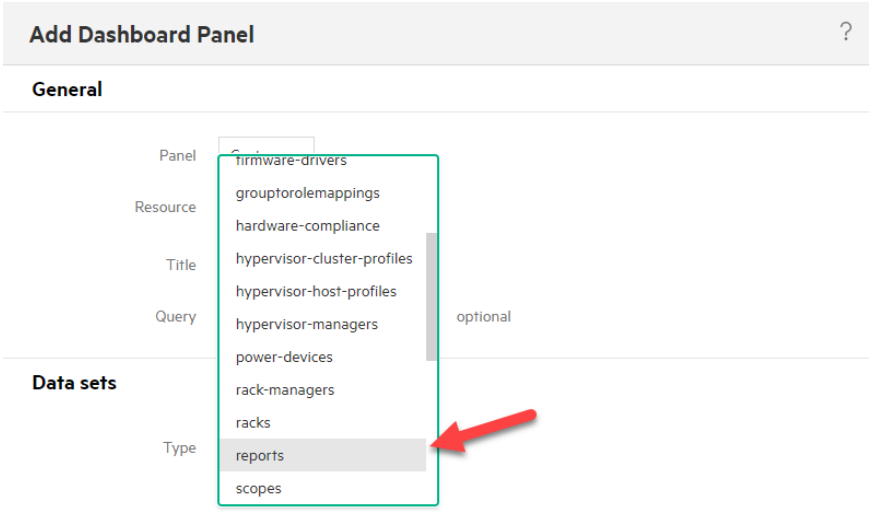
3. Select *Add* from the Actions menu



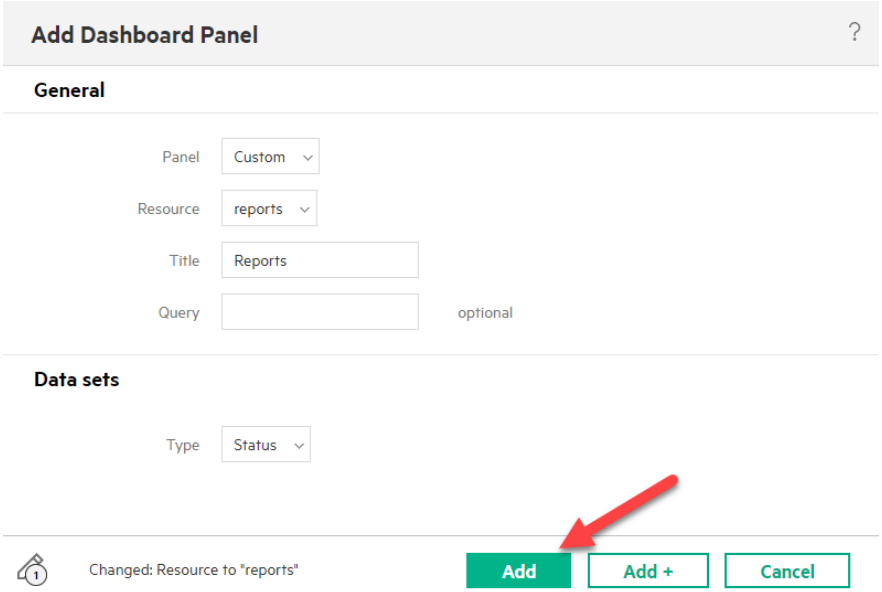
4. From the Add Dashboard Panel menu, select the information to be presented. In this example we will add a Dashboard Panel to show the reports available in HPE OneView. Click the *down-arrow* next to the resource drop-down list.



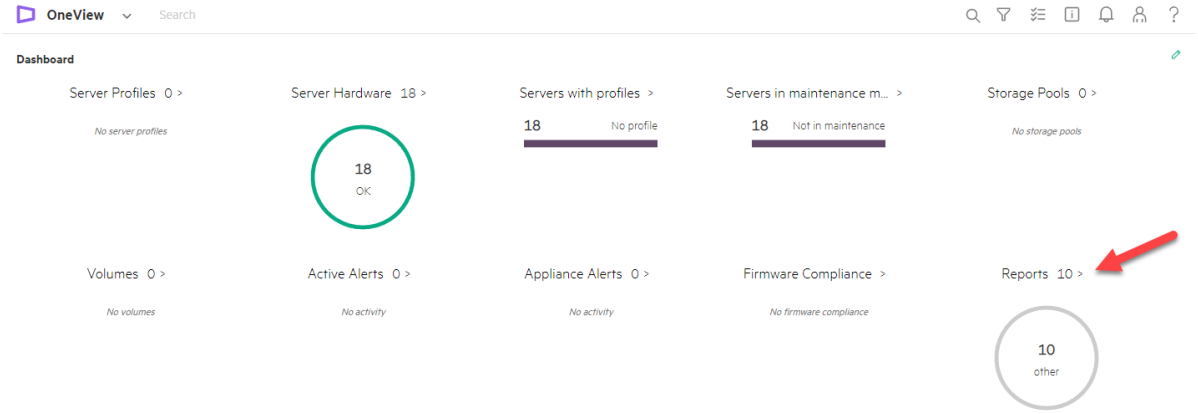
5. Scroll down the list and select *reports*



6. Click *Add*

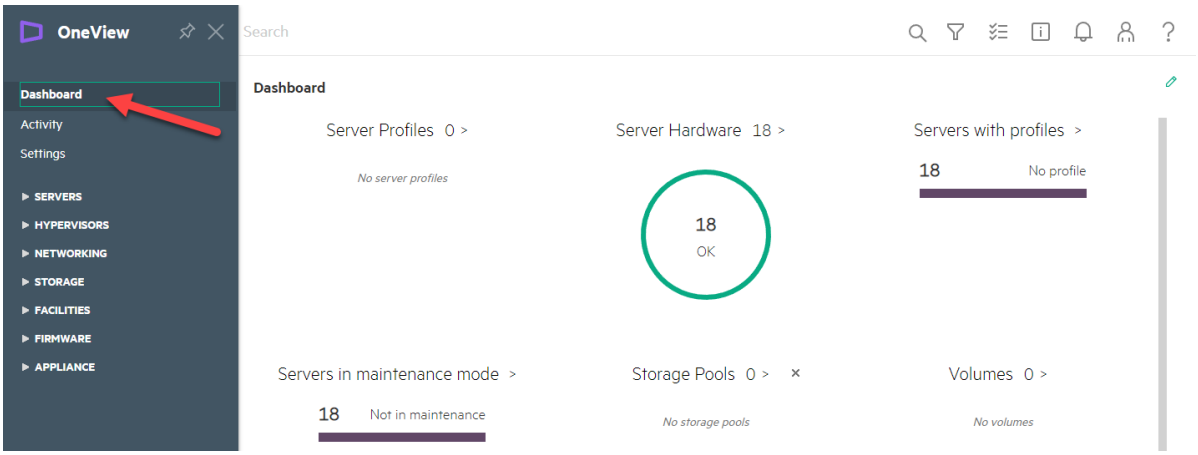


7. The Reports Dashboard panel is now available.

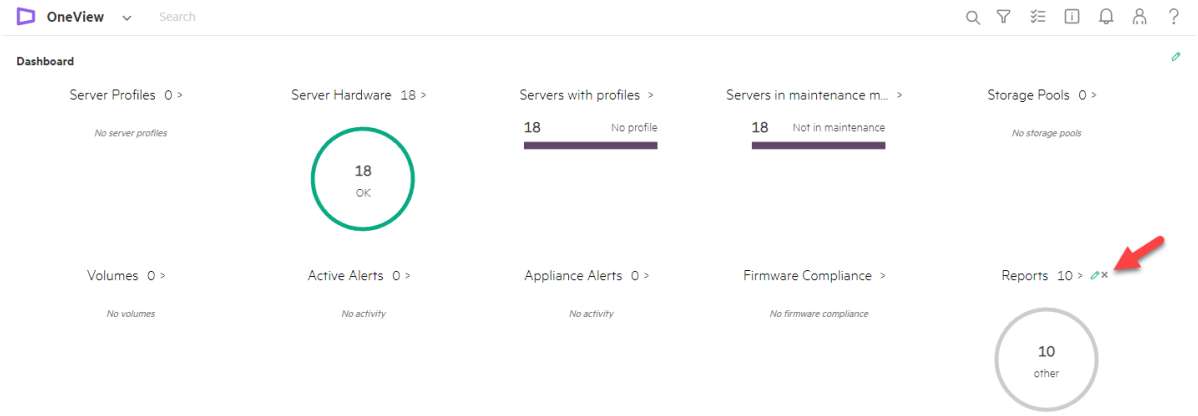


Removing a Dashboard Panel from the HPE OneView Dashboard

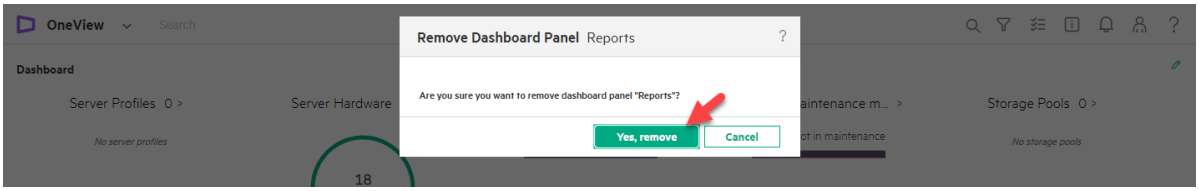
1. From the Top-Level Menu, select *Dashboard*



2. Hover your mouse over the item to be removed and an *X* will appear



3. To remove the item, click on the *X*.



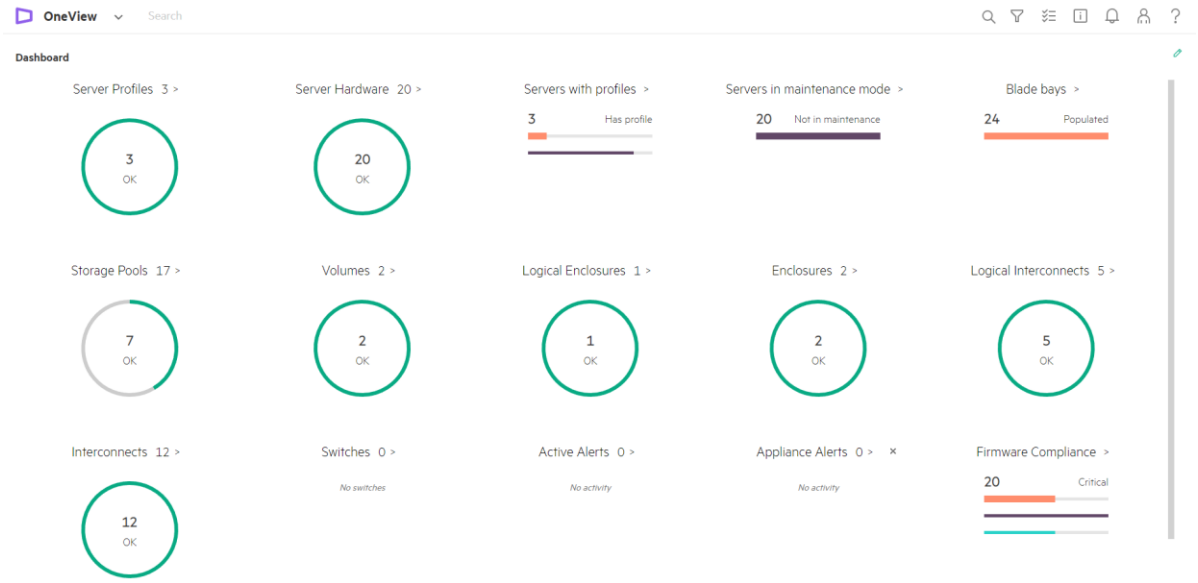
4. The item is removed from the dashboard

Alerts and Monitoring

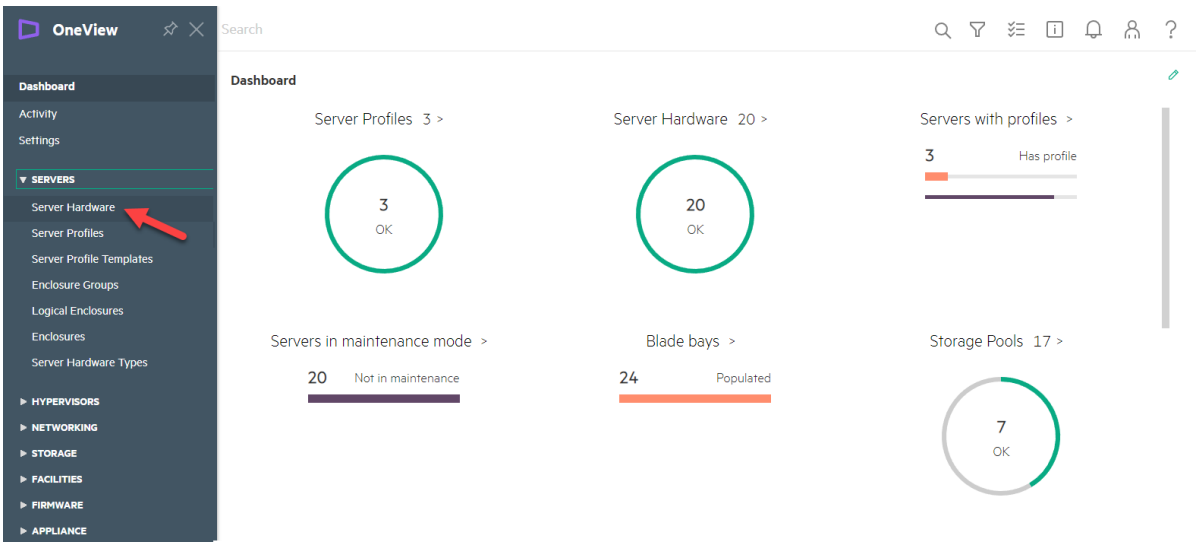
Prior to physical and power delivery configuration, HPE OneView provides a Utilization panel where a summary of the current usage of each metric available for a resource can be monitored. Each type of resource provides specific metrics that are collected from the management processor and displayed. The values depicted provide the value of the metric during the most recent five-minute period.

Having configured the physical and power delivery topology of your environment, you can now begin to monitor and analyze its use of power and cooling resources. Power utilization monitoring allows you to identify and eliminate areas of waste while thermal monitoring helps reduce overcooling and fix hot spots.

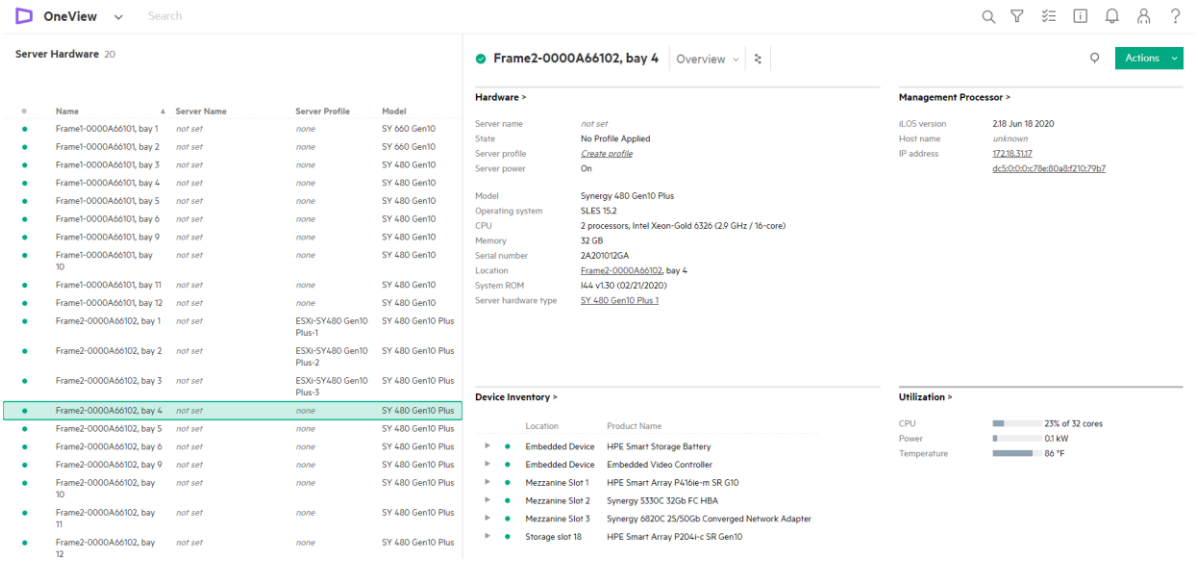
1. The *Dashboard*, which is the default view when logging into the appliance, provides an overview of activity and alerts.



2. From the top-level menu, expand the *SERVERS* option and then select *Server Hardware*



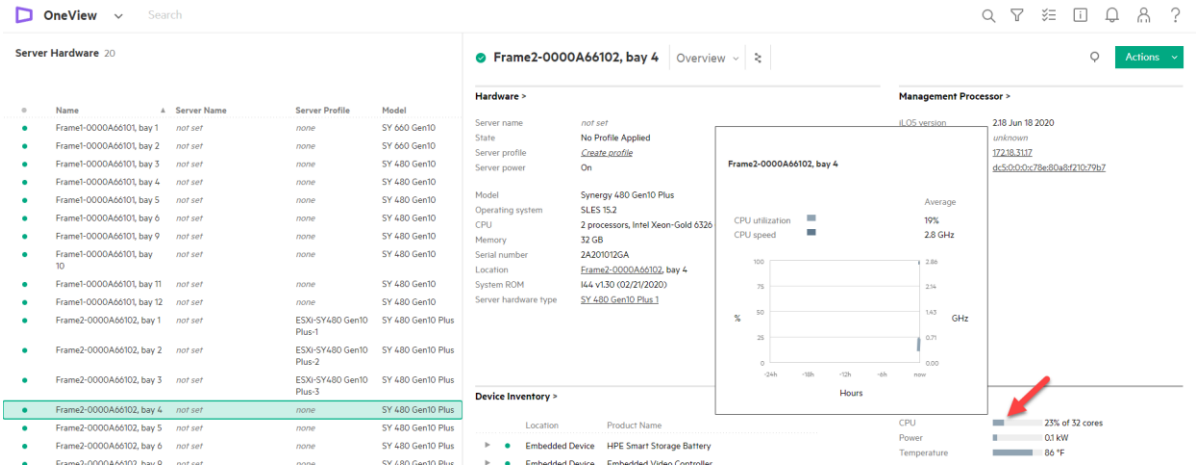
3. Select the desired hardware resource from the menu.
4. The Utilization panel located within the details pane shows the metrics available for monitoring for the resource. The utilization metrics available to be monitored depends on the resource type:
   - Server hardware: CPU, power (including power cap) and temperature
   - Enclosures: power and temperature (Synergy Frame)
   - Power Delivery Devices: power



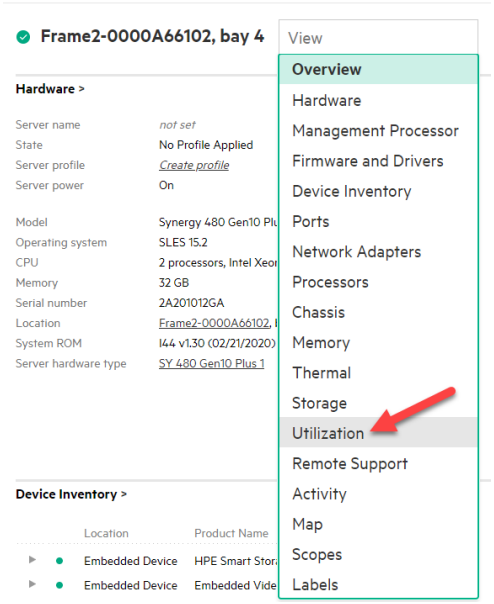
Note:

If you wish to change the temperature and size parameters to be displayed in a localized fashion, you must set the default Language in your browser for HPE OneView to display them correctly.

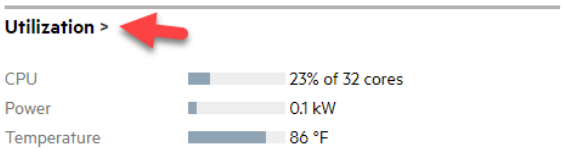
5. Flyovers showing the past 24 hours' worth of CPU, Power or Temperature data are available by moving the pointer over the desired metric.



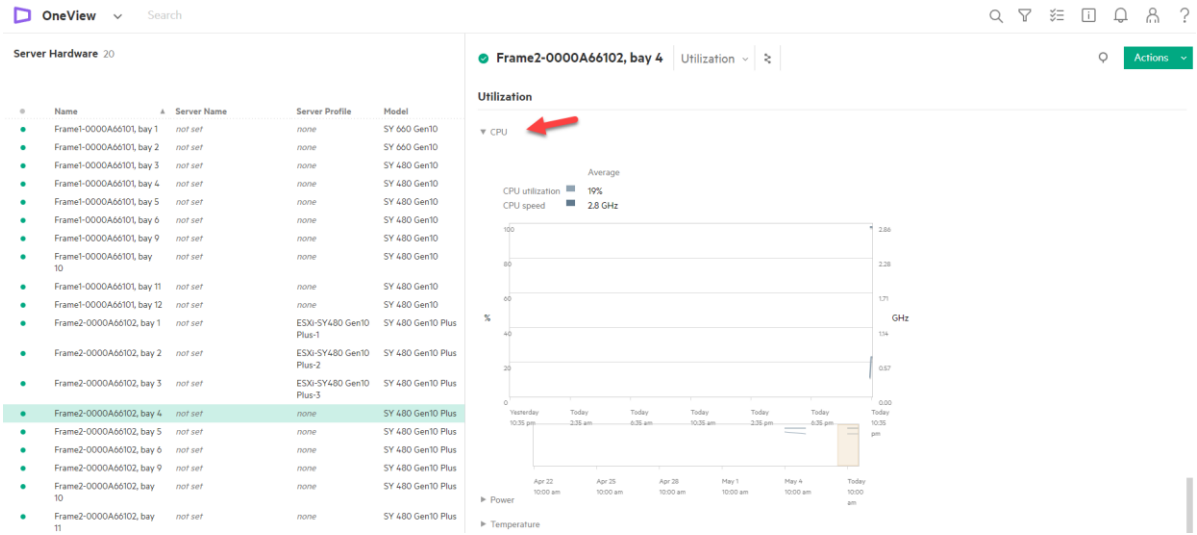
6. Selecting the *Utilization* panel heading or selecting Utilization from the view menu allows display and navigation of all available history of a specified metric.



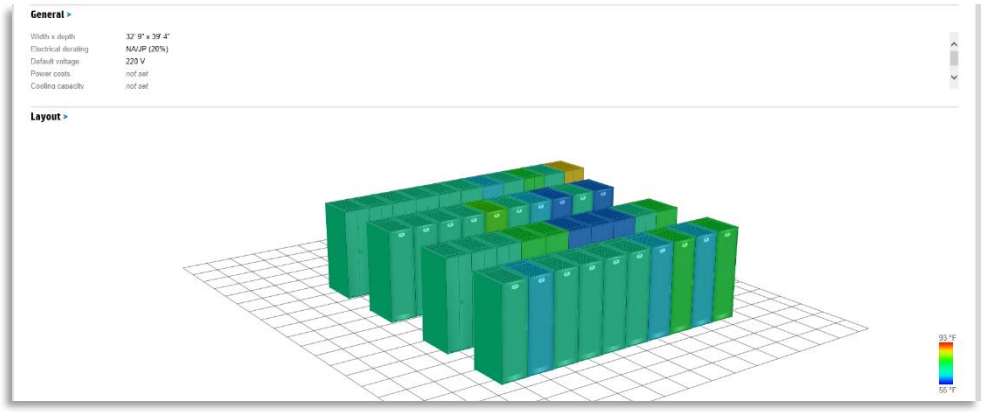
OR



7. Once selected, the details pane will show the first available metric for the device expanded. By default, the last 24 hours of information is shown on the graph. However, the date bar below the graph allows selecting any available date range to be displayed.



8. HPE OneView allows you to view areas in your data center that are insufficiently cooled due to various reasons such as poor airflow, concentration of excessive heat output, or wrap-around airflow at the ends of aisles. Likewise, it is possible to determine areas that are being overcooling and wasting cooling resources. HPE OneView's 3D visualization of the data center shows the peak observed temperature of each rack the last 24 hours.

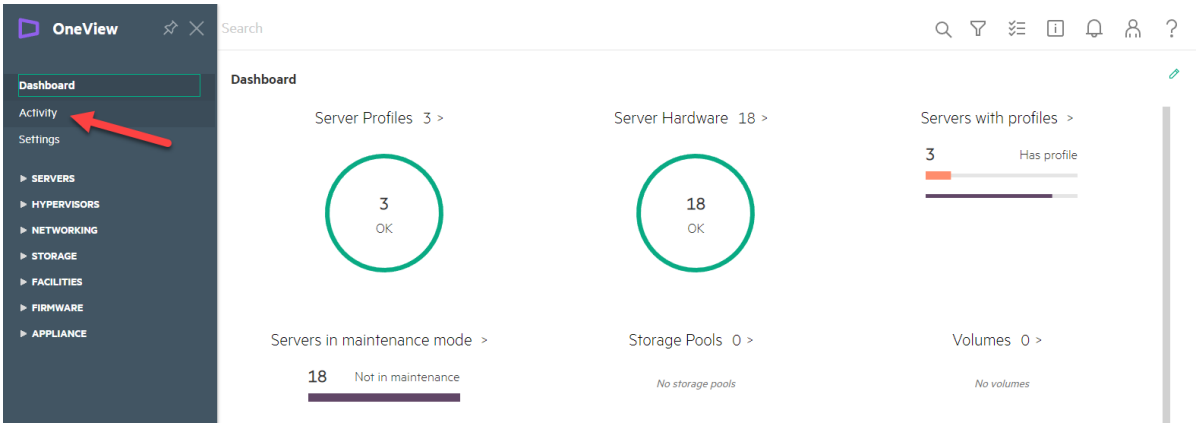


Viewing Activity, Alerts and Tasks

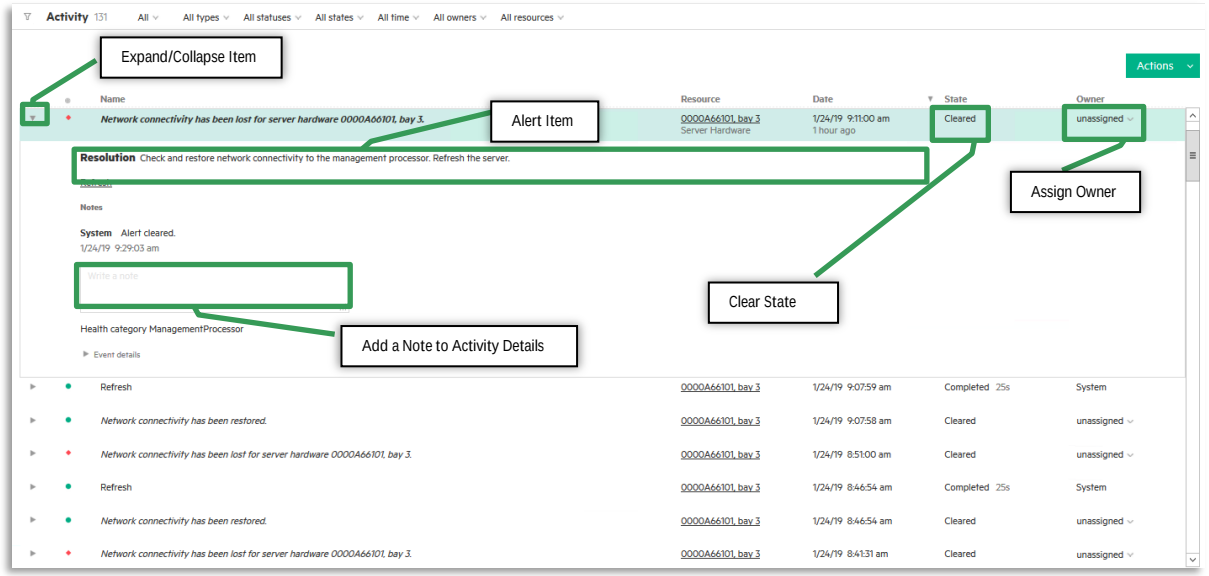
Various health alerts are recorded regarding the lifecycle management of your data center and IT equipment. This capability enables you to be notified of events that may arise such as:

- Create / Delete / Modify Networks
- Firmware Update
- Pre-Failure warnings
- Uplink Status of Logical Interconnects
- New potential overload conditions precipitated by addition of new hardware
- Thermal capacity of devices in rack exceeds specified thermal limit
- Lack of power delivery redundancy to devices attached to power delivery devices

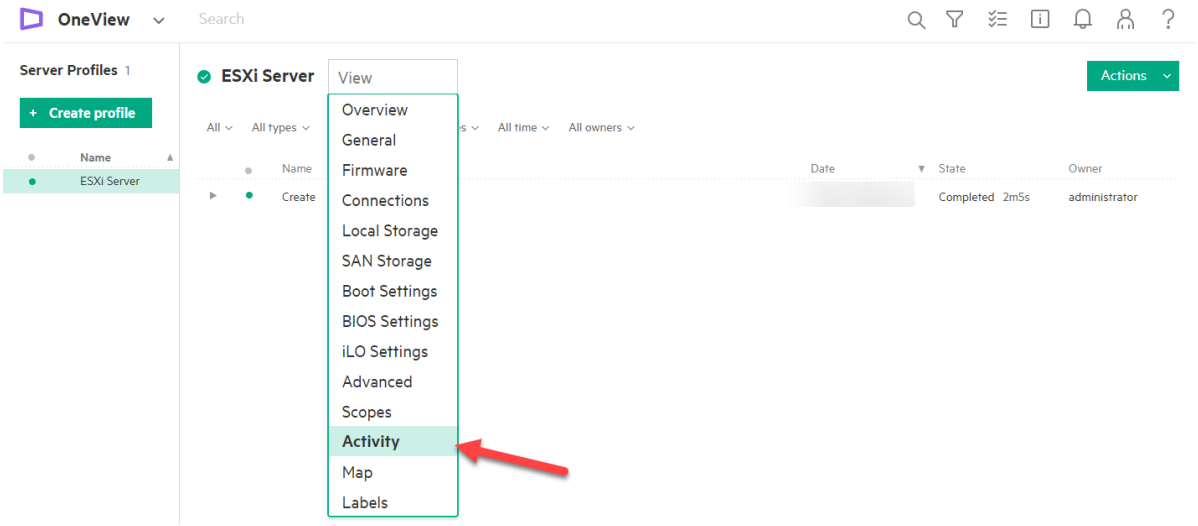
1. From the Top-Level Menu, select *Activity*.



2. This page is the list of all activity within the appliance.



3. You can also expand the hardware resource (Server Hardware, Server Profile, Enclosure, Logical Interconnect, etc.) and look at the alert view to see the problem description. The details from the alert can most times be used to identify and help fix the problem.

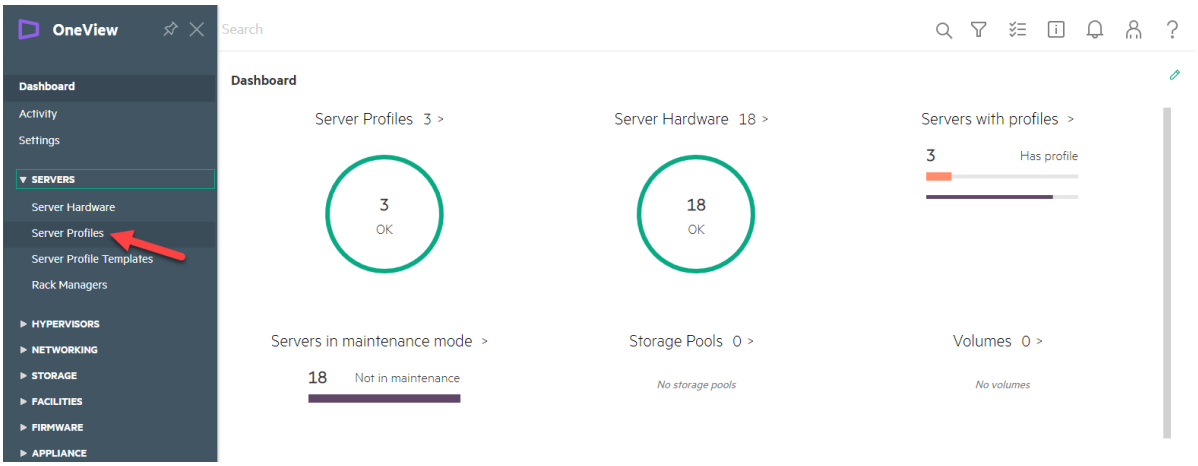


Multi-use Commands

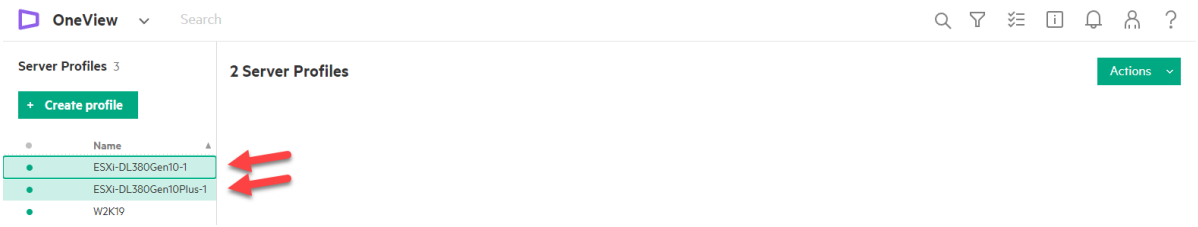
When making some changes or issuing some commands, it is possible to send those commands to multiple entities at one time. In this example we will power multiple servers on at once.

Issuing the Power On Command to Multiple Servers

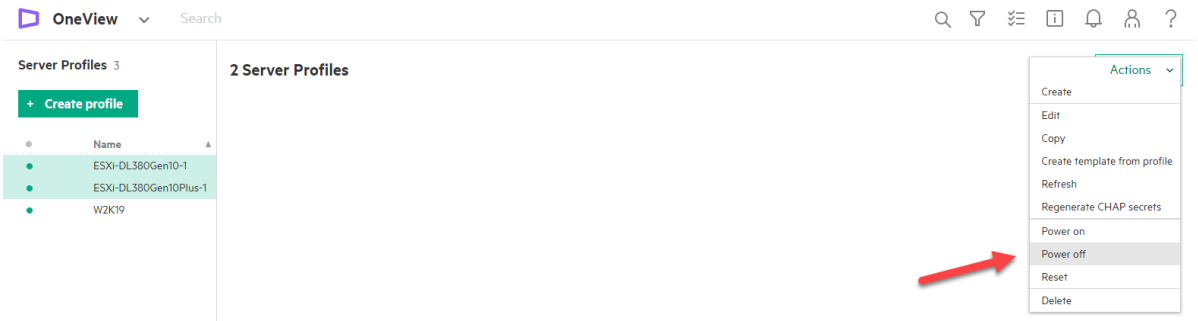
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



2. If the column, select the server profiles that you would like to manage. To select multiple items, hold down the *control* key while left clicking the desired server profiles.



3. From the Actions menu, select *Power off*



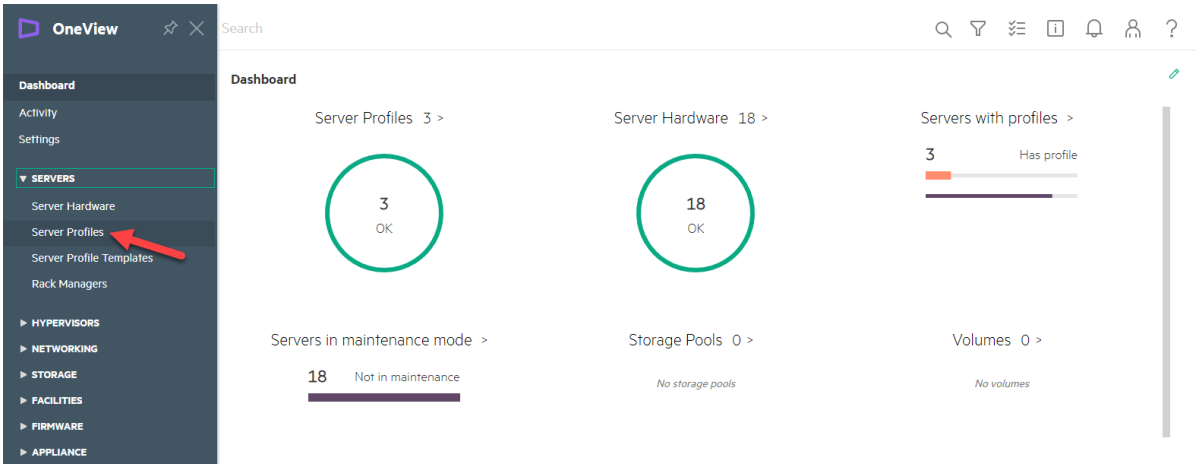
Changing the hardware for a Server Profile

Changing the hardware for a Server Profile allows the software defined server to be moved to a different piece of physical hardware. HPE OneView provides profile mobility between different adapters and different hardware generations. Server profiles can also be moved across enclosure groups (managed by the sane OneView instance or Synergy Composer).

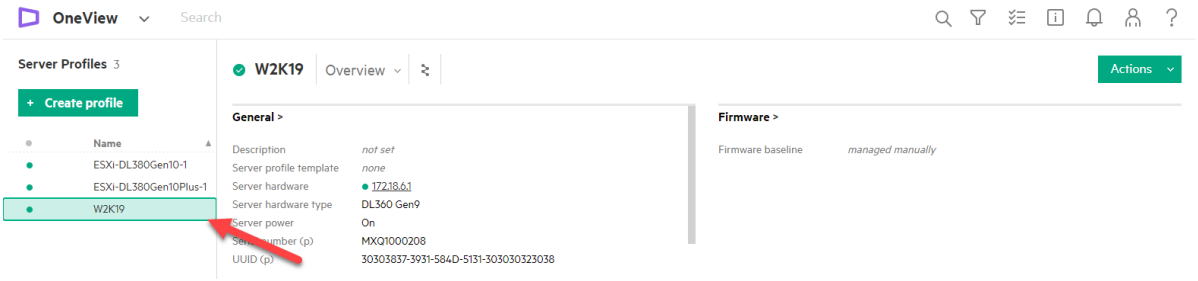
Server profiles using shared DAS local storage can be migrated within the enclosure containing the local storage drives (Synergy only), and the drives will follow the server profile on migration.

Server profiles using SAN storage can be migrated to any supported server with access to the SANs being used to access the volumes and the volume attach configuration will follow the server profile on migration.

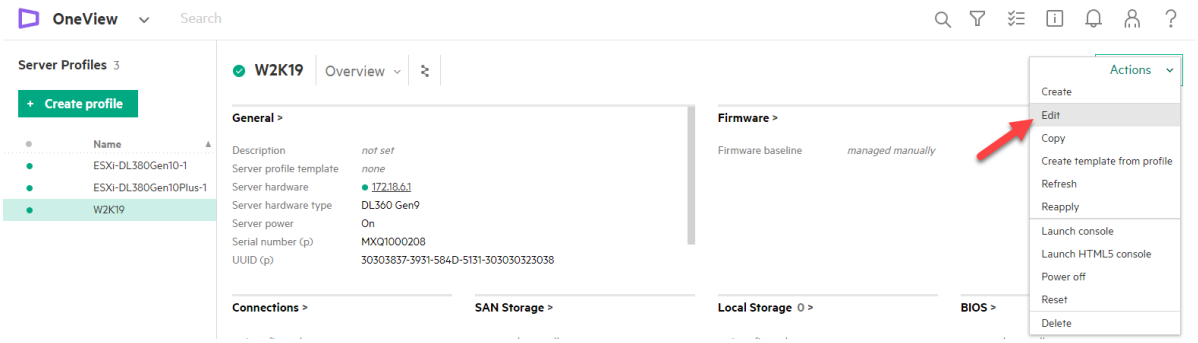
1. From the Top-level menu, expand the *SERVERS* option and then select *Server Profiles.*



2. Select the server profile to be changed.

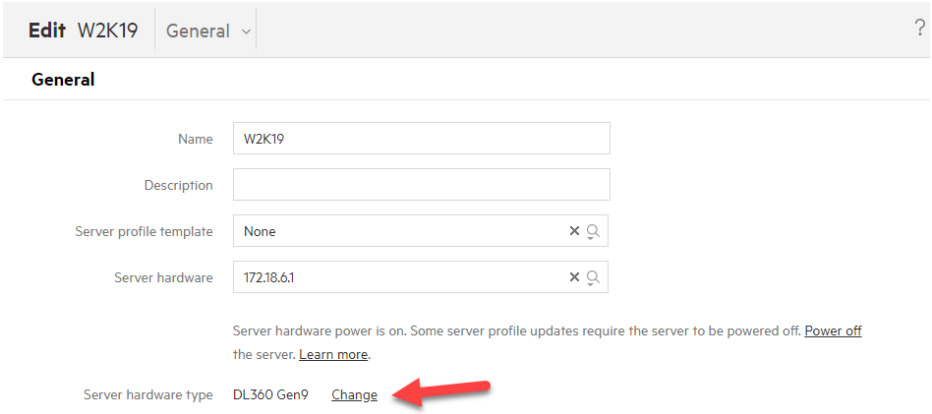


3. From the Actions menu, select *Edit*

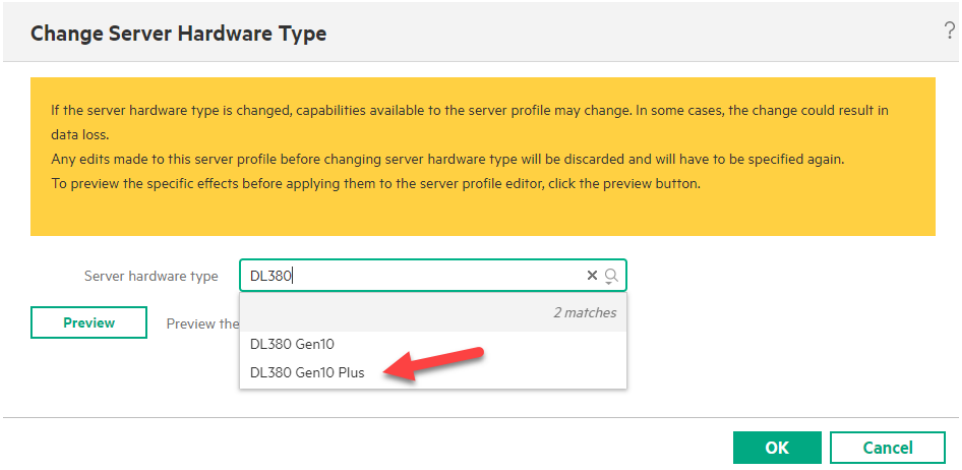


4. The profile can be changed by editing either the specific *Server Hardware* bay assignment, by changing the *Server Hardware Type* and then selecting the *Server Hardware Bay Assignment* or by changing the *Enclosure Group (Synergy only).* Click *Change* next to either *Server hardware type* or *Enclosure Group (Synergy only)*

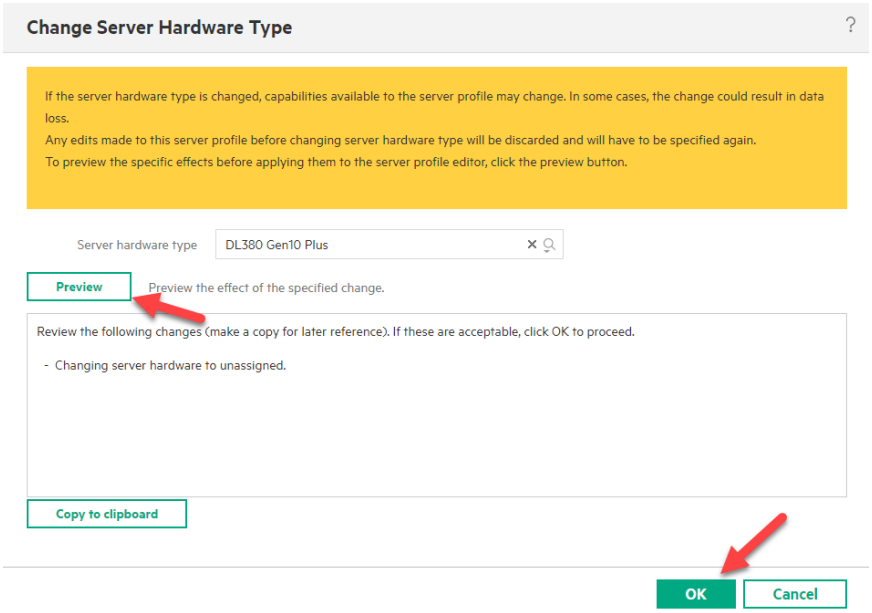
5. From the Change Server Hardware Type and Enclosure Group dialog box, select the drop-down for the type of profile mobility needed. For example, select the *Change* next to *Server hardware type*.



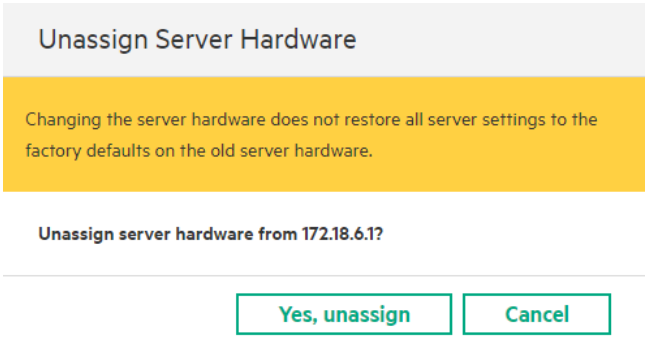
6. From the dropdown list, select the desired *Server hardware type*



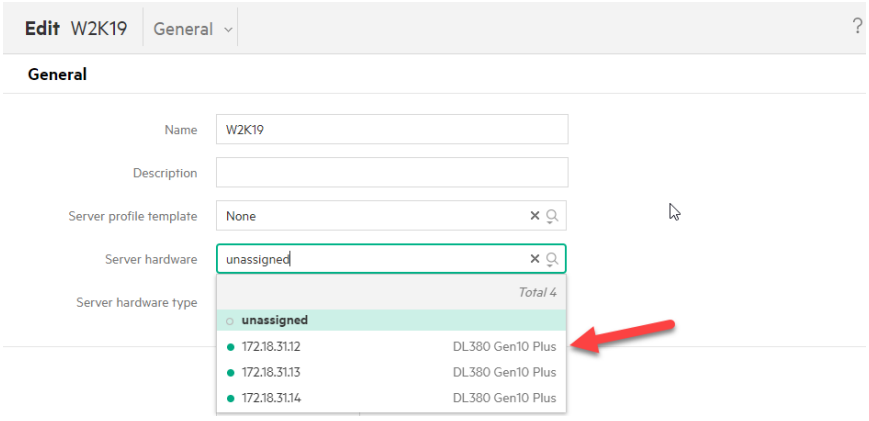
7. You can *Preview* what the Server hardware type change will do and then if acceptable then Click *OK*



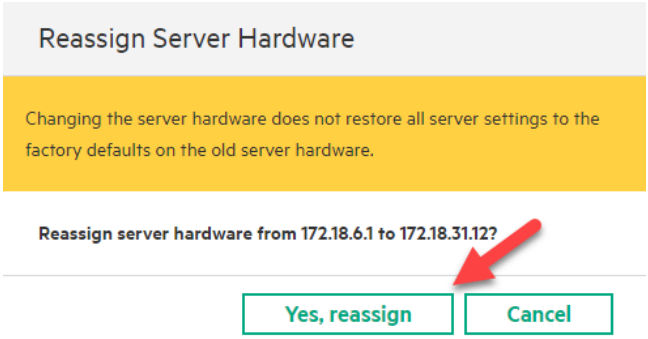
8. If the server profile is still assigned to hardware agree to unassign the hardware.



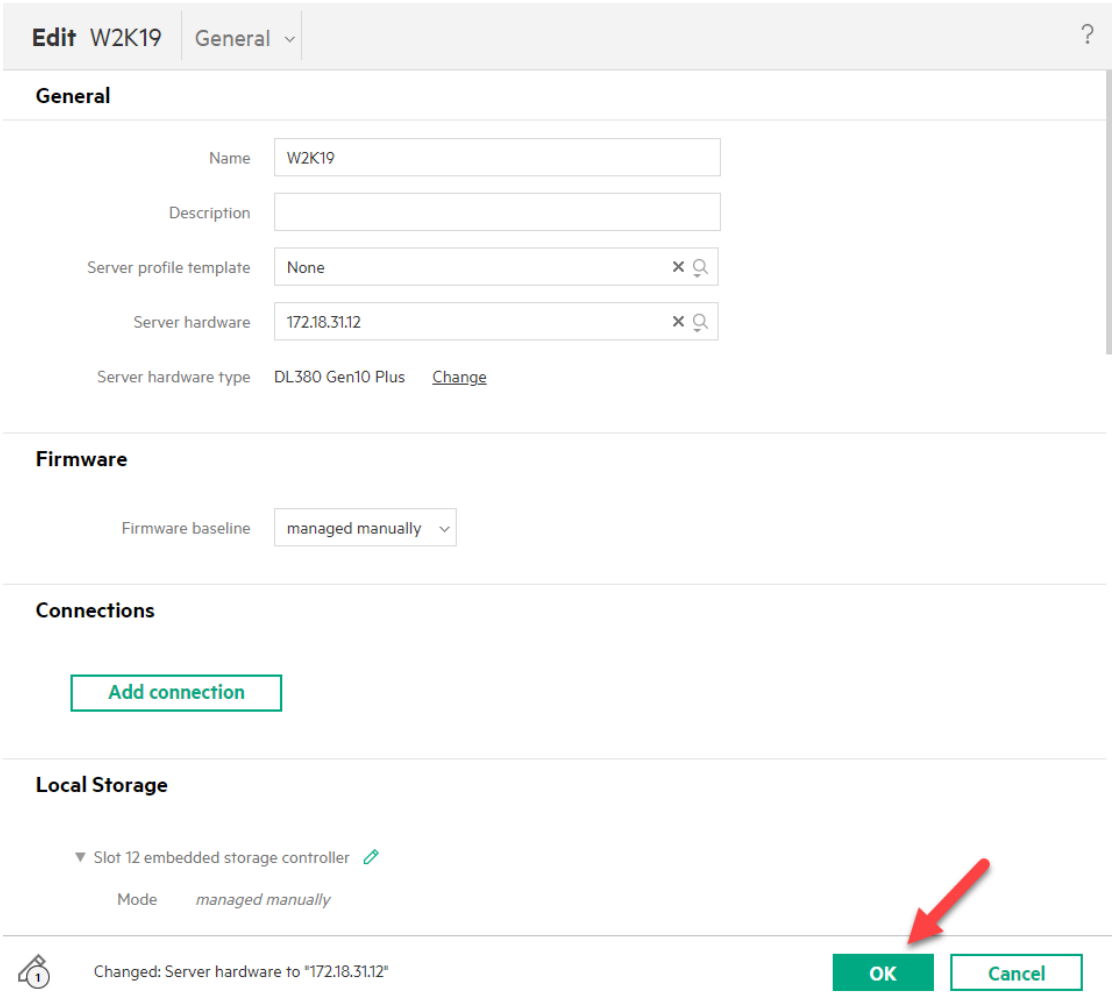
9. Using the *Server hardware* drop-down list, select the device bay that the server profile will be moved to



10. You will now see the following message to reassign the profile to the new hardware and if acceptable click *Yes, reassign*.



11. Click *OK* to begin the profile migration



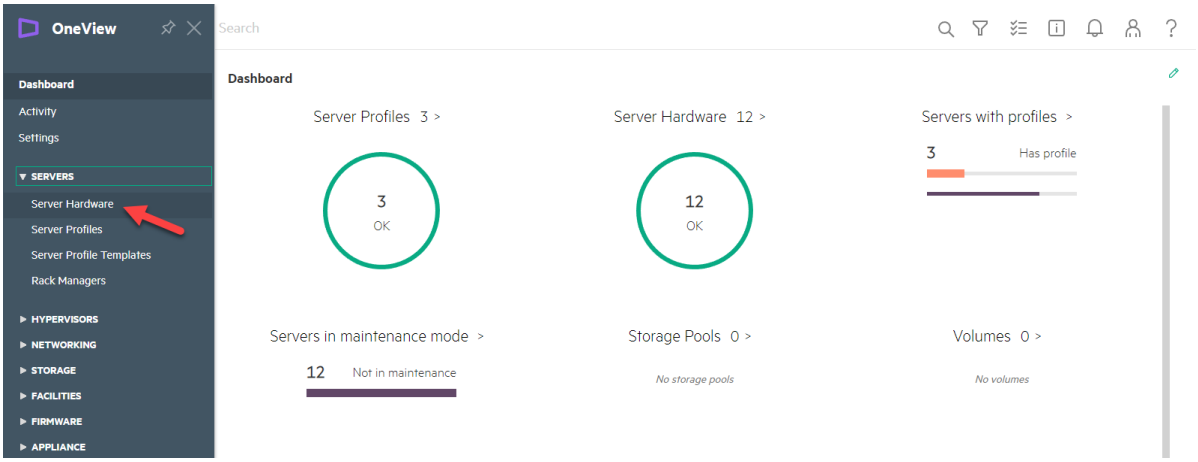
Putting a Server in Maintenance Mode

Performing routine maintenance operations on servers causes many events to be generated on the associated server hardware resource and server profile. If notification features are enabled, the events cause many email notifications and forwarded SNMP traps to be sent. While the maintenance activity is in progress, you might not want to receive all the notifications.

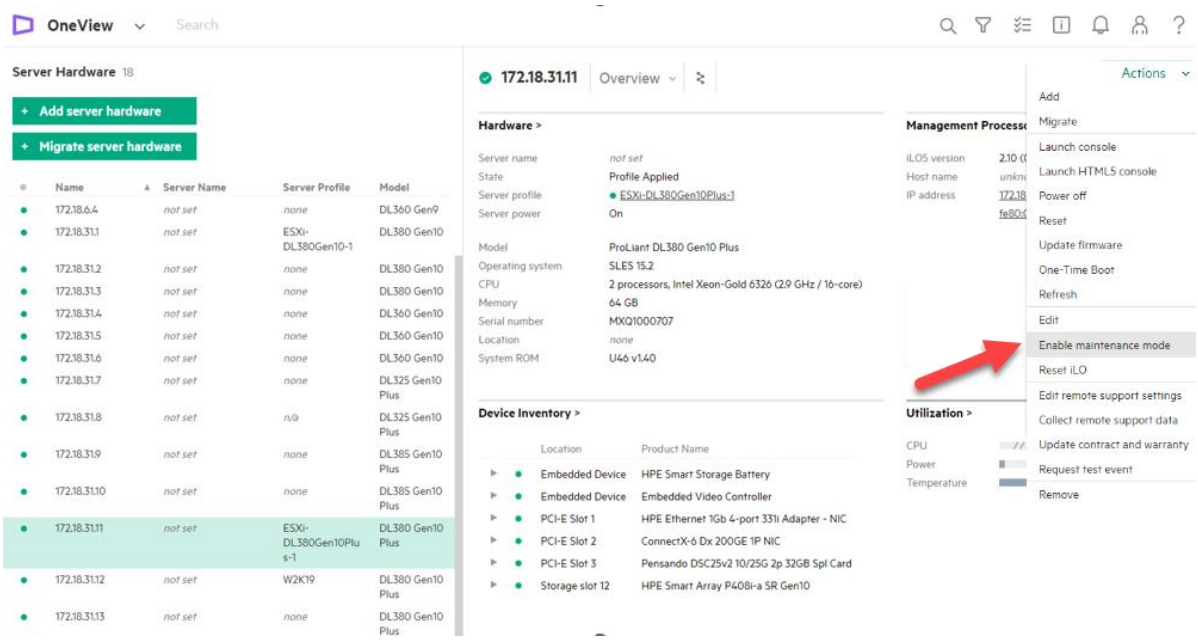
Enabling server maintenance mode prevents the appliance from sending any email notifications or forwarding any SNMP traps that are related to the server hardware and its associated profile. While the notifications are blocked, maintenance mode does not affect normal server or profile operations, and all events generated on the server are seen on the HPE OneView appliance UI.

Disabling maintenance mode causes email notifications and SNMP trap forwarding to return to normal. No attempt is made to send any events that occurred during the maintenance mode. However, if there are any active alerts when maintenance mode is disabled, a single event will be sent, alerting that the server has events that require attention.

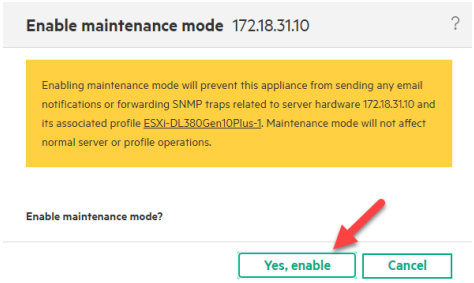
1. From the Top-level menu, expand the *SERVERS* option and then select *Server Hardware*.



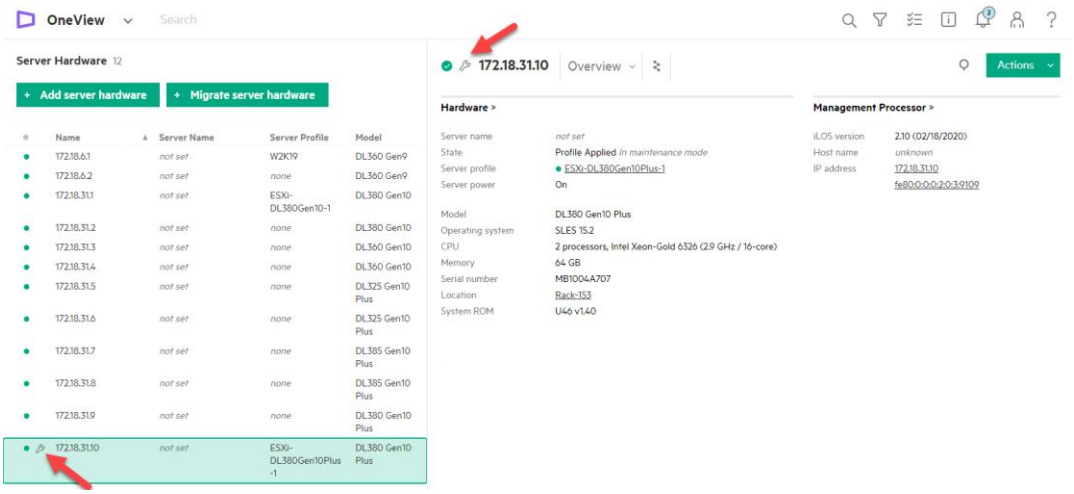
2. Select the Server that you want to put into maintenance mode, choose the *Actions* menu and select *Enable maintenance mode*.



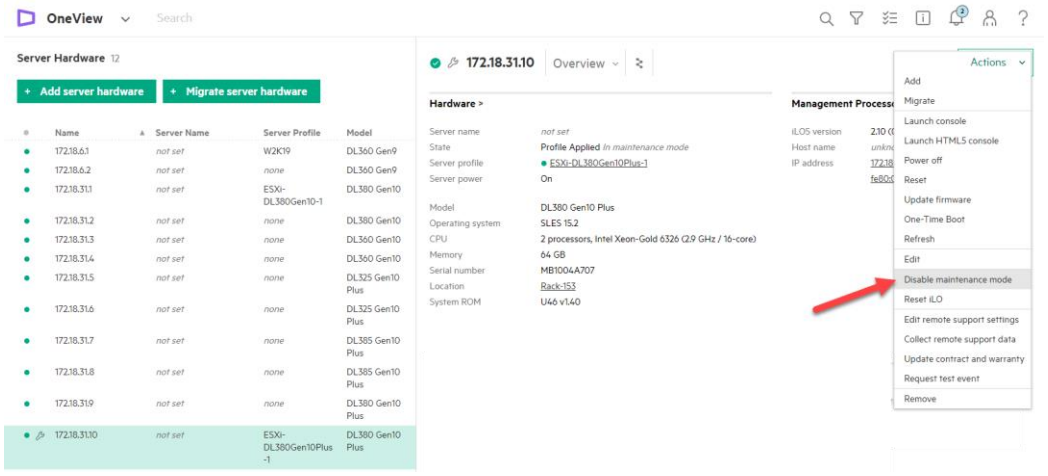
3. To Enable Maintenance Mode you must click on *Yes, enable*



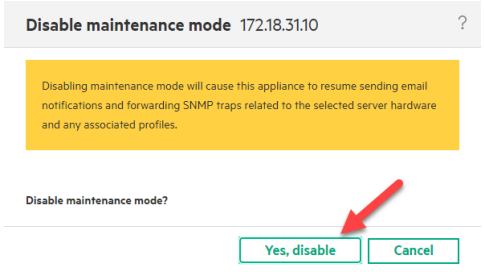
4. You will now see a spanner icon next to the Server that has been placed in maintenance mode.



5. Once the issues have been resolved for the Server you can then disable maintenance mode in order to return the Server back to reporting any errors that occur from that point onwards. Select the Server and choose the *Actions* menu and then select *Disable maintenance mode*.



6. If you wish to Disable Maintenance Mode then you can then click on *Yes, disable*. The Server will then be returned to service.



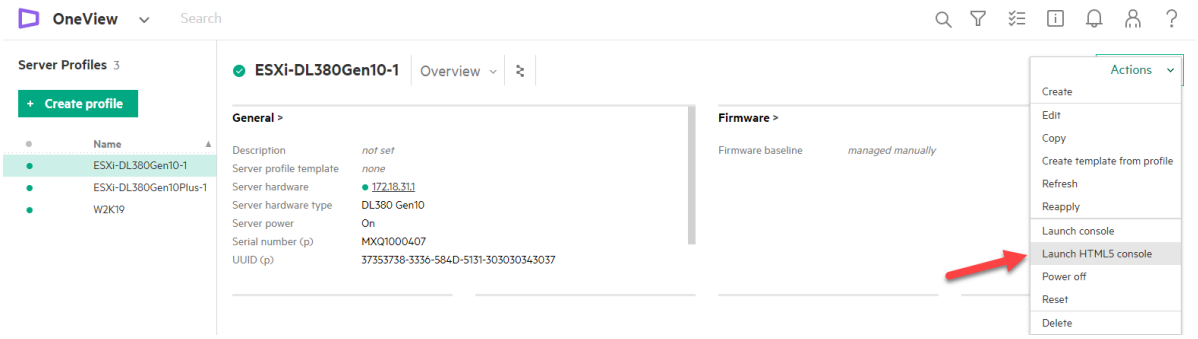
Launch HTML5 Console

With the release of OneView 5.3 a new feature was added to launch directly from within OneView, the HTML5 iLO Remote Graphic Console. This will work iLO4 or iLO5 which means that it covers all the Gen8, Gen9 and Gen10 HPE Servers.

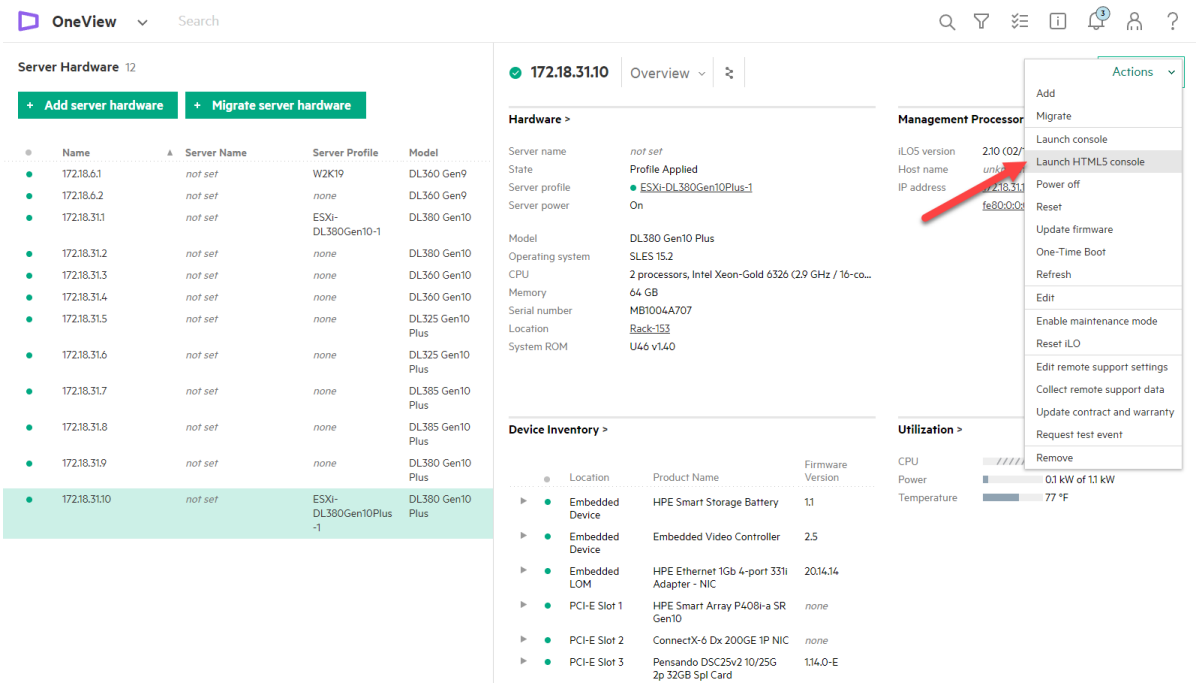
HTML5 Console for iLO4 requires a minimum firmware level of 2.70. Upgrading the iLO4 firmware to 2.70 or later will also allow the HTML5 Console to work directly in the iLO interface as well.

For iLO5, while there has been a HTML5 Console available from within the iLO interface for this feature to work in OneView directly requires iLO5 firmware 2.14 or later.

There are two locations that the HTML5 Console can be launched from within OneView for the *Servers* option under *Server Profiles* or still under the *Servers* option *Server Hardware*.

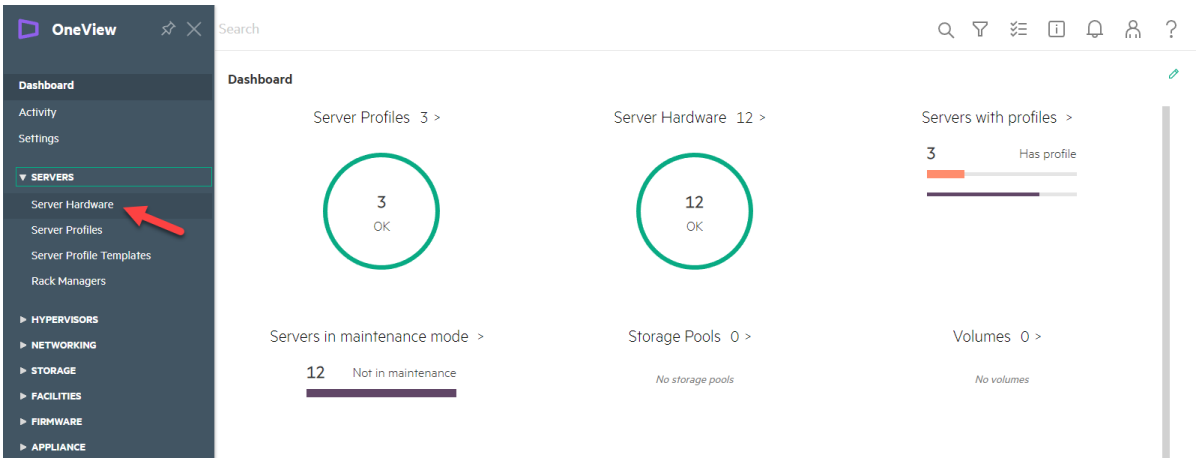


Or

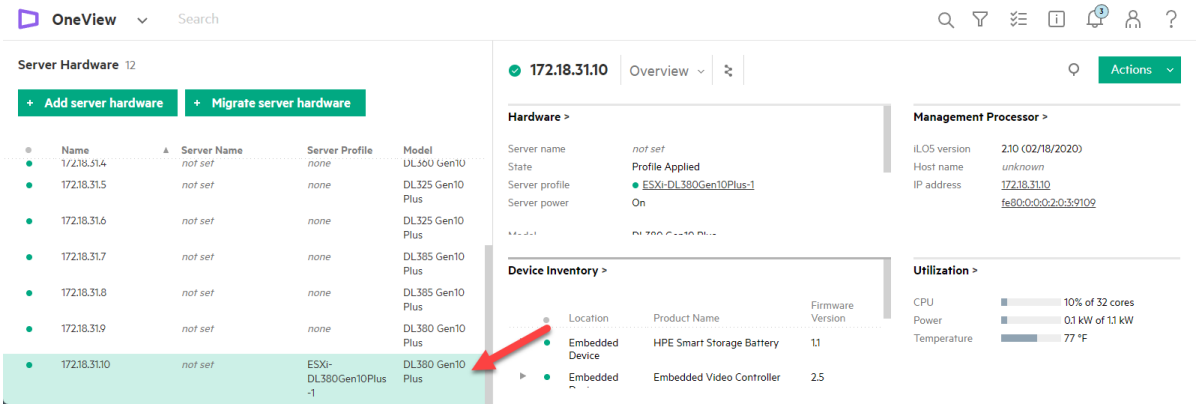


Set One-Time Boot Option on Server

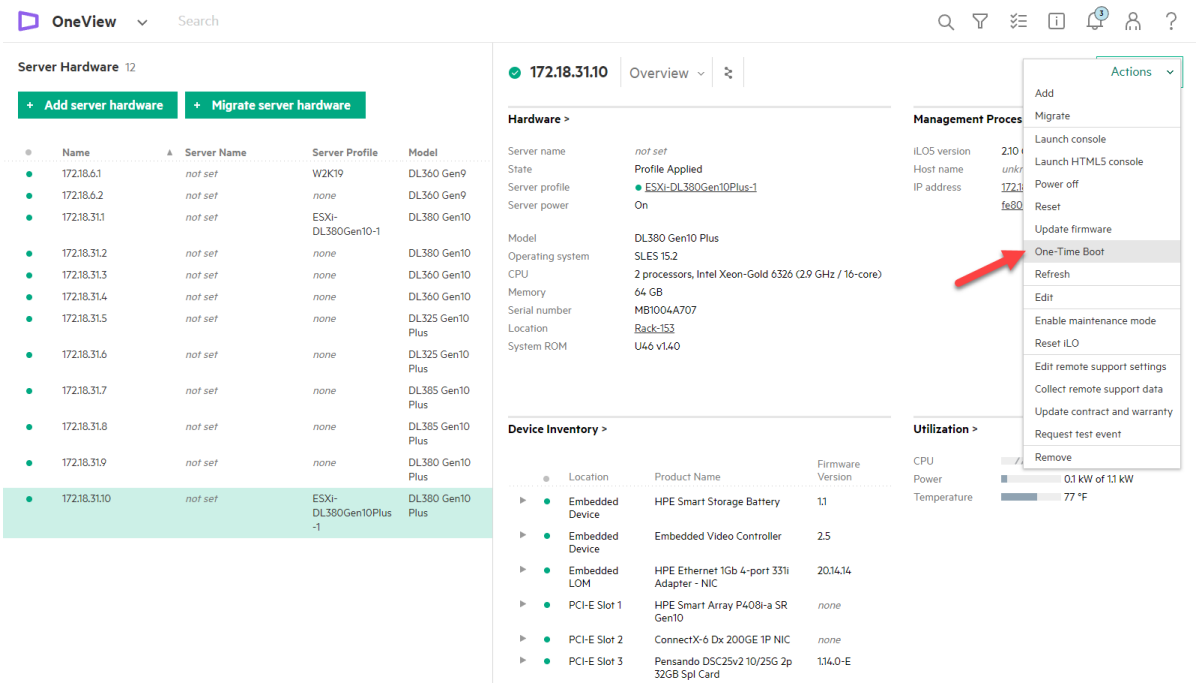
1. From the top-level menu, Expand the *SERVERS* option and then select *Server Hardware*



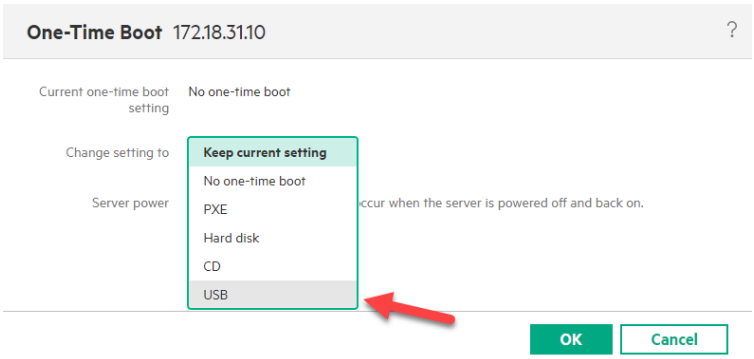
2. Select the desired server from the menu



3. From the actions menu, select One-Time Boot



4. From the One-Time Boot dialog window, select the boot mode that you need



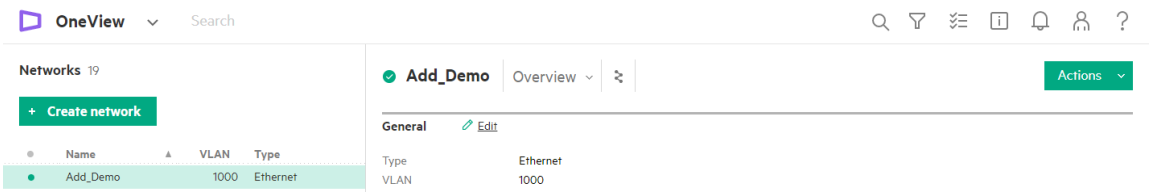
5. Click *OK*.

6. The one-time boot option will be executed the next time the server is powered off and back on again. Or if the server was powered off prior to this setting change then when it is next powered on.

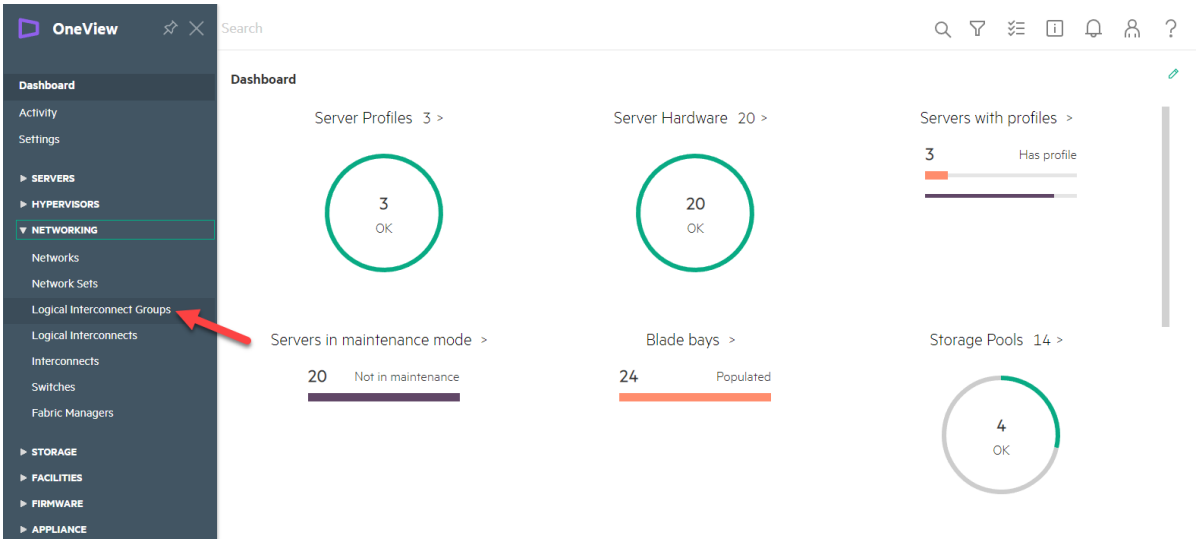
Add New Networks to a Logical Interconnect Group

You can either add a network to a Uplink Set or if there is a Network Set configured (as part of an uplink Set) then you can add the new Network to the Network Set.

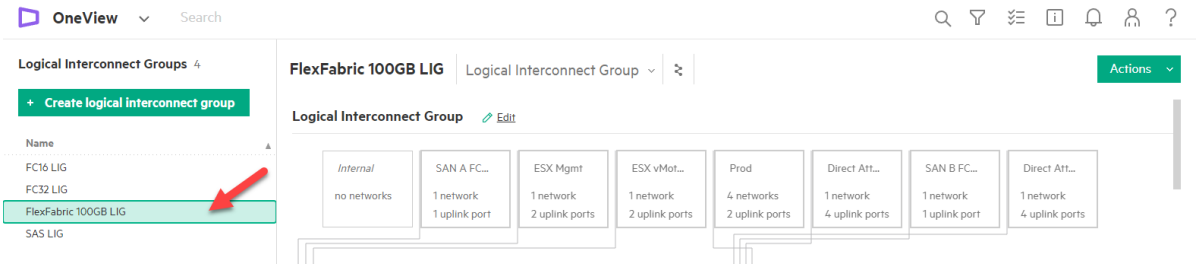
1. Create the new Ethernet network in HPE OneView. The new network is called *Add_Demo*.



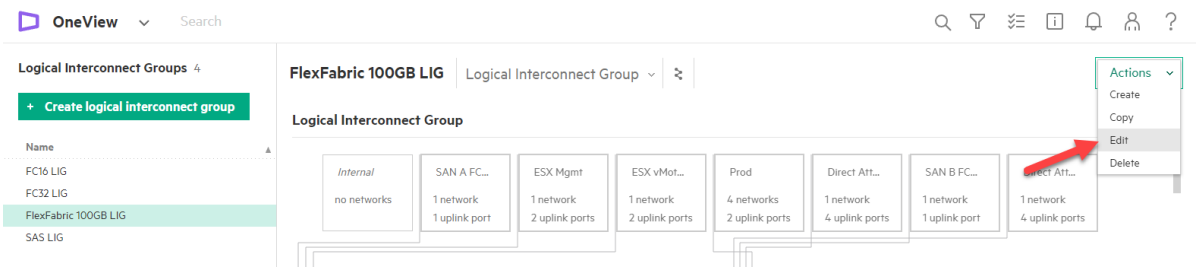
2. From the top-level menu, expand the *NETWORKING* option and then select *Logical Interconnect Groups*



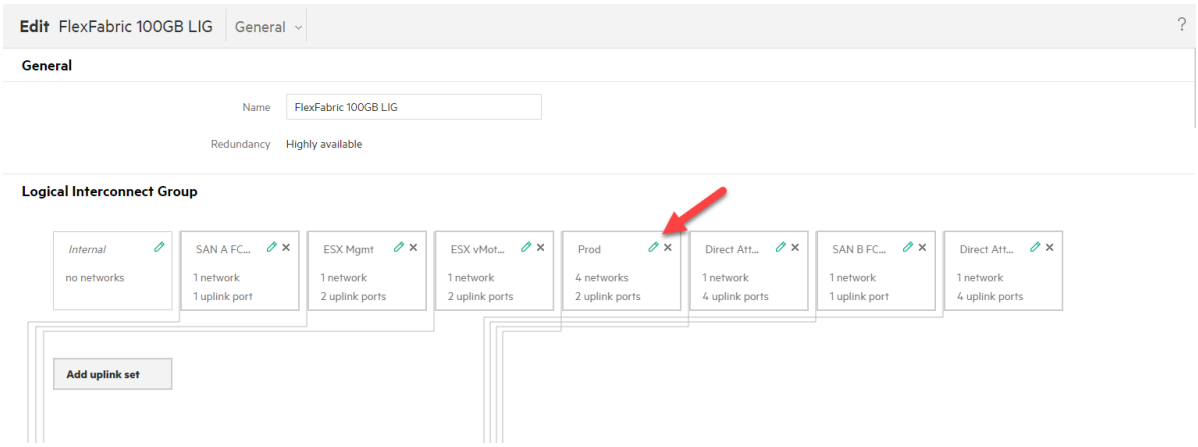
3. Select the Logical Interconnect Group to be edited from the menu



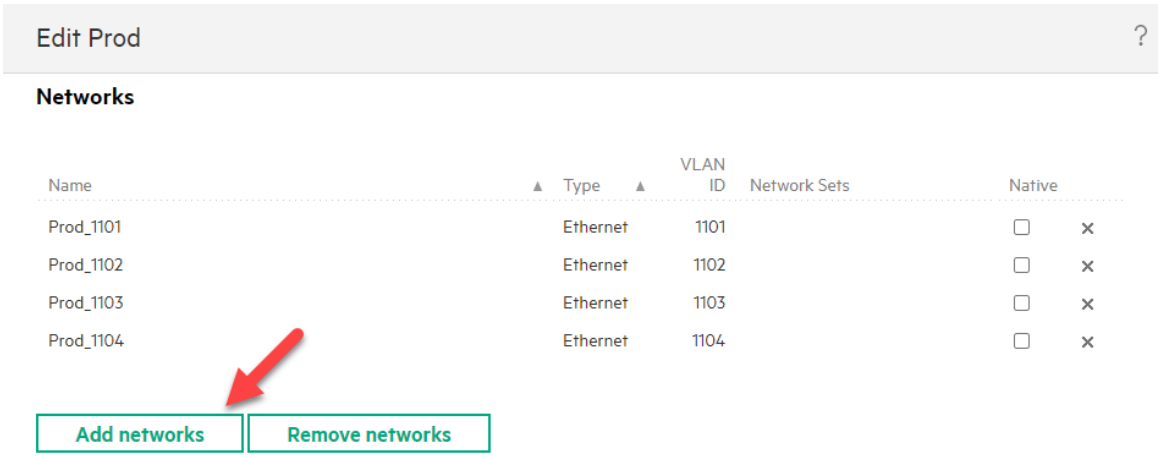
4. From the Actions menu of the Logical Interconnect Group, select *Edit*



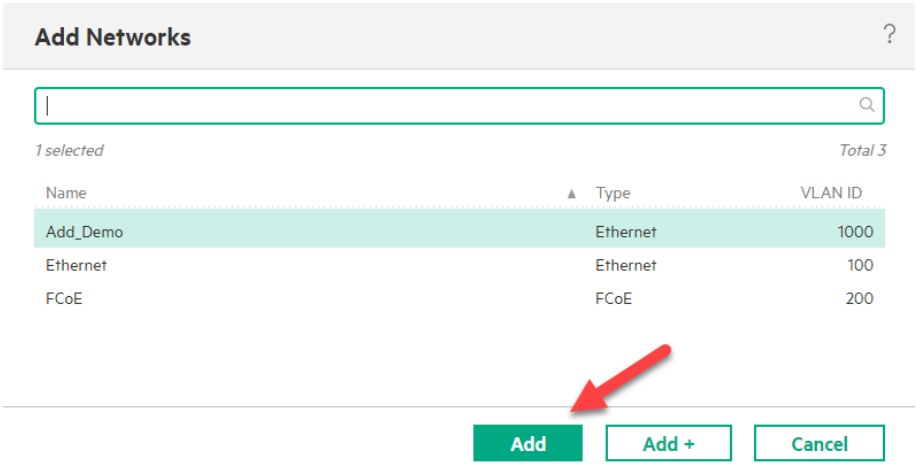
5. Select the pencil icon to add the new Network(s) to an existing Uplink Set.



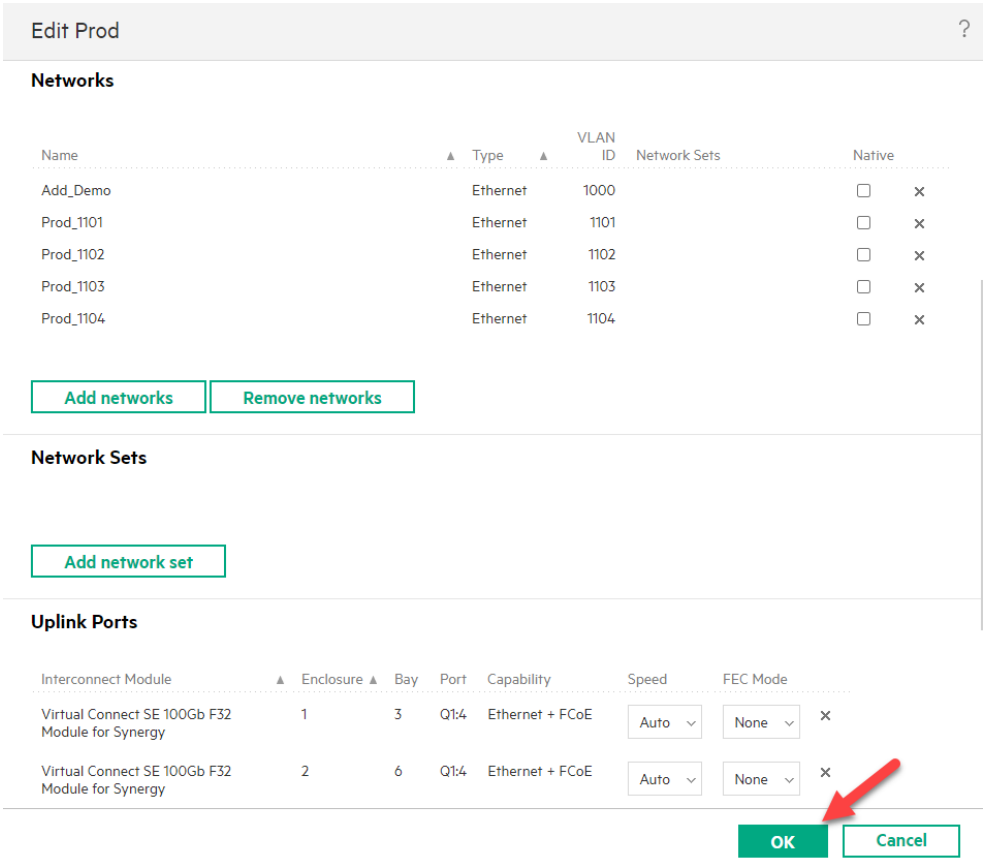
6. Scroll down to the networks section, select *Add networks*



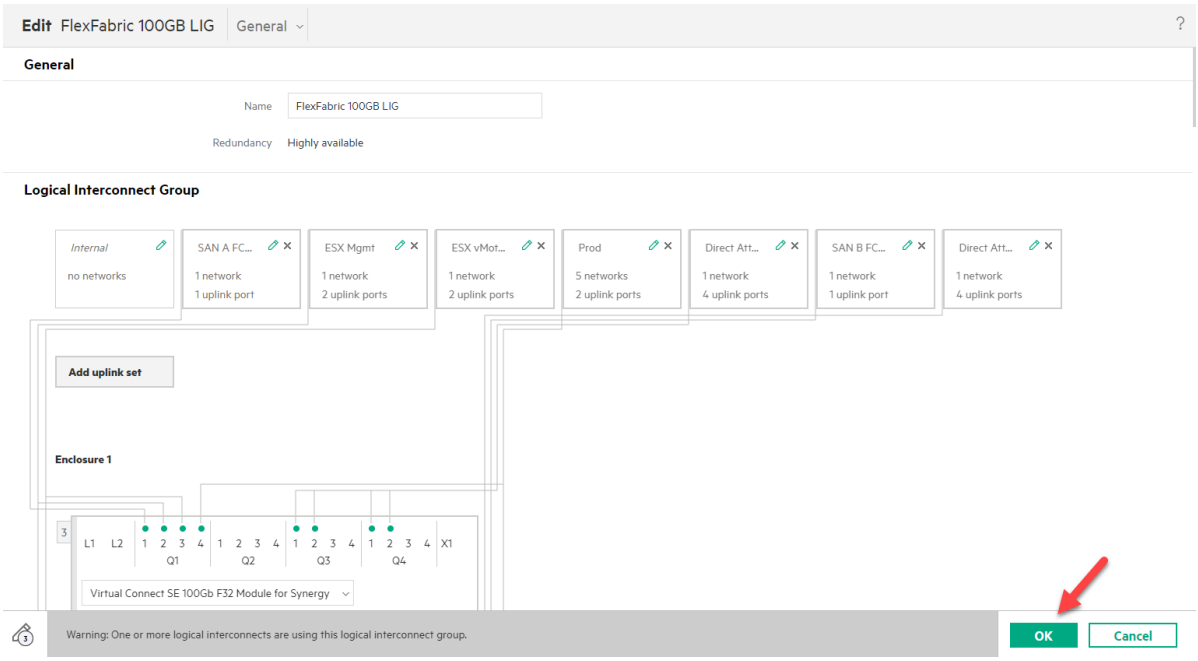
7. Select the Add_Demo network and click *Add*



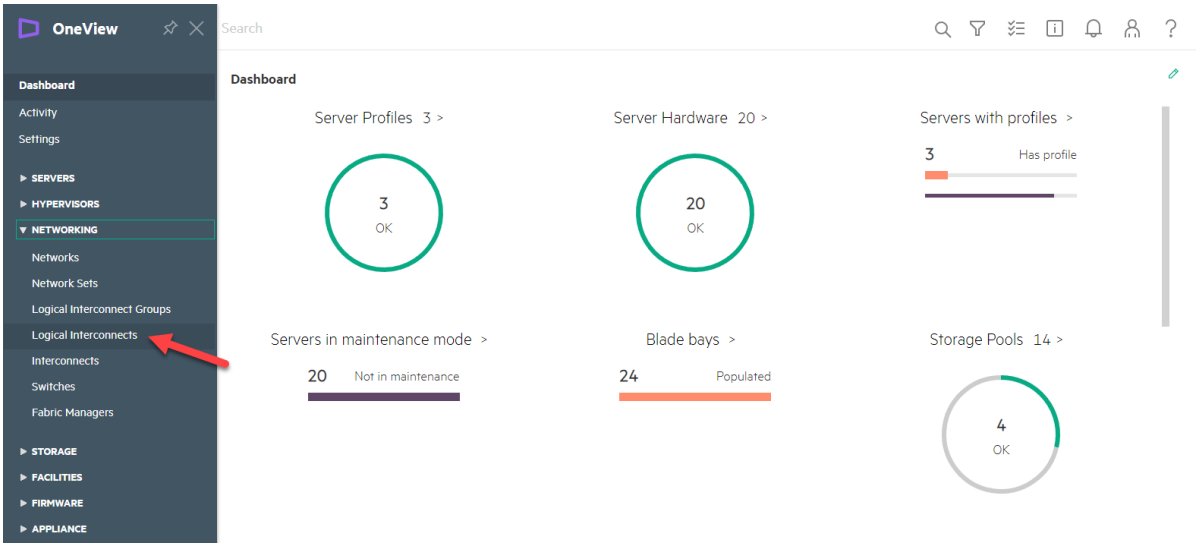
8. Click *OK* to add the network to the Uplink Set



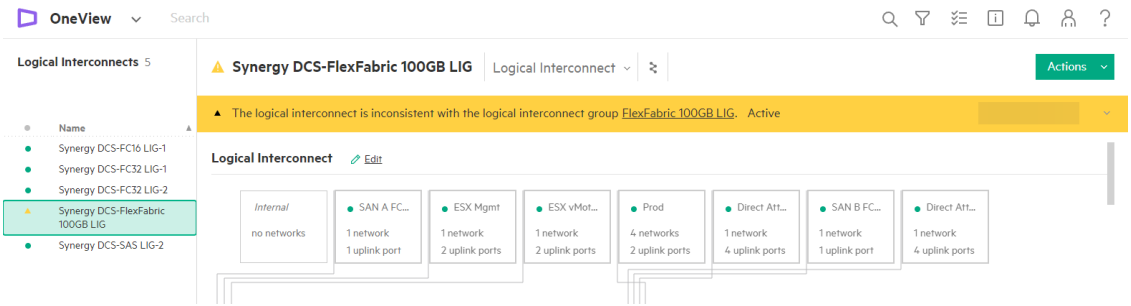
9. Click *OK* to update the Logical Interconnect Group



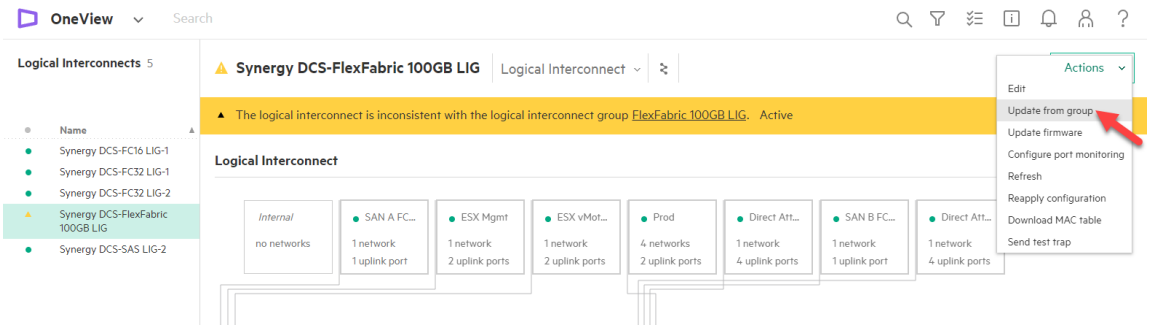
10. Now that the *Logical Interconnect Group* has been updated, the *Logical Interconnects* that were created from importing the Enclosure will report they are no longer consistent with the group. From the top-level menu, expand the *NETWORKING* option and then select *Logical Interconnects*



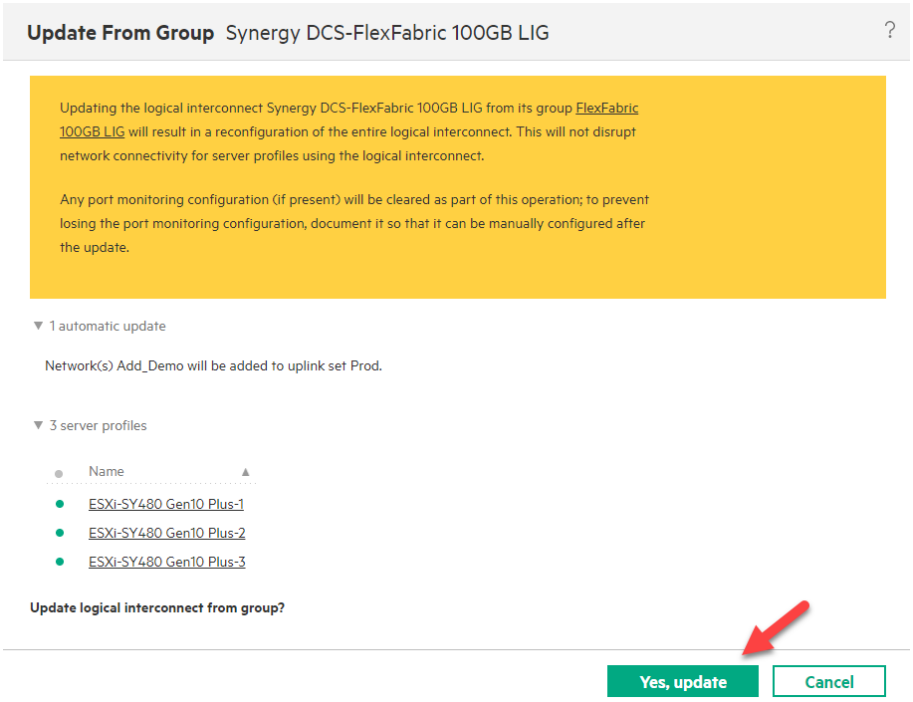
11. Select the Logical Interconnect that requires updating from the menu. Notice that the Logical Interconnect Group is shown as being inconsistent with the Logical Interconnect Group



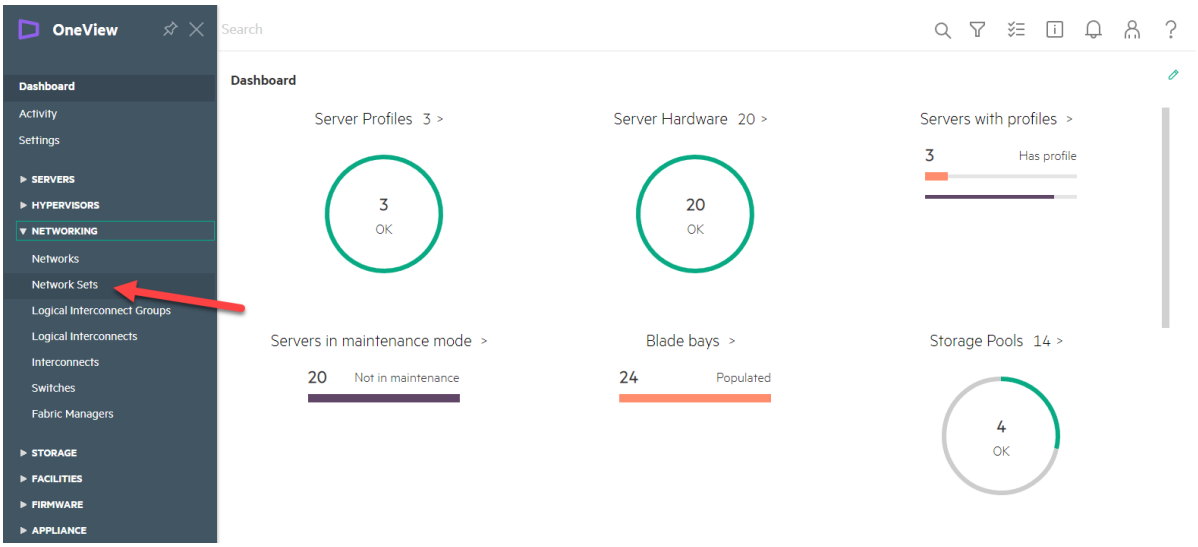
12. Open the Actions menu, and then *Update from group*. Repeat for any other *Logical Interconnects* that require updating.



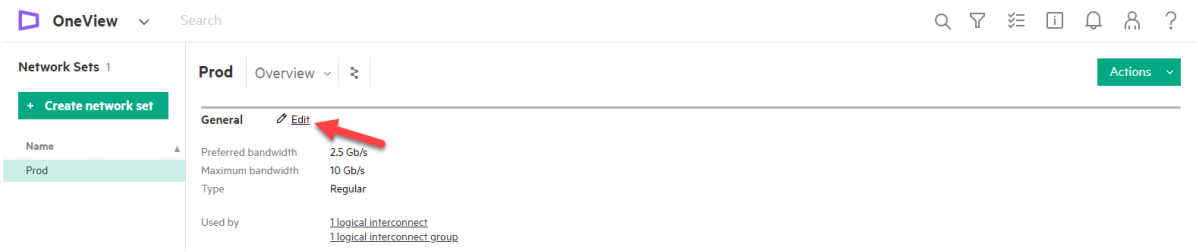
13. You are now shown the impact of the changes so that you can choose the make the changes to the Logical Interconnect



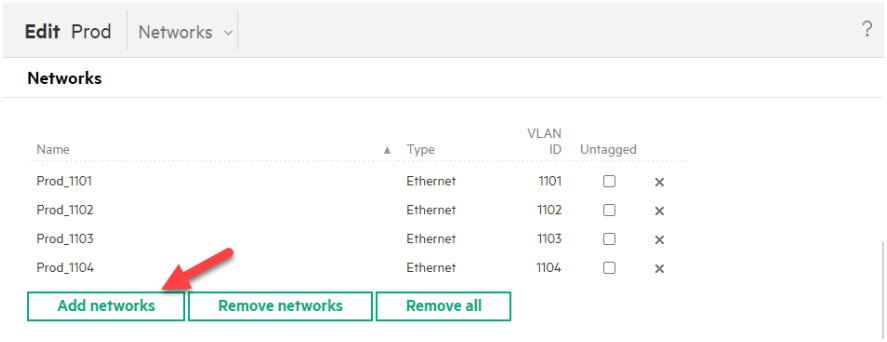
14. To add the new network via a Network Set, from the top-level menu, expand the *NETWORKING* option and then select *Network Sets*



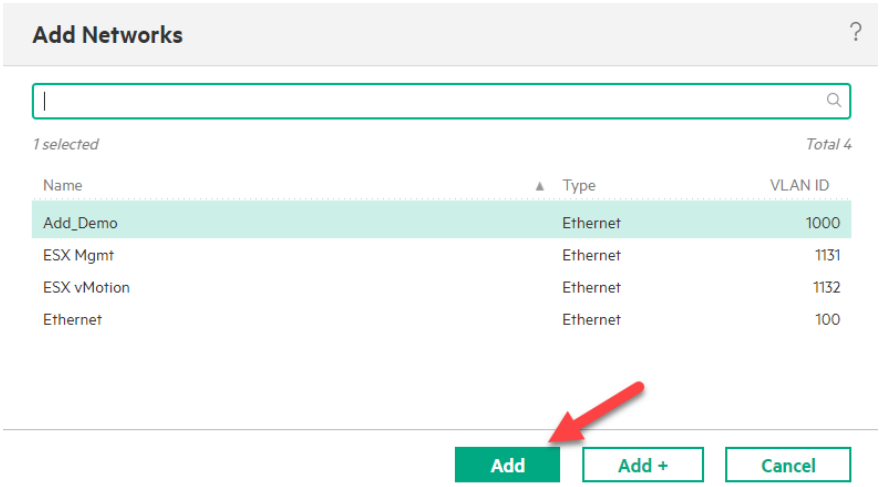
15. Select the desired Network Set from the left and menu and then click on *Edit*



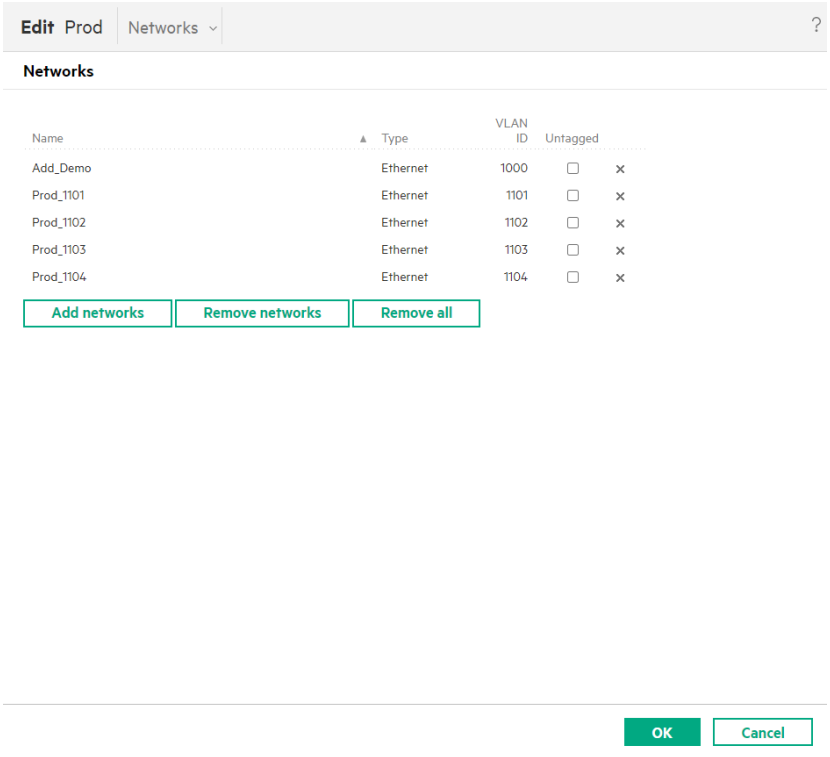
16. In the Networks section, select *Add networks*



17. Select the Add_Demo network and Click *Add.*



18. Click *OK* to apply the changes to the Network Set

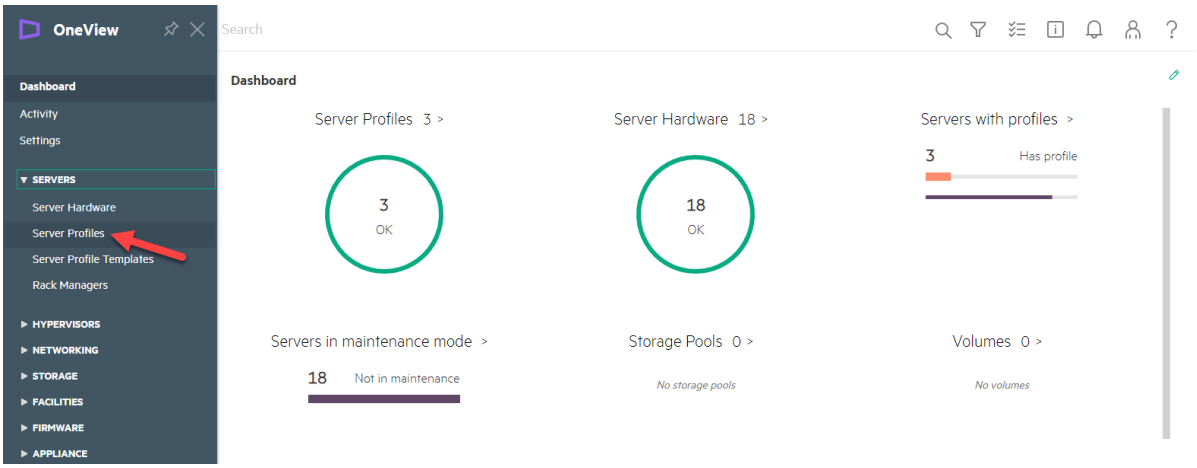


Information

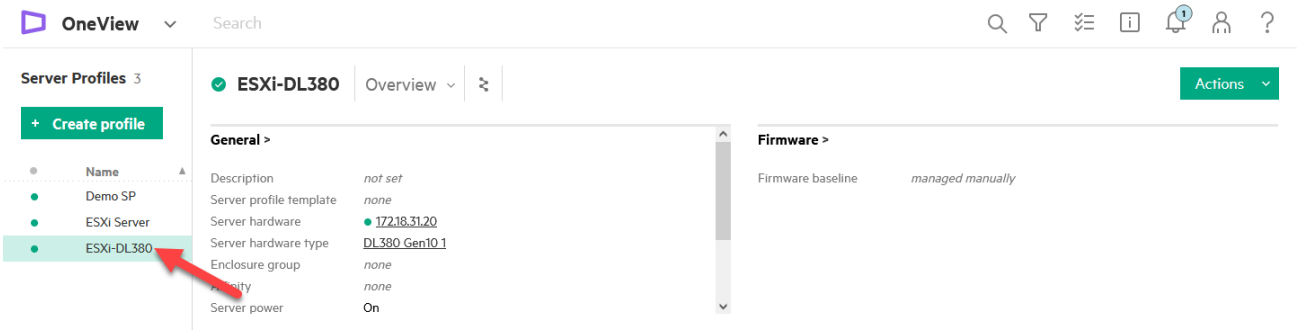
Adding a *Network* to a Network Set does not require a Server to be powered off and will deploy the updated *Network Set* configuration automatically.

Create a Server Profile Template from existing server profile

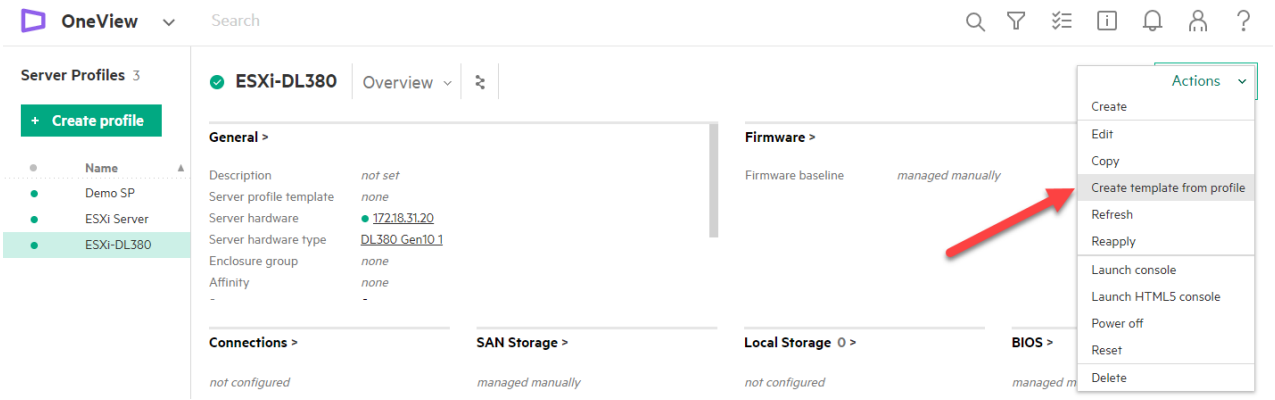
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



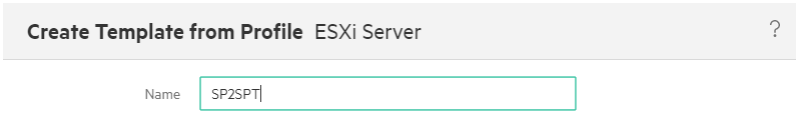
2. From the left hand menu select the server profile that you want to make the template from



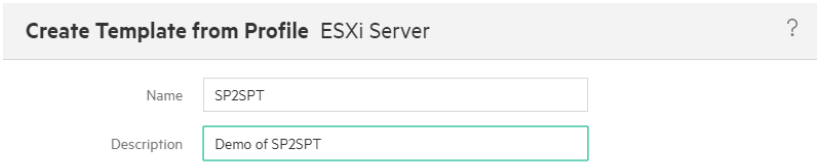
3. Open the Actions menu and select *Create template from profile*



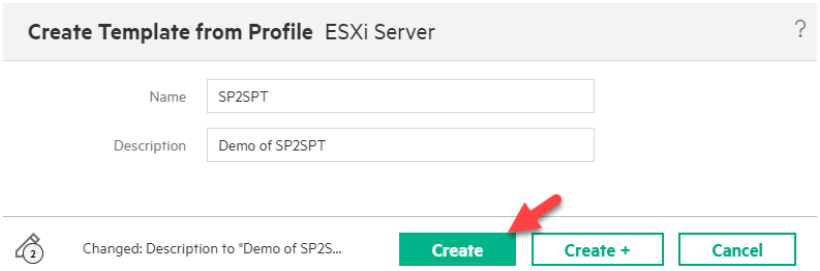
4. Enter a *Name* for the Server Profile Template



5. Enter a *Description* for the Server Profile Template



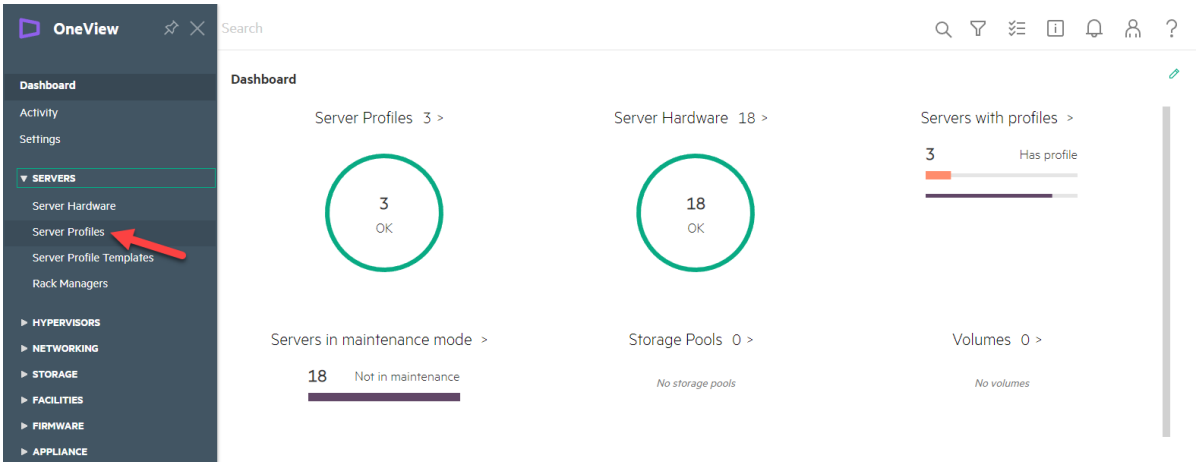
6. Click *Create*



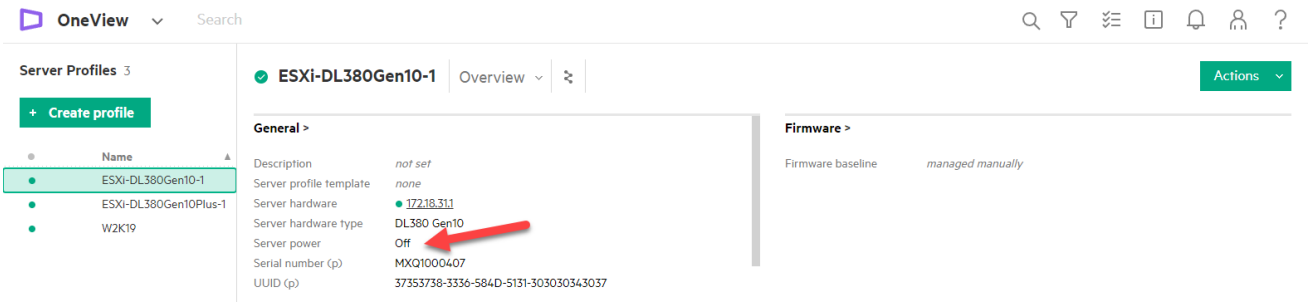
Edit Server Profile

Once a profile has been applied, you can edit the profile to make changes, and fix issues that may have been encountered. It is possible to edit the existing Network Connections by modifying existing assigned Network and / or Bandwidth without needing to first Power Off the server. Other Server Profile edits will require the Server Profile to be powered off.

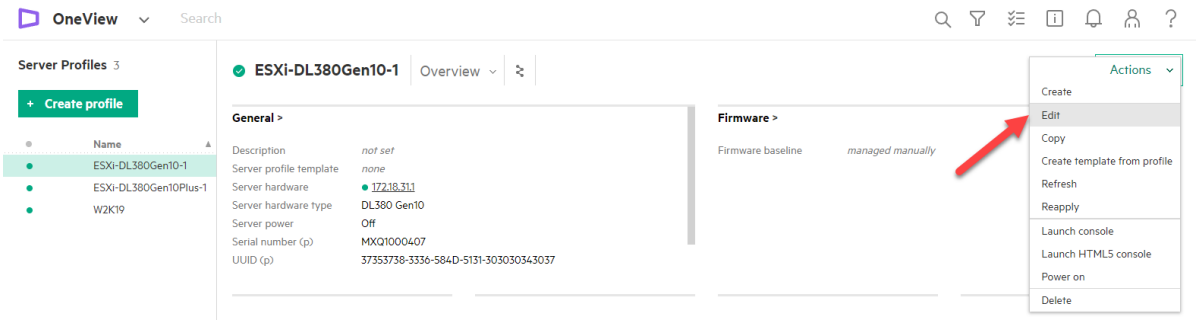
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



2. Select the server to be edited from the menu and verify that the Server is powered off.

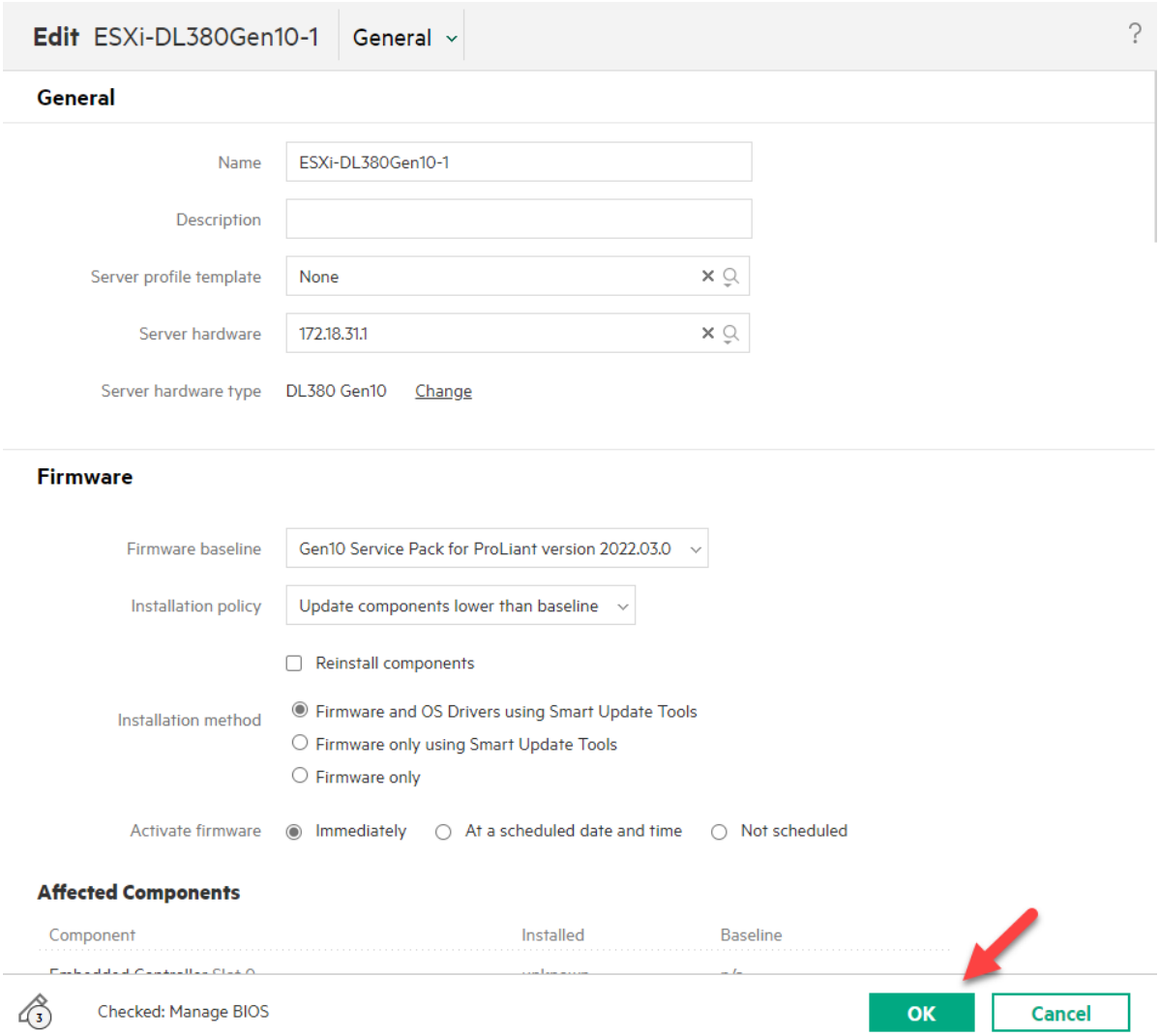


3. Select the Actions menu, then select *Edit*.



4. Make the necessary changes to the server profile (i.e. Bandwidth adjustment, add a Network Connection, etc.), depending on the Server Profile that you are editing.

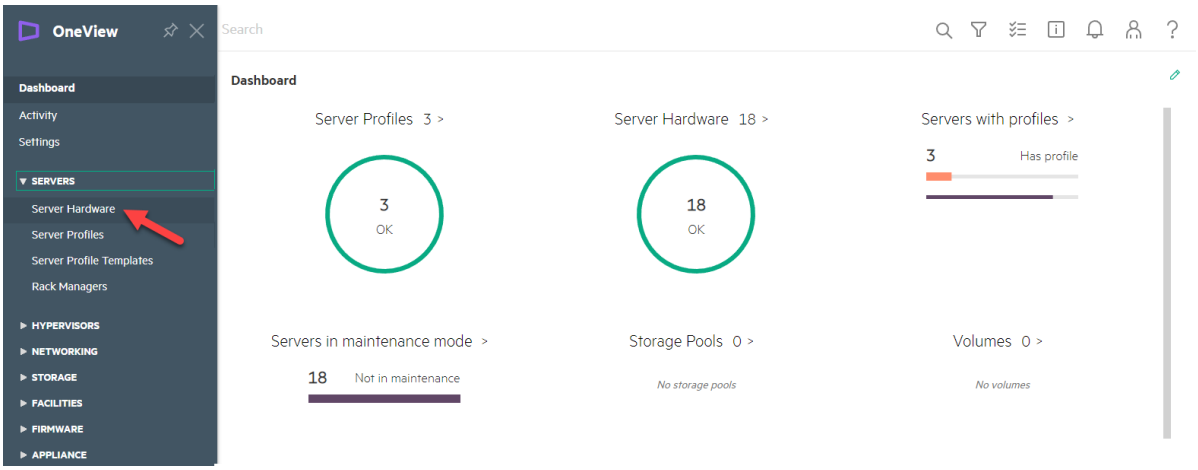
5. Click the *OK* button to save the changes to the Server Profile.



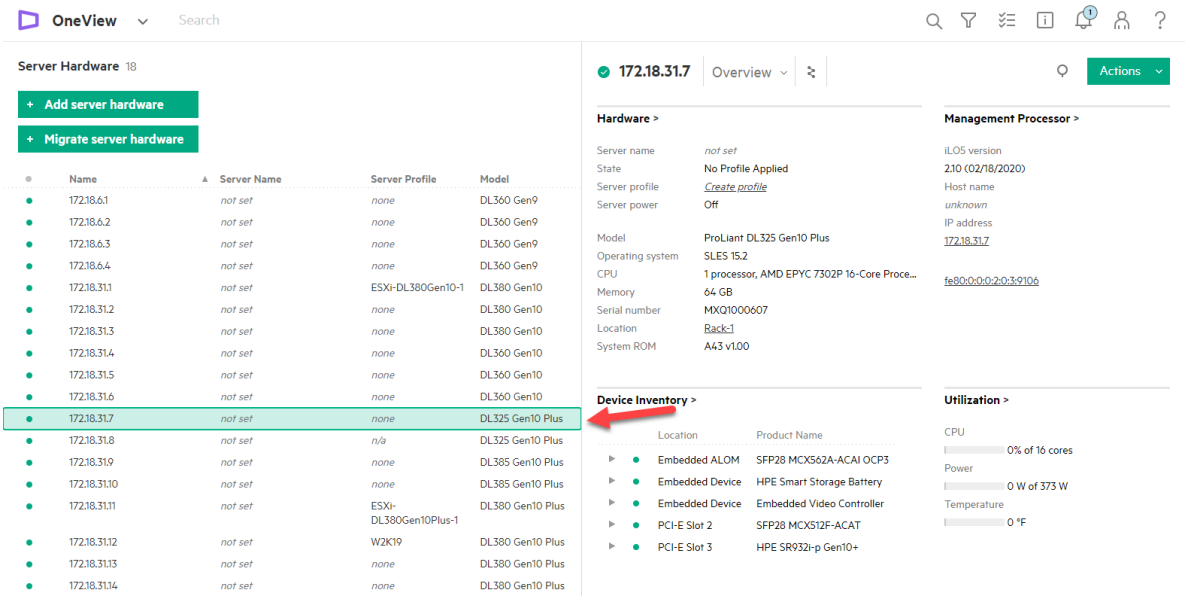
6. Notice the server does not have its firmware reapplied, and only the changes that have been made are applied.

Assign a Server Profile to a newly discovered server

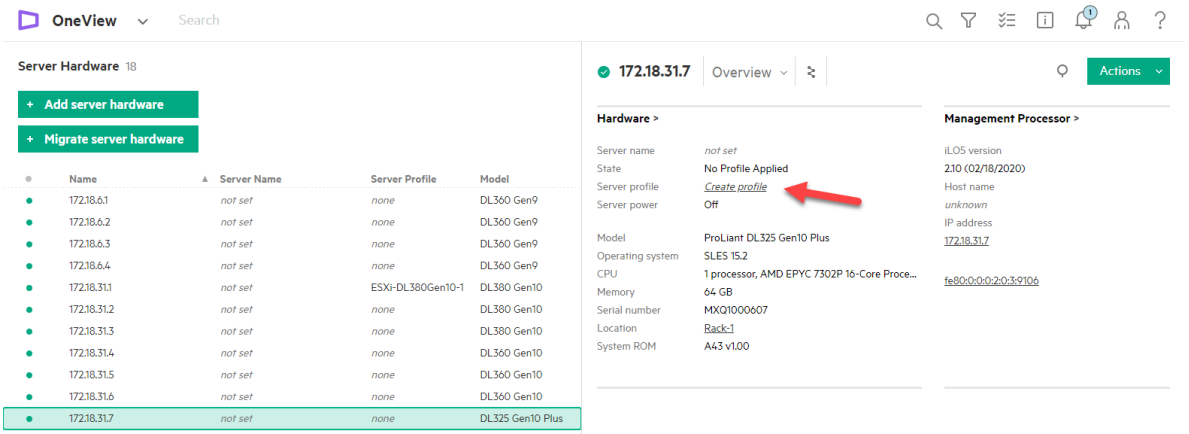
1. From the Top-Level menu, expand the *SERVERS* option and then select *Server Hardware*.



2. Select the server from the menu



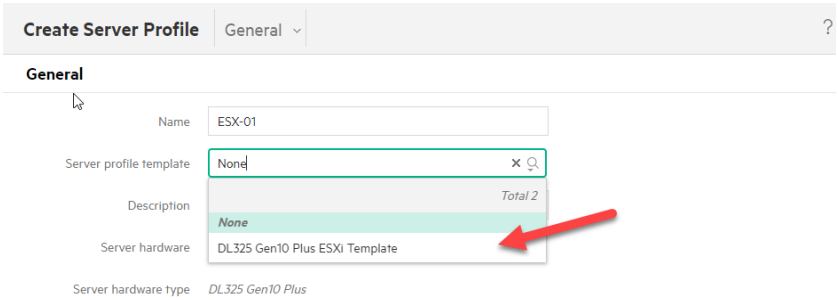
3. From the Overview section, select Create profile



4. Enter a Name for the server profile

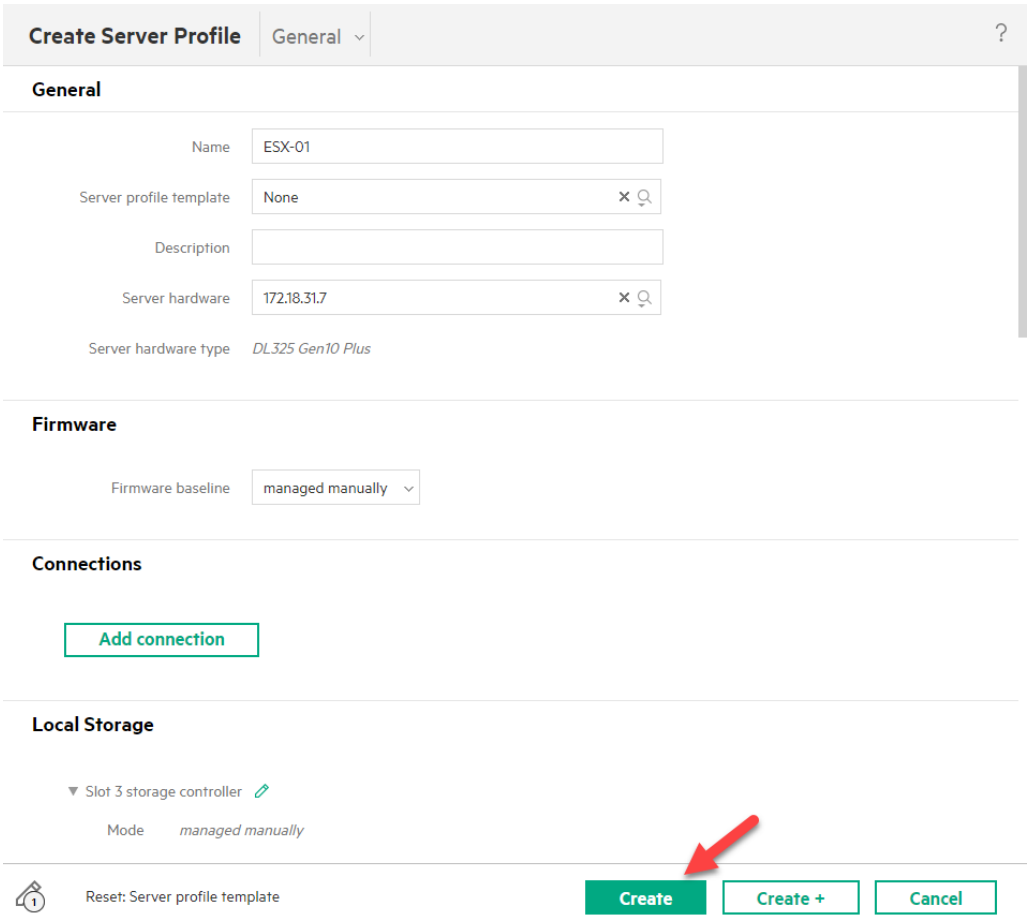


5. (Option - A) Select a Server profile template from the dropdown list



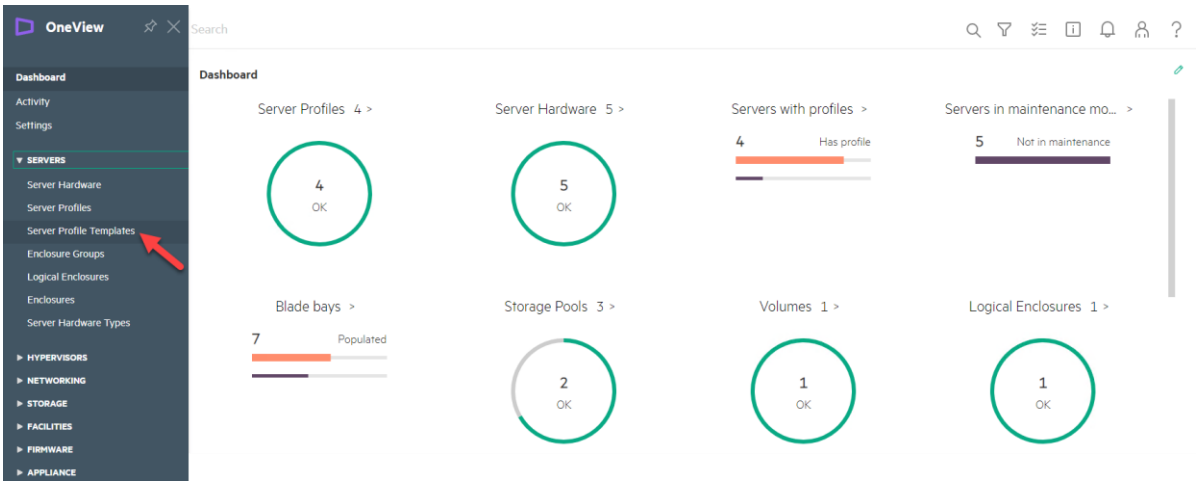
6. (Option – B) Create an individual server profile – follow the process located here

7. Click *Create*

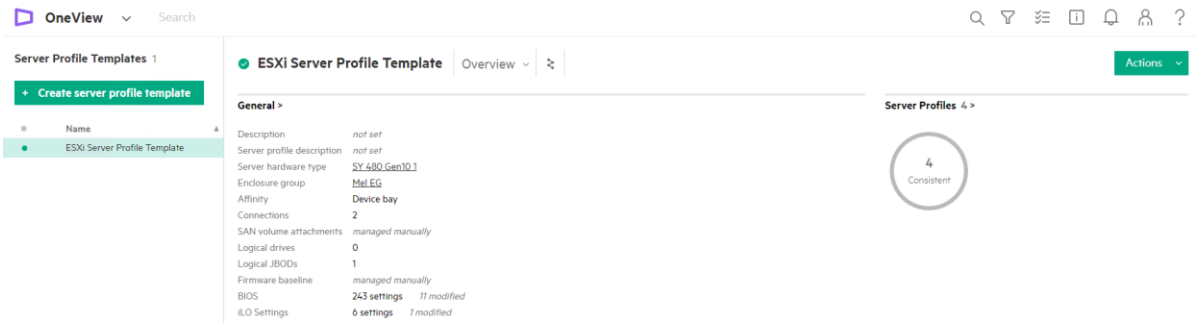


Perform rolling cluster update on ESX cluster

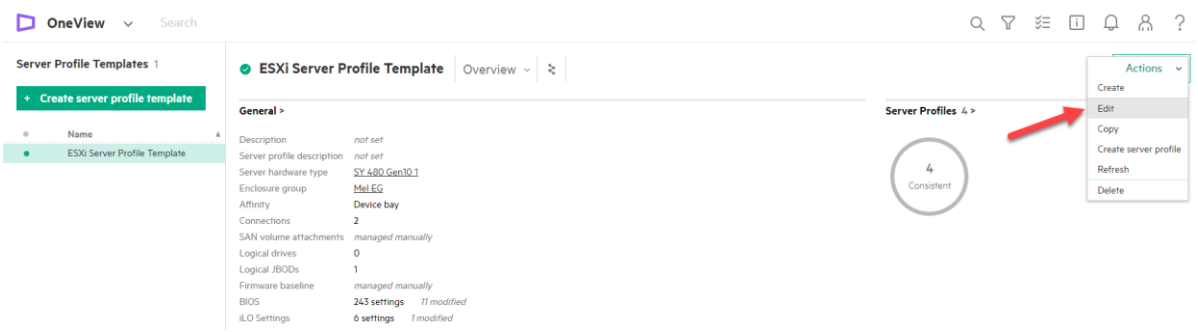
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profile Templates*



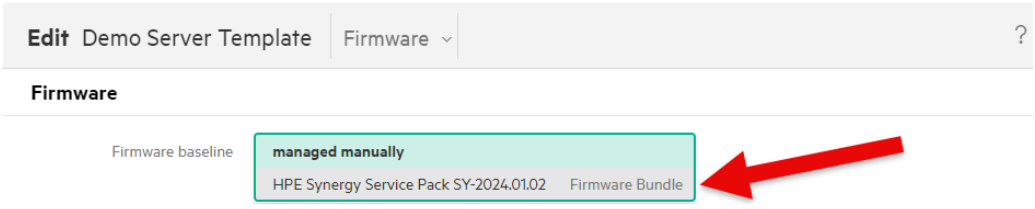
2. From the menu, select the desired *server profile template*



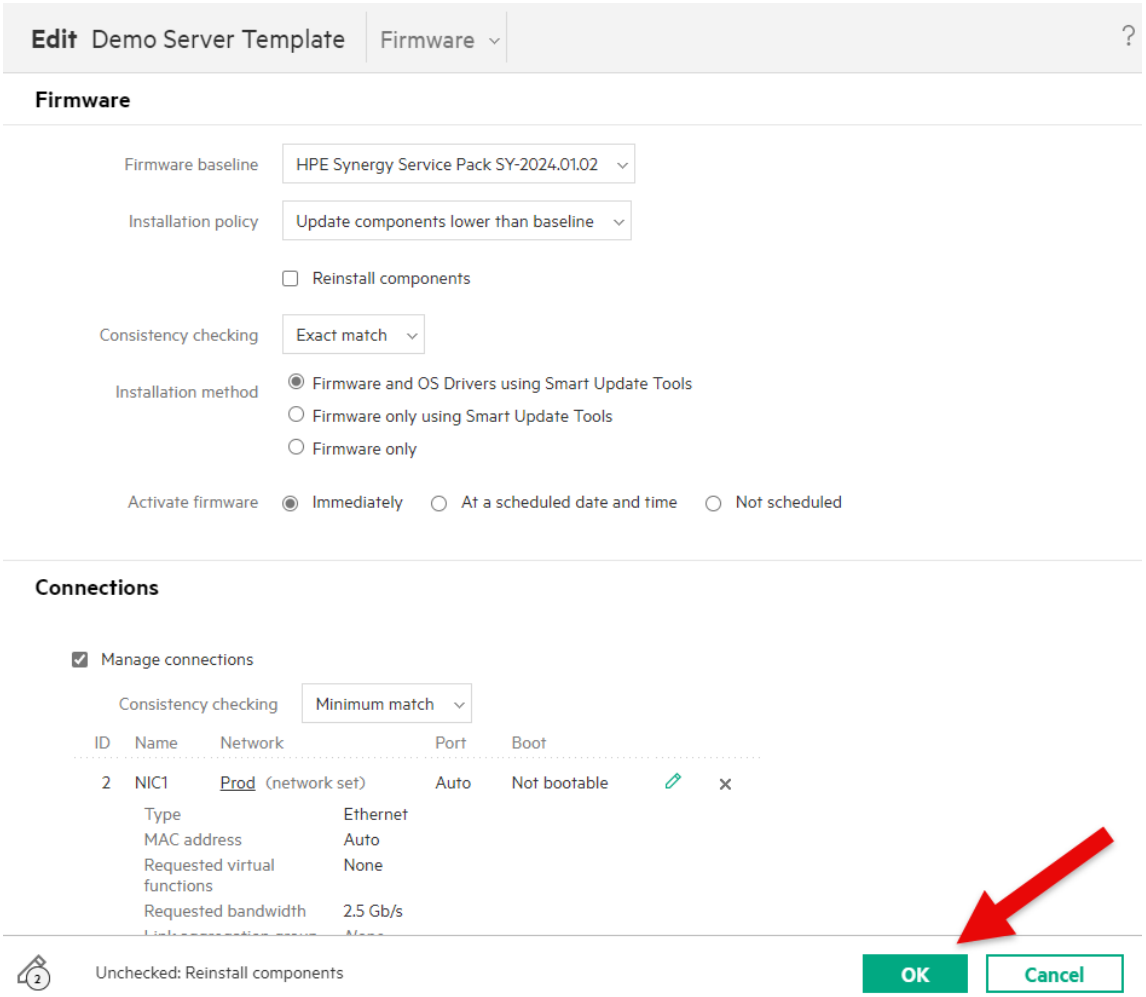
3. From the actions menu, select *Edit*



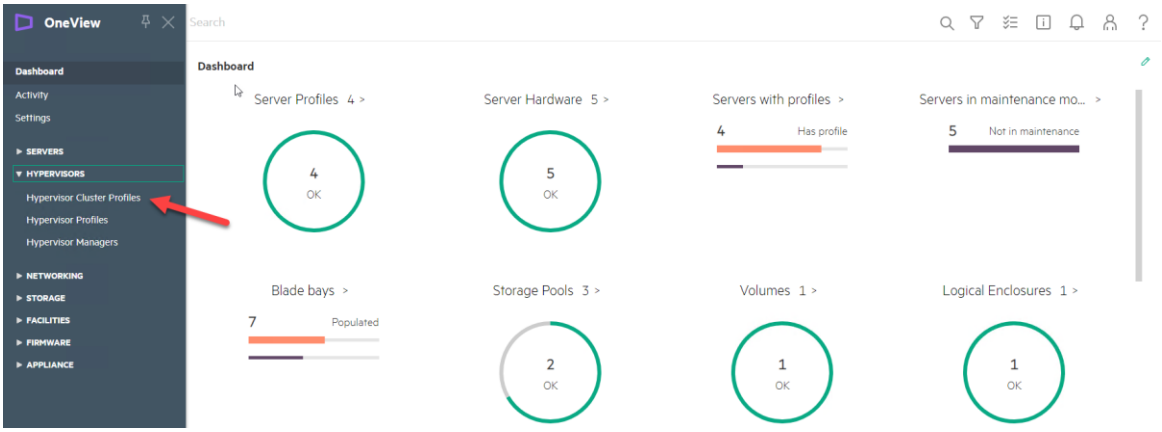
4. In the Firmware section of the server profile template, use the dropdown list to select the new firmware



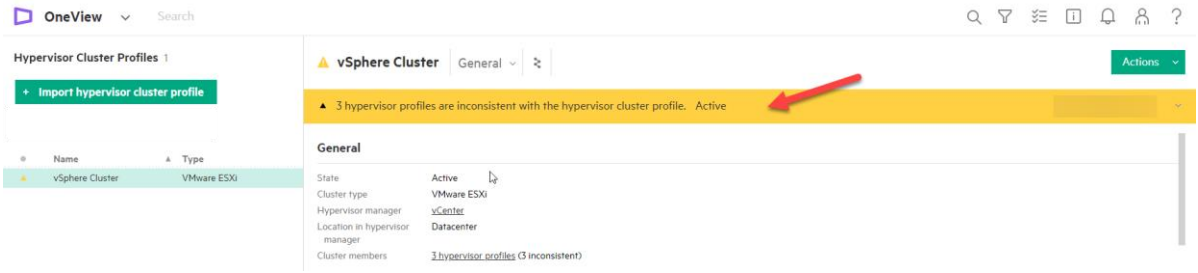
5. Click *OK* to close the server profile template.



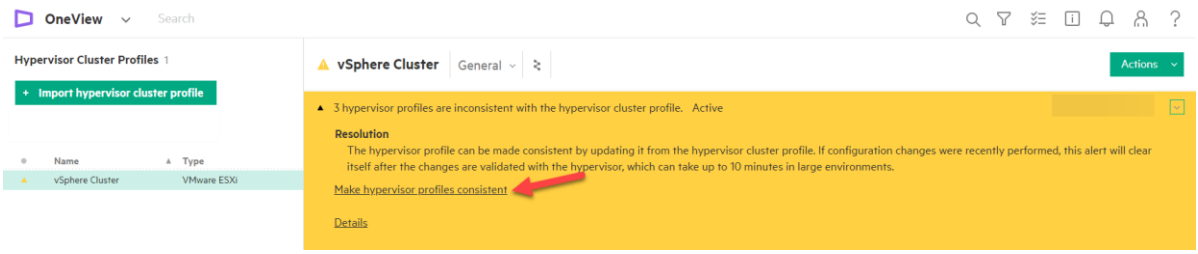
6. From the Top-Level Menu, expand the *HYPERVISORS* option and then select *Hypervisor Cluster Profiles*.



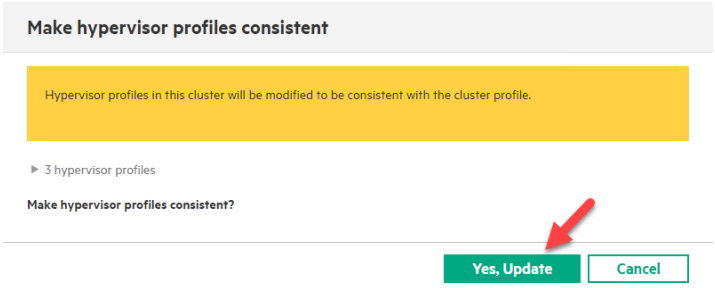
7. From the menu, select the desired *cluster profile* and click on the *warning message* to expand it



8. Click Make hypervisor profiles consistent



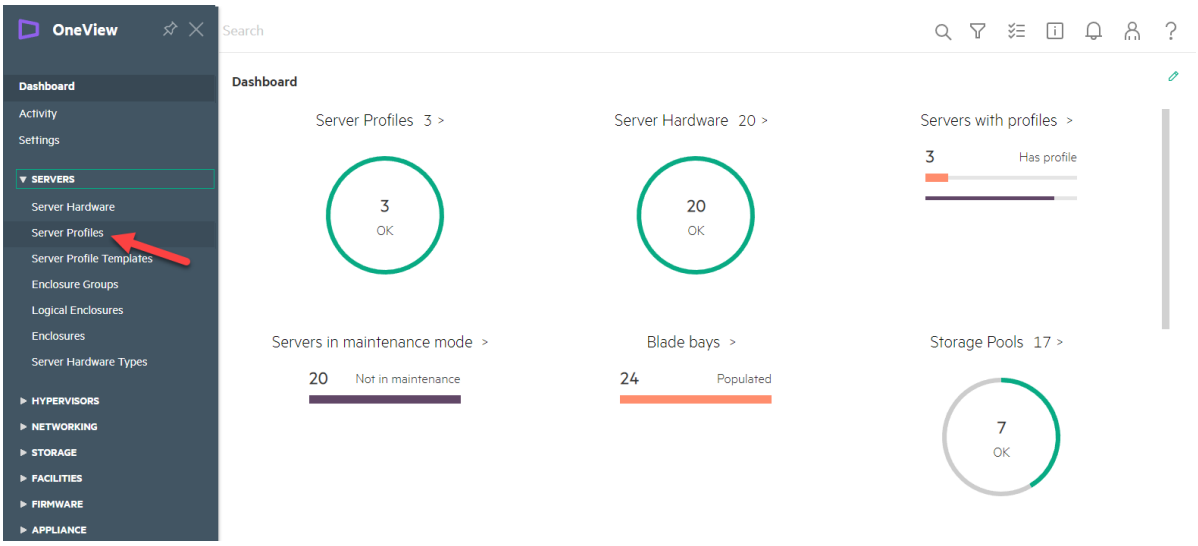
9. In the Make hypervisor profiles consistent dialog box, select Yes, Update.



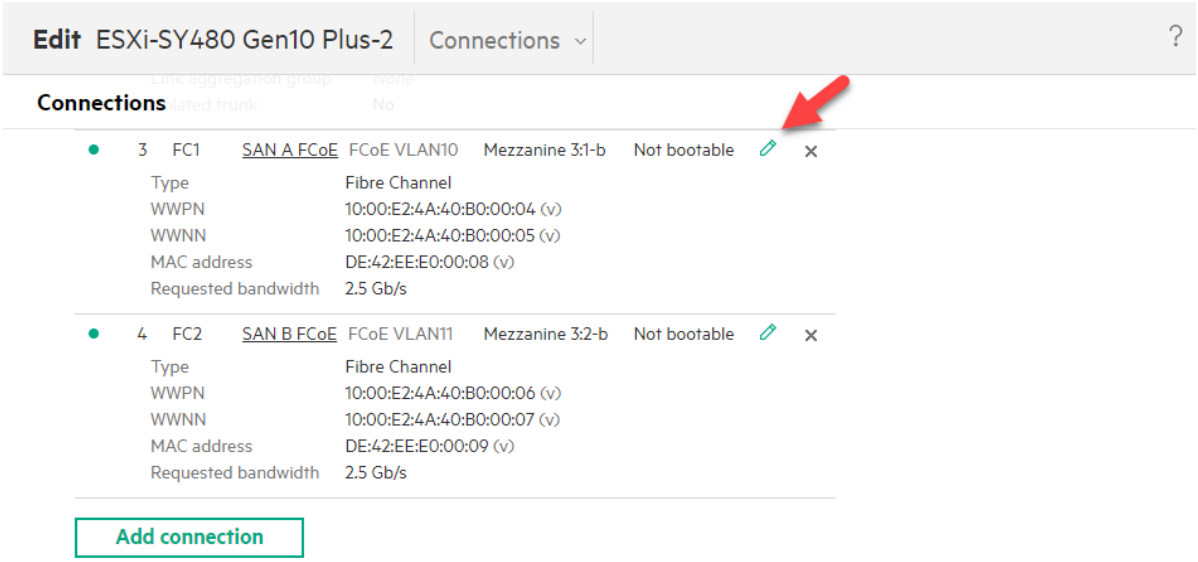
Configuring Boot from third party LUNs in a Server Profile

Configuring a server to boot from an unmanaged third-party SAN storage LUN can be performed by editing the server's SAN connection in the profile and configure it with the third-party LUN's WWN and LUN. Server profile network connection edits will require the server to be Powered Off. It is the administrator's responsibility to configure the third-party storage device to present the LUN to the server's connection WWPN on the SAN.

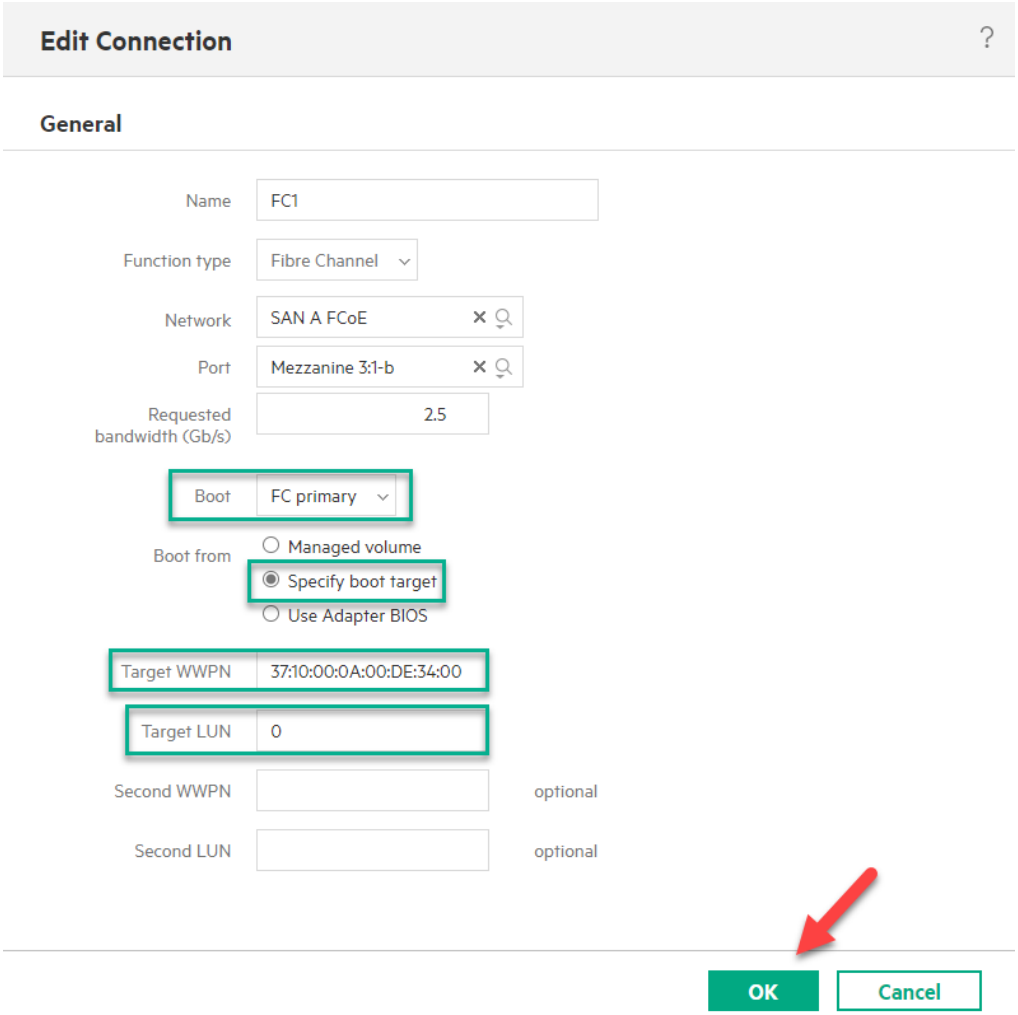
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



2. Select the server profile to configure and invoke the Edit action on the server profile. Within the profile editor, edit the connections to configure to boot from a third-party LUN.

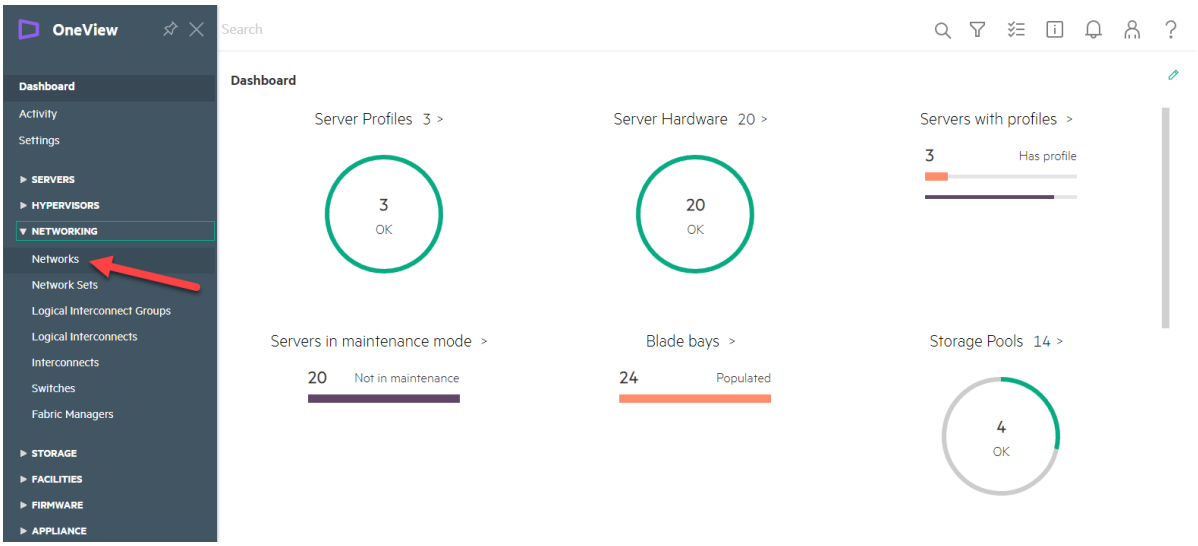


3. Configure the connection to be a boot connection (primary or secondary) and select the "Specify boot target" option to supply the SAN identity of the third-party LUN – as a WWN and LUN number. Click OK twice to save the connection and profile configuration.

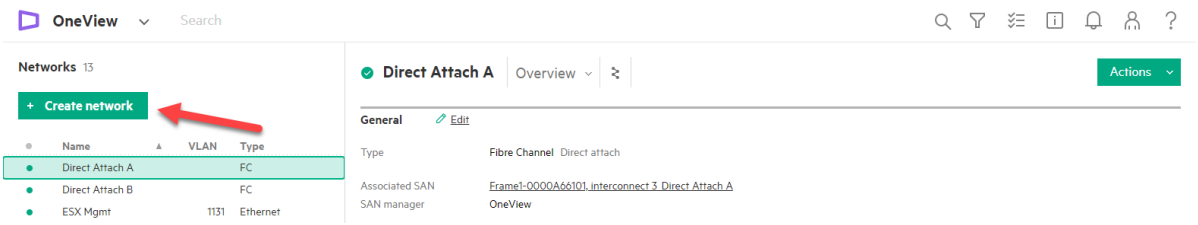


Adding an Ethernet Network

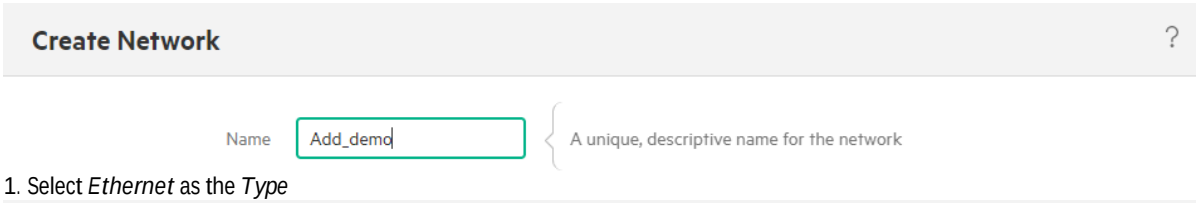
1. From the Top-Level menu, expand te *NETWORKING* option and then select *Networks*.



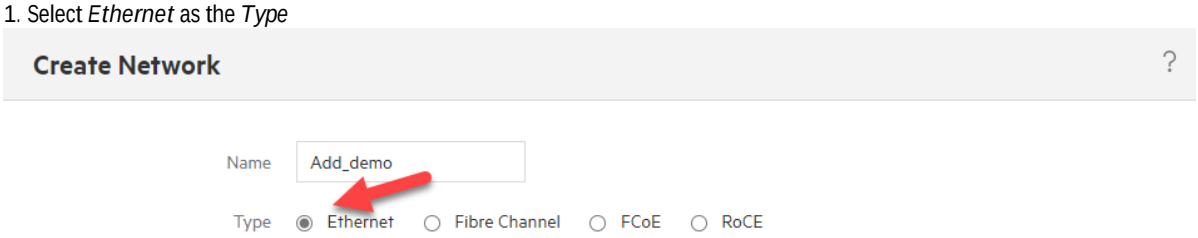
2. Once on the *Networks* screen, click the + *Create network* button on the far left.



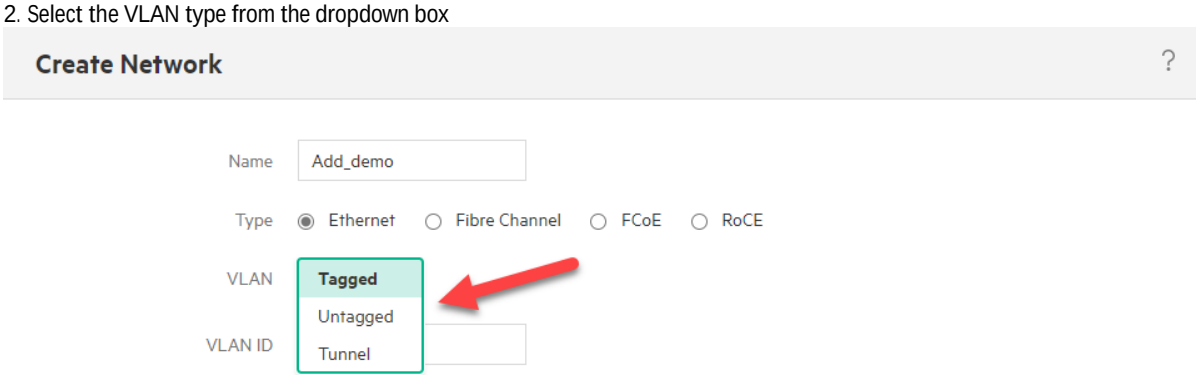
3. In the Create Network Dialog box enter the name of the network. The *Name* is not case-sensitive. The name can contain spaces and special characters.



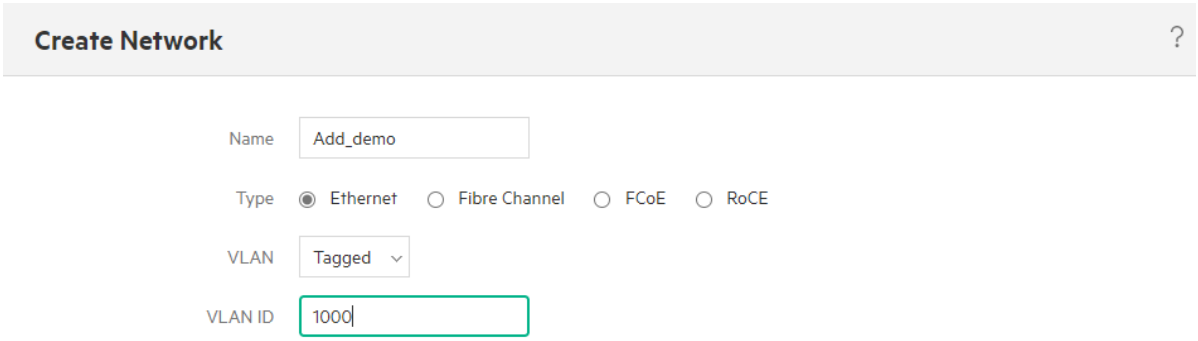
1. Select *Ethernet* as the *Type*



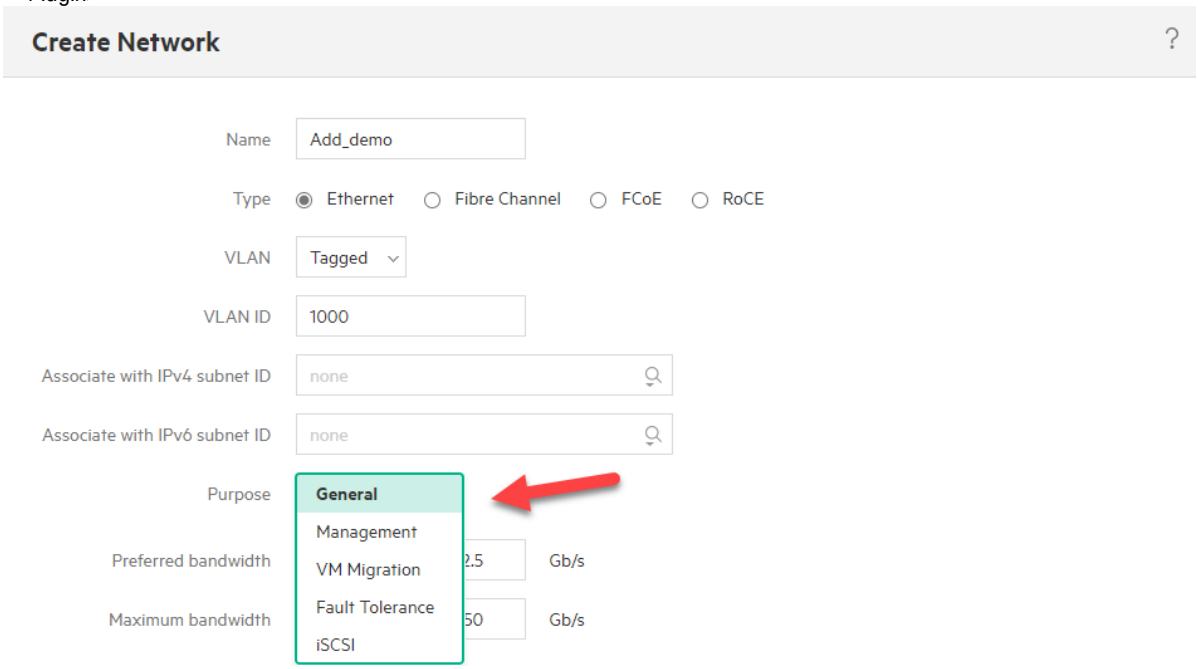
2. Select the VLAN type from the dropdown box



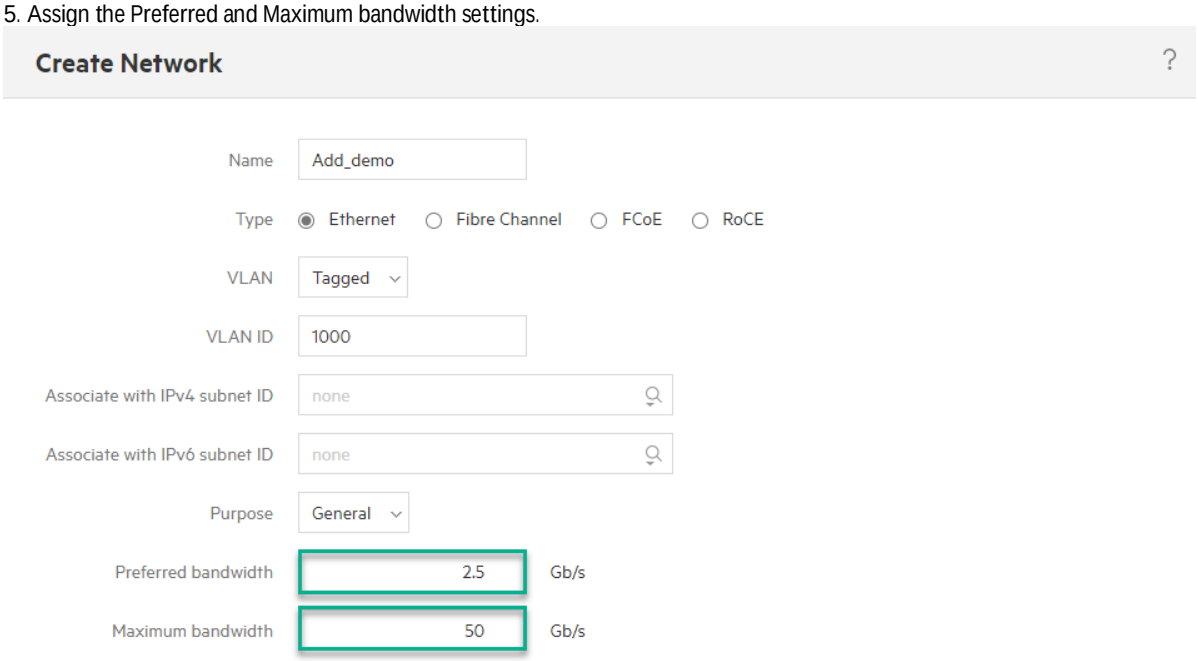
3. Enter the *VLAN ID*.



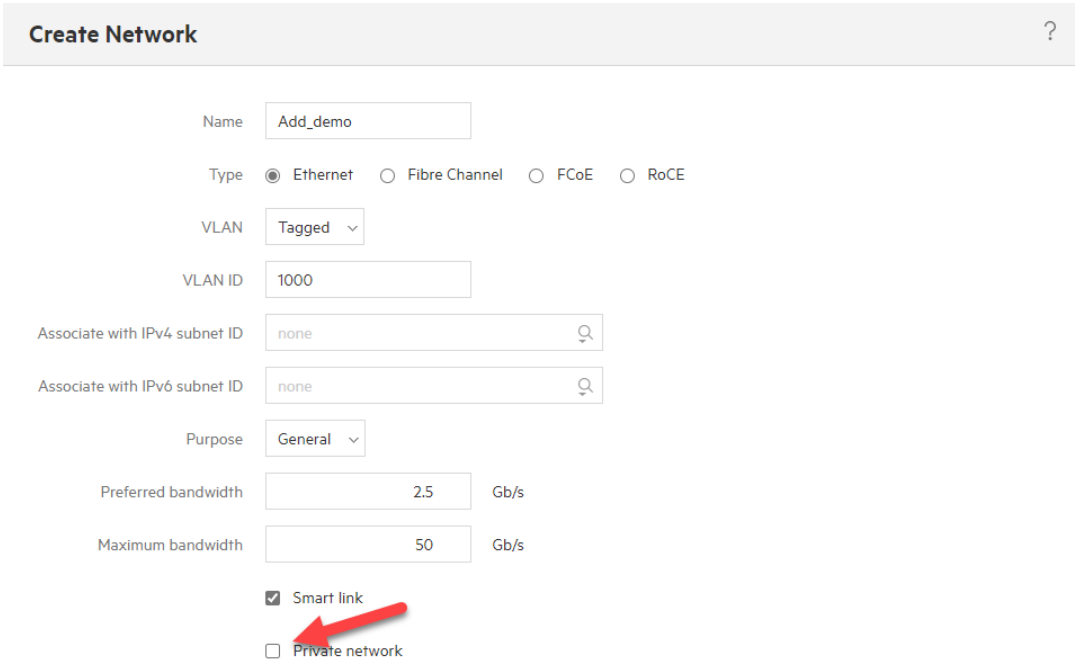
4. Select the Purpose of the network from the dropdown list. The *Purpose* drop-down selection is used by the HPE OneView for OneView for vCenter Plugin



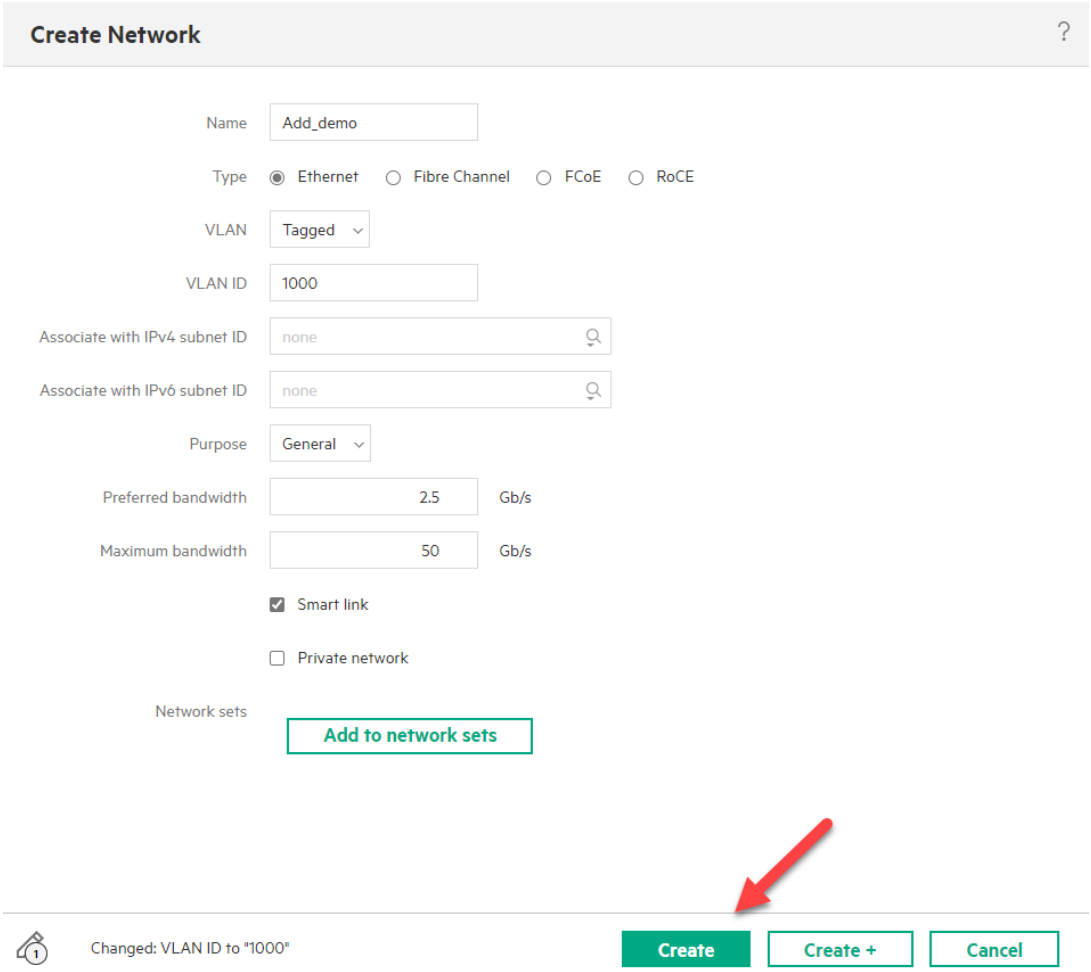
5. Assign the Preferred and Maximum bandwidth settings.



6. Enable any network options needed. *Smart Link* will automatically be selected by default. Selecting *Private Network* will mimic PVLAN behavior in that all assigned Network Connections will all be in an isolated network.

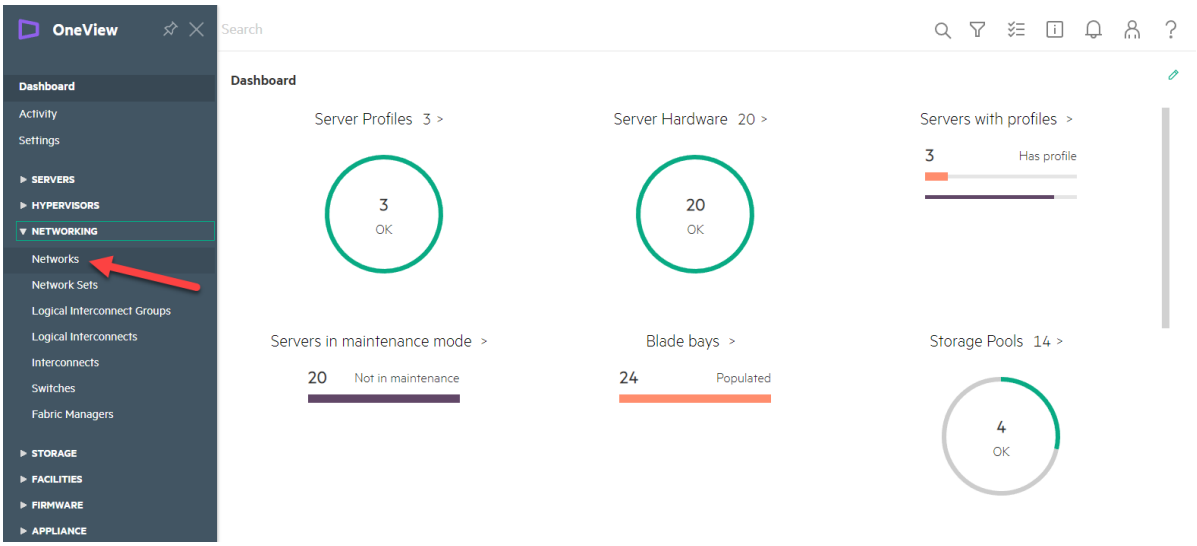


7. Click the *Create* button to create the new Ethernet Network and close the *Create Network* dialog box. You can also select the *Create+* button to continue creating more Networks – e.g. Create the B-Side Ethernet Network.

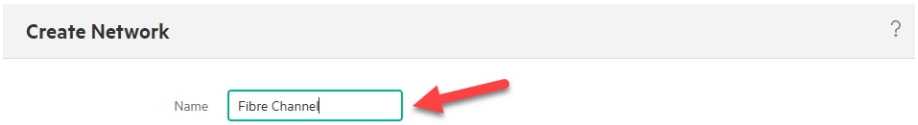


Adding a Fibre Channel Network

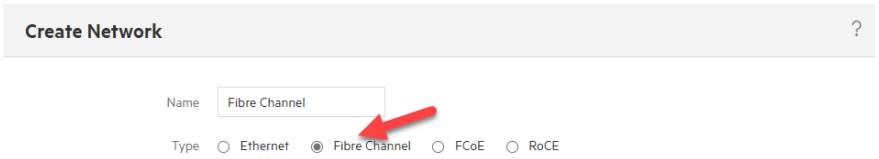
1. From the Top-Level Menu, expand the *NETWORKS* option and then select + *Create network* button.



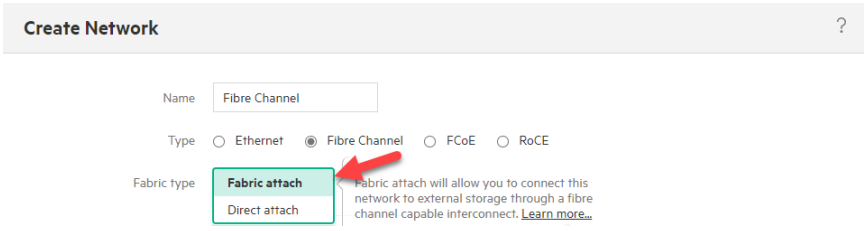
2. In the Create Network dialog box, enter the *Name* of the Fibre Channel network



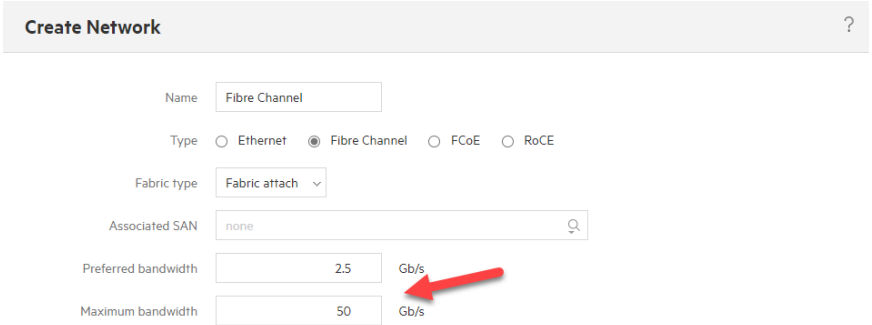
3. Select *Fibre Channel* as the *Network Type*



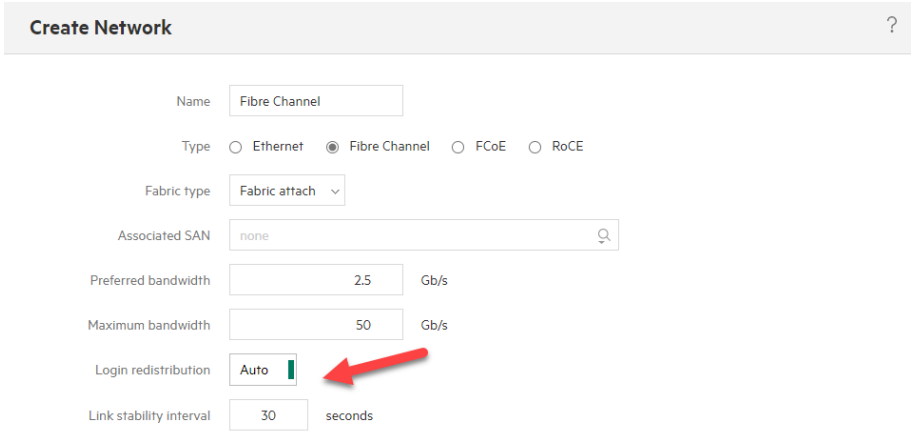
4. Select *Fabric Attach* as the *Fabric Type*



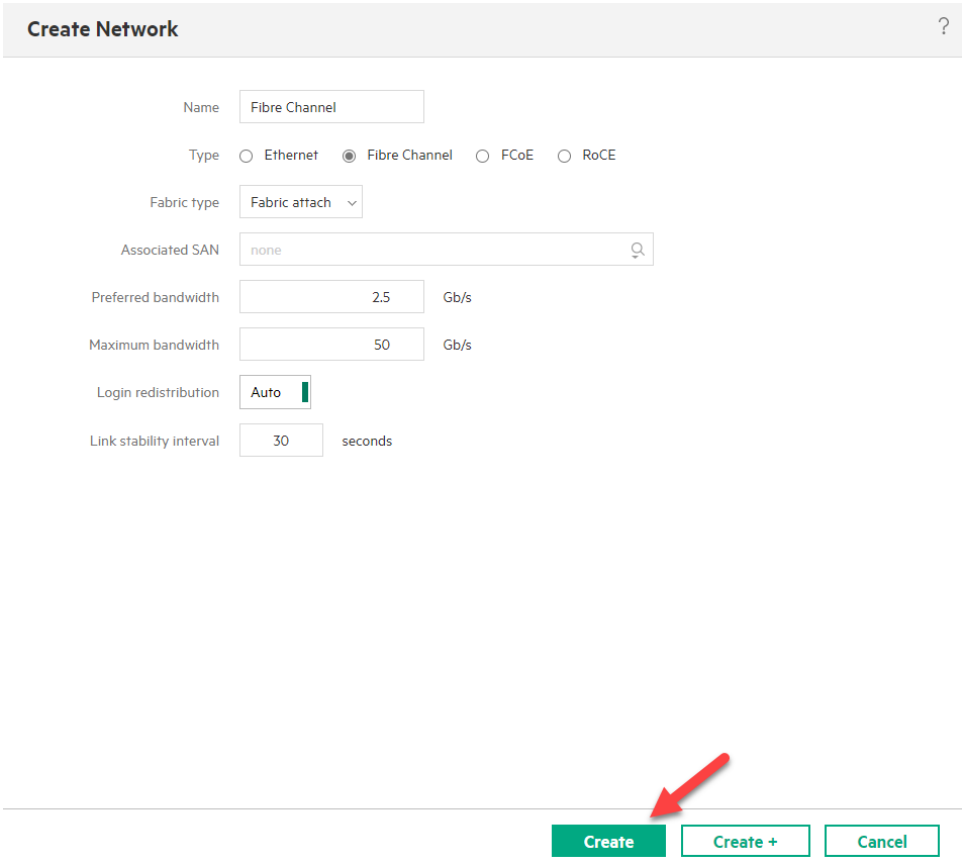
5. Set the *Preferred Minimum and Maximum Bandwidth*.



6. Set the desired *Login redistribution* and *Link stability interval* to be used.

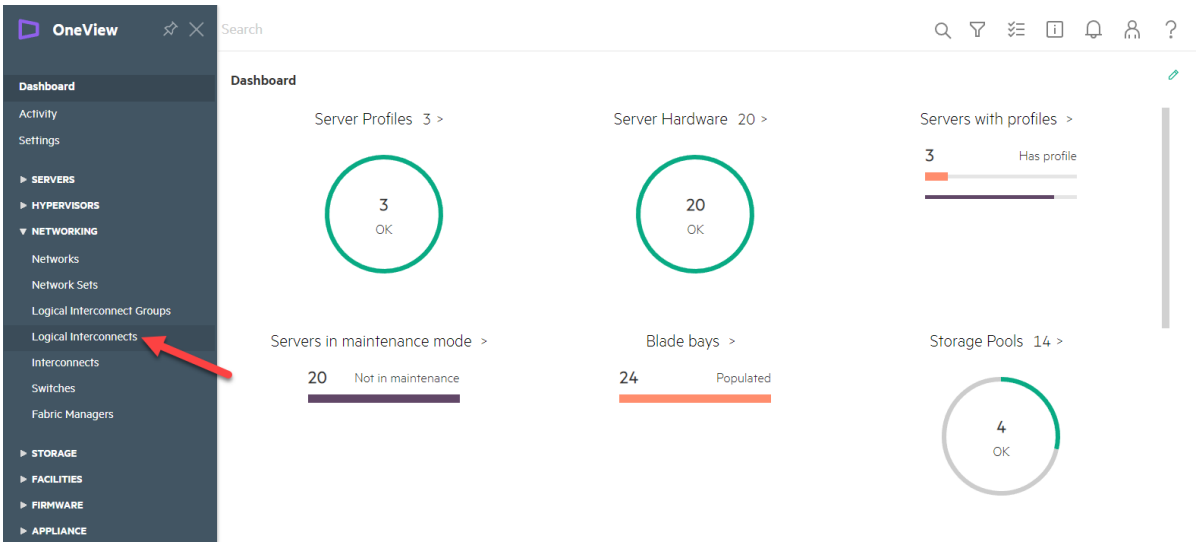


7. Click the *Create* button to create the new Ethernet Network and close the Create Network dialog box. You can also select the *Create+* button to continue creating more Networks.

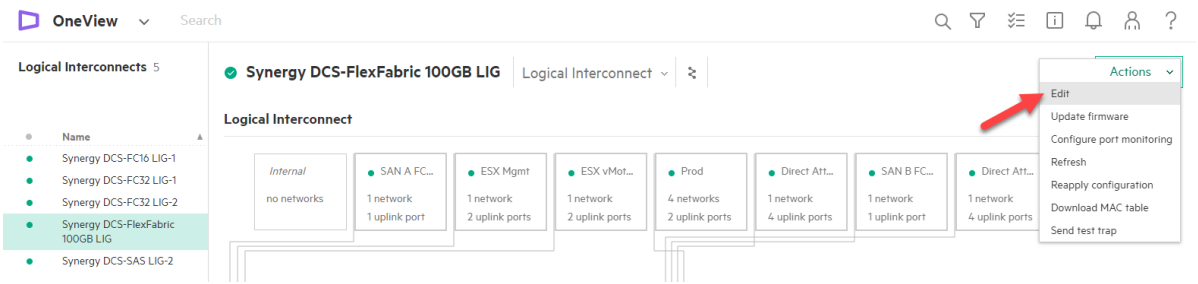


Adding an Ethernet Uplink to a Logical Interconnect

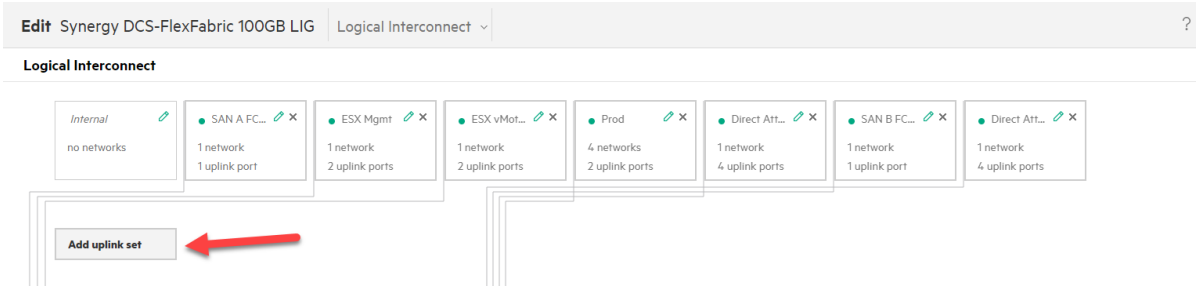
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Logical Interconnects*.



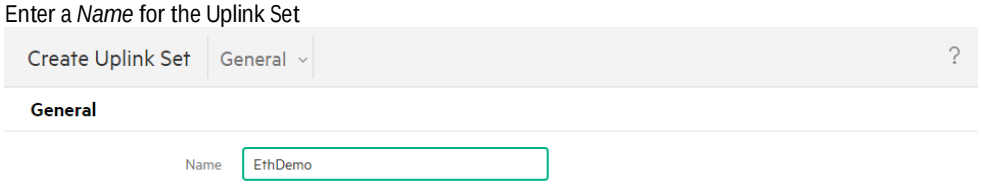
2. From the menu, select the Logical Interconnect to be edited. Using the Actions menu, select *Edit*.



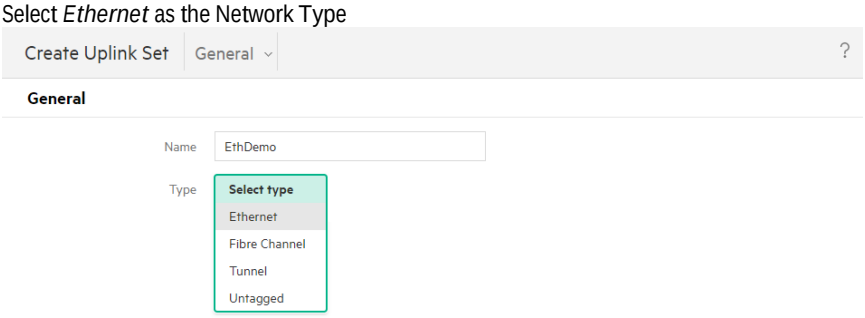
3. In the Edit window, select *Add uplink set*.



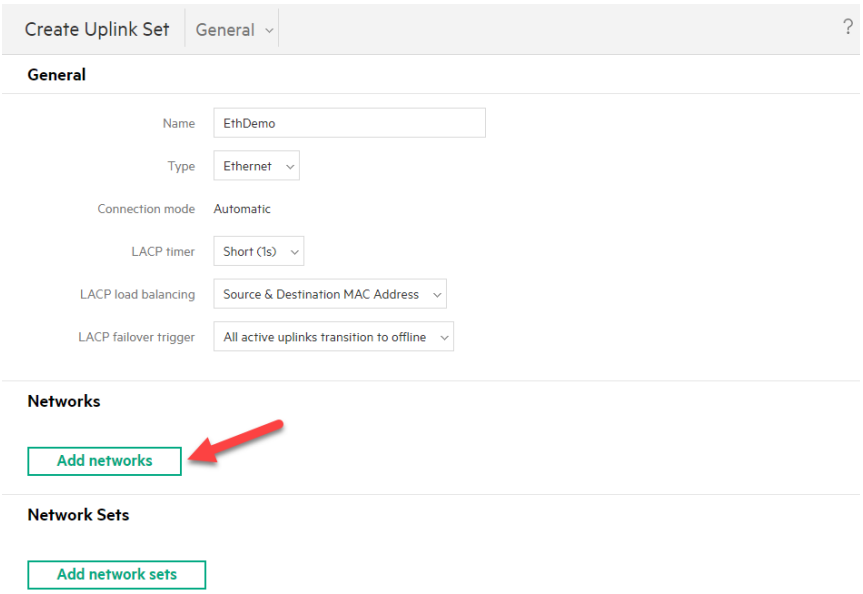
4. Enter a *Name* for the Uplink Set



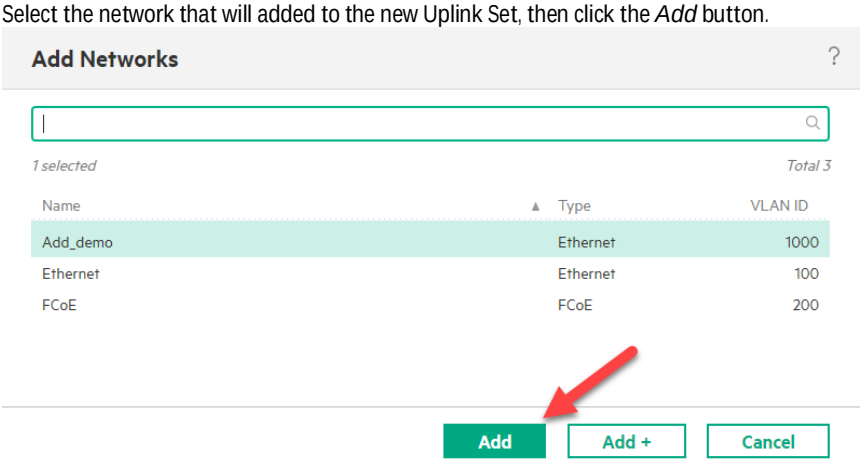
5. Select *Ethernet* as the Network Type



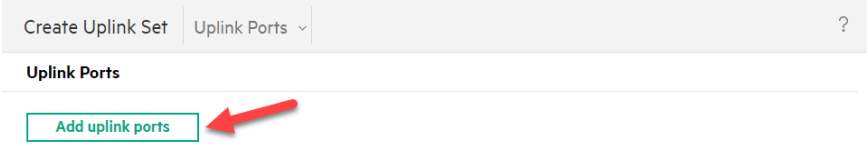
6. Select the *Add Networks* button



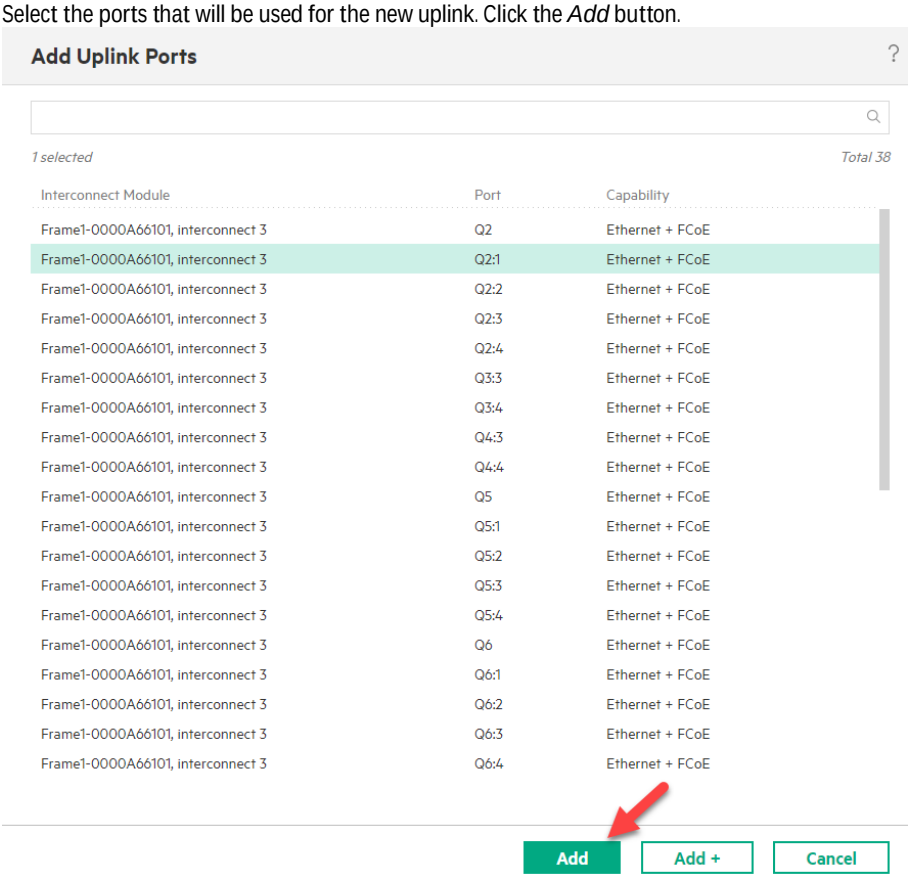
7. Select the network that will added to the new Uplink Set, then click the *Add* button.



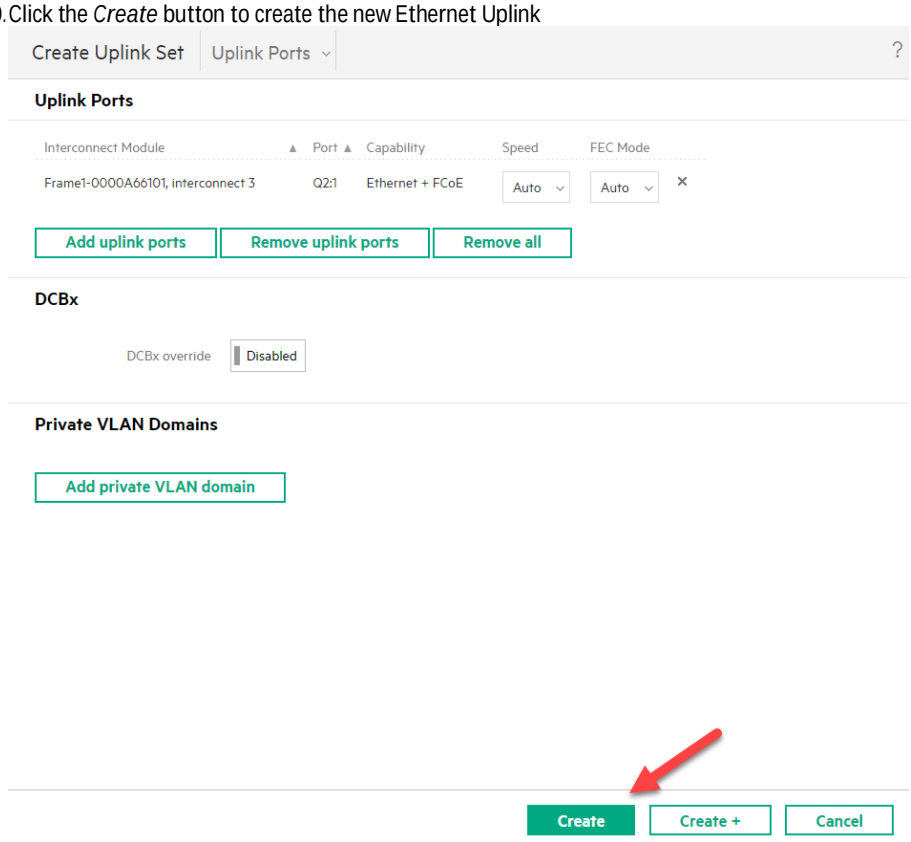
8. Select the *Add uplink ports* button.



9. Select the ports that will be used for the new uplink. Click the *Add* button.



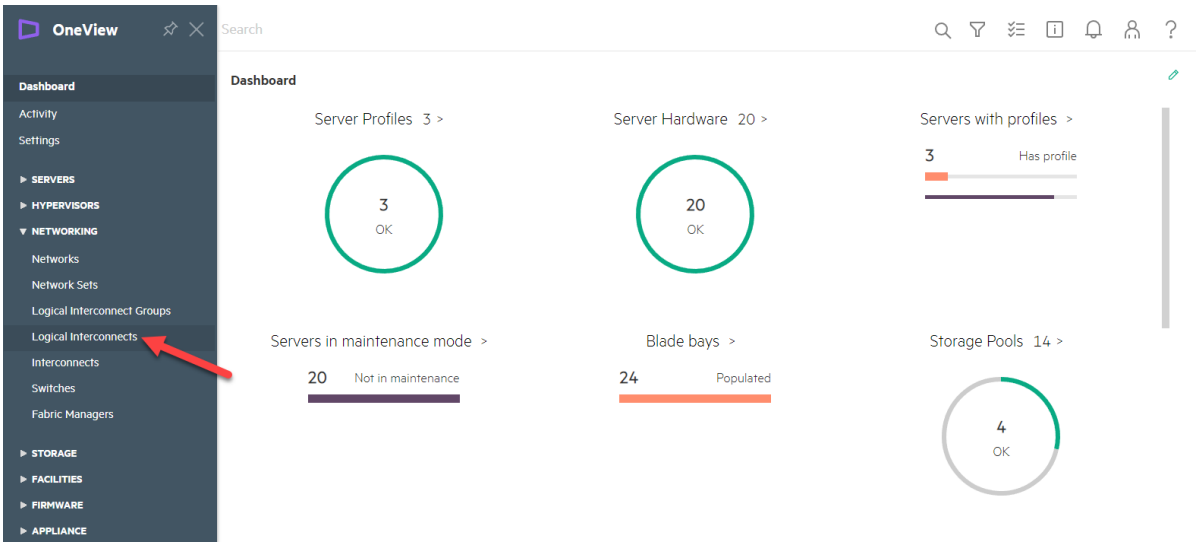
10. Click the *Create* button to create the new Ethernet Uplink



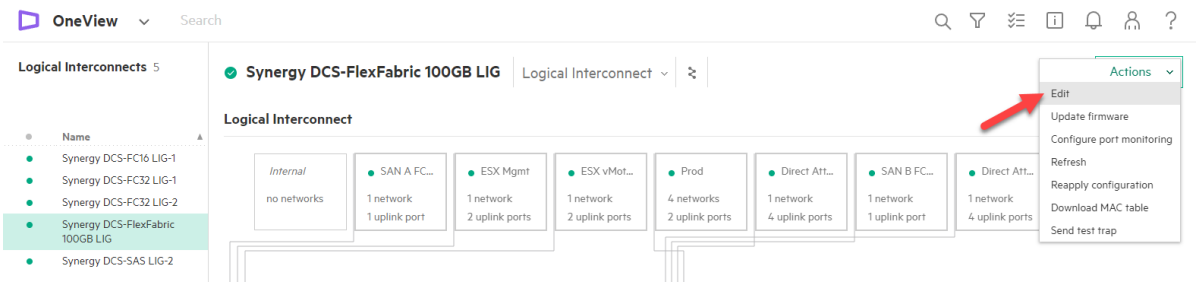
11. Click the *OK* button to enable the new Ethernet Uplink

Adding a Fibre Channel Uplink

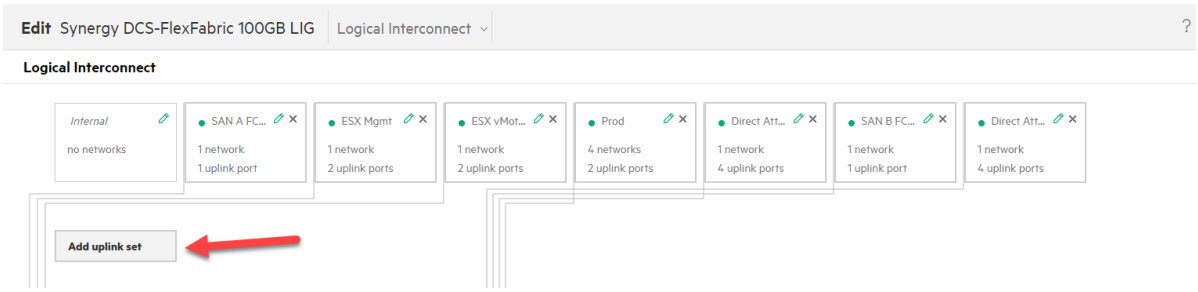
1. From the Top-Level Menu, expand the *NETWORKING* option and then select *Logical Interconnect*.



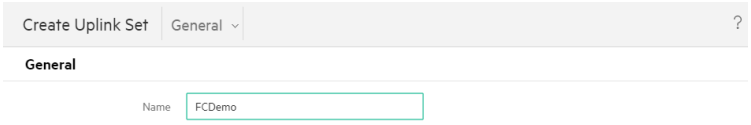
2. From the menu, select the Logical Interconnect to be edited. Using the Actions menu, select *Edit*.



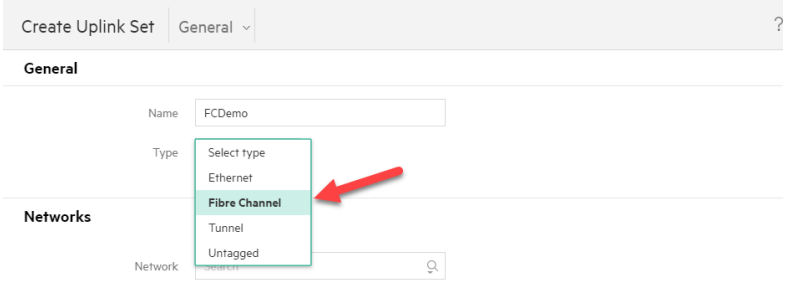
3. In the Edit window, select *Add Uplink Set*.



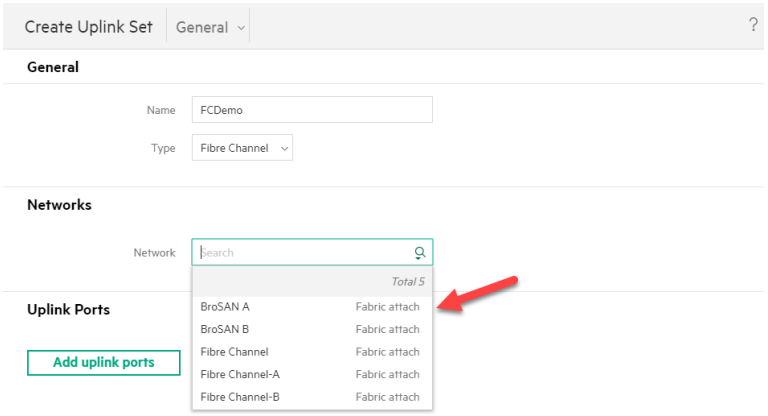
4. Enter a *Name* for the Uplink Set



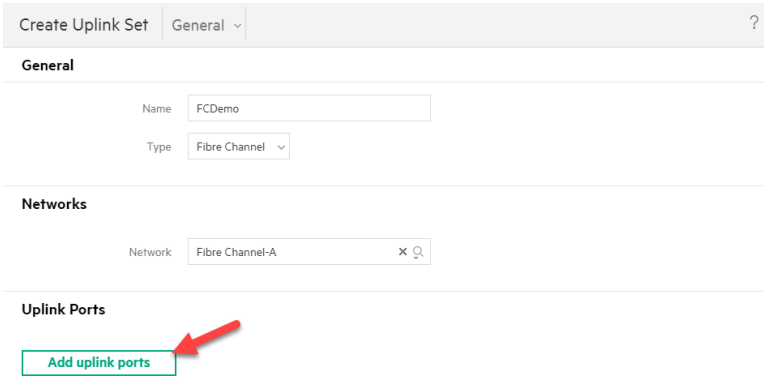
5. From the Type drop down list select *Fibre Channel*.



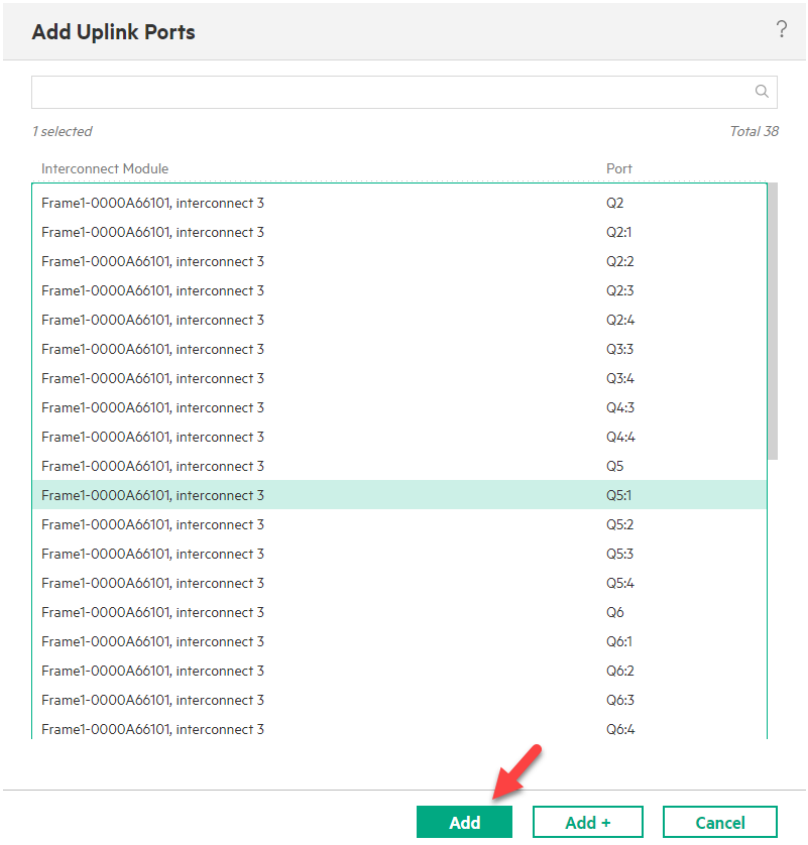
6. In the Networks section, select the desired SAN Fabric *Network* from the drop-down list.



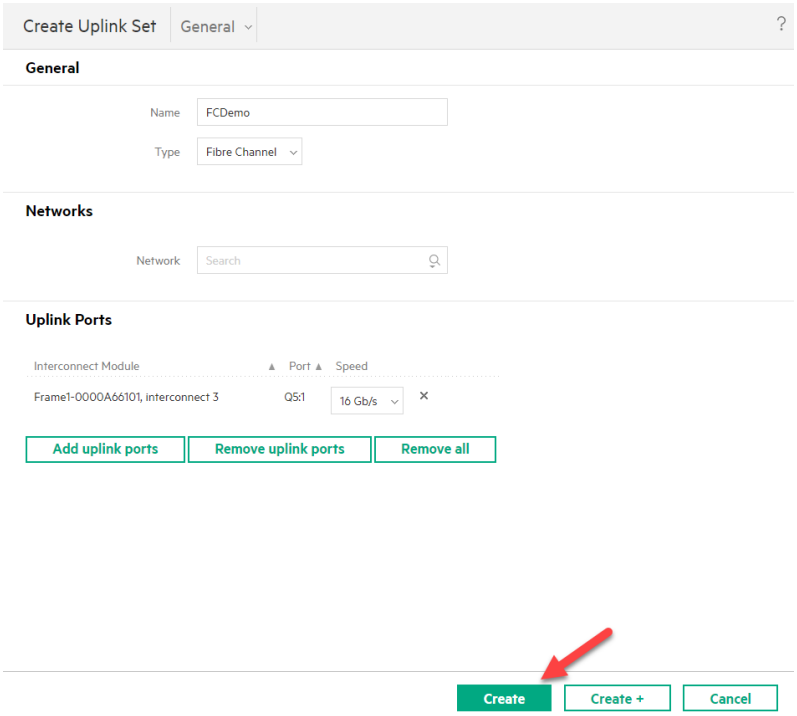
7. Under the Uplink Ports heading, click *Add uplink ports*



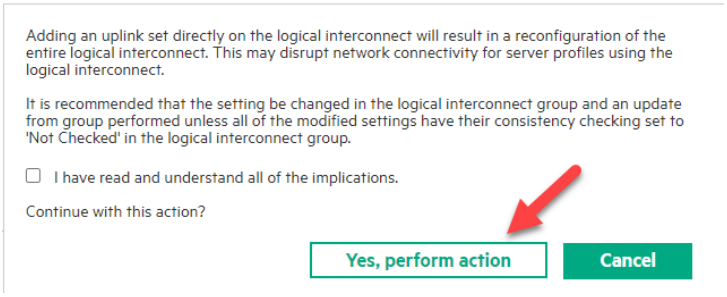
8. In the Add Uplink Ports to Uplink dialog, select at least one port for the uplink then click *Add*.



9. Click the *Create* button to finalize the Fibre Channel Uplink.



10. As we are adding a new uplink set the Logical Interconnect will be reconfigured and the following warning will be shown, if acceptable then check the box and then click *Yes, perform action.*



11. Click *OK* to save the changes to the *Logical Interconnect*.

Create Additional Storage Volume Templates for StoreServ Volumes

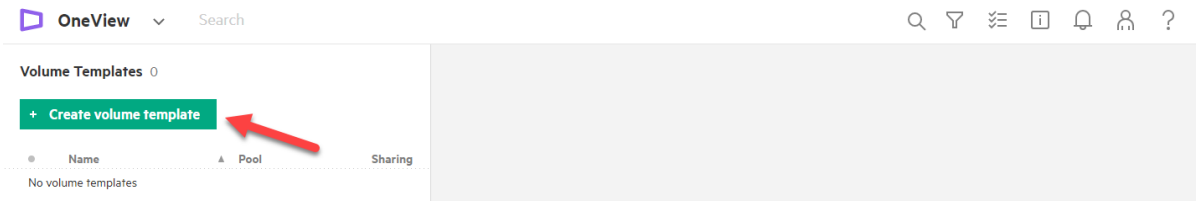
Storage Volume Templates allow the Storage Administrator to specify a set of volume properties when creating multiple volumes or to enforce certain volume property settings when other admins are creating volumes. Another way to restrict access / visibility of Storage Volume Templates is via Scopes. Storage Volume Templates are not required in order to provision Storage Volumes (unless the HPE OneView global storage setting to require a volume template is enabled – described later).

Create a storage volume template as follows.

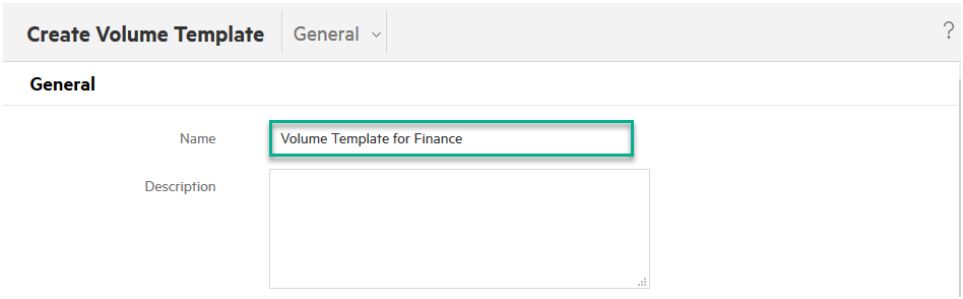
1. From the Top-Level menu, expand the *STORAGE* option and then select *Volume Templates*.



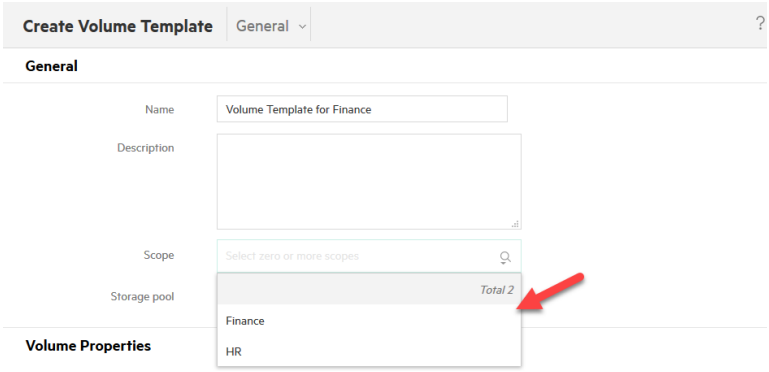
2. Click *Create volume template* button



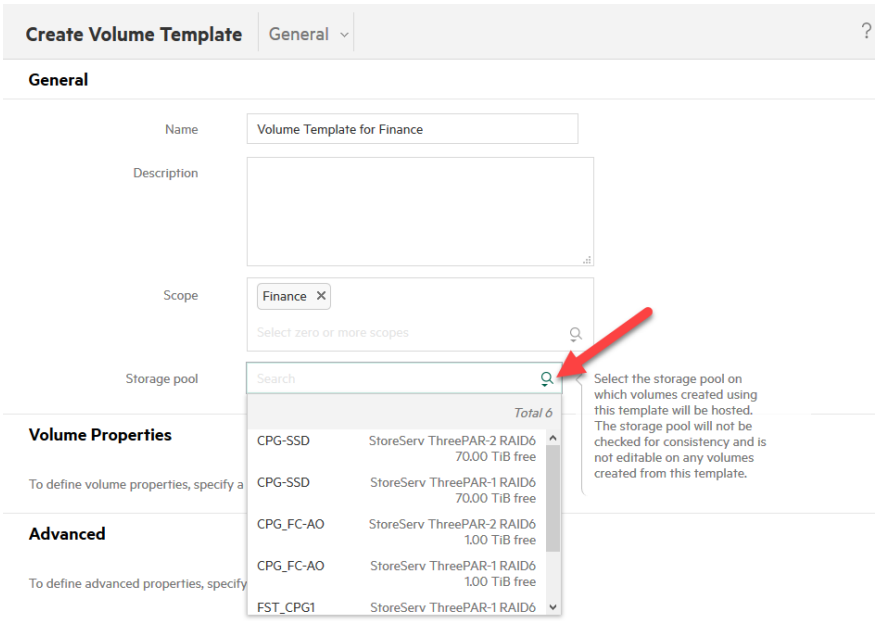
3. In the Create Volume Template screen, enter a *Name* for the Volume template and an optional description.



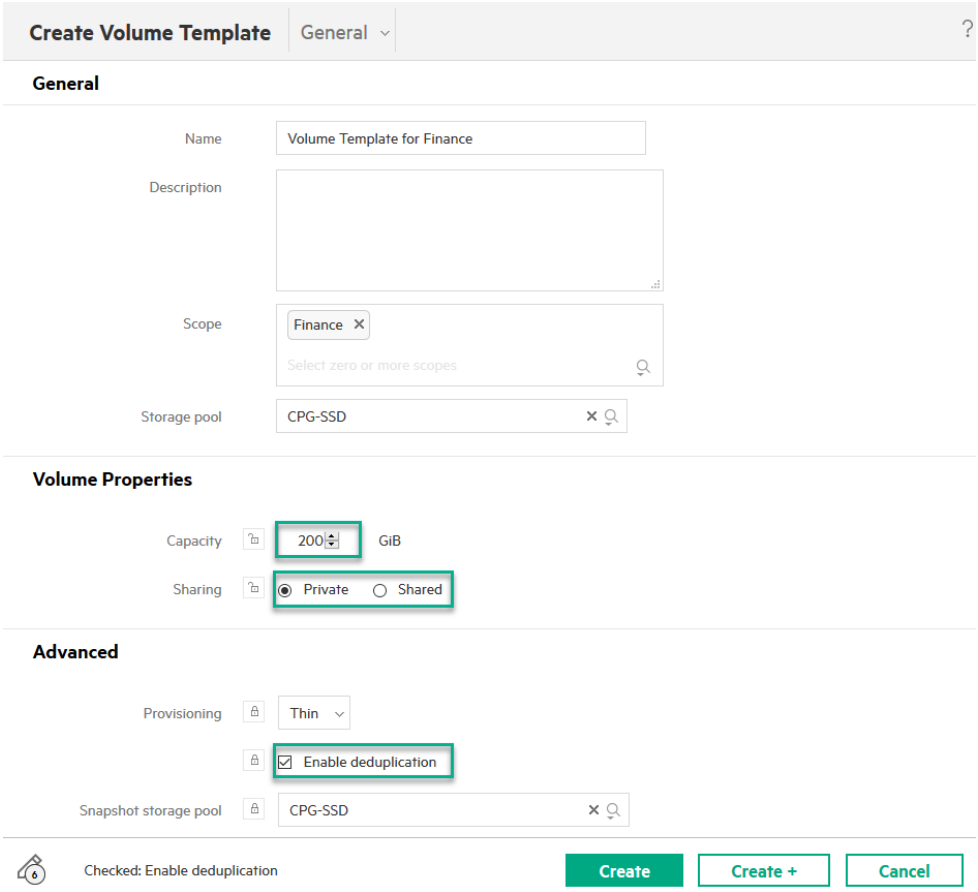
Optionally assign the volume template to a scope. Only users in the scope will be able to use the volume template and it will not be available to users in other scopes.



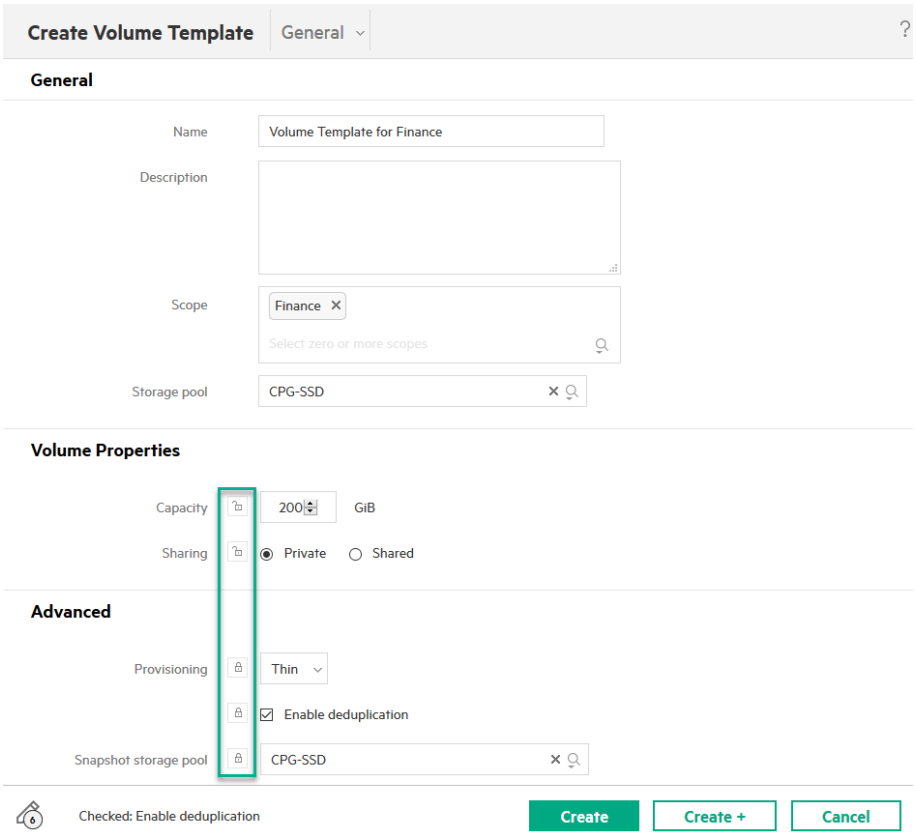
4. Using the storage pool drop down list, select the *Storage pool* the volume template will create volumes from.



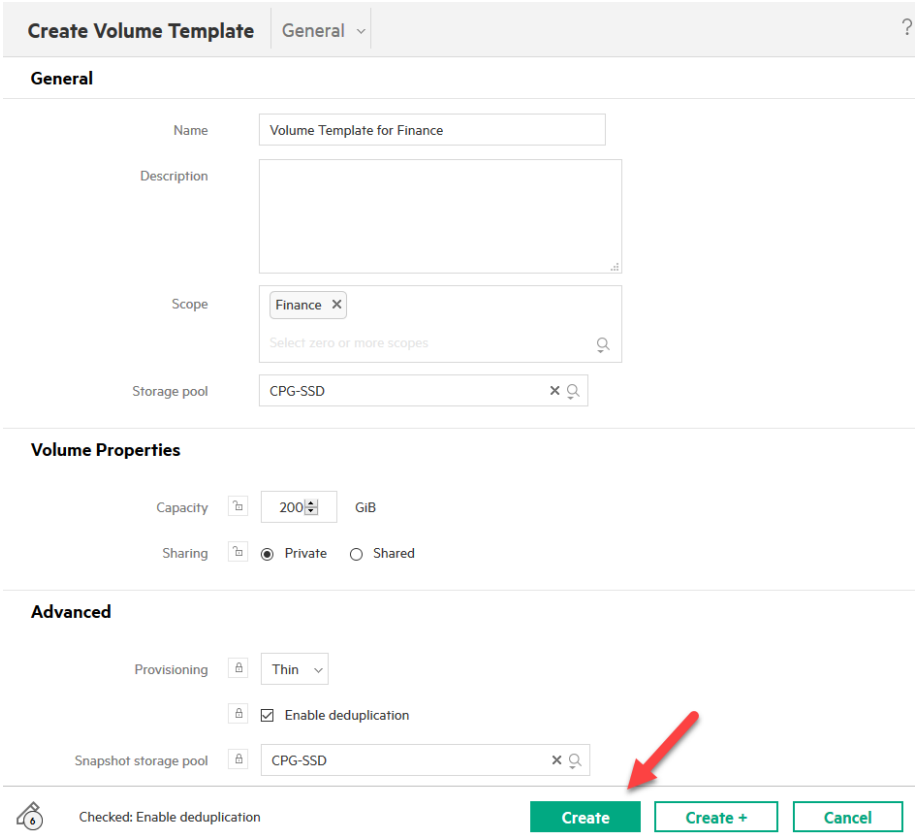
5. Once the volume template's storage pool is selected, the volume template is populated with the volume properties specific to volumes created within the pool. Select the volume property settings as desired.



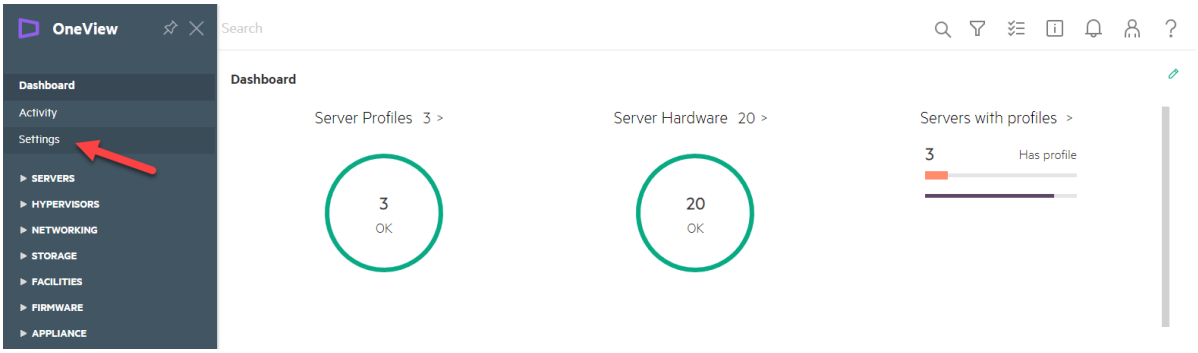
6. Next, select the enforcement mode for each volume property. Volume properties which are *locked* are not editable when a volume is created using the template. Volume properties which are *unlocked* are editable when a volume is created using the template. Click the lock icons to toggle property enforcement between *locked* and *unlocked*.



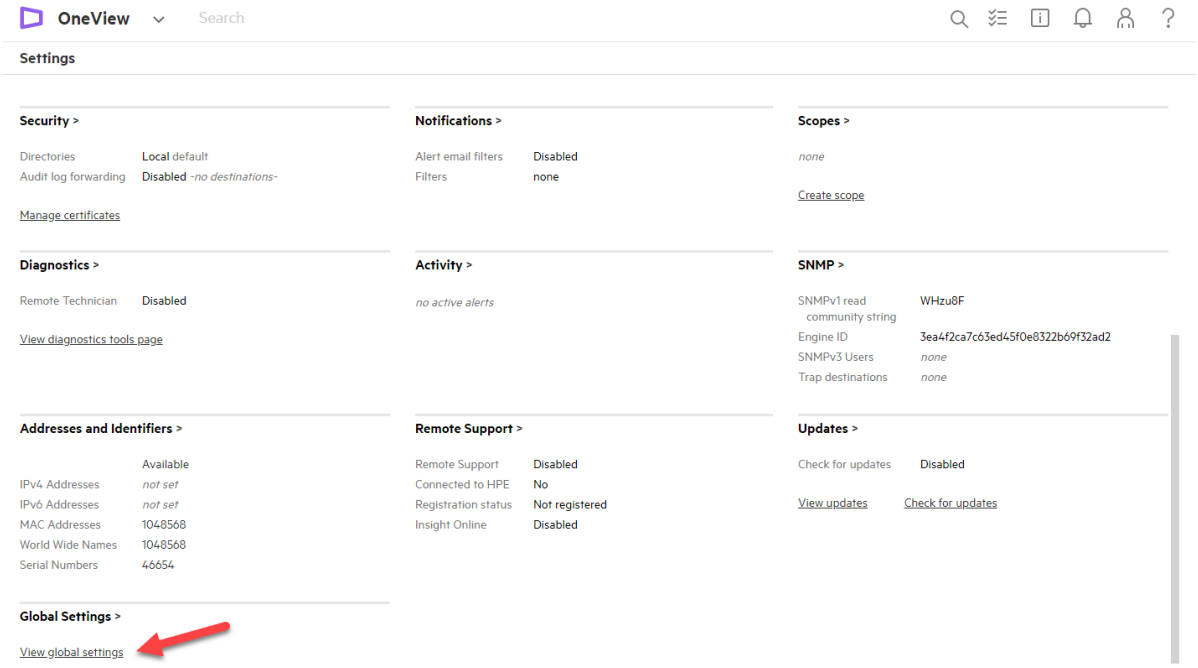
7. Then click the *Create* or *Create+* button to create the volume template.



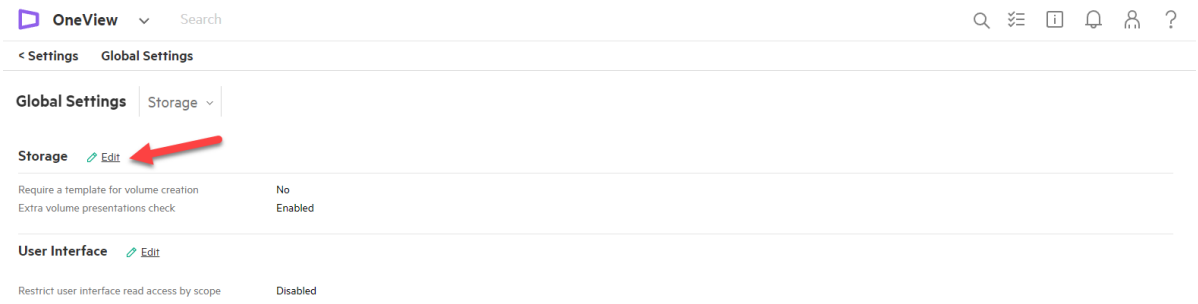
8. (Optional) If the Storage administrator wants to require that non-storage administrators must use storage volume templates when creating volumes, the *Require template for Volume Creation* Global Policy needs to be set, which is in the *Settings menu*.



9. In the Settings *Storage* section, click the *Edit* icon.



10. Click *Edit* and then change the toggle to *Require a template for volume creation* whenever non-storage administrators create volumes. Click *OK* to apply the setting

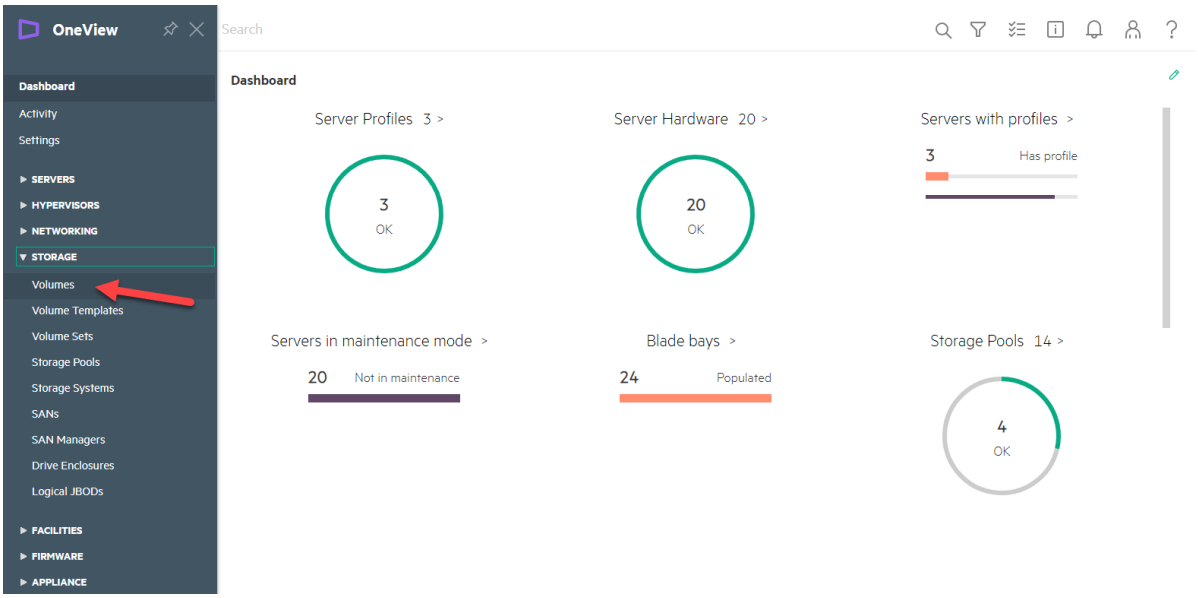


Create Additional StoreServ Storage Volumes

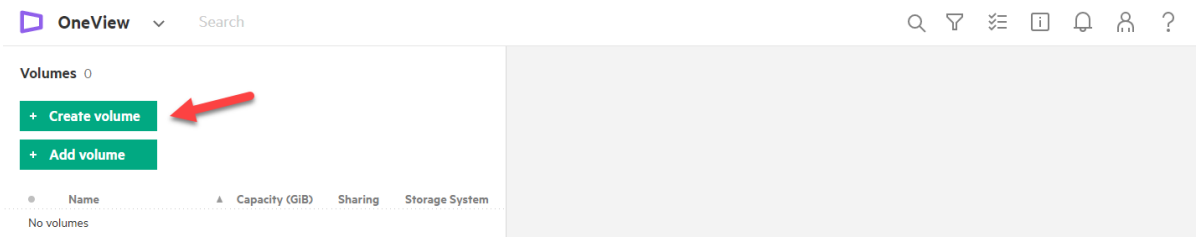
Volumes can be created independent of server profiles within the *Volumes* view, under the Storage column of the Top-Level Menu within the UI or created as part of a server profile. When created using the Volumes view, the volume's lifecycle will be independent of server profiles (i.e. "permanent"). When created as part of a server profile, the volume's lifecycle can optionally be tied to the server profile (i.e. "non-permanent", also called "Ephemeral") such that when the server profile is deleted, the volume will be deleted as well.

Volumes can be created by either server or storage administrator roles.

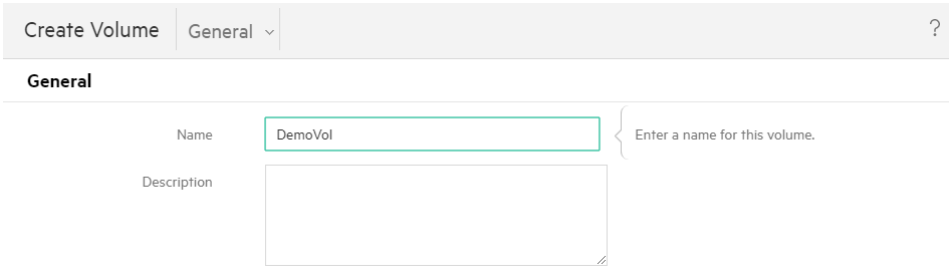
1. From the Top-Level menu, expand the *STORAGE* option and then select *Volumes*.



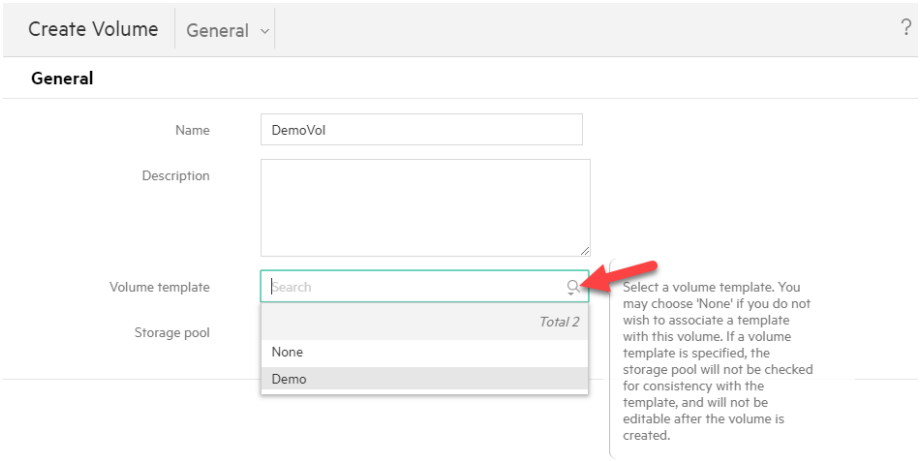
2. Click the *Create volume* button.



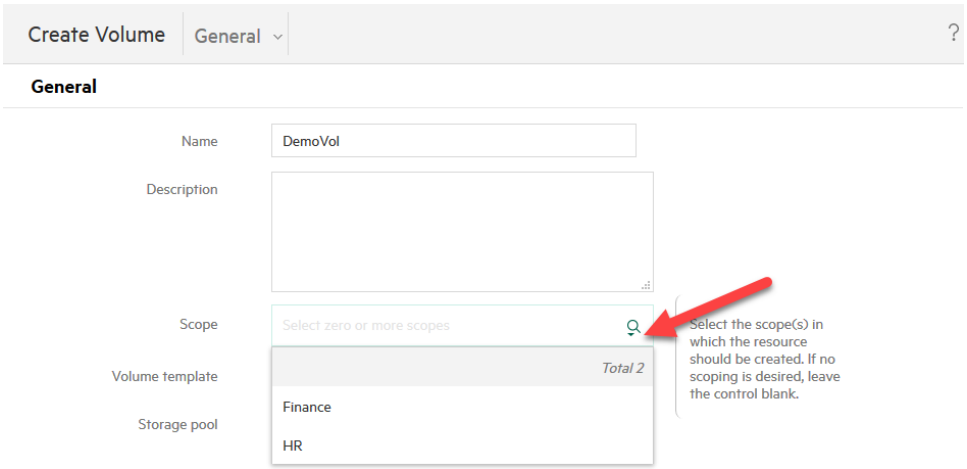
3. In the Create Volume screen, enter a *Name* and optionally a *Description* for the volume.



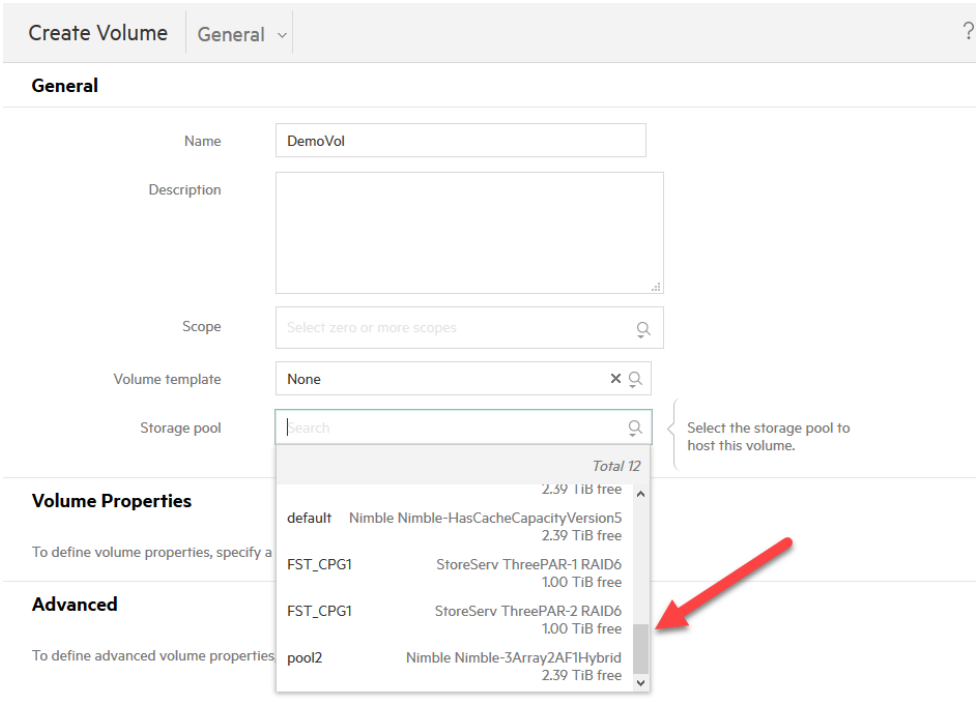
4. In the Create Volume screen, the options can be restricted if the Storage Administrator has forced Volume Creation to be provisioned from a Volume Template. Otherwise, the administrator creating the *Volume* may choose whether it will be associated with an available Volume Template or not. When creating a volume from a volume template select the template.



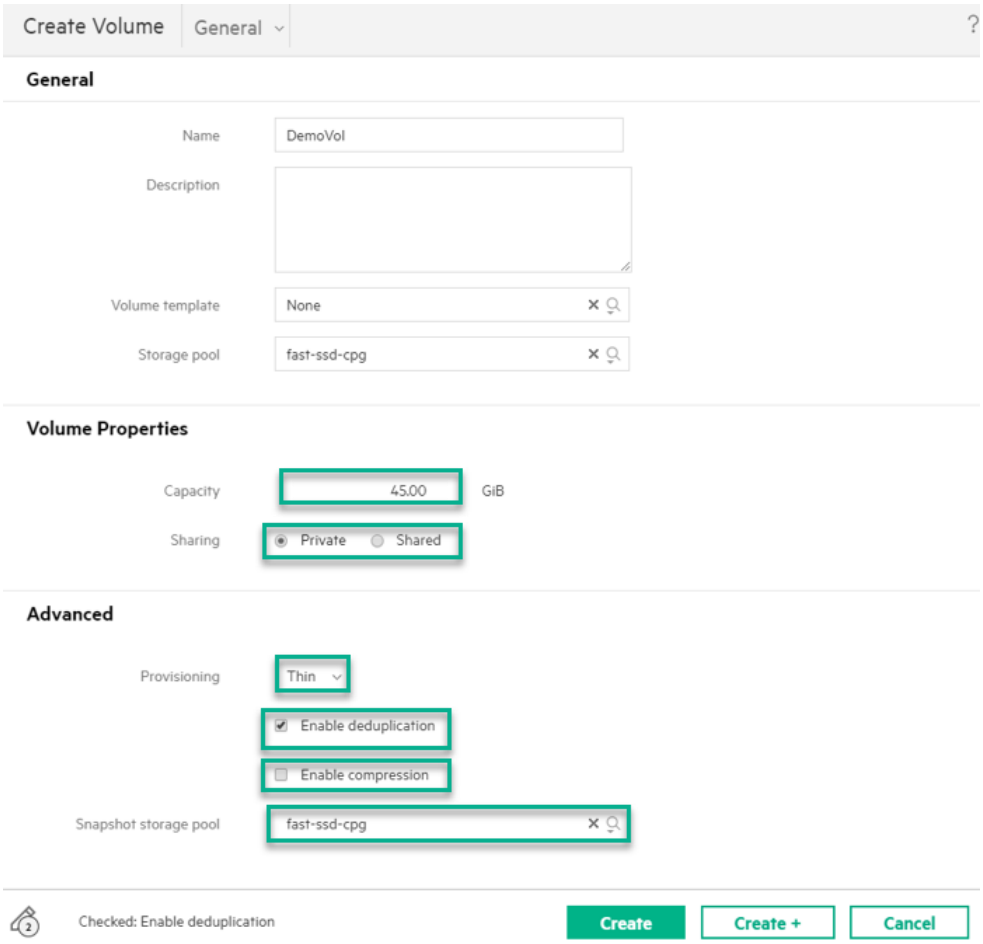
Optionally assign the volume to a scope, so only user with that scope can use the volume.



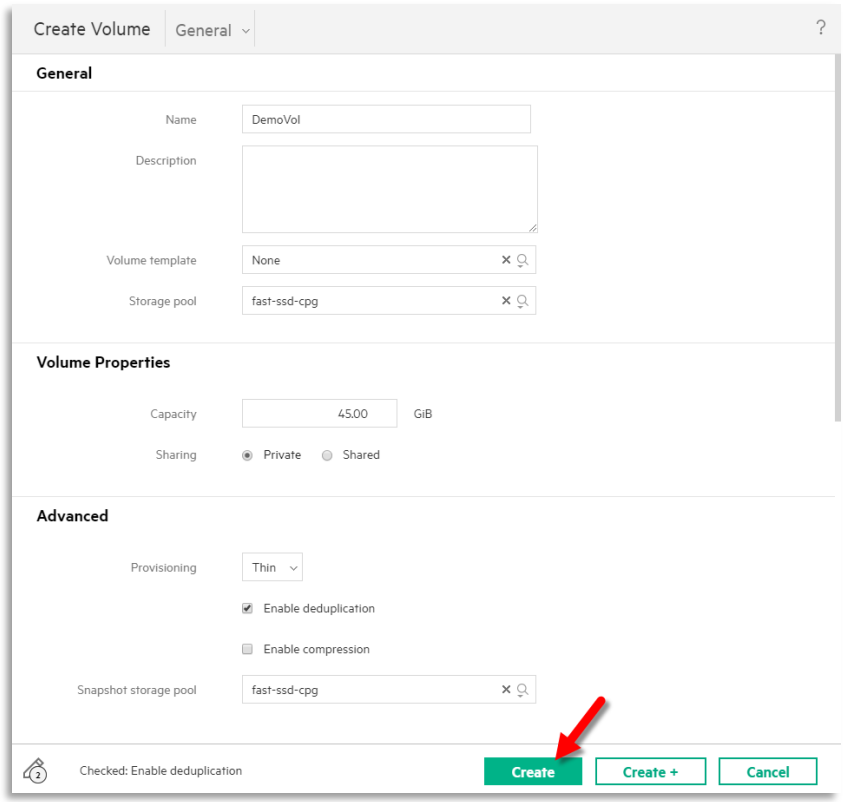
5. If not associated with a volume template, select the *Storage pool* for the volume



6. After selecting a volume template or storage pool, the Volume properties will be populated with the properties that can be set for the volume. Set the *Volume Properties* for the volume.



7. Click *Create* or *Create+* button to create the volume.

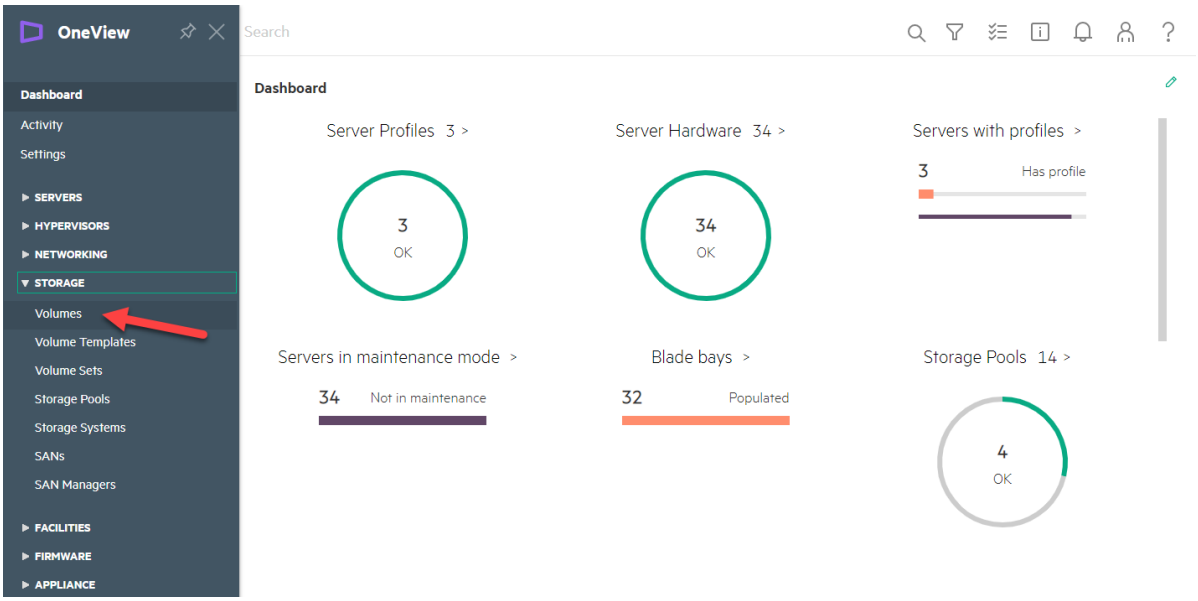


Note:
When creating volumes, HPE OneView attempts to name volumes on the storage system as close as possible to volume names in HPE OneView. When the HPE OneView volume name is not a valid volume name on the storage system (unsupported characters, too long, already exists, etc.), HPE OneView will remove illegal characters, shorten and ensure the name is unique to create a legal name on the storage system. Any scripting communicating with both systems needs to be aware of this.

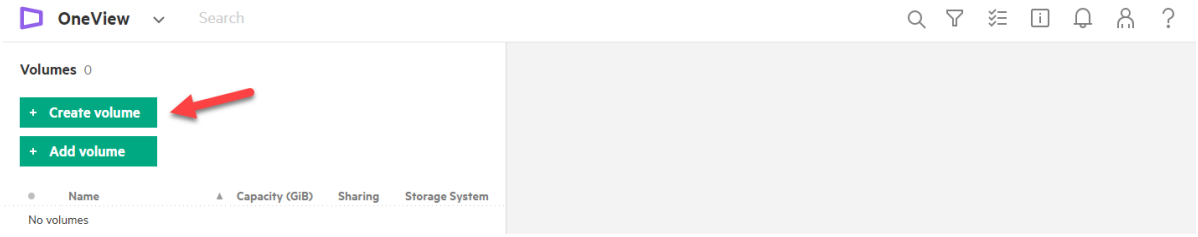
Configuring 3PAR Thin Dedupe on Volumes

HPE 3PAR StoreServ storage systems running Inform OS 3.2.1 MU1 and later support Thin Deduplication provisioning on SSD storage pools. To create volumes using Thin Deduplication provisioning, perform the following.

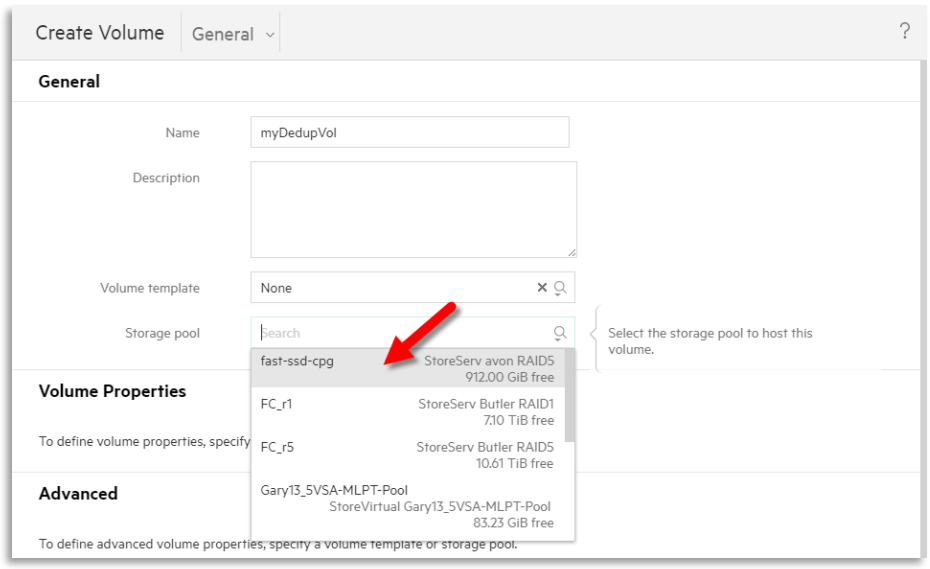
1. From the top-level menu, expand the *STORAGE* option and then select *Volumes*.



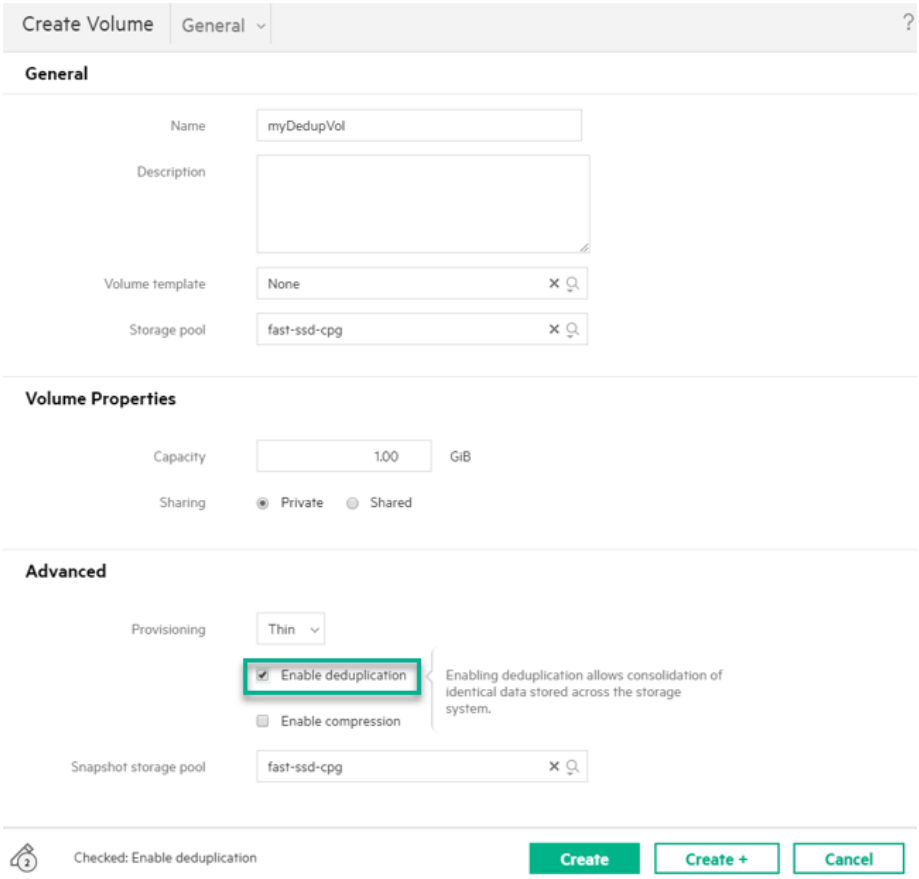
2. Select *Create volume* from the pane.



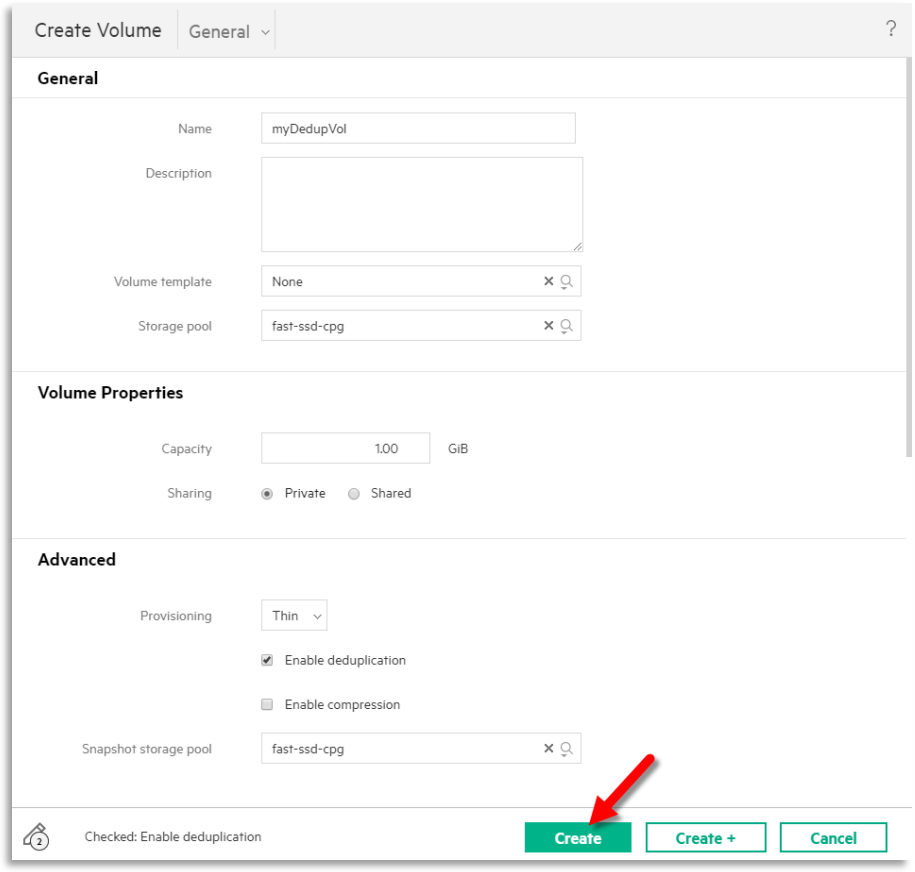
3. Select an SSD drive type storage pool on a StoreServ storage system supporting Thin Deduplication.



4. Select the *Enable deduplication* provisioning type for the volume.

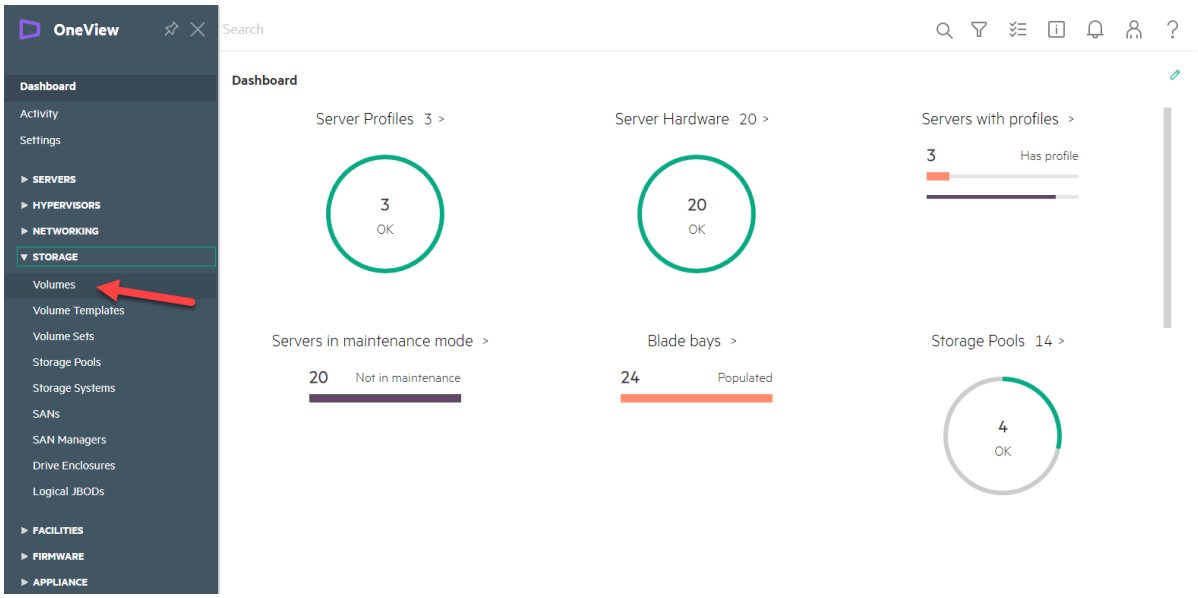


5. Click *Create* or *Create+* to create the volume.

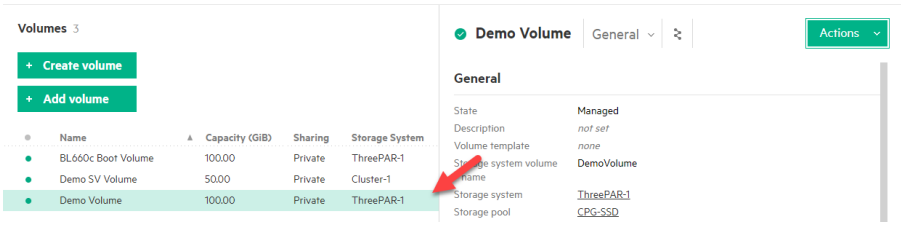


Create Storage Snapshots

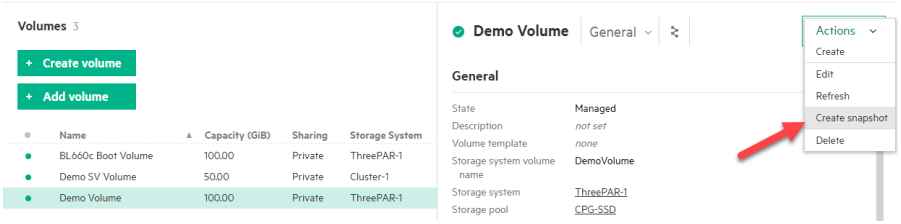
1. From the top-level menu, expand the *STORAGE* option and then select V*olumes*.



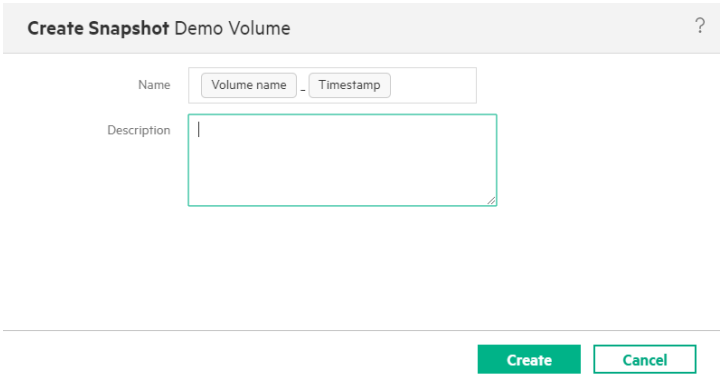
2. From the menu, select the *desired volume* that will have the snapshot taken



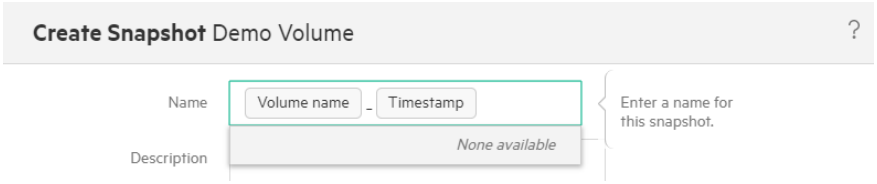
3. From the Actions menu, select *Create snapshot*.



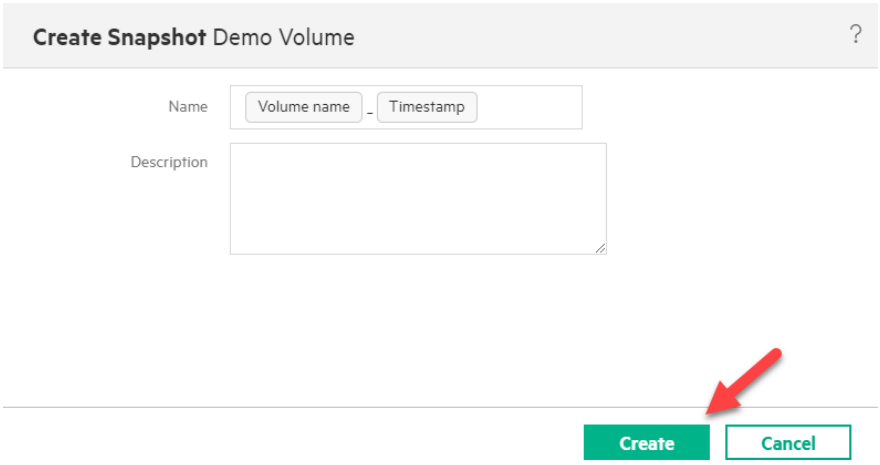
4. In the Create Snapshot window, enter a *Description* for the snapshot



A. (Optional) You will notice that a Name is already created using the variables of [Volume Name]_[Timestamp]. This can be changed by selecting inside of the *Name* dialog box and editing the data within.

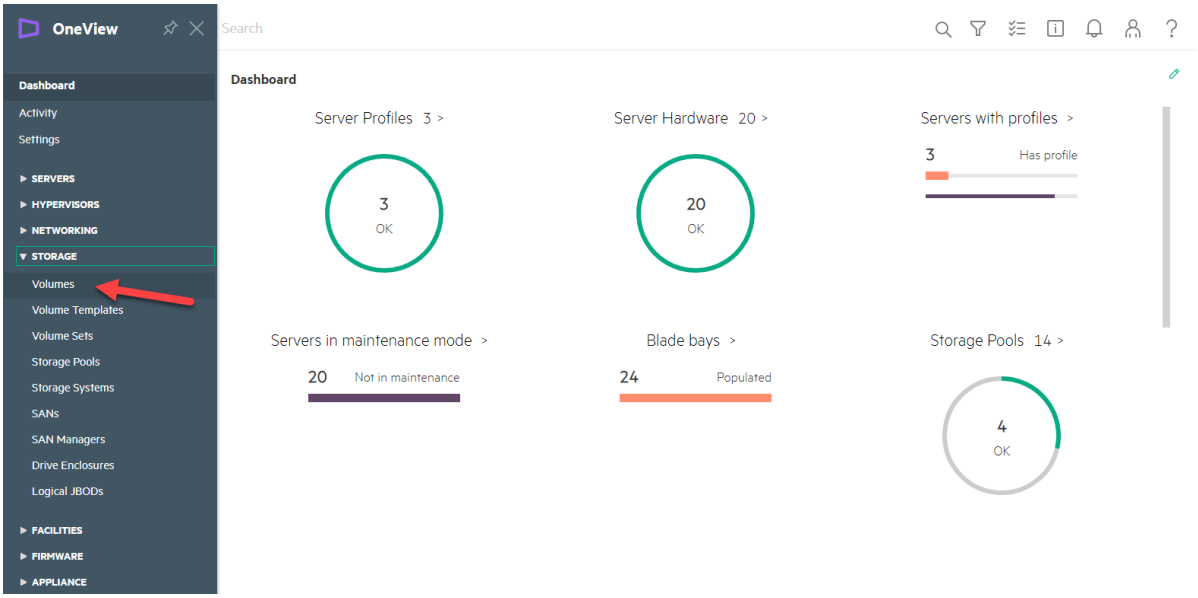


5. Click *Create* to create the snapshot

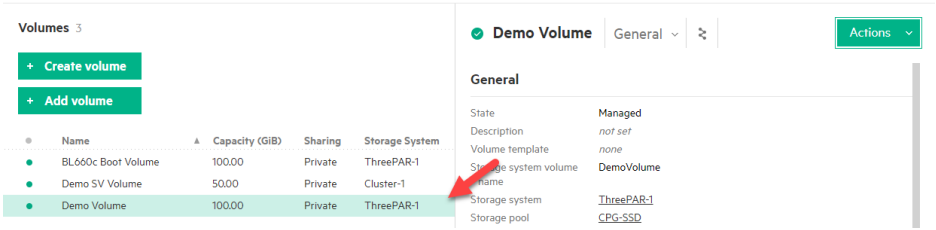


Viewing Storage Snapshots

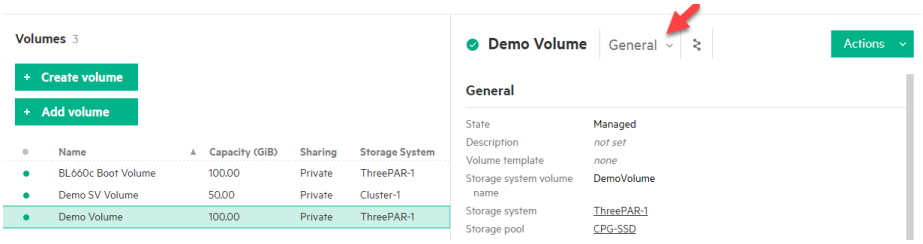
1. From the top-level menu, expand the *STORAGE* option and then select *Volumes*.



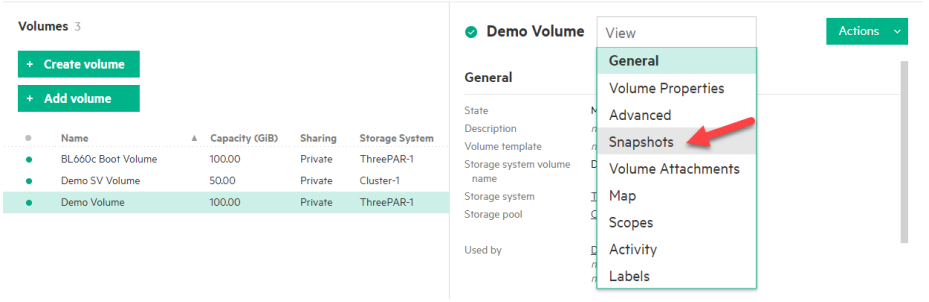
2. From the menu, select a volume to view the snapshots associated with that volume.



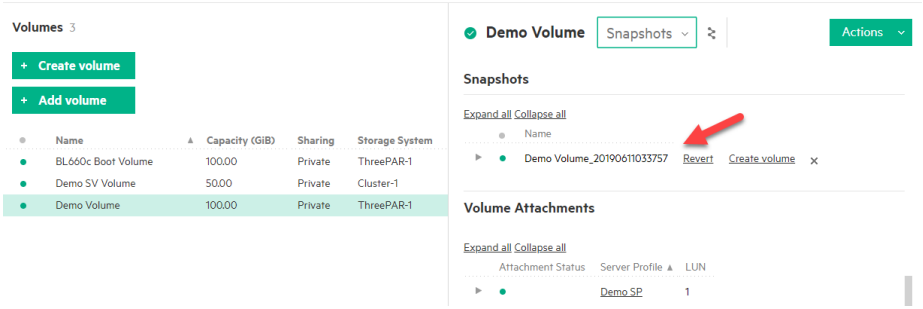
3. Open the *General* menu for the volume



4. Select *Snapshots* from the menu.

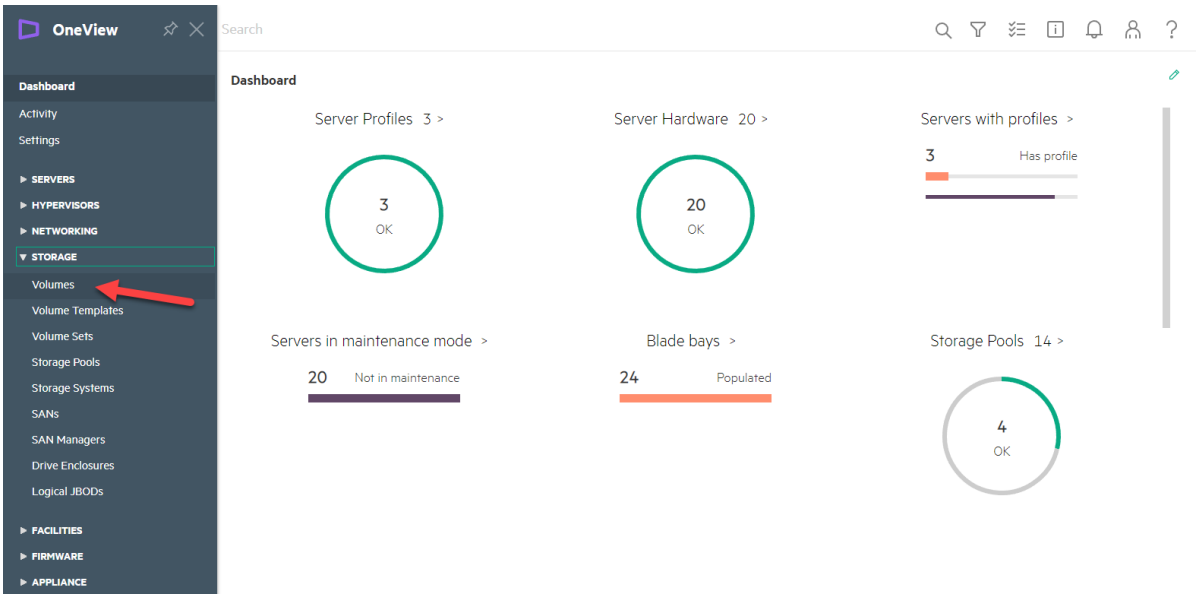


5. Examine the details of the snapshots available

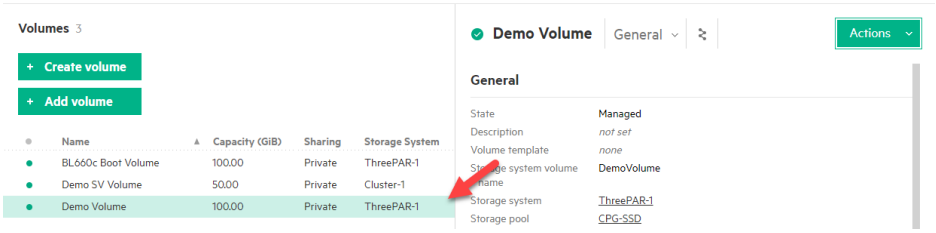


Deleting Storage Snapshots

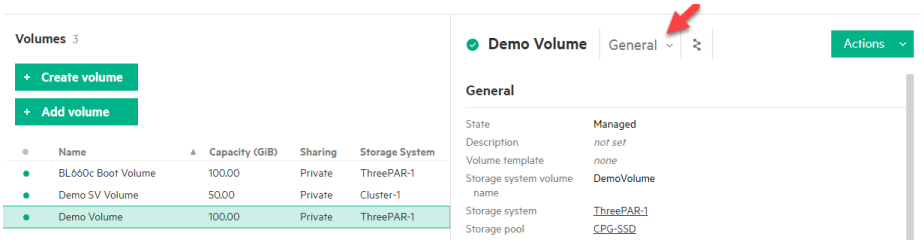
1. From the top-level menu, expand the *STORAGE* option and then select *Volumes*.



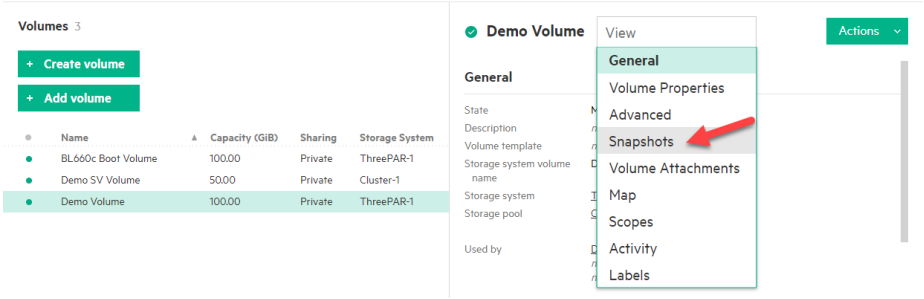
2. From the menu, select a volume to view the snapshots associated with that volume.



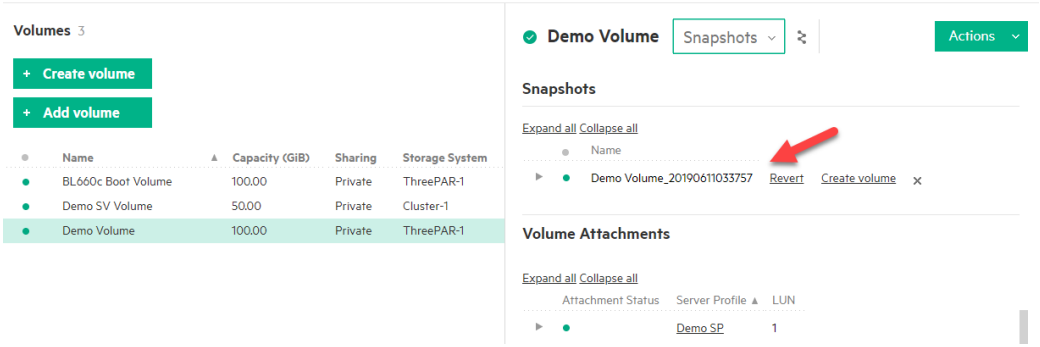
3. Open the *General* menu for the volume



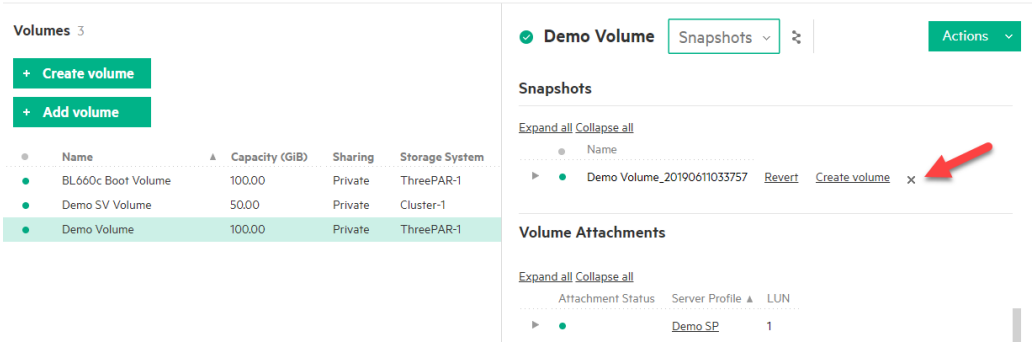
4. Select *Snapshots* from the menu.



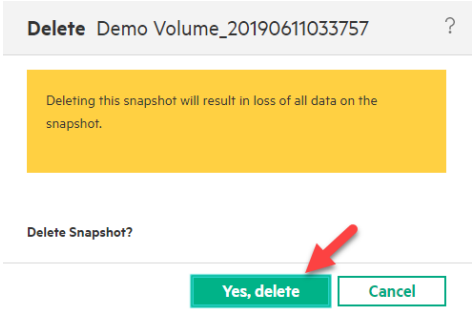
5. Examine the details of the snapshots available



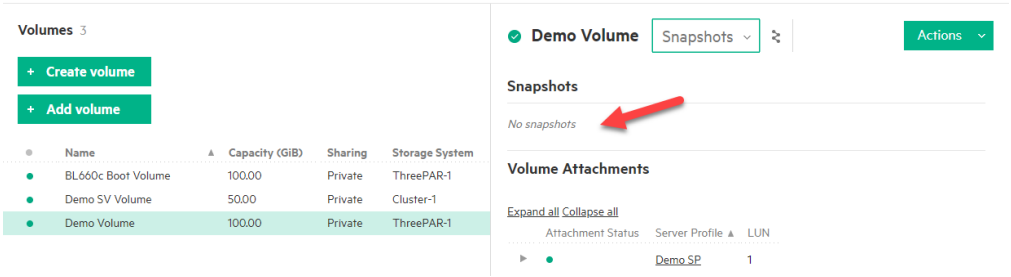
6. Click the *X* next to the snapshot information to delete the desired snapshot



7. Select *Yes, delete* on the delete snapshot confirmation dialog

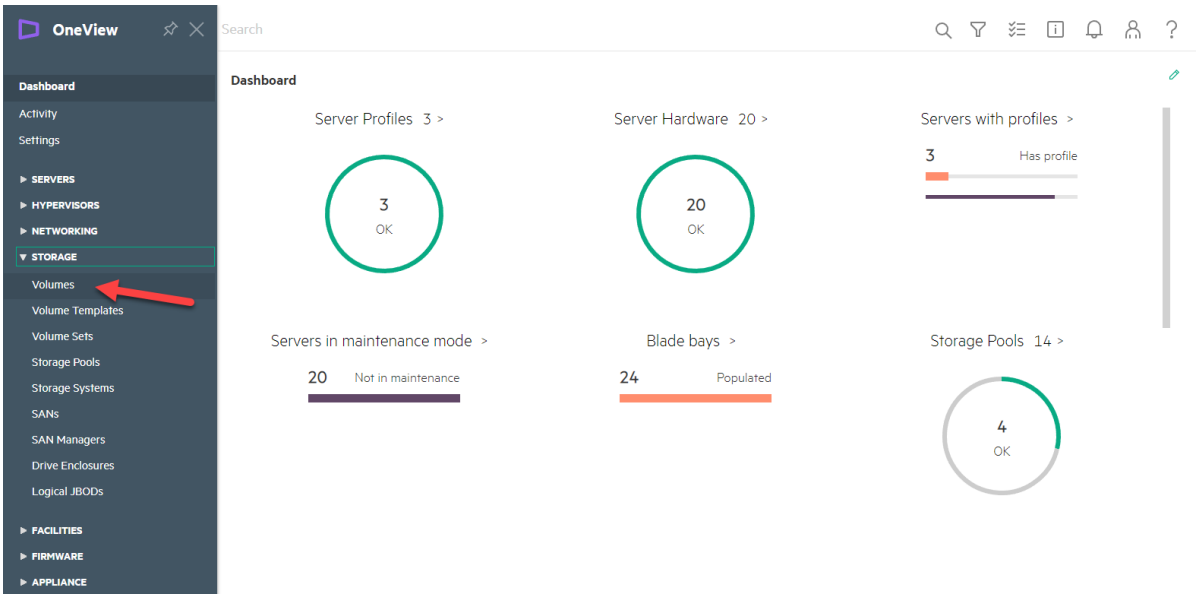


8. Verify that the snapshot has been removed from the volume

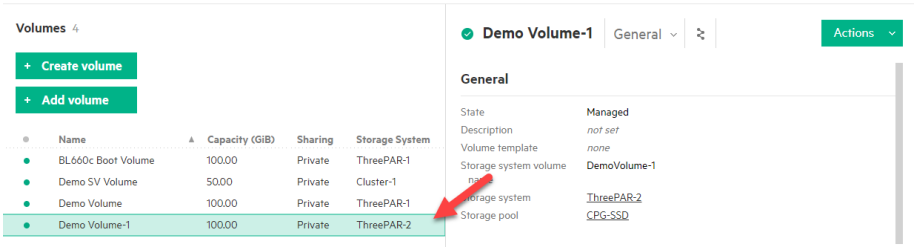


Reverting to previous Storage Snapshots

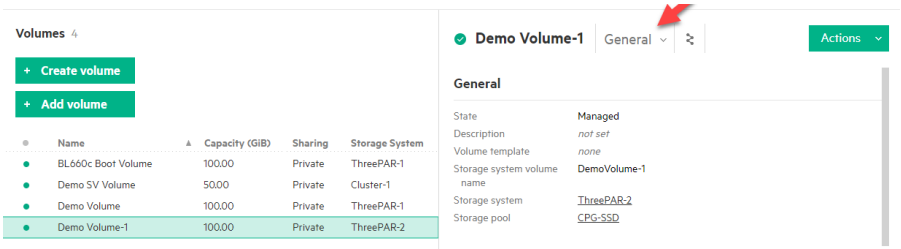
1. From the top-level menu, expand the *STORAGE* option and then select *Volumes*.



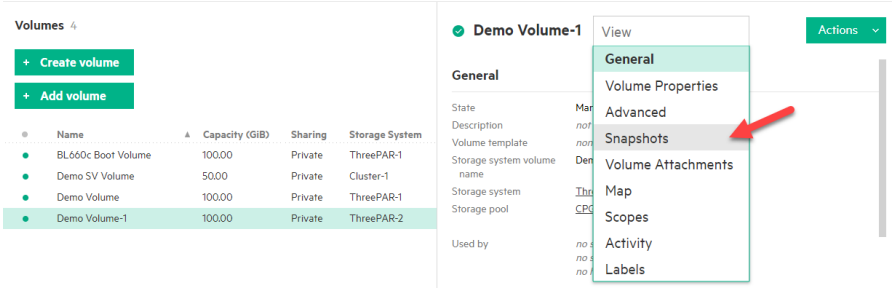
2. From the menu, select a volume to view the snapshots associated with that volume.



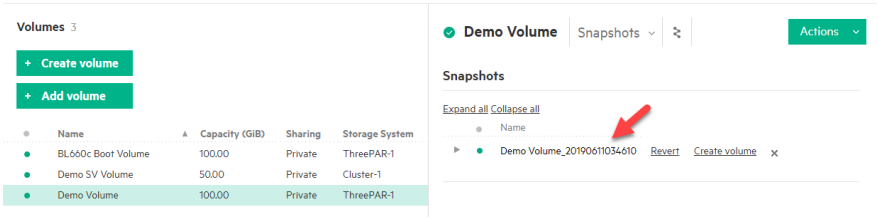
3. Open the *General* menu for the volume



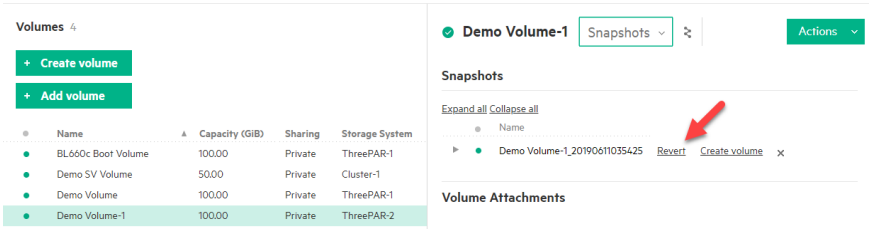
4. Select *Snapshots* from the menu.



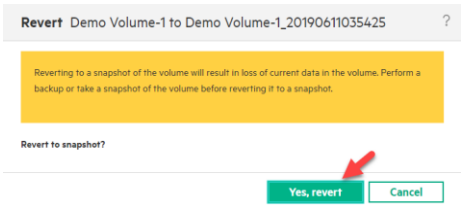
5. Examine the details of the snapshots available



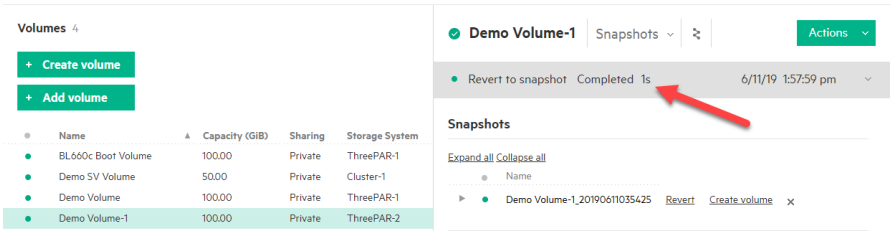
6. Select the *Revert* hyperlink



7. Select *Yes, revert* on the Revert Snapshot confirmation dialog

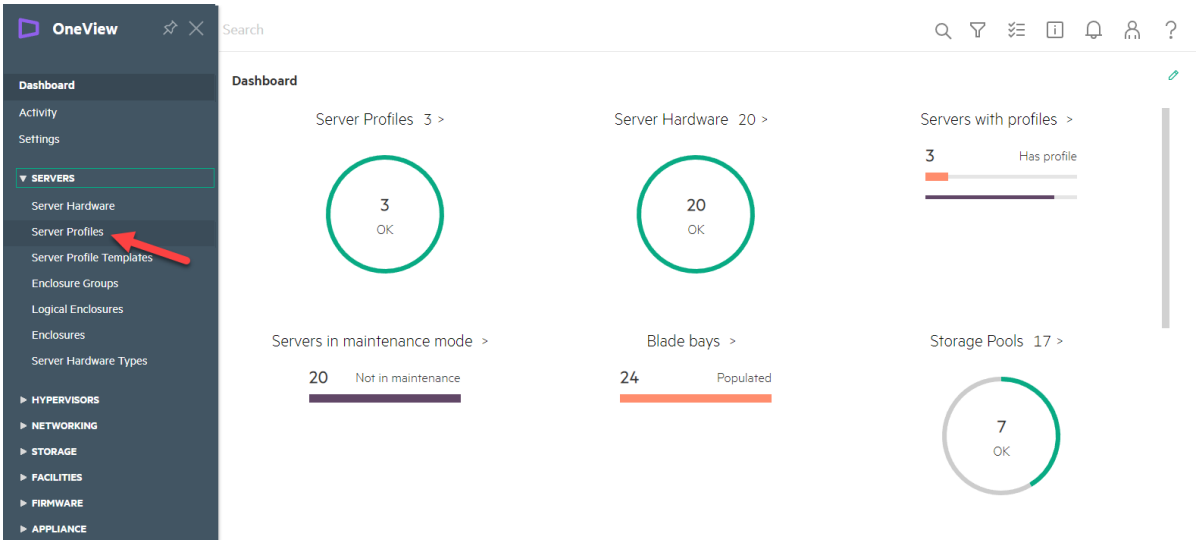


8. Verify that the revert process completed successfully

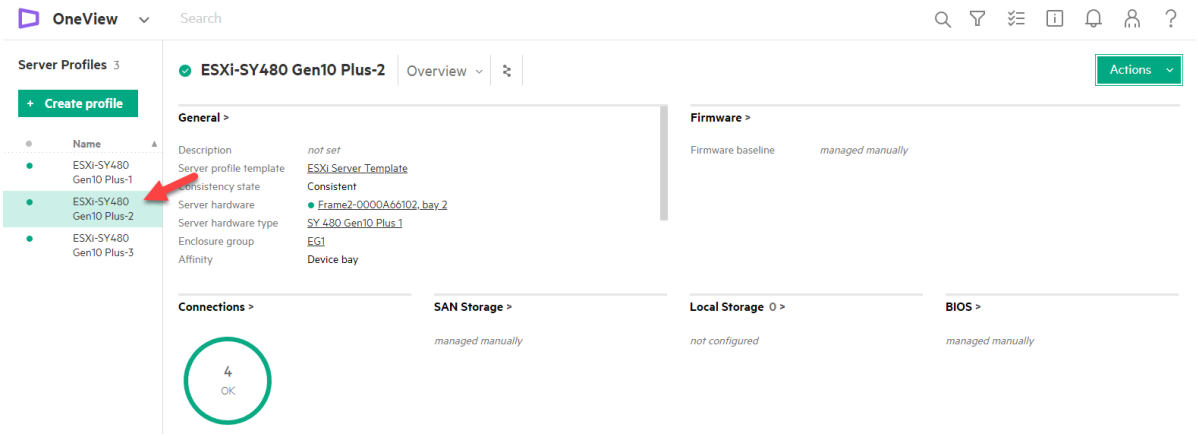


Removing Networks from a Server Profile

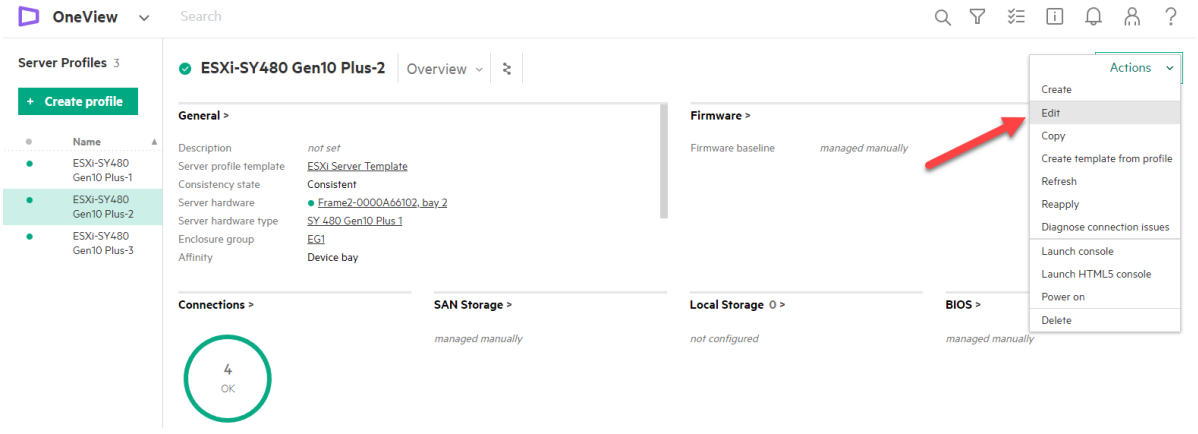
1. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*



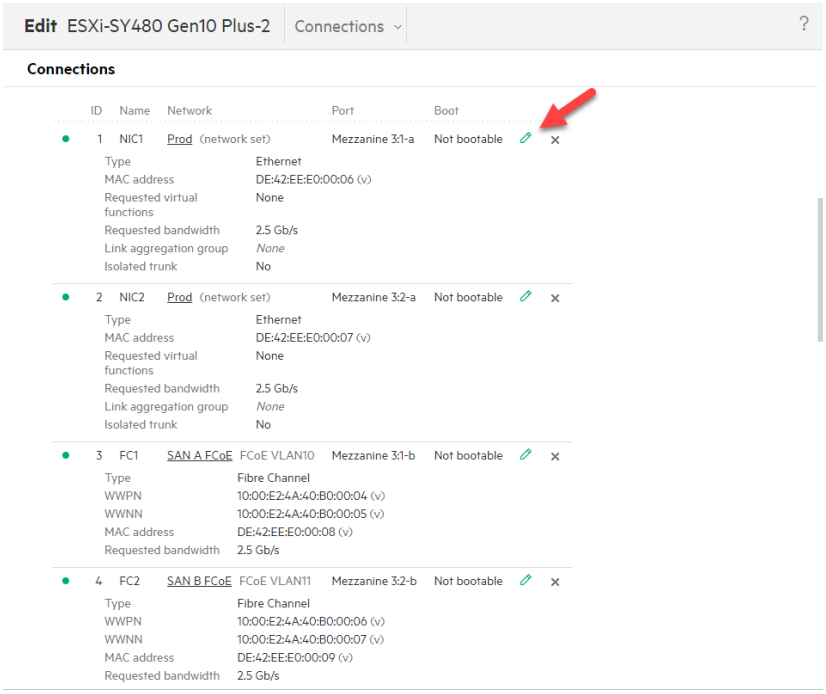
2. Select the server profile you want to edit from the menu on the left



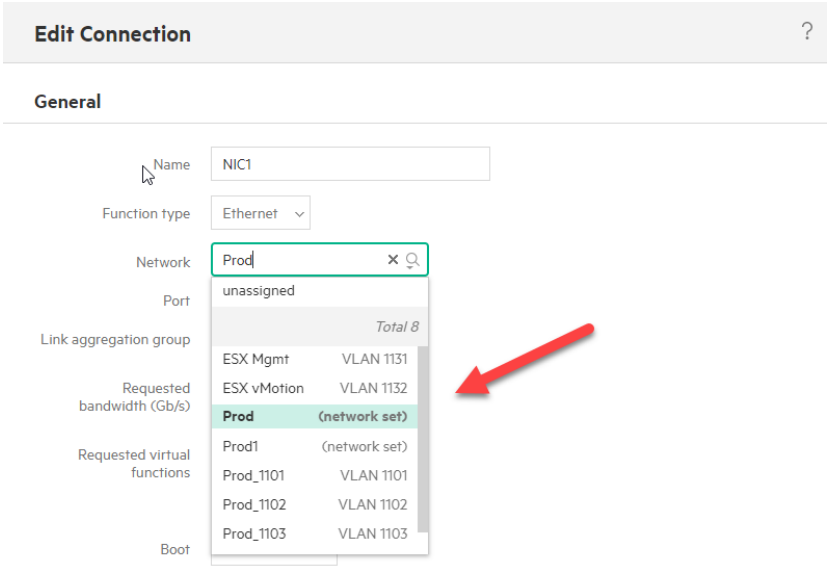
3. From the Actions menu, select *Edit*.



4. Scroll down to the connections section of the Server Profile Dialog and *click* on the pencil to edit.



5. Add / change the Network for the connection.

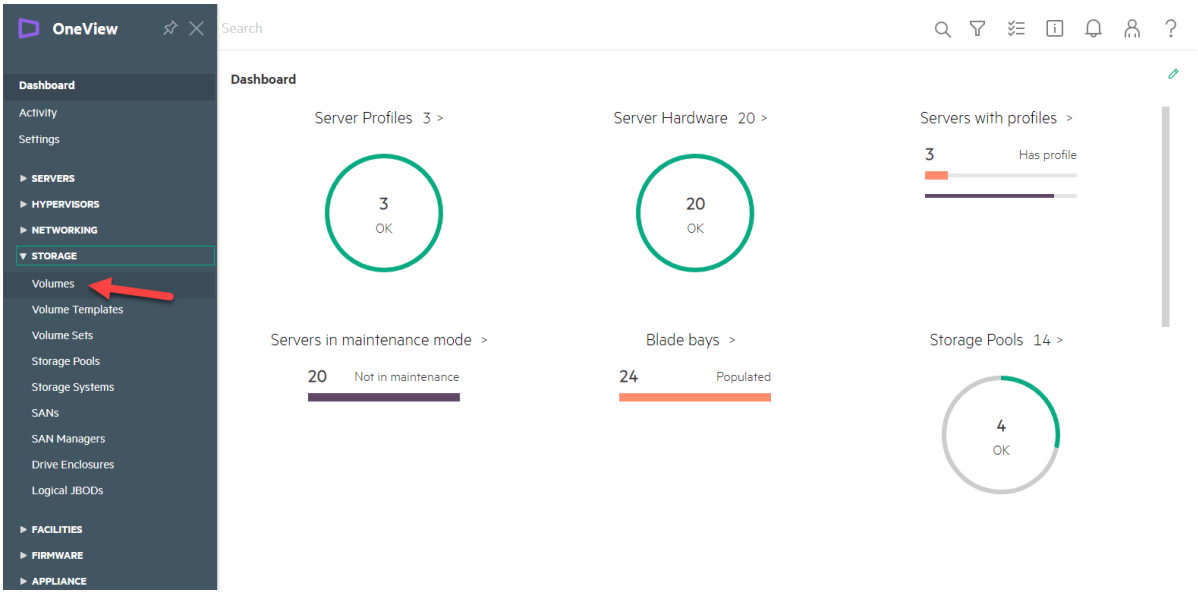


6. Click the *OK* button to save the changes to the Server Profile.

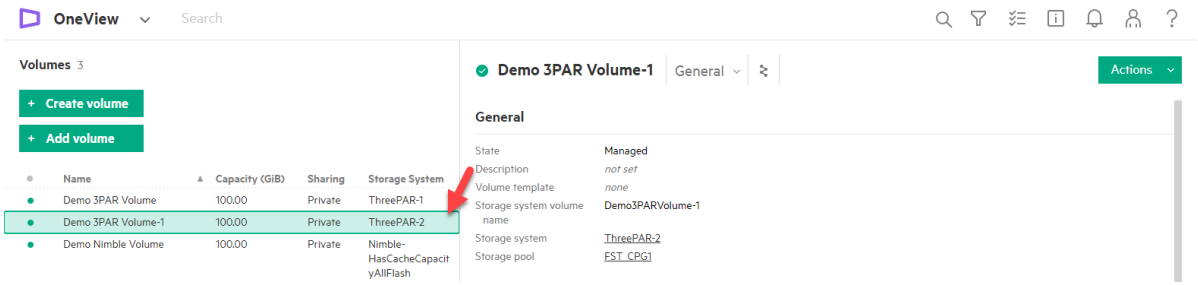
Deleting a volume from HPE OneView

In this Use Case you will remove a volume from HPE OneView.

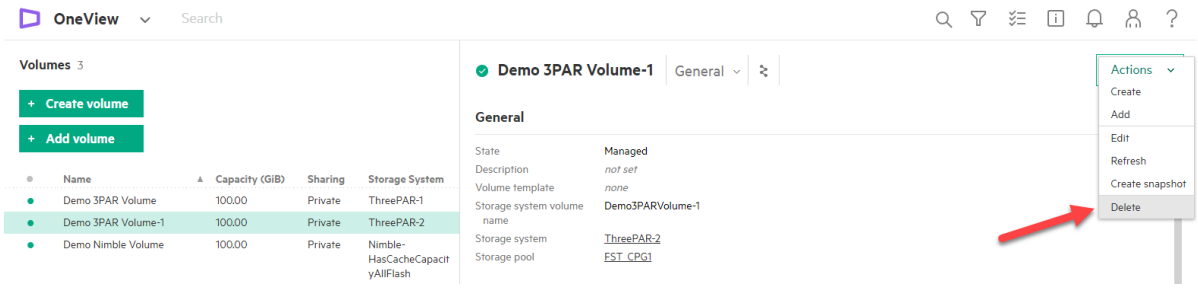
1. From the Top-Level Menu, expand the *STORAGE* option and then select Volumes



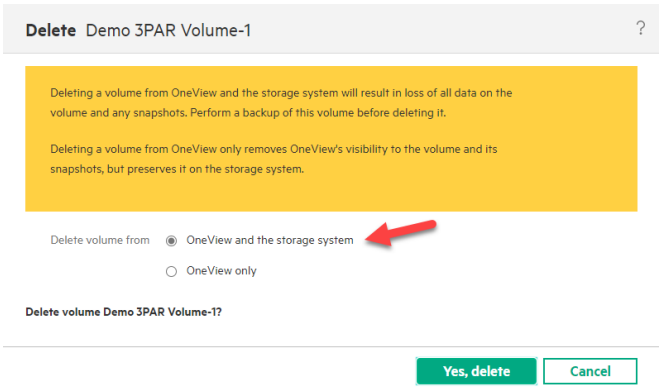
2. Select the volume to be deleted from the menu.



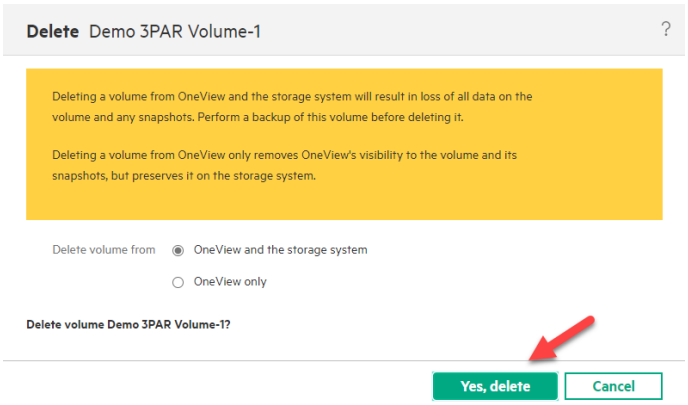
3. From the Actions menu, select *Delete*.



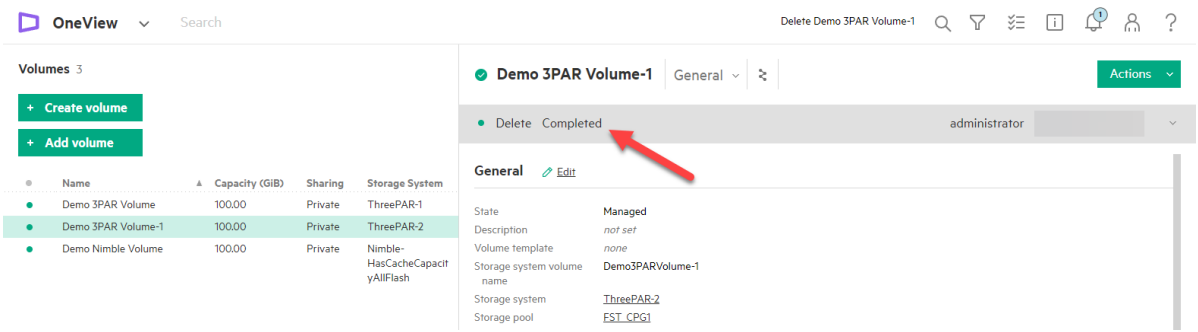
4. Select the desired type of volume deletion



5. Click the *Yes, delete* button remove the volume.



6. Verify that the volume has been deleted



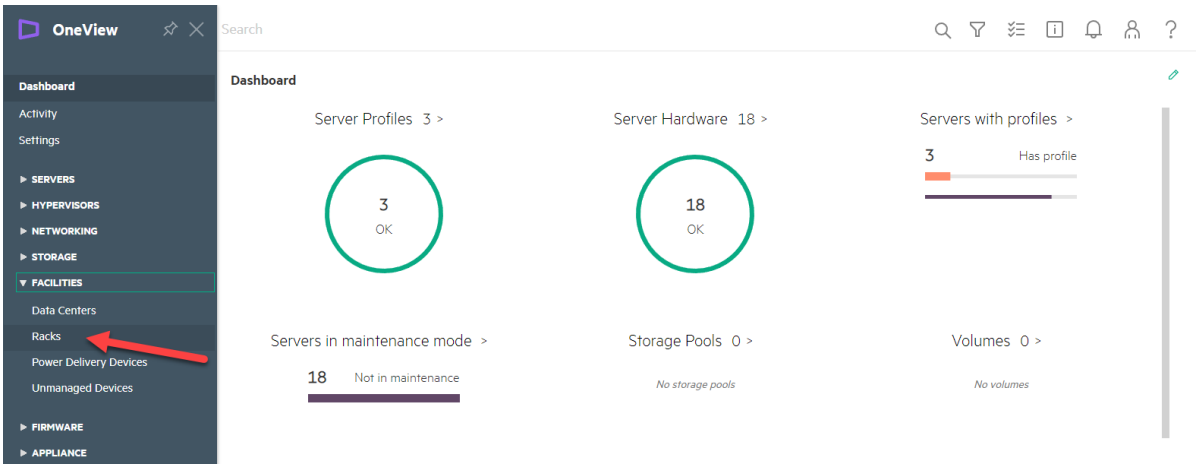
Adding New Racks Based on Location Discovery Services

Racks are automatically created based on LDS. HPE ProLiant Servers mounted in HPE Intelligent Series Racks are automatically grouped in racks in the proper positions. The initial rack names are provided by the Rack Serial Number.

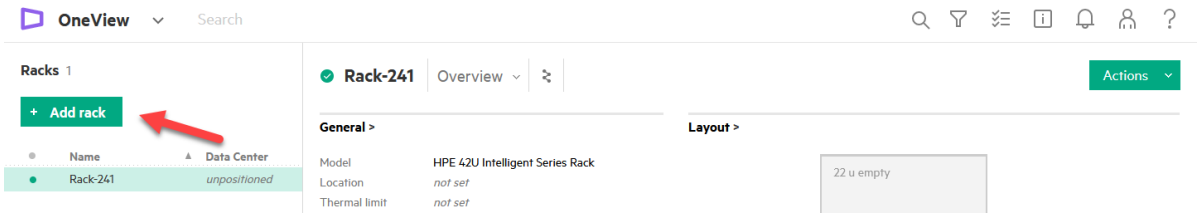
Adding Servers to Racks without Location Discovery Services (LDS)

If LDS is not present, racks are not automatically created for rack mount servers. ProLiant servers may be added to racks previously created via enclosure discovery or racks may be created manually and have servers added to them. For either option, begin by navigating to the Racks screen.

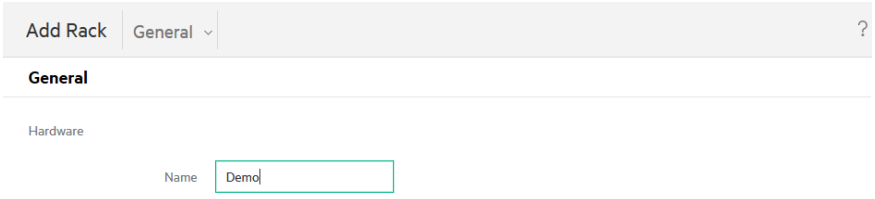
1. From the Top-Level Menu, expand the *FACILITIES* option and then select *Racks*.



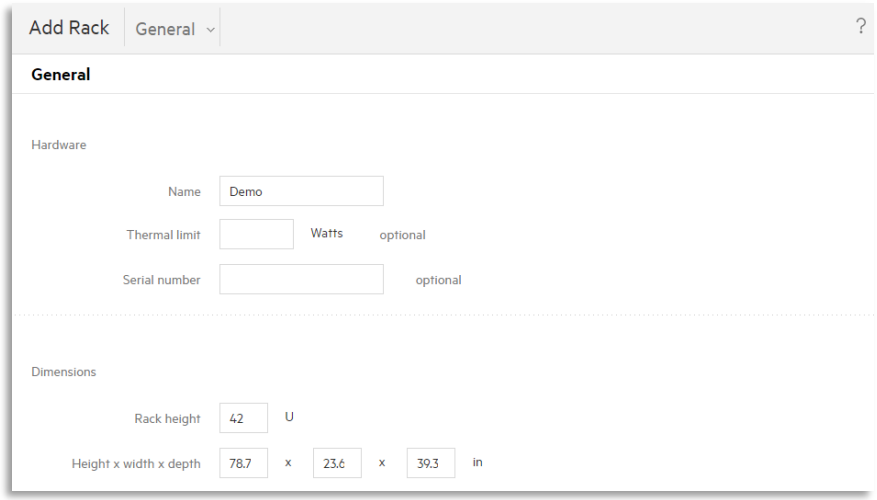
2. On the Racks screen, select the *Add rack* button in the left panel.



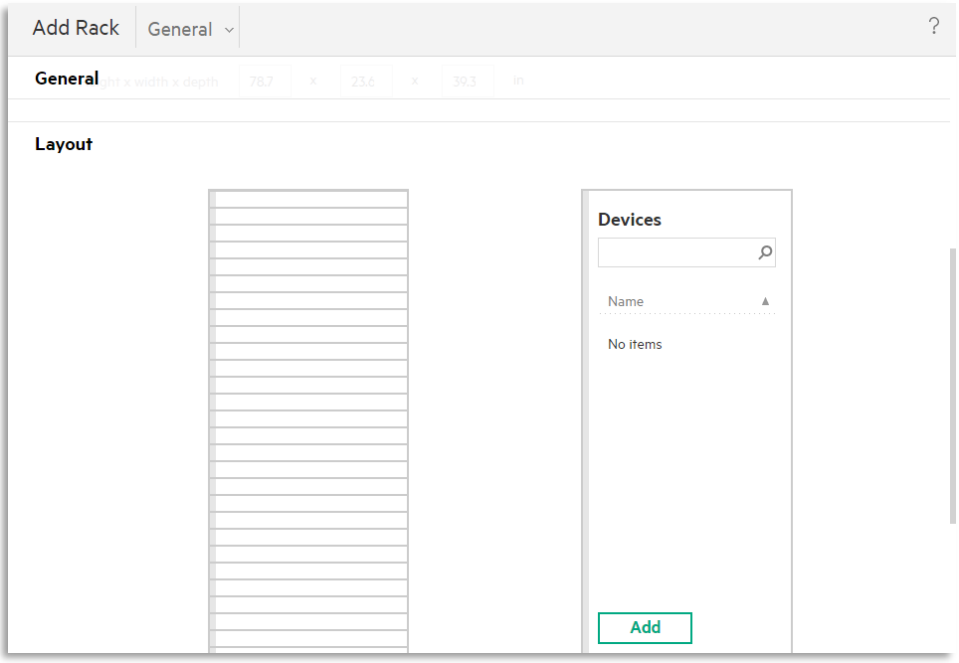
3. Once on the Add Rack screen, enter a *Name* for the Rack



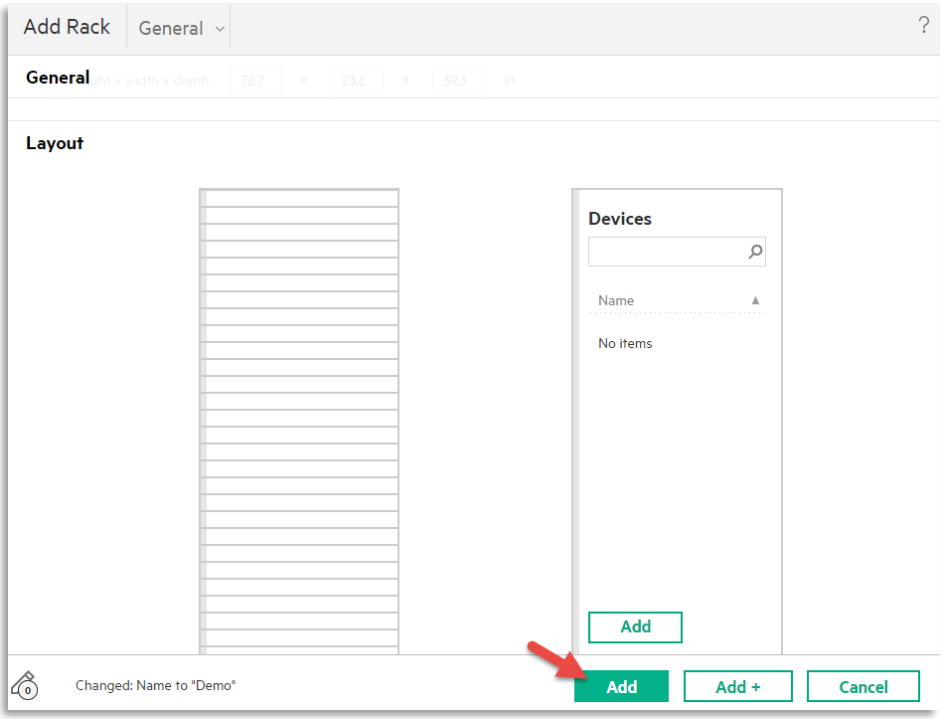
4. In the General pane, enter the details about the rack (thermal limit, serial number, U-height and dimensions)



5. The Layout panel consists of a visual representation of the rack and its slots, a list of available devices and a search box to find the desire systems and enclosures. From this panel, you can add, remove, and rearrange devices within the rack and edit the device details. To place a device, drag and drop it in the desired location.

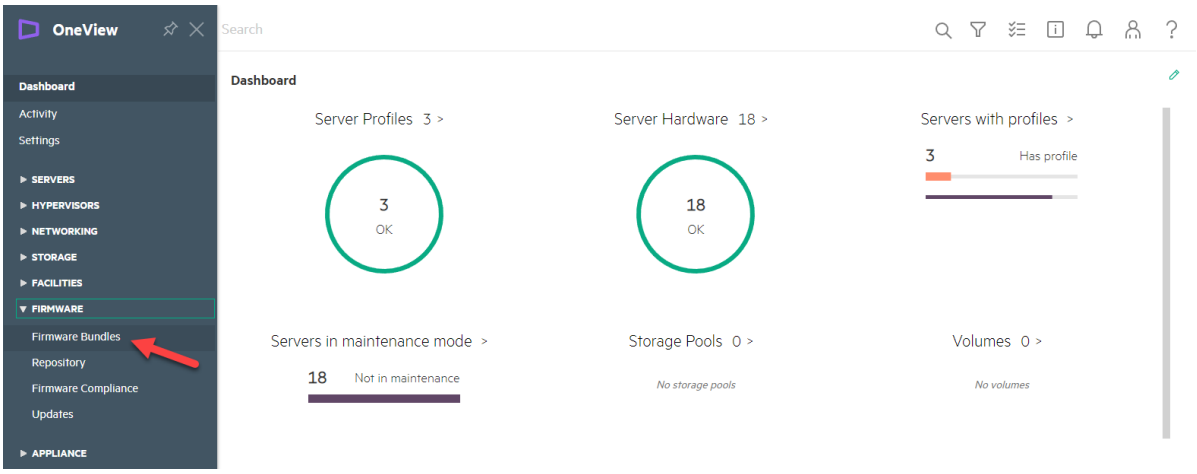


6. Once the rack has been configured, select Add to complete the setup or Add + if additional racks need to be created.



Adding a Service Pack for ProLiant (SPP) or Synergy Service Pack (SSP) Bundle

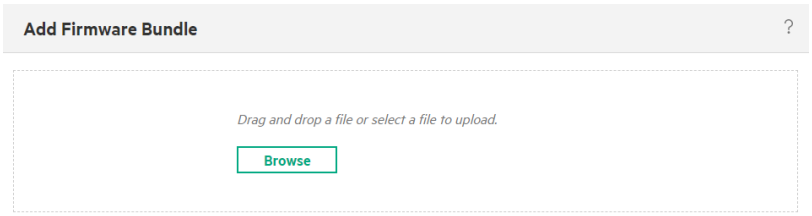
1. From the Top-Level Menu, expand the *APPLIANCE* option and then select *Firmware Bundles*



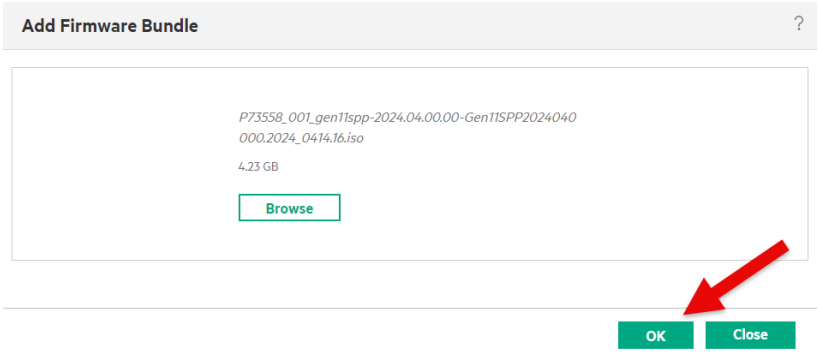
2. To upload an SPP / SSP Bundle, click the +*Add Firmware Bundle* button



3. On the Add Firmware Bundle window, click on the *Browse* button, and select the SPP / SSP ISO to upload.



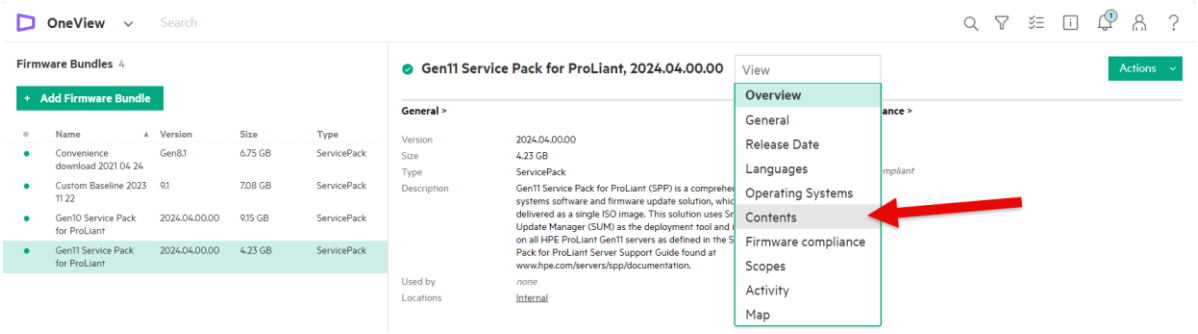
4. Once selected, click the *OK* button. You can also drag-and drop firmware bundles (SPP / SSP) within Windows environments. You can navigate away from the Firmware Bundle screen to other areas within the UI, as the upload process is a background process within the browser.



The SPP / SSP upload will begin. You can click the *Close* button in the lower right, as that will only close the dialog box and not cancel the upload.

Note:
Do not close the browser window until the Firmware Upload task has completed. You can click on the Close button in the Add Firmware Bundle dialog as the upload is a background thread within the web application.

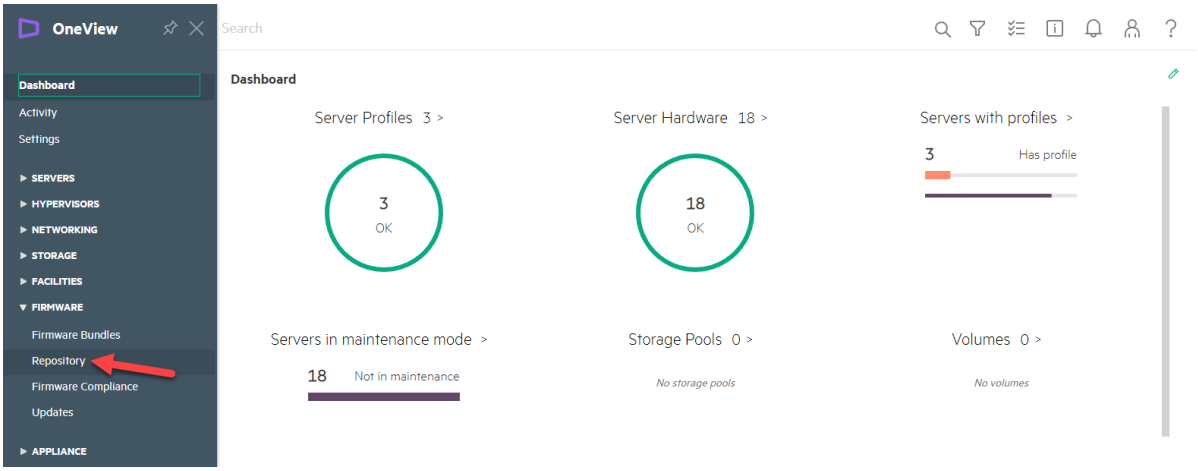
5. After the SPP / SSP has been uploaded, you can examine the contents



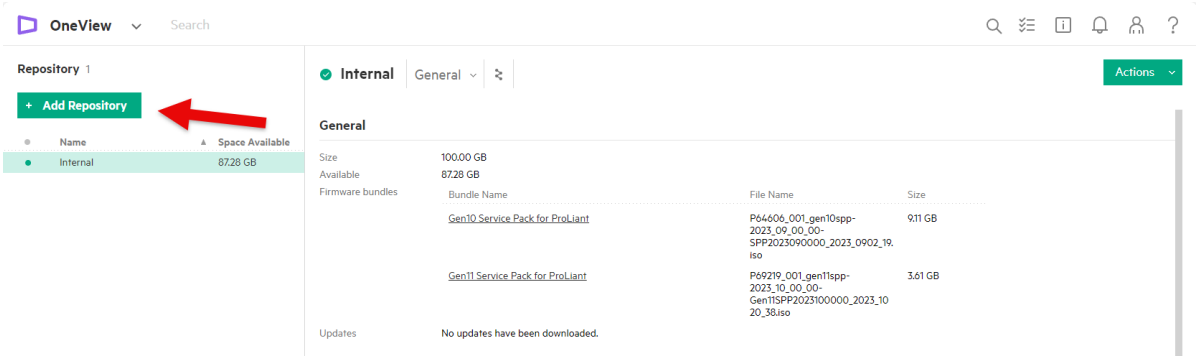
Adding an External SPP / SSP Repository

HPE OneView 3.1 or newer supports external firmware repositories.

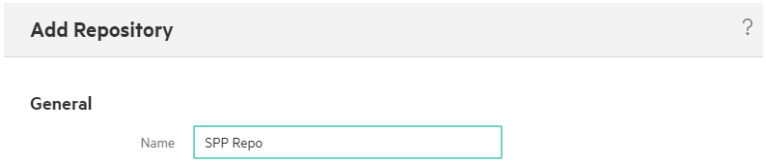
1. From the Top-Level Menu, select *Firmware* and then *Repository*.



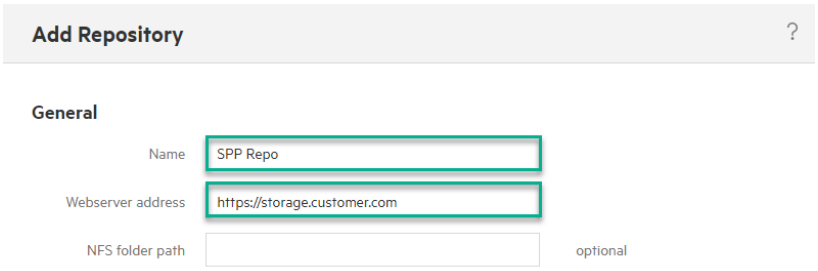
2. On the side of the page, click on the + *Add Repository* button



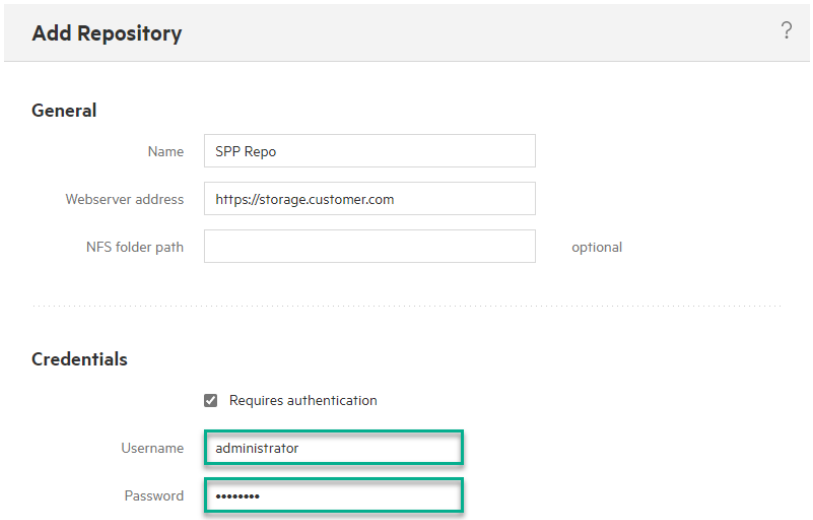
3. In the Add Repository menu, enter a name for the Repository.



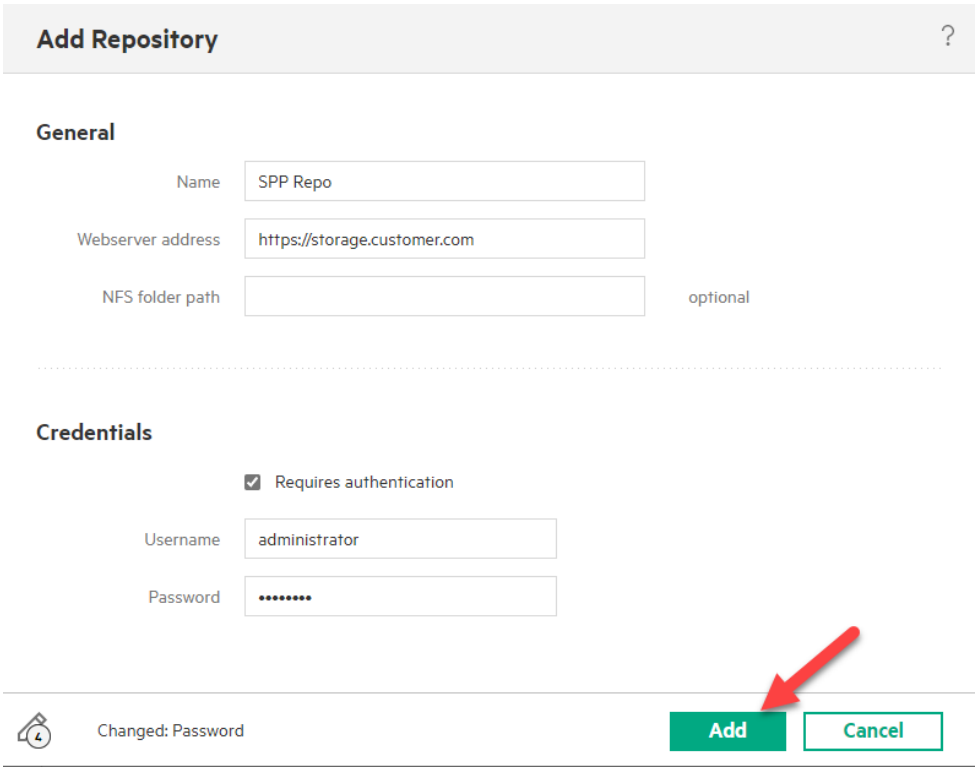
4. In the Add Repository menu, enter a webserver address for the Repository.



5. In the Add Repository menu, enter the credentials to access the Repository.



6. Click the *Add* button to finalize the repository.

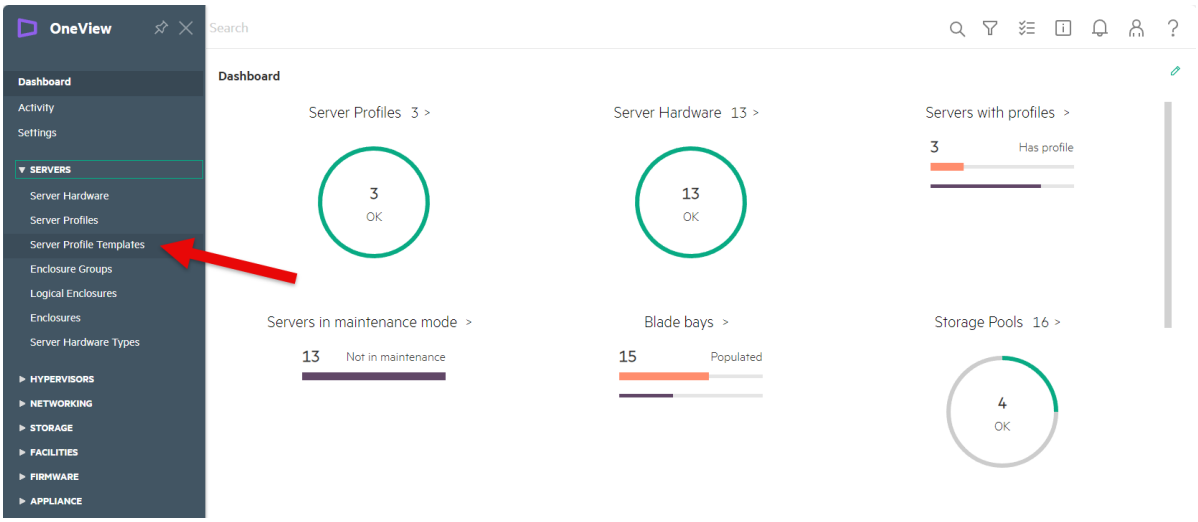


Updating the Firmware Baseline for Servers deployed with Server Profile Templates

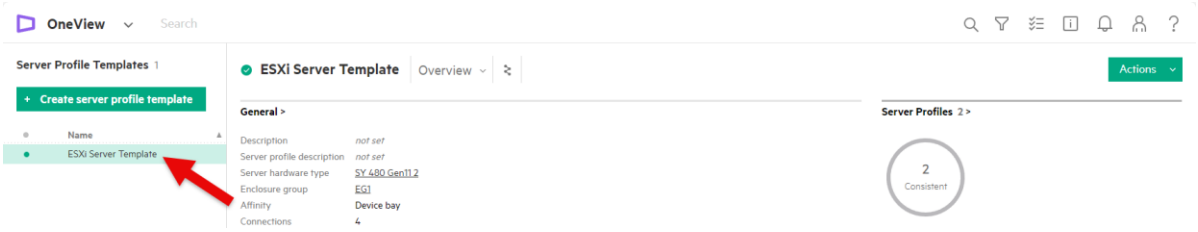
Server Profiles created from Templates in HPE OneView are monitored for compliance with the desired Template. When inconsistencies are detected, the profile is flagged as no longer being consistent with the template.

If a change is made to the firmware baseline were made, then the user can update a single profile or all via the server profile template. This will bring the selected profiles back in compliance with the Server Profile Template.

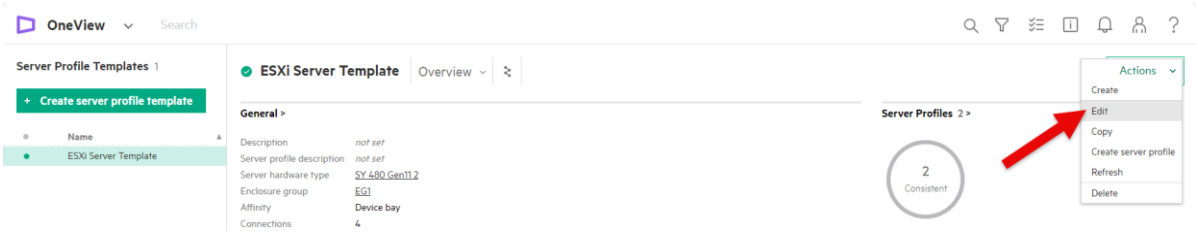
1. Ensure that a firmware bundle is uploaded to the HPE OneView appliance
2. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profile Templates*.



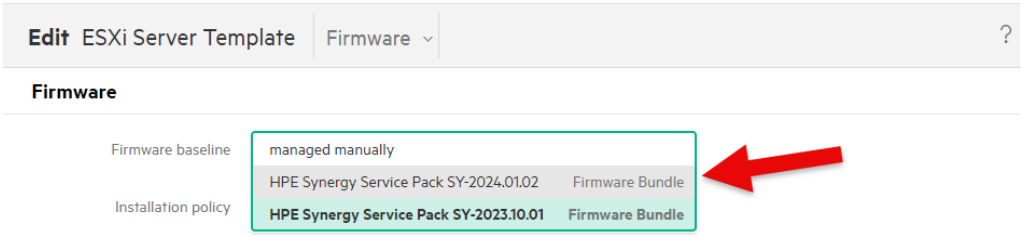
3. From the menu, select the server profile template to be updated.



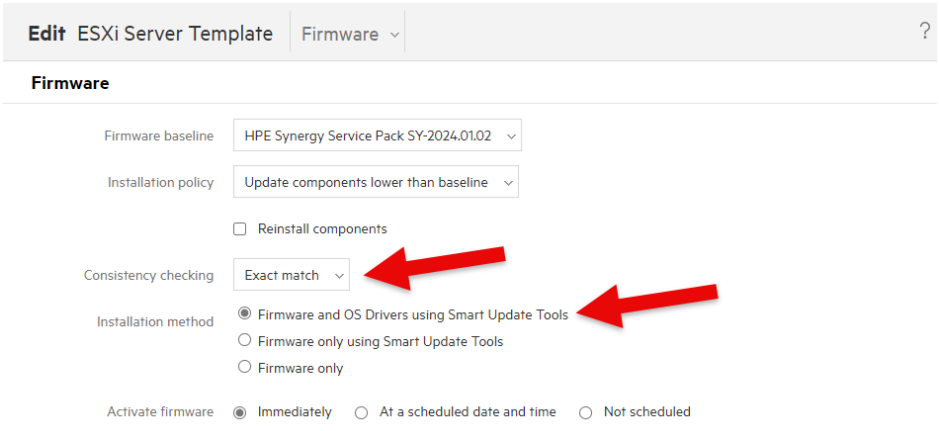
4. From the actions menu, then select *Edit*.



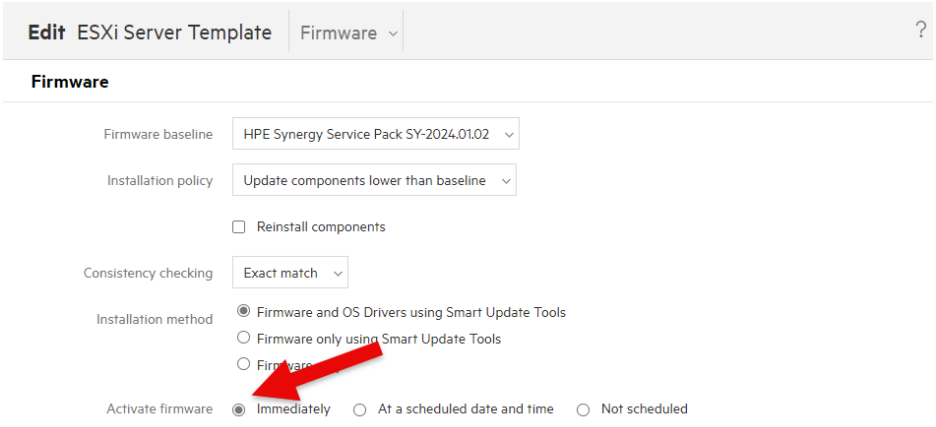
5. In the *Firmware* section of the Edit Profile page, select the Firmware baseline to be used for the Server Profile Template.



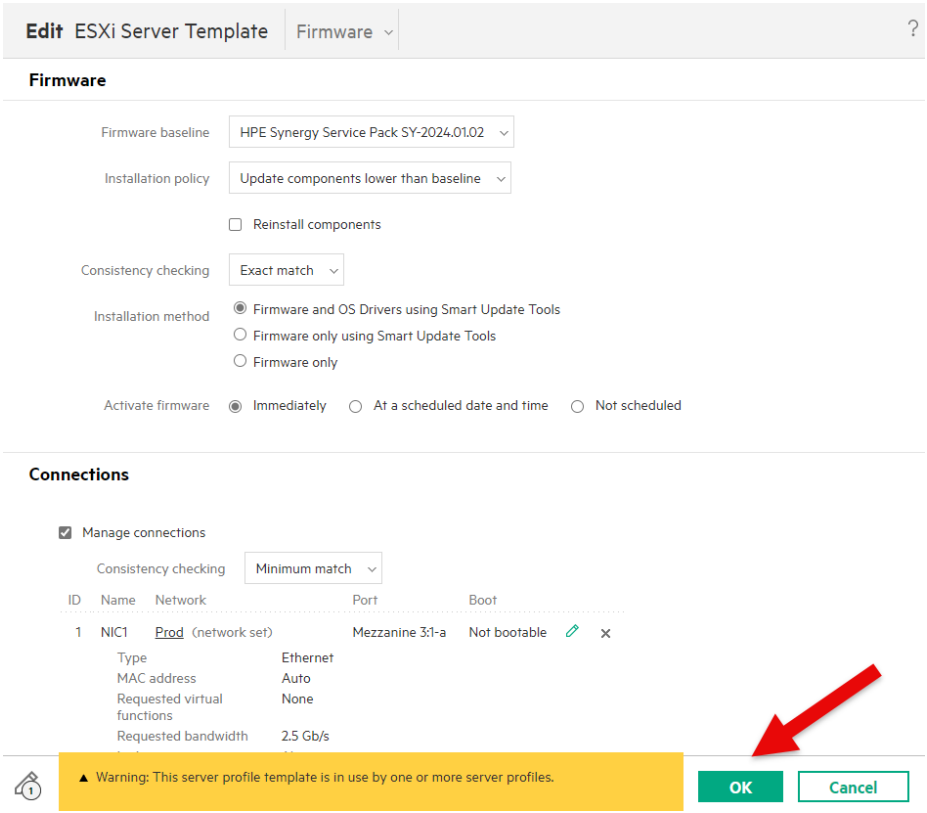
6. Select the method to deploy the firmware baseline update. If either of the options using the *HPE Smart Update Tools* is selected then the firmware or driver updates will be done while the systems are online. If the *firmware only* option is selected then the firmware will be updated offline using Intelligent Provisioning.
Note: *To ensure that the Server Profiles based on the Server Profile Template show that they are not consistent Consistency Checking needs to be enabled*



7. Select when the firmware updates will be applied

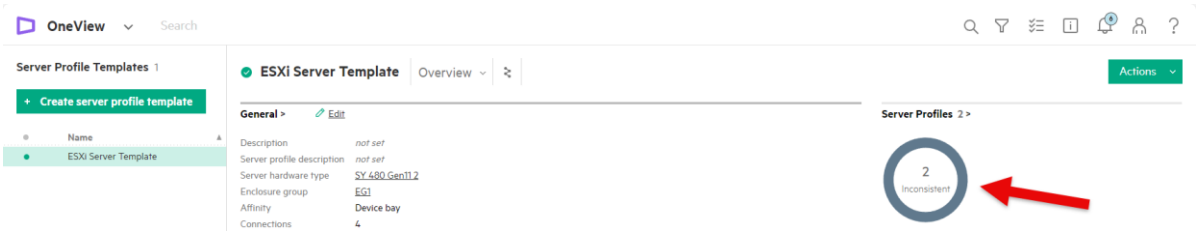


8. Click *OK* to apply the changes.

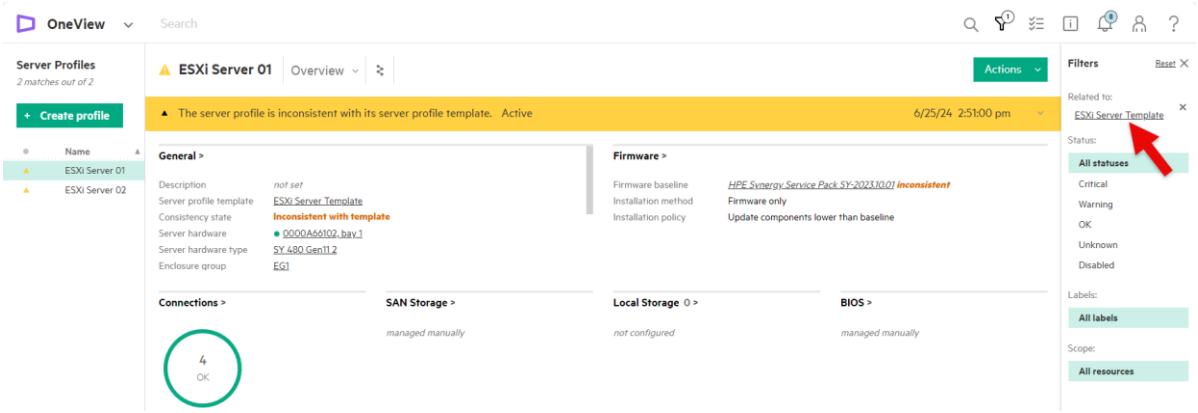


9. The server profile template will be updated with the new firmware baseline

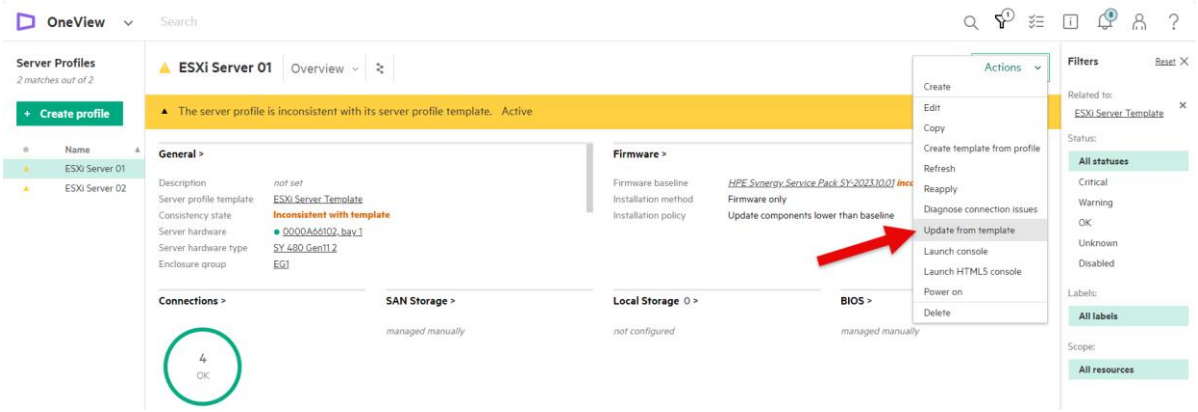
10. Notice that the Server Profiles are not shown as being inconsistent with the Server Profile Template. Click the *Server Profiles* doughnut to view the server profiles using this template.



11. When you click on server profiles within the server profile template an automatic filter will show only those Server Profiles that are based on the Server Profile Template. Select the relevant Server Profiles that you want to update based on the changes in the Server Profile Template.

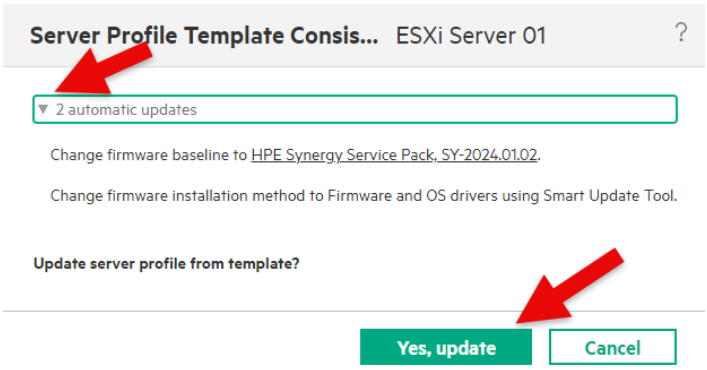


12. From the actions menu, select *Update from template*



13. Select, *Yes, update* when the Update from Template Dialog box appears, other messages and warnings will appear in this box depending on what is being updated / changed on the Server Profile from the Server Profile Template.

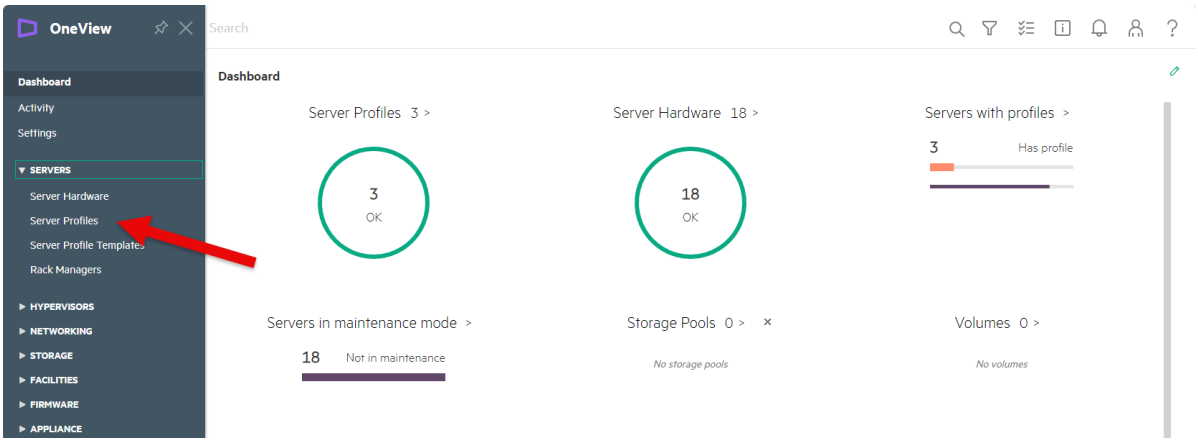
    Note: *You can expand to see what the updates / changes to the Server Profile will be.*



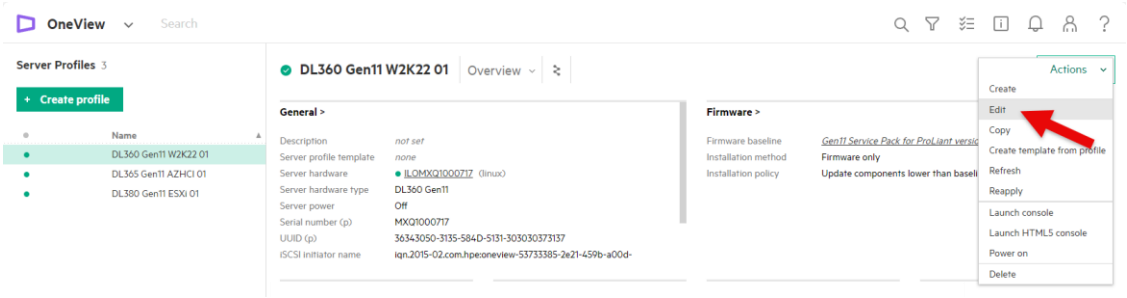
14. The selected server profiles will now be updated with the changes from the server profile template.

Updating the Firmware Baseline for Single Servers with Profiles Assigned

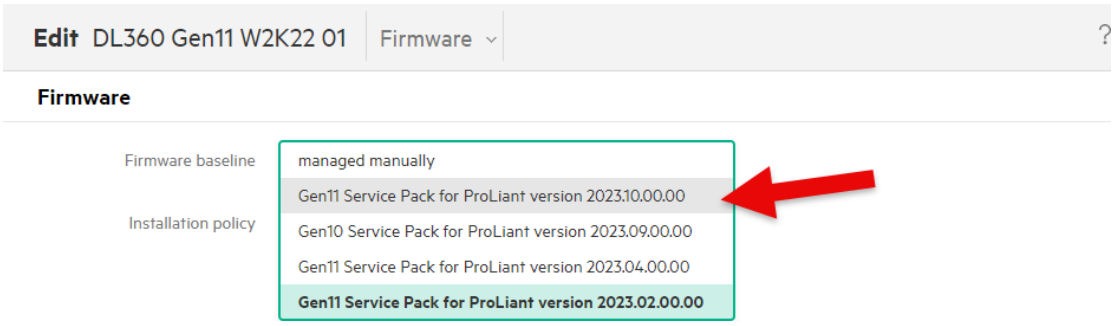
1. Ensure that the firmware bundle is uploaded to the HPE OneView appliance
2. From the Top-Level Menu, expand the *SERVERS* option and then select *Server Profiles*.



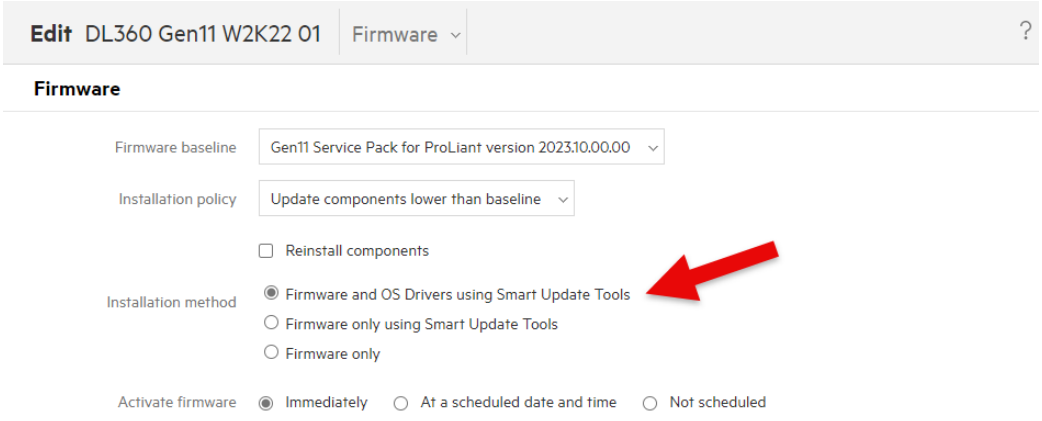
3. Select the server profile to be modified, then select *Edit* from the actions menu.



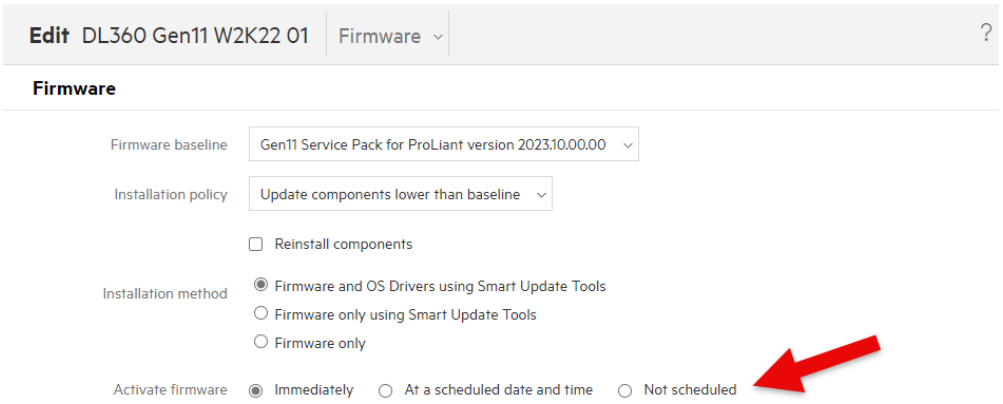
4. In the *General* section of the Edit Profile page, select the *Firmware baseline* to be used for the Server Profile from the dropdown box.



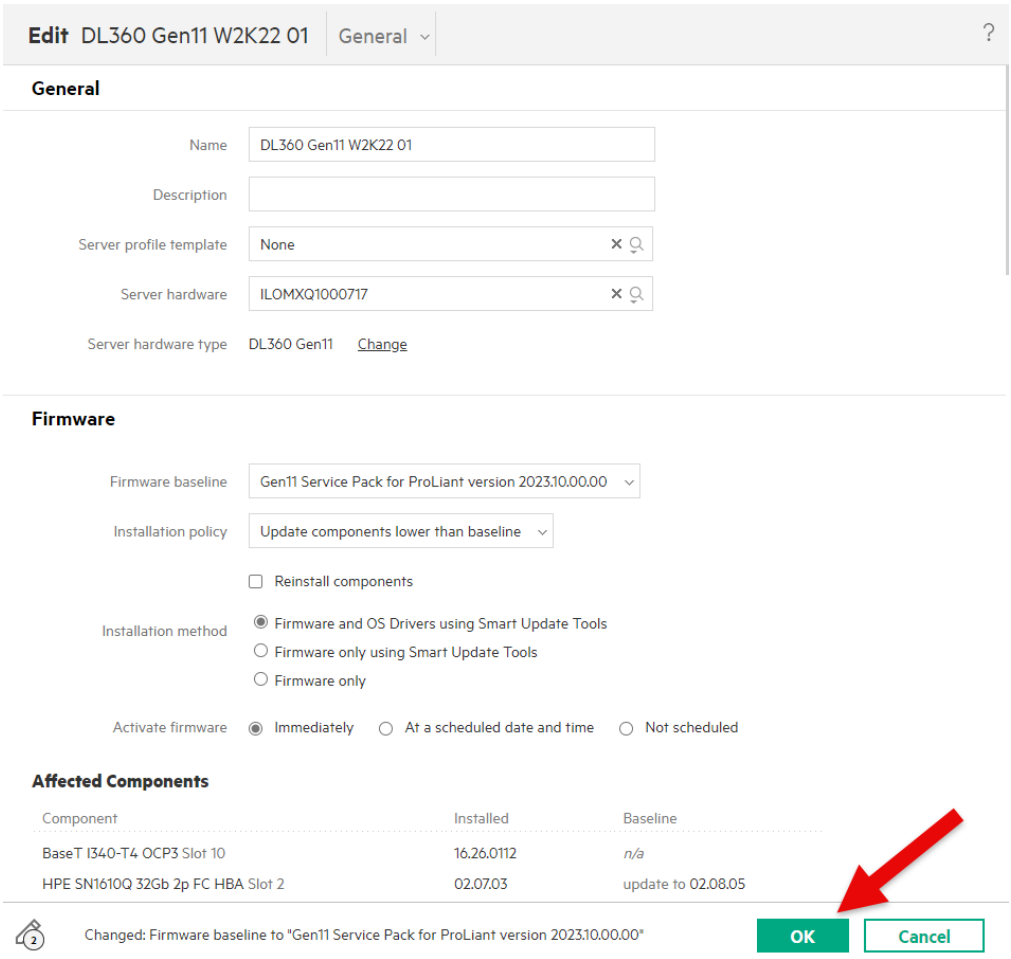
5. Select the method to deploy the firmware baseline update. If either of the options using the *HPE Smart Update Tools* is selected then the firmware or driver updates will be done while the systems are online. If the *firmware only* option is selected then the firmware will be updated offline using Intelligent Provisioning.



6. Select when the firmware updates will be applied

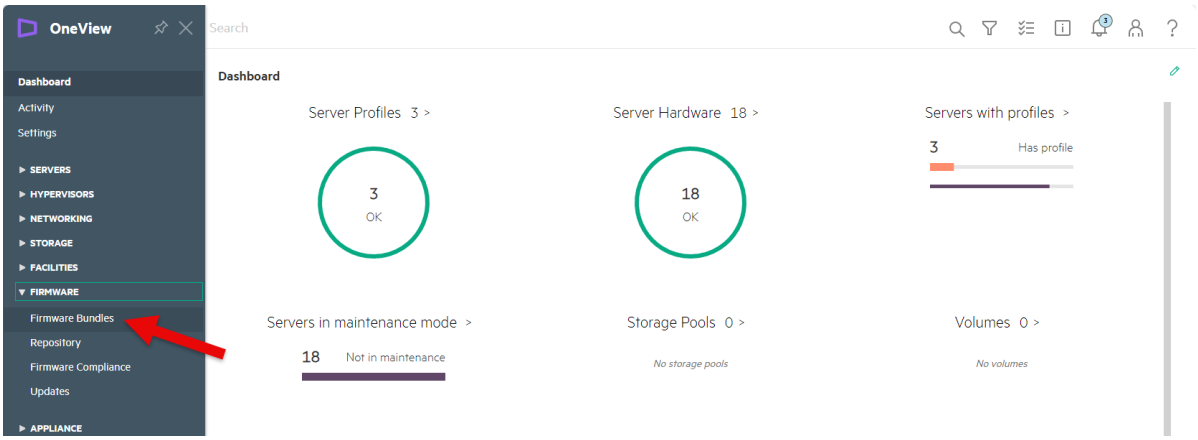


7. Click *OK* to apply the changes.

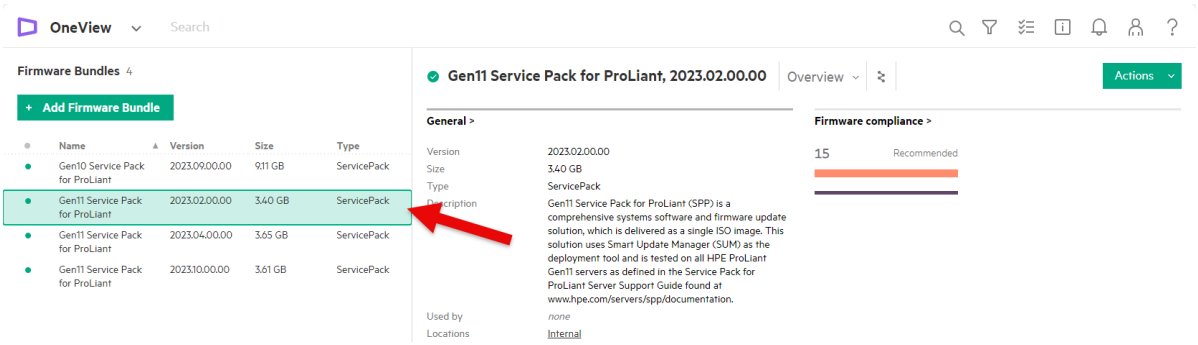


Deleting a Service Pack for ProLiant (SPP) / Synergy Service Pack (SSP) Bundle

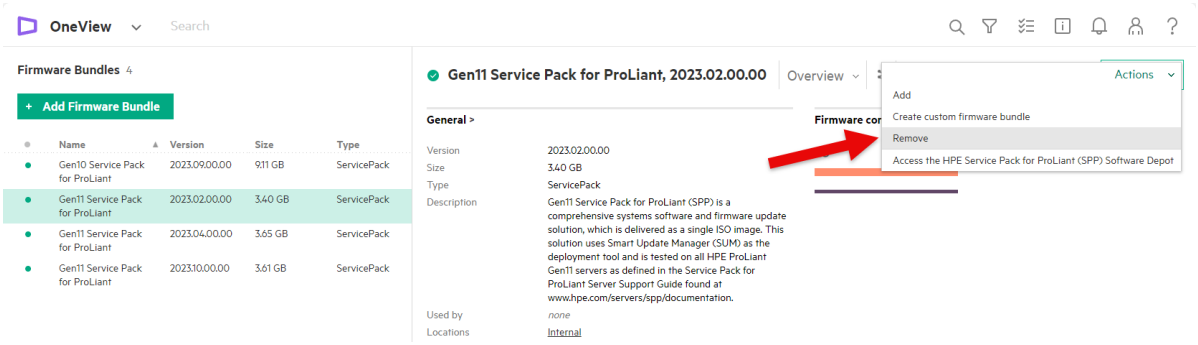
1. From the Top-Level Menu, expand the *APPLIANCE* option and then select *Firmware Bundles*



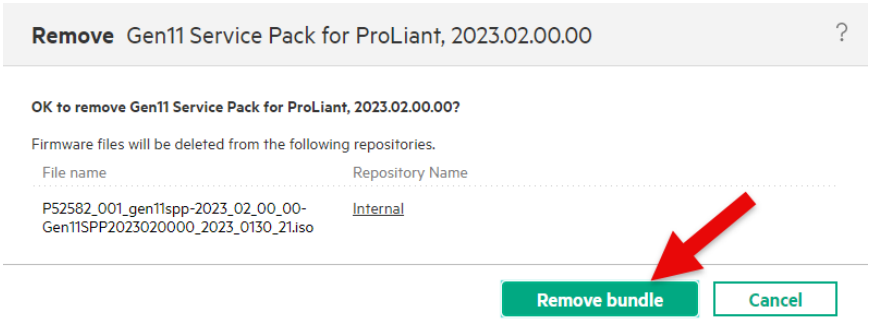
2. Select the firmware bundle to be removed.



3. From the actions menu select *Remove*.



4. From the Remove HPE Service Pack dialog box, select *Yes, remove*

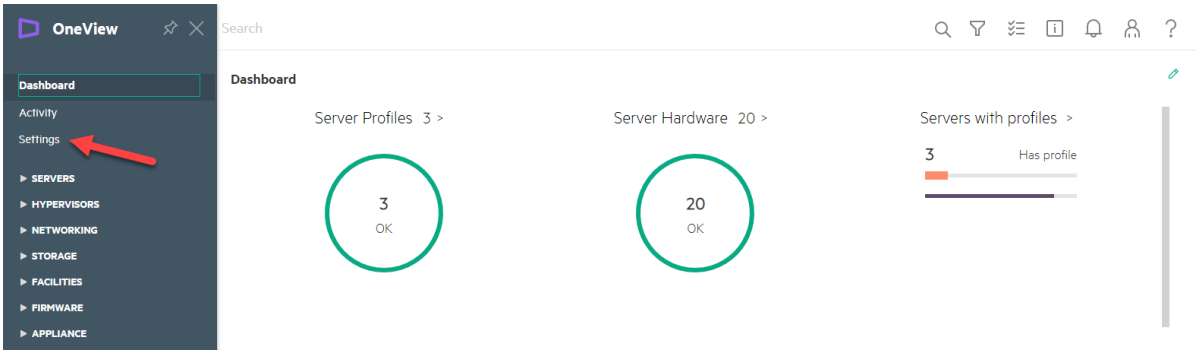


5. Confirm that the firmware bundle was removed from the HPE OneView appliance

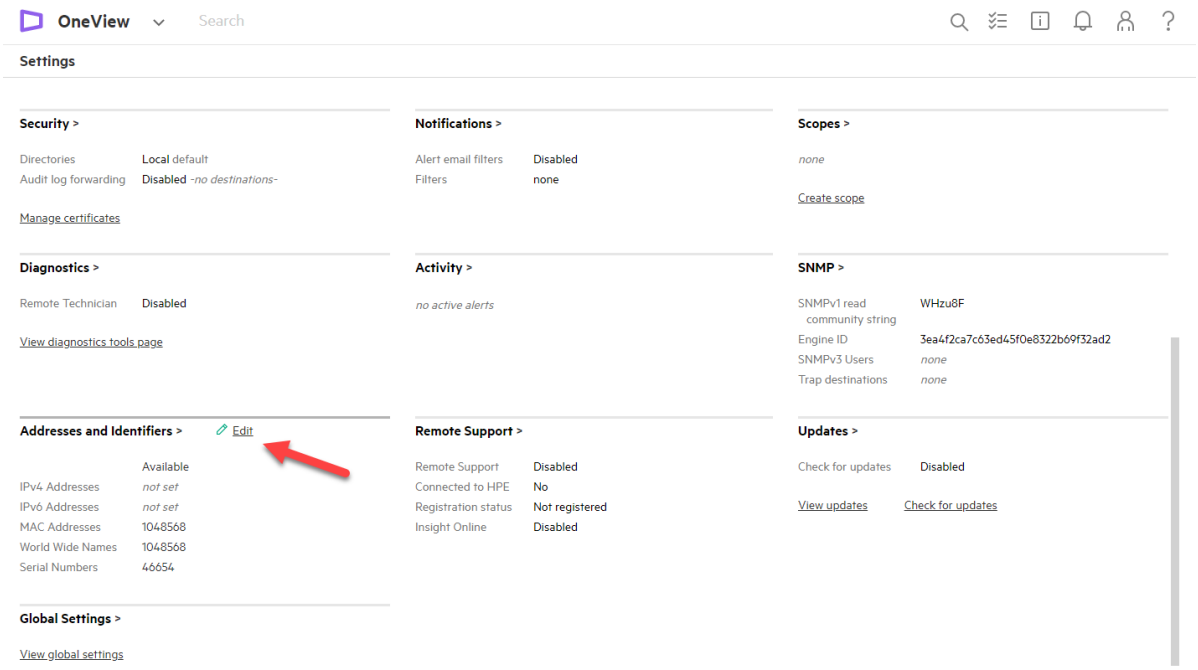
Modifying Virtual ID Pools

HPE OneView has the ability to pool address ranges. HPE OneView provides address ranges by using Locally Administered Addresses[7], including Auto Generated pools that can greatly expand the pool capacity. By default, there are ~1 million ID's per MAC and WWN pools.

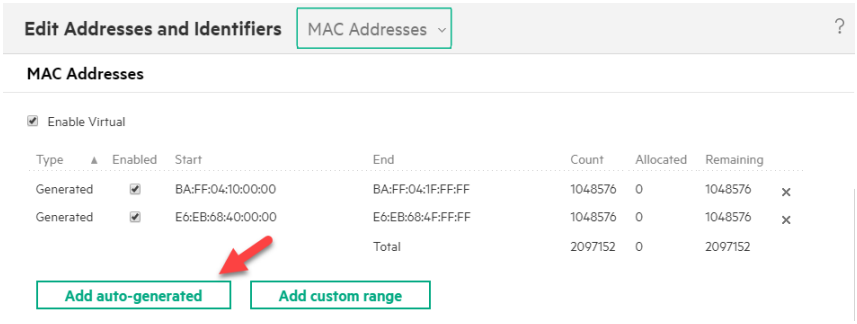
1. From the Top-Level Menu, select *Settings*.



2. On the Settings window, you will see a section called Addresses and Identifier. Click the heading for *Addresses and Identifiers*



3. Select the *Add auto-generated* button to create a new range of addresses for the pool or *Add custom range*.



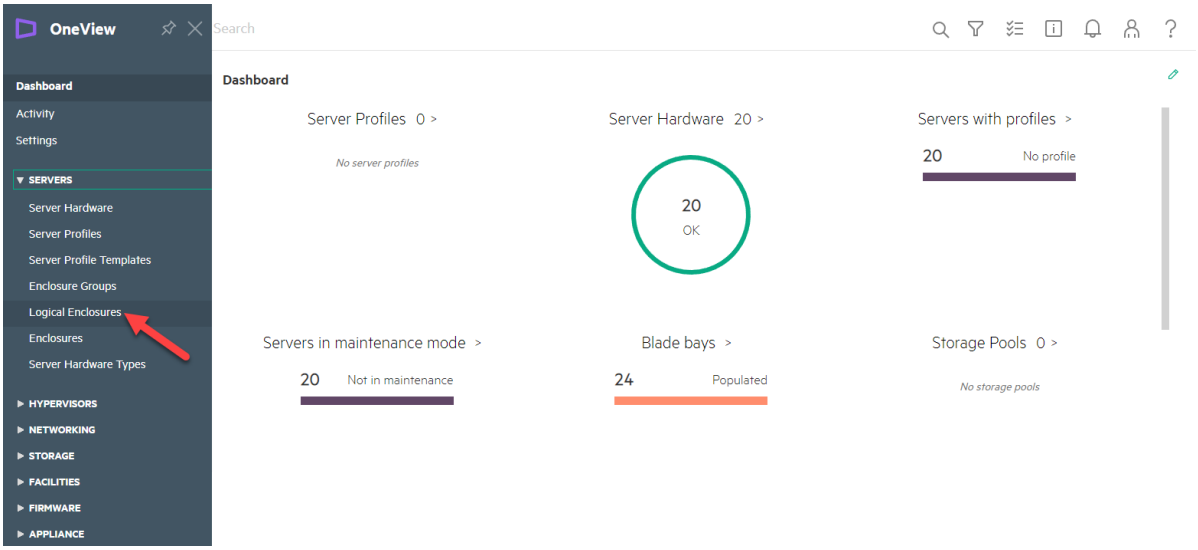
[7] http://en.wikipedia.org/wiki/MAC_address, review *Address Details* section.

Synergy Static IP Address Assignment for Compute Modules and Interconnects

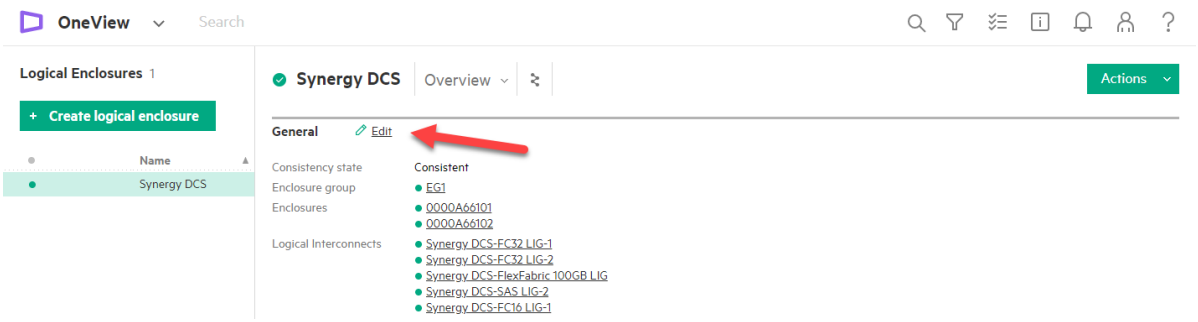
With the release of 5.2 a new feature allows you to assign Static IP Addresses to the iLO's for the Compute Modules as well as the Modules in the Synergy Frames. Previously you had to provide IP Addresses via the Synergy Composer Address Pool or via a DHCP Server that was on the same Management Network that the HPE Synergy Composers were connected to.

If your Synergy Enclosure Groups were created prior to v5.2 you can now still go back and edit them to manually assign addresses once you have upgraded your HPE Synergy Composer to v5.2 or later.

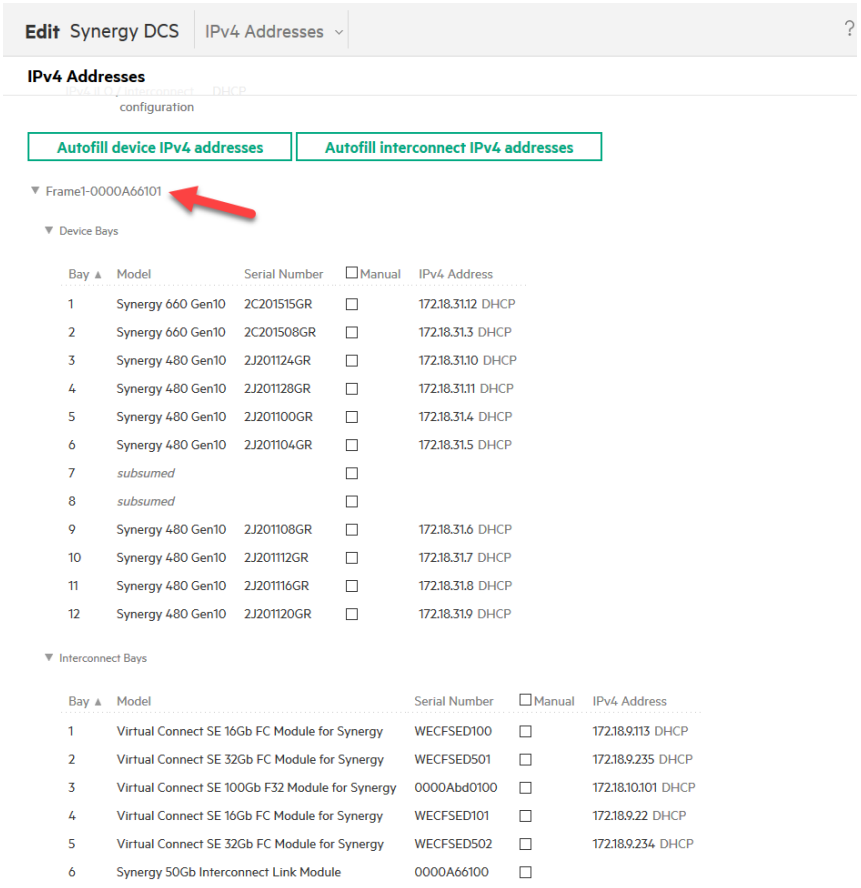
1. From the Top-Level menu, expand the *SERVERS* option and then select *Logical Enclosures*.



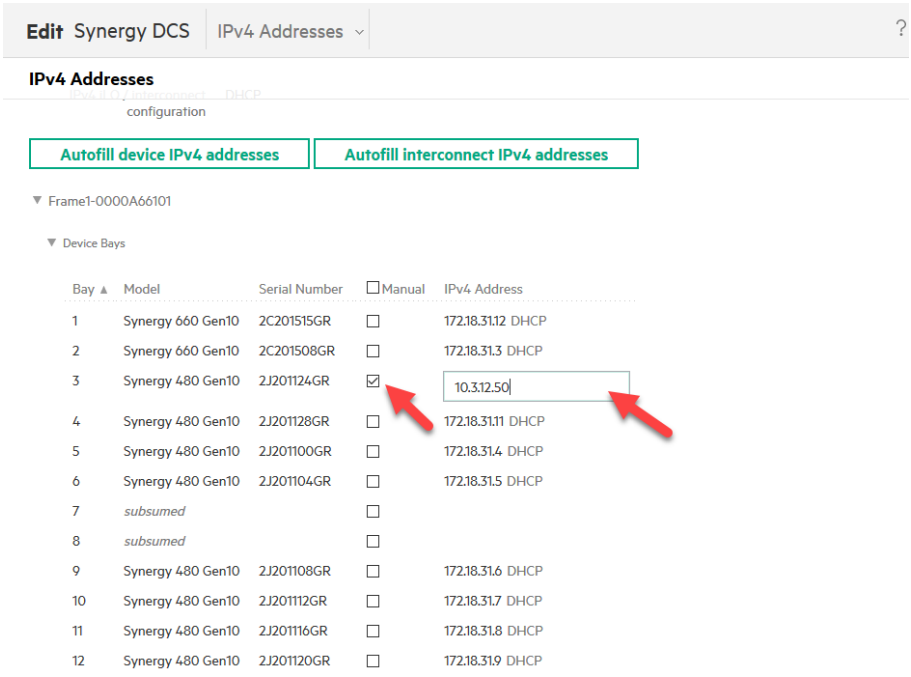
2. Select the Logical Enclosure that you want to *Edit*.



3. Expand the Frame that you want to modify the IP Address



4. For the Compute Modules you can set the IP Address for the iLO by clicking the box in the *Manuel* column and then entering the new IP Address that you want it to be changed to.

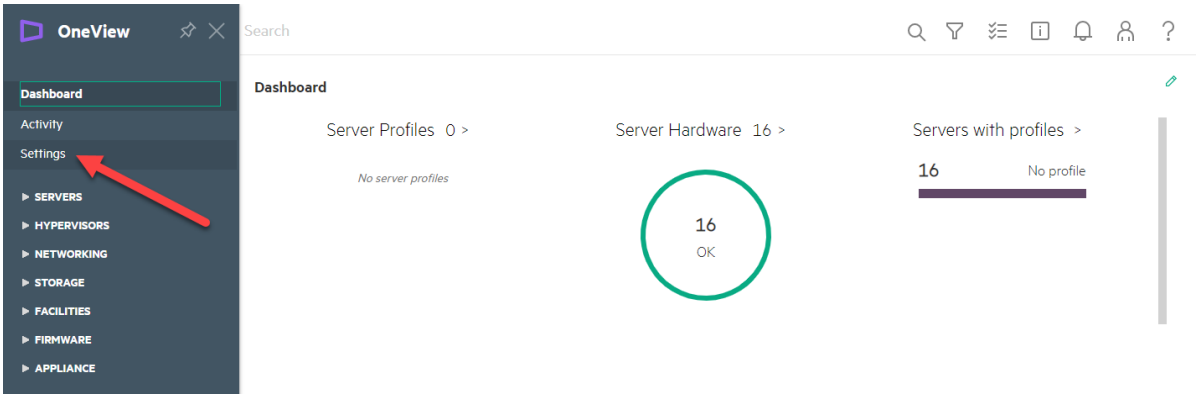


5. Once you have made the changes that you require you can click *OK* to save the changes and the new IP addresses will be assigned.

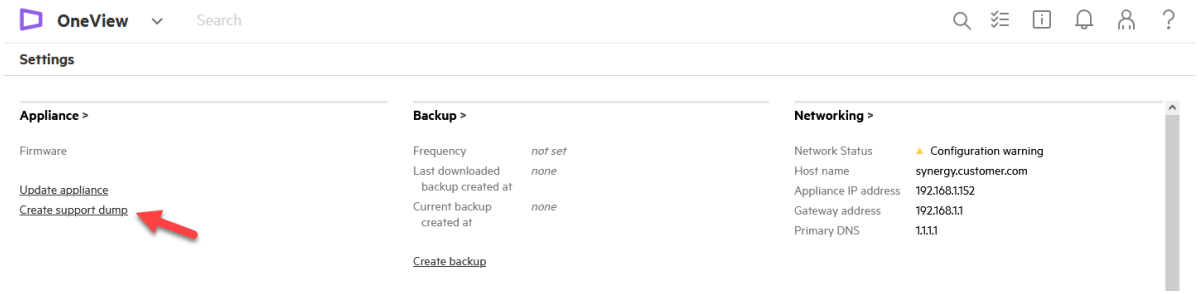
Creating a Support Dump

As with any product, occasionally there will be a situation that will require you to engage support. HPE OneView provides a Support Dump option to help with this process. There are two Support Dump options, and each contain different information: The Appliance and Logical Interconnects.

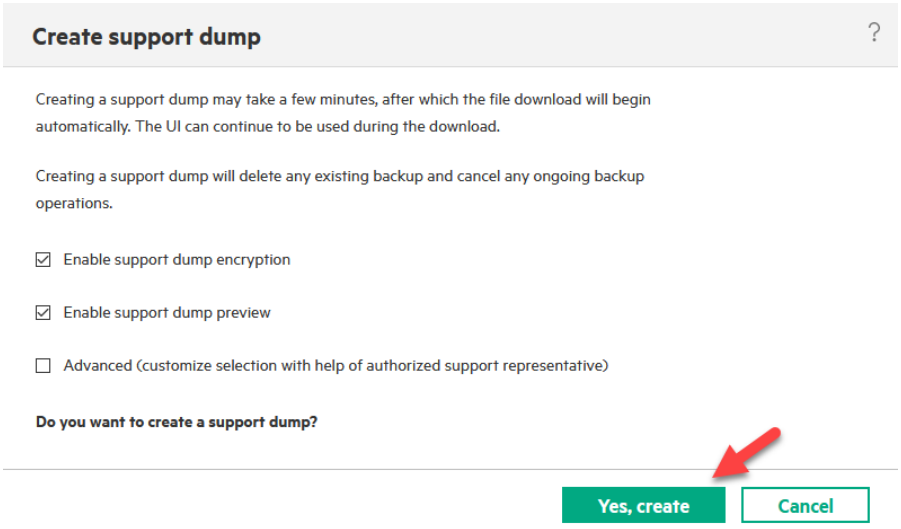
1. From the Top-Level menu, select *Settings*.



2. In the Appliance section, click *Create support dump*. It may take a minute or two to collect the Support Dump logs. The Support Dump may also be very large. This Support Dump collects information about the Appliance.



3. In the create support dump dialog, select *Yes, create*



4. Wait while the support dump is created



5. When completed the SDMP file(s) will be downloaded via your browser. Contact your HPE Support Representative and provide the information collected above.

Appendix

Appendix A: Sample HPN 5900CP FCF Switch Configuration

In this appendix, you will find a sample HPE 5900CP switch configuration setup as an FCoE FCF.

```
#
 version 7.1.045, Release 2307
#
 sysname HPN5900CP_FCF1
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
#
 lldp global enable
#
 system-working-mode advance
 password-recovery enable
#
 fcoe-mode fcf
#
vsan 1
#
vsan 100
#
vsan 200
#
vsan 300
#
vsan 400
#
vsan 500
 zone default-zone permit
#
vsan 600
#
vlan 1
#
vlan 100
 fcoe enable vsan 100
#
vlan 200
 fcoe enable vsan 200
#
vlan 300
 fcoe enable vsan 300
#
vlan 400
 fcoe enable vsan 400
#
vlan 500
 fcoe enable vsan 500
#
vlan 600
 fcoe enable vsan 600
#
qos map-table dot1p-lp
 import 0 export 0
 import 2 export 0
```

```
 import 3 export 1
 import 4 export 0
 import 5 export 0
 import 6 export 0
 import 7 export 0
#
traffic classifier DCBX operator or
 if-match acl 4000
#
traffic behavior DCBX
 remark dot1p 3
#
qos policy DCBX
 classifier DCBX behavior DCBX mode dcbx
#
 stp global enable
#
interface NULL0
#
interface FortyGigE1/0/49
 port link-mode bridge
#
interface FortyGigE1/0/50
 port link-mode bridge
#
interface FortyGigE1/0/51
 port link-mode bridge
#
interface FortyGigE1/0/52
 port link-mode bridge
#
interface M-GigabitEthernet0/0/0
 ip address 16.71.148.39 255.255.252.0
#
interface Ten-GigabitEthernet1/0/9
 port link-mode bridge
 description To vSAN100 Avon FCoE
 port link-type trunk
 port trunk permit vlan 1 100
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr be group 1 byte-count 15
 qos wrr af1 group 1 byte-count 15
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/10
 port link-mode bridge
 description To vSAN100 Avon FCoE
 port link-type trunk
 port trunk permit vlan 1 100
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
```

```
 qos wrr be group 1 byte-count 15
 qos wrr af1 group 1 byte-count 15
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/11
 port link-mode bridge
 description To vSAN300 Avon FCoE
 port link-type trunk
 port trunk permit vlan 1 300
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr be group 1 byte-count 15
 qos wrr af1 group 1 byte-count 15
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/12
 port link-mode bridge
 description To vSAN300 Avon FCoE
 port link-type trunk
 port trunk permit vlan 1 300
 priority-flow-control auto
 priority-flow-control no-drop dot1p 3
 lldp tlv-enable dot1-tlv dcbx
 qos trust dot1p
 qos wrr be group 1 byte-count 15
 qos wrr af1 group 1 byte-count 15
 qos wrr af2 group sp
 qos wrr af3 group sp
 qos wrr af4 group sp
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
 qos apply policy DCBX outbound
#
interface Ten-GigabitEthernet1/0/45
 port link-mode bridge
#
interface Ten-GigabitEthernet1/0/46
 port link-mode bridge
#
interface Ten-GigabitEthernet1/0/47
 port link-mode bridge
#
interface Ten-GigabitEthernet1/0/48
 port link-mode bridge
#
interface Fc1/0/1
#
```

```
interface Fc1/0/2
#
interface Fc1/0/3
#
interface Fc1/0/4
#
interface Fc1/0/5
#
interface Fc1/0/6
#
interface Fc1/0/7
#
interface Fc1/0/8
#
interface Fc1/0/13
#
interface Fc1/0/14
#
interface Fc1/0/15
 port access vsan 100
#
interface Fc1/0/16
 port access vsan 200
#
interface Fc1/0/17
#
interface Fc1/0/18
#
interface Fc1/0/19
#
interface Fc1/0/20
#
interface Fc1/0/21
#
interface Fc1/0/22
#
interface Fc1/0/23
#
interface Fc1/0/24
#
interface Fc1/0/25
#
interface Fc1/0/26
#
interface Fc1/0/27
#
interface Fc1/0/28
#
interface Fc1/0/29
 port access vsan 200
#
interface Fc1/0/30
 port access vsan 200
#
interface Fc1/0/31
 port access vsan 100
#
interface Fc1/0/32
 port access vsan 100
#
interface Fc1/0/33
#
```

```
interface Fc1/0/34
#
interface Fc1/0/35
#
interface Fc1/0/36
#
interface Fc1/0/37
 port access vsan 300
#
interface Fc1/0/38
#
interface Fc1/0/39
 port access vsan 500
#
interface Fc1/0/40
 port access vsan 600
#
interface Fc1/0/41
#
interface Fc1/0/42
#
interface Fc1/0/43
#
interface Fc1/0/44
#
interface Vfc9
 port trunk vsan 100
 bind interface Ten-GigabitEthernet1/0/9
#
interface Vfc10
 port trunk vsan 100
 bind interface Ten-GigabitEthernet1/0/10
#
interface Vfc11
 port trunk vsan 300
 bind interface Ten-GigabitEthernet1/0/11
#
interface Vfc12
 port trunk vsan 300
 bind interface Ten-GigabitEthernet1/0/12
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 15
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 0 0
#
line vty 16 63
 user-role network-operator
#
 ip route-static 0.0.0.0 0 16.71.148.1
```

```
#
 snmp-agent
 snmp-agent local-engineid 800063A2807848593E27C600000001
 snmp-agent log all
 snmp-agent sys-info contact Gary
 snmp-agent sys-info location Gary's 5900 in Fort Collins
 snmp-agent sys-info version v3
 snmp-agent group v3 AuthPriv privacy write-view Viewdefault
 snmp-agent group v3 admin write-view All2View
 snmp-agent mib-view included All2View iso
 snmp-agent mib-view included AllView snmp
 snmp-agent usm-user v3 admin
 snmp-agent usm-user v3 user2 AuthPriv cipher authentication-mode sha
$c$3$Ab59L60oVtFqqCqlIMf4cWTexOXWOdjBuRhAODHuCM8FH6FX3yM= privacy-mode aes128
$c$3$PyZHaO3tBpxQyP8ZTclauuQJ6VgRYmTjxmwD8QS0n3ohLA==
#
 ssh server enable
#
 ntp-service source M-GigabitEthernet0/0/0
 ntp-service unicast-server 16.110.135.123
#
acl number 4000 name DCBX
 rule 0 permit type 8906 ffff
 rule 5 permit type 8914 ffff
#
user-profile gary
#
radius scheme system
 user-name-format without-domain
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
```

```
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user root class manage
 password hash
$h$6$Tax11rbZMQx6sAG8$3HM+5G1XxjJpd6GJaMYka+3lHi83NFqDMSCvvCZSdulELTBe2C6QqQtoerEP4JoAYw9yqtcu8oyhUSDWXvv+CQ==
 service-type ftp
 service-type ssh telnet http https
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
return
```

Appendix B: REST API

REST (Representational State Transfer) is a web service format that uses basic Create, Read, Update and Delete (CRUD) operations that are performed on resources using HTTP POST, GET, PUT and DELETE. To learn more about general REST concepts, see:

http://en.wikipedia.org/wiki/Representational_state_transfer

HPE OneView has a resource-oriented architecture that provides a uniform REST interface. Every resource has one Uniform Resource Identifier (URI) and represents a physical device or logical construct and may be manipulated using REST API's. To view the list of resources, see *HPE Composable Infrastructure Controller REST API Reference* located in the Online Help of the appliance [https://{ip}/help/cic/en/content/images/api/].

Resource operations

Basic Create, Read, Update and Delete (CRUD) operations are performed on the appliance resources via the standard HTTP POST, GET, PUT and DELETE methods. RESTful interfaces are based on the World Wide Web standards, thus most modern web servers can support these operations without modification.

Restful API's are stateless. The resource state is maintained by the resource manager and is reported as the resource representation. Any application state must be maintained by the client and it may manipulate the resource locally, but until a PUT or POST is made, the resource as known by the resource manager is not changed.

Table 15. REST HTTP Operations

Operation	HTTP Verb	Description
Create	POST URI <Payload = Resource data>	New resources are created using the POST operation and including relevant data in the payload. On Success the Resource URI is returned.
Read	GET URI	Returns the requested resource representation(s)
Update	PUT URI <Payload = Update data>	Update an existing resource using the update data.
Delete	DELETE URI	Delete the addressed resource

URI format

All the appliance URIs point to resources and the client does not need to modify or create URIs. The URI for specific resource is static and follows this format: https://{appl}/rest/{resource name}. The three parts are described below.

Table 16. URI Format

https://{appl}	The appliance addresses.
/rest	Type of URI.
/{resource name]	Name of the appliance resource such as server-profile.

Data transfer format

The appliance resources support JSON (JavaScript Object Notation) as the standard for exchanging data using a REST API. If JSON is not specified in the REST API call, then the default is JSON.

To learn more about JSON, go to www.json.org.

Appendix C: Accessing the REST API with PowerShell

The HPE OneView PowerShell Library is available for download at https://github.com/HewlettPackard/POSH-HPEOneView, . The library requires at least the Windows Management Framework 3.0 (aka PowerShell 3.0) to be installed, and the .Net 4.0 Client Framework. Windows Management Framework 4.0 (aka PowerShell 4.0) that ships with Windows 8.1 / 8.1 Update is supported. The HPE OneView POSH Library Installer will assist you with the installation of these two required components if not found on the system.

Please visit the HPE OneView Online Documentation page (at https://hpe-docs.gitbook.io/posh-hpeoneview/), or use the get-help PowerShell cmdlet, for all available CMDLETs and the associated help.

For OneView 5.0 or later PowerShell Library can only be installed using the Microsoft PowerShell Gallery (https://www.powershellgallery.com/packages?q=HPE+OneView). Please use the Find-Module, Save-Module and Install-Module PowerShellGet Cmdlets.

Using PowerShell

Note:
The following example assumes the HPE OneView POSH Library is installed.

The HPE OneView PowerShell library is a self-contained module that you first need to import or add to your PowerShell Session Profile. After the module has been successfully imported, you must first execute *Connect-HPOVmgmt* in order to authenticate to the appliance. You can then execute other cmdlets to perform the desired action.

There are 5 primary CMDLETs to interact with the HPE OneView appliance:

- Connect-OVmgmt
- Send-OVRequest
- New-OVResource
- Set-OVResource
- Remove-OVResource

Accessing the REST API with Python

Python comes with a few libraries that can complete REST requests like httplib2 and urllib2, these libraries are rather difficult to use and require a lengthy learning curve. Another python library called "Requests" has solved the learning curve, cleaned up REST requests and made them very easy to use. For a full comparison take a look at https://en.wikipedia.org/wiki/Requests_(software)

This overview of using Python to create REST requests will feature the Requests library.

The full HPE OneView Python Library can be found at https://github.com/HewlettPackard/oneview-python

Requests

Requests (http://docs.python-requests.org/en/latest/) is an easy to use REST request Python library.

How to get Requests
To get requests follow the steps on the Requests website here: http://docs.python-requests.org/en/latest/user/install/#install

The best method would be to use pip (the python package manager) to install requests:

```
> pip install requests
```

Creating and executing a request

To execute a request is very simple. First look at the following code:

```
uri = '/rest/login-sessions'
method = 'POST'
data = {
        'userName': username,
        'password': password,
    }
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json',
        'Accept-Language': 'en_US',
    }
     url = 'https://' + hostname + uri
    response = requests.request(method, url, data=json.dumps(data), headers=headers, verify=False)
```

A request is made up for 4 items:

- Method - HTTP Method (e.g. POST, PUT, GET, etc.)
- URL - URL for the new Request object.
- Body (or data) - Any data we want to pass in
- Headers - HTTP headers, including request type and authentication key

Example: Logging In

Below is a fully working example of using Python + Requests to login to an appliance and collect the session ID:

```
#!/usr/bin/env python
# © Copyright 2013 Hewlett-Packard Development Company, L.P.
import json
import requests


def main(hostname, username, password):

    uri = '/rest/login-sessions'
    method = 'POST'
    data = {
        'userName': username,
        'password': password,
    }
    headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json',
        'Accept-Language': 'en_US',
    }

    url = 'https://' + hostname + uri
    response = requests.request(method, url, data=json.dumps(data), headers=headers, verify=False)

    if response.status_code == 200:
        print (response.json()['sessionID'])
    else:
        print (response.json()['errorCode'] + ': ' + response.json()['message'])

if __name__ == '__main__':

    hostname = 'host.domain.com'
    username = 'administrator'
    password = 'password'

    main(hostname, username, password)
```

Appendix D: Configuring a Brocade SAN switch for HPE OneView REST API access

HPE OneView supports a SAN Manager type "Brocade FOS Switch", which communicates with Brocade SAN switches using their REST API. This section documents requirements for setting up the switch to support operation with this HPE OneView SAN Manager.

System requirements

- HPE OneView software version 5.0 or later
- Brocade switch FOS version 8.2.0b or later

Note:
Brocade FOS version 8.x is supported on Gen5 (16Gb) & Gen6 (32Gb) switches. If you have Gen4 (8Gb) or earlier switches these are not supported with HPE OneView 7.0 or later.

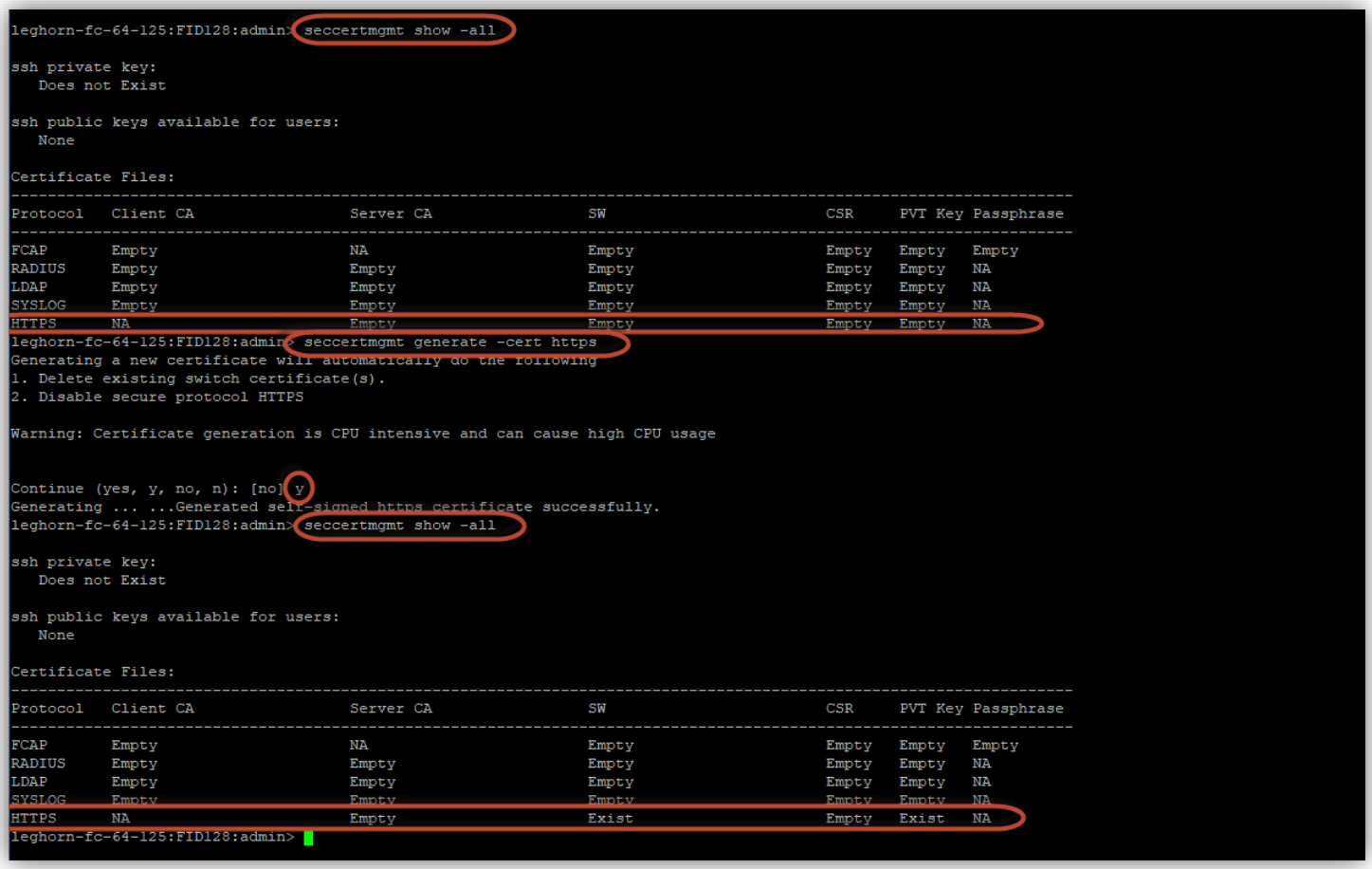
- OneView must have a network path to connect to the Brocade switch using HTTP (TCP port 80) or HTTPS (TCP port 443).

Brocade switch configuration requirements

For OneView to manage SAN zoning via a Brocade switch, it must be configured as follows:

1. The switch must be running in "Native" switch mode. It must not be running in "Access Gateway" mode with NPIV.
2. FOS must be configured with username/password credentials for OneView to login to the switch that is authorized to perform zoning configuration changes.
3. The FOS REST API is enabled by default. If it has been disabled, it must be enabled.
    a. To reenable the Fabric OS REST interface, enter: *mgmtapp --enable REST*
4. Each OneView Brocade FOS switch SAN Manager will use one REST session on the switch. The switch should be configured to allow at least as many sessions as OneView instances which will be configuring zoning on the switch. The default max session count is 3.
    a. To set the max number of sessions to 4, enter: *mgmtapp --config -maxrestsession 4*
5. Each fabric (virtual or non-virtual) configured on the Brocade switch will be discovered by the OneView Brocade FOS switch SAN Manager, creating a SAN in OneView. Fabrics must be created on the switch outside of OneView before OneView will discover them. The name of the SAN in OneView will be read from the "Fabric Name" configured on the Brocade switch.

6. OneView supports connecting to the Brocade switch REST interface via HTTP (port 80) or HTTPS (port 443). In order to use HTTPS, the switch must be configured with an HTTPS certificate. Following is an example process in FOS 8.2.0b for ensuring a HTTPS certificate exists, and generating one if not. Check your Brocade switch user documentation for the commands required for other FOS versions.



Additional Resources

HPE OneView Support via HPE Support Center
- HPE OneView Online Help
- HPE OneView Release Notes
- HPE OneView Support Matrix
- HPE OneView Installation Guide
- HPE OneView User Guide
- HPE OneView REST API Reference
- HPE OneView Firmware Management White Paper

http://www.hpe.com/info/oneviewcommunity
- HPE OneView Community Forums

https://github.com/HewlettPackard/POSH-HPEOneView
- HPE OneView PowerShell Library

https://github.com/HewlettPackard/oneview-python
- HPE OneView Python Library

https://github.com/HewlettPackard/oneview-golang
- HPE OneView Golang bindings for OneView API's

https://github.com/HewlettPackard/oneview-ansible-collection
- Ansible Collection and sample playbooks for HPE OneView

https://github.com/HewlettPackard/oneview-chef
- Cookbooks for Chef for HPE OneView resources

https://github.com/HewlettPackard/oneview-puppet
- Puppet module for managing HPE OneView resources

For other HPE OneView Composable Partners with integrations to HPE OneView
https://www.hpe.com/info/composablepartners

Learn more at
http://www.hpe.com/info/OneView

Sign up for updates

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed.

P13648-029, July 2024

Hewlett Packard Enterprise