Apporto NextGen On-Premises Deployment Guide

Version: BETA

The purpose of this document is to aid Apporto customers in setting up on-premises installations of Apporto NextGen software. Please review the section on known issues before beginning deployment.

Last updated 03 June 2025

Overview

Introduction

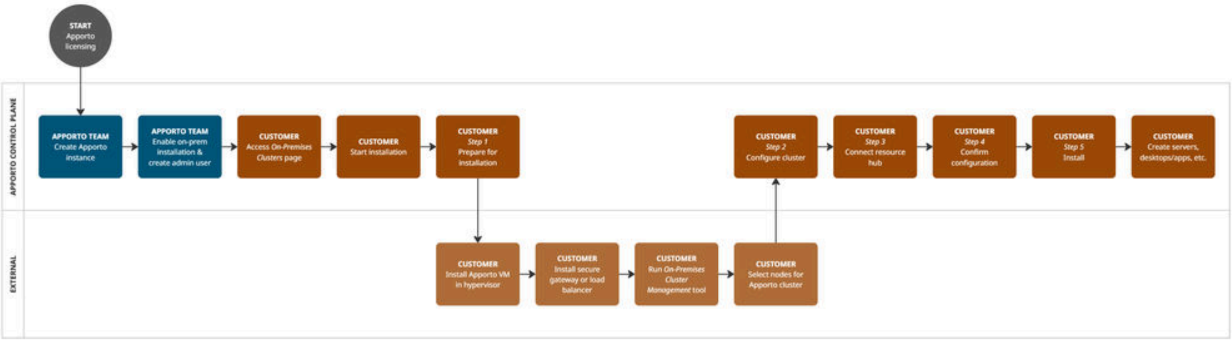
Apporto NextGen virtual desktop software is available for deployment to both cloud and on-premises environments. In both cases, the control plane is hosted in the cloud, making Apporto a hybrid system. This document details how an on-premises customer can connect their infrastructure to Apporto. Additional assistance may be provided by the Apporto Support team.

Product description

On-premises deployment of Apporto NextGen involves the following:

- **Apporto appliance cluster**
  This Kubernetes cluster converts standard Remote Desktop Protocol (RDP) traffic to Apporto's Hyperstream. It consists of three (3) nodes deployed as virtual appliances.
- **Gateway or load balancer**
  This appliance sits in front of the appliance cluster, provides secure remote access for external users over https, and balances loads across Apporto node connections. You may use either the Apporto-provided secure gateway or your own preferred load balancer or content delivery controller.

Deployment process


START Apporto licensing
APPORTO CONTROL PLANE
EXTERNAL
APPORTO TEAM Create Apporto instance
APPORTO TEAM Enable on-prem installation & create admin user
CUSTOMER Access *On-Premises Clusters* page
CUSTOMER Start installation
CUSTOMER *Step 1* Prepare for installation
CUSTOMER Install Apporto VM in hypervisor
CUSTOMER Install secure gateway or load balancer
CUSTOMER Run *On-Premises Cluster Management* tool
CUSTOMER Select nodes for Apporto cluster
CUSTOMER *Step 2* Configure cluster
CUSTOMER *Step 3* Connect resource hub
CUSTOMER *Step 4* Confirm configuration
CUSTOMER *Step 5* Install
CUSTOMER Create servers, desktops/apps, etc.

Prerequisites

To get started, ensure that the following prerequisites are met to ensure a successful deployment.

Browser requirements

Apporto is built to enable applications and desktops to run seamlessly via an HTML5/WebGL-compatible browser. This includes leading browsers like Google Chrome, Firefox, Safari, and Microsoft Edge. While it may also function on other HTML-supporting browsers, Apporto validates its functionality against the latest releases of these four browsers.

> Google Chrome is recommended for optimal performance.

Apporto instance

Once your Apporto license has been executed, the Apporto team will set up your Apporto instance using the instance name (URL) determined during onboarding. Afterward, the Apporto Support team will provide your initial control plane login for configuration of your instance and desktops.

Hypervisors

Apporto NextGen can be deployed in a virtual environment on hypervisors or you may use physical servers.

> Physical servers are not required unless you have a desire to present physical GPU cards without the loss of performance and extra licensing fees associated with hypervisor pass-thru. Virtualized environments are recommended for the ability to utilize snapshots and automation for creation of virtual machines.

Apporto validates its functionality against the following hypervisors.

Hypervisor	Supported by Apporto
VMware vSphere	Version 6.5 Version 8.0 COMING SOON
Nutanix Prism	Operating system 6.5+
Proxmox Virtual Environment	Version 8.0+ COMING SOON

> Apporto recommends that customers consider the capacity required to scale out the VDI/RDS deployment and Apporto node cluster as user adoption increases. For new deployments, a solid backup and disaster recovery plan is important to maintain a high level of service.

> ⚠ Some features might not be supported on all hypervisor platforms/versions. See the feature documentation for details.

Components

The following table lists the minimum requirements for the Apporto NextGen on-premises components.

Apporto appliance	Minimum each	Required
Apporto manager node	1vCPU, 4GB RAM, 50GB OS Disk, 50GB Data Disk	One is required per cluster
Apporto worker nodes	2vCPUs, 8GB RAM, 50GB OS Disk, 50GB Data Disk	At least two are required per cluster

Apporto gateway	1vCPU, 4GB RAM, 50GB Disk	Required if you are not using your own preferred load balancer or content delivery controller

Virtual machines

Workloads and sizing guidelines

Apporto recommends referring to Microsoft's guidelines on VM sizing to support Apporto system workloads: Session host virtual machine sizing guidelines for Azure Virtual Desktop and Remote Desktop Services .

Network

IP addresses

Each deployed component will require a static IP address to be assigned during configuration.

Fully qualified domain names (FQDNs)

FQDNs--including for Apporto's rdp-mgmt-gateway--must be configured for the hyperstream endpoints that will connect to your load balancer or gateway.

Required ports

The following are a list of common network ports used by Apporto NextGen. Ensure that your firewall allows the required traffic flow for the various components.

Direction	VM type	Source/destination	Port	Protocol	Details
Ingress	Apporto appliance	Admin network	443	TCP	Cluster node management interface
		Secure gateway or load balancer	30443	TCP	HTTP traffic for Apporto hyperstream and related services
	Apporto secure gateway	Admin network	8443	TCP	Management interface for the secure gateway
		User network	443	TCP	User-initiated traffic to the Apporto hyperstream cluster--source set to match customer's policy
Egress	Apporto appliance	DNS servers	53	TCP/UDP	DNS servers used in the local environment
		NTP servers	123	UDP	NTP servers used in the local environment
		Active Directory (AD)	389, 636	TCP	AD port as desired by customer
		Public IPs	443	TCP	Apporto-required public services (container registries, management services, etc.)
		VDI/RDSH servers	3389	TCP	RDP access to the VDI/RDSH servers to be used with hyperstream
		Nutanix Prism	9440	TCP	Access to Nutanix management APIs for use in automation (required if using Nutanix)

		VMware vCenter	443	TCP	Access to VMware management APIs for use in automation (required if using VMware)
	Apporto secure gateway	DNS servers	53	TCP/UDP	DNS servers used in the local environment
		NTP servers	123	UDP	NTP servers used in the local environment
		Public IPs	443	TCP	Apporto-required public services (container registries, management services, etc.)
		Apporto appliance	30443	TCP	HTTP traffic for Apporto hyperstream and related services

SSL certificates

Apporto NextGen requires SSL certificates to secure all traffic. If you're using your own gateway or load balancer, install an SSL certificate within your appliance. If you will be using an Apporto-supplied gateway, refer to the section on adding a gateway for information on how to set up your certificate.

Licensing

Windows support is covered in this Beta release. Linux and Mac OS will be addressed in future versions.

In addition to your Apporto license, you should ensure you have the appropriate Microsoft licenses required when planning to utilize a single-session or multi-session virtual desktop deployment. Similarly, you should verify licensing compliance for any third-party applications running in the VDI or RDS environments.

Apporto provides general recommendations for Microsoft licenses. Consult your Microsoft licensing partner or Microsoft's licensing documentation for the latest requirements and compliance guidelines for your specific usage.

Scenario	Required licenses
RDS on Windows Server	Windows Server license RDS CALs (per user or per device) Office/M365 licenses (if needed)
VDI on Windows 10/11	Windows Enterprise E3/E5 Microsoft 365 E3/E5 or Windows VDA standalone Office/M365 licenses (if needed) Windows 11 volume licenses + SA (if needed)

Group policy settings

To optimize the performance and functionality of Remote Desktop Services (RDS) servers and VDI desktops in an Apporto deployment, specific settings must be configured. Apporto recommends configuring the following policy settings and applying them to the RDS servers and VDI desktops.

Apporto RDS/VDI settings

Use the table below to help you configure your system to work with Apporto.

Category	Setting	Recommended value

Remote session environment	Configure compression for RemoteFX data	Enabled
Remote session environment	RDP compression algorithm	Optimized to use less network bandwidth
Remote session environment	Configure H.264/AVC hardware encoding for remote desktop connections	Enabled
Remote session environment	Configure image quality for RemoteFX adaptive graphics	Enabled
Remote session environment	Image quality	Medium
Remote session environment	Configure RemoteFX adaptive graphics	Enabled
Remote session environment	RDP experience	Optimize for minimum bandwidth
Remote session environment	Enable RemoteFX encoding for RemoteFX clients designed for Windows 2008 R2 SP1	Enabled
Remote session environment	Prioritize H.264/AVC 444 graphics mode for remote desktop connections	Enabled
Remote session environment	Use advanced RemoteFX graphics for RemoteApp	Enabled
Remote session environment	Use hardware graphics adapters for all remote desktop services connections	Enabled
RemoteFX for Windows Server 2008 R2	Optimize visual experience for remote desktop services sessions	Enabled
RemoteFX for Windows Server 2008 R2	Visual experience	Rich multimedia
Security	Require secure RPC communication	Disabled
Security	Require use of specific security layer for remote (RDP) connections	Enabled
Security	Security layer	Negotiate
Security	Require user authentication for remote connections by using network-level authentication	• General setting = Disabled • Setting if SSO to the desktop is being used = Enabled
Security	Set client connection encryption level	Enabled
Security	Encryption level	Low level

Additional Microsoft settings

Customers should also configure policy settings for Session Limits, Enable Fair Share to manage resources efficiently across multiple users in multi-session deployments, and profile management. See the following links for more information:

- Microsoft Fair Share - Fair Share technologies are enabled by default in Remote Desktop Services
- Microsoft FSLogix - What is FSLogix - FSLogix

Deployment

Deployment of Apporto is handled through the on-premises installer tool within the Apporto NextGen control plane. Full deployment includes the following:

- Apporto control plane setup
- On-premises cluster installation
- Hyperstream configuration and node discovery
- Load balancer or secure gateway installation
- Support tunnel setup

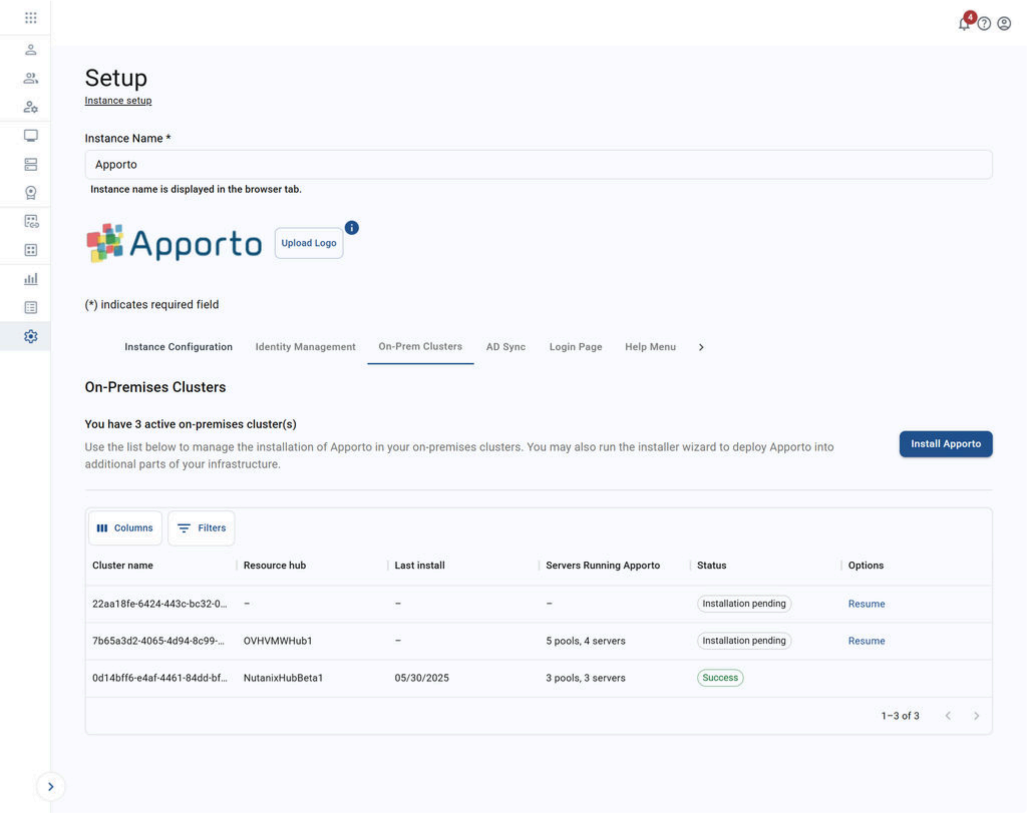
Accessing the control plane

Once your Apporto instance and initial administrator account have been set up, sign in to the control plane. Navigate to the *Setup* page, and click on the **On-Prem Clusters** tab.

For more information on signing in to the control plane,

On-premises clusters

From the *Setup* section, the “On-Prem Clusters” tab contains a view of all existing on-premises clusters that are connected to Apporto.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

On-Premises Clusters

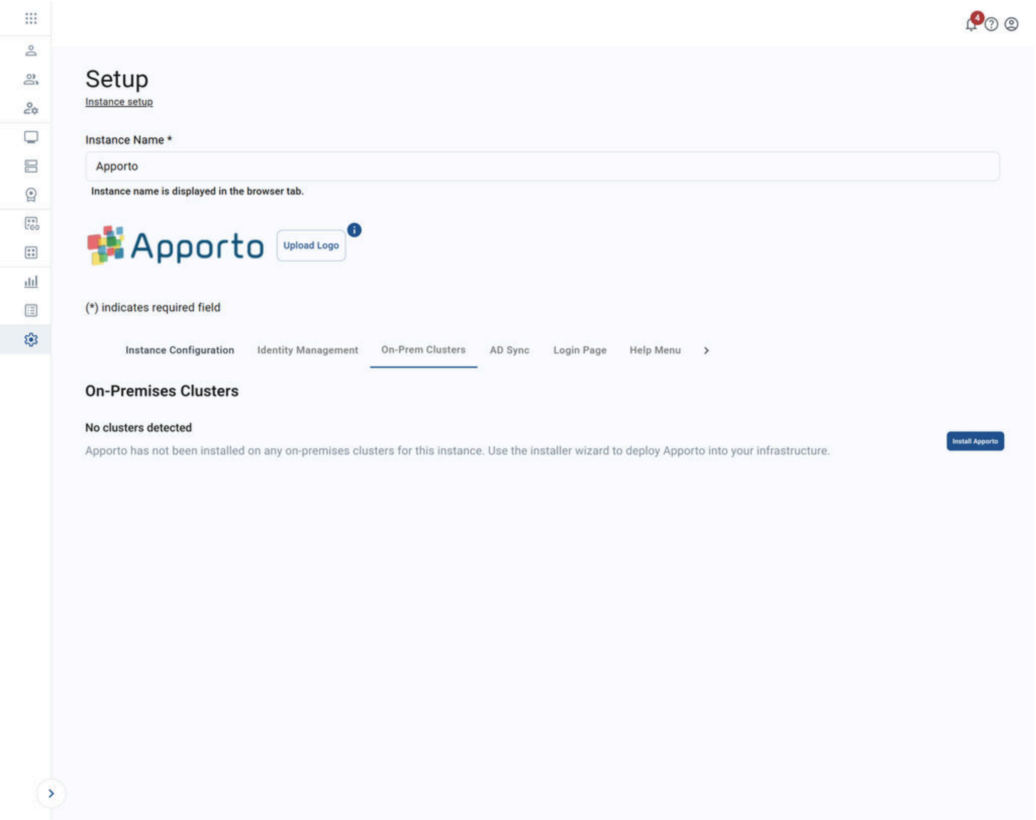
You have 3 active on-premises cluster(s)

Use the list below to manage the installation of Apporto in your on-premises clusters. You may also run the installer wizard to deploy Apporto into additional parts of your infrastructure.

Cluster name	Resource hub	Last install	Servers Running Apporto	Status	Options
22aa18fe-6424-443c-bc32-0...	–	–	–	Installation pending	Resume
7b65a3d2-4065-4d94-8c99-...	OVHVMWHub1	–	5 pools, 4 servers	Installation pending	Resume
0d14bff6-e4af-4461-84dd-bf...	NutanixHubBeta1	05/30/2025	3 pools, 3 servers	Success	

1–3 of 3

If no clusters have been set up yet, a message will instruct you to start a new installation.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

On-Premises Clusters

No clusters detected

Apporto has not been installed on any on-premises clusters for this instance. Use the installer wizard to deploy Apporto into your infrastructure.

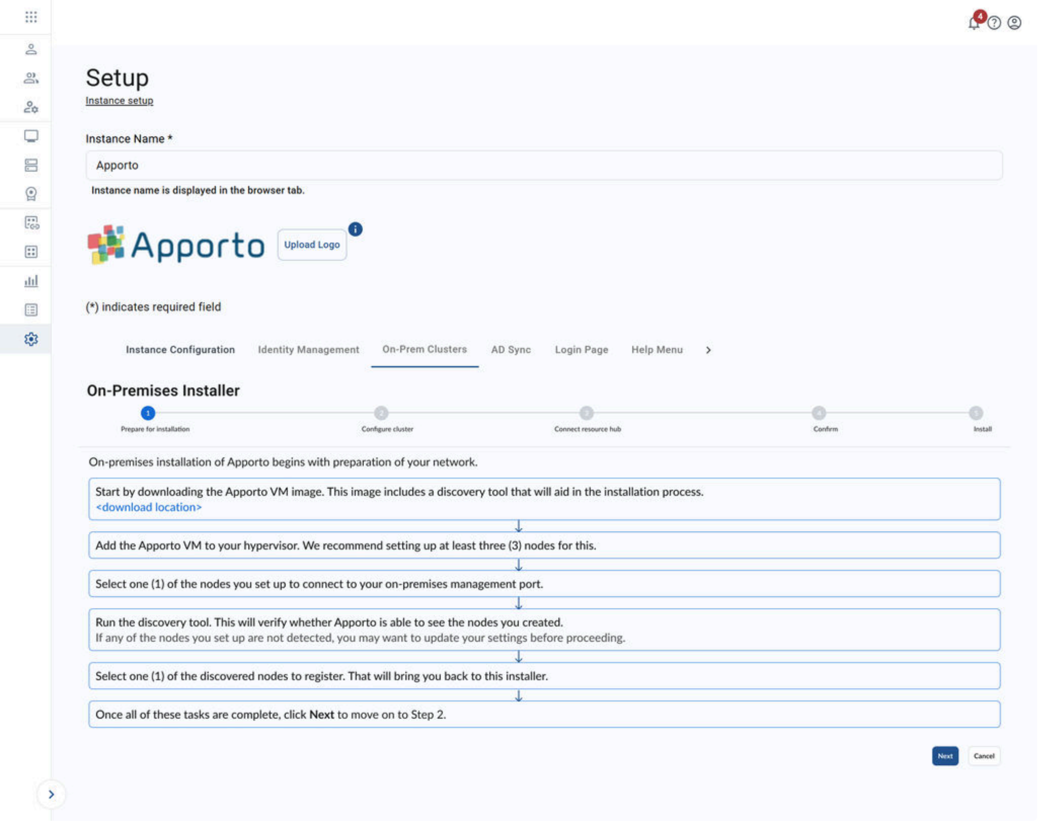
Installations of new clusters may be started at any time by clicking the **Install Apporto** button to trigger the installer wizard. You may also resume an incomplete installation by clicking **Resume** from the cluster list.

On-premises installer

To set up a new on-premises cluster, follow the steps below. Some tasks need to be completed outside of the Apporto NextGen control plane.

Step 1

The initial step of the installer explains how to install the Apporto VM into your hypervisor.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

On-Premises Installer

On-premises installation of Apporto begins with preparation of your network.

Start by downloading the Apporto VM image. This image includes a discovery tool that will aid in the installation process.
<download location>

Add the Apporto VM to your hypervisor. We recommend setting up at least three (3) nodes for this.

Select one (1) of the nodes you set up to connect to your on-premises management port.

Run the discovery tool. This will verify whether Apporto is able to see the nodes you created.
If any of the nodes you set up are not detected, you may want to update your settings before proceeding.

Select one (1) of the discovered nodes to register. That will bring you back to this installer.

Once all of these tasks are complete, click **Next** to move on to Step 2.

Download the Apporto VM file that is appropriate to your hyperstream provider’s file format, and then follow the onscreen instructions for node registration. Packaged with the VM is a node discovery tool that will pass information back to the cluster installer.

⚠ The VM file download link is not currently working. Please navigate to https://apporto-public-assets.s3.amazonaws.com/vm-images/apporto-cluster-node/releases/2025-1-0-BETA1/apporto-cluster-node-2025-1-0-BETA1.ova in a browser window.

Refer to the additional instructions for your hypervisor (additional hypervisor compatibility will be provided in future releases):

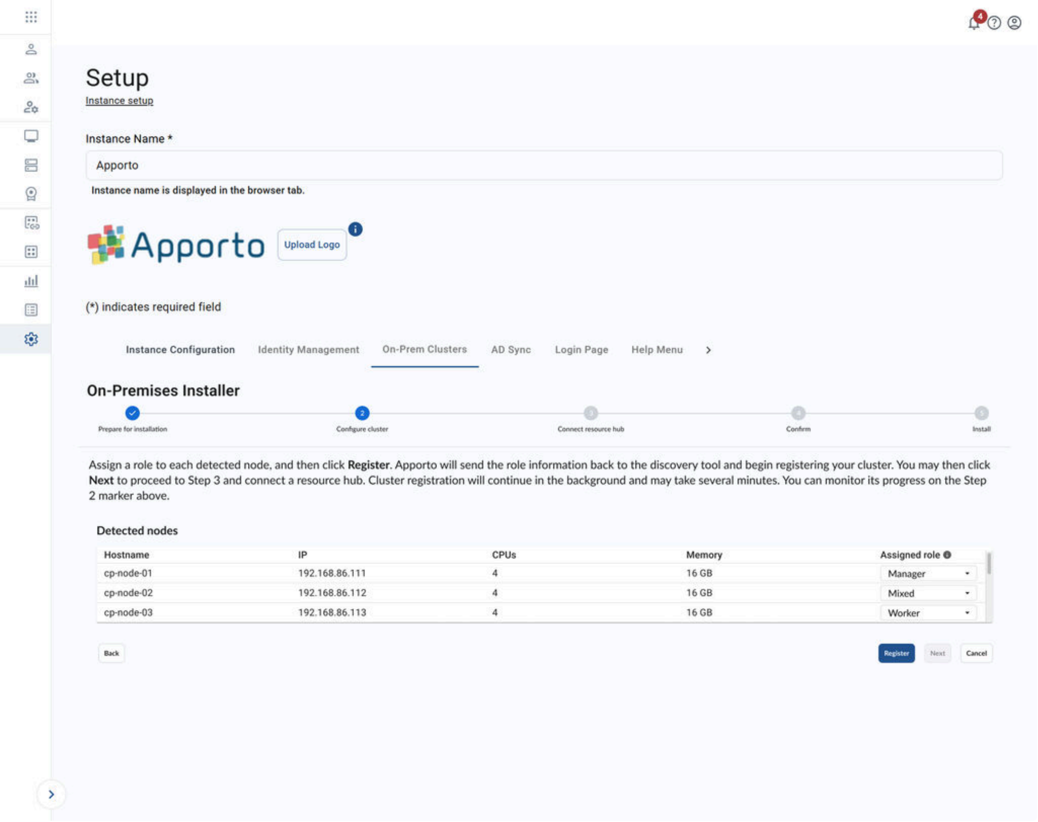
- Nutanix Prism
- VMware vSphere
- Proxmox Virtual Environment COMING SOON

If you experience any issues with node discovery, enable the support tunnel and contact Apporto Support for assistance.

Once the Apporto VM is installed, set up your gateway or load balancer.

Step 2

Once you are transferred back to the installer, Step 2 will display the nodes you selected.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

On-Premises Installer

Assign a role to each detected node, and then click **Register**. Apporto will send the role information back to the discovery tool and begin registering your cluster. You may then click **Next** to proceed to Step 3 and connect a resource hub. Cluster registration will continue in the background and may take several minutes. You can monitor its progress on the Step 2 marker above.

Detected nodes

Hostname	IP	CPUs	Memory	Assigned role
cp-node-01	192.168.86.111	4	16 GB	Manager
cp-node-02	192.168.86.112	4	16 GB	Mixed
cp-node-03	192.168.86.113	4	16 GB	Worker

You must have at least one manager and two worker nodes in your cluster. Select a role for each node. The available node types are:

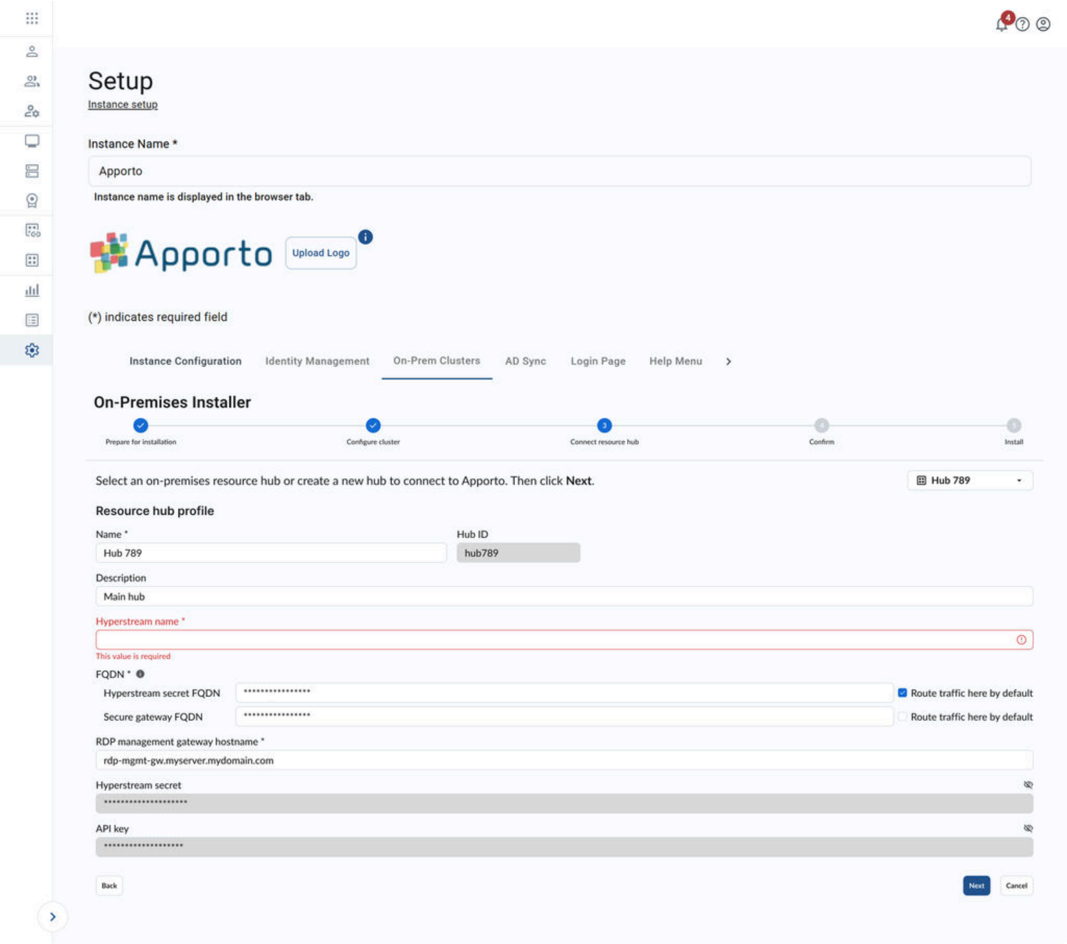
- Manager - This node will connect to the control plane.
- Mixed - If the same node will perform both functions, select this role.
- Worker

Once you have selected a role for each node, click **Register** for the installer to push a registration key to each node. This process may take several minutes, but you will see a confirmation message when registration begins and the **Next** button will be unlocked. You may proceed to Step 3 while registration is running.

Step 3

To connect Apporto to the servers that will be running virtual desktops and applications, the cluster must be linked to a resource hub. If you have already created one or more on-premises resource hubs, you may select the appropriate one from the resource hub dropdown. Existing values will populate in the Step 3 form, and any missing mandatory values can be filled in.

You may also select the “Create new” option from the dropdown to create a resource hub on the fly. Please note that the hub values in this form are the minimum needed for cluster installation. Additional resource hub values can be configured by going to the *Resource Hubs* section of the control plane. You can learn more about resource hub values in the Apporto Help Center.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

On-Premises Installer

Select an on-premises resource hub or create a new hub to connect to Apporto. Then click **Next**.

Hub 789

Resource hub profile

Name *: Hub 789

Hub ID: hub789

Description: Main hub

Hyperstream name *:

This value is required

FQDN *

Hyperstream secret FQDN: **************** ☑ Route traffic here by default

Secure gateway FQDN: **************** □ Route traffic here by default

RDP management gateway hostname *: rdp-mgmt-gw.myserver.mydomain.com

Hyperstream secret: ********************

API key: *******************

The table below shows the resource hub values that relate to cluster installation.

Field	Datatype	Required?	Notes
Name	String	Yes	
Hub ID	String	System-generated	This value will be generated by the system and used in back-end processes.
Description	String	No	
Hyperstream name	String	Yes	
Hyperstream secret FQDN	String	Conditional	At least one of the FQDN values must be entered; both can be filled if appropriate.
Secure gateway FQDN	String	Conditional	
RDP management gateway hostname	String	Yes	
Route traffic here by default	Boolean	Yes	If both FQDN values are entered, one of them must be selected for traffic routing. If only one FQDN is entered, the system will auto-select the matching radio button.
Hyperstream secret	String	System-generated	
API key	String	System-generated	

For the beta version, the hyperstream and RDP management gateway hostnames must be all lowercase.

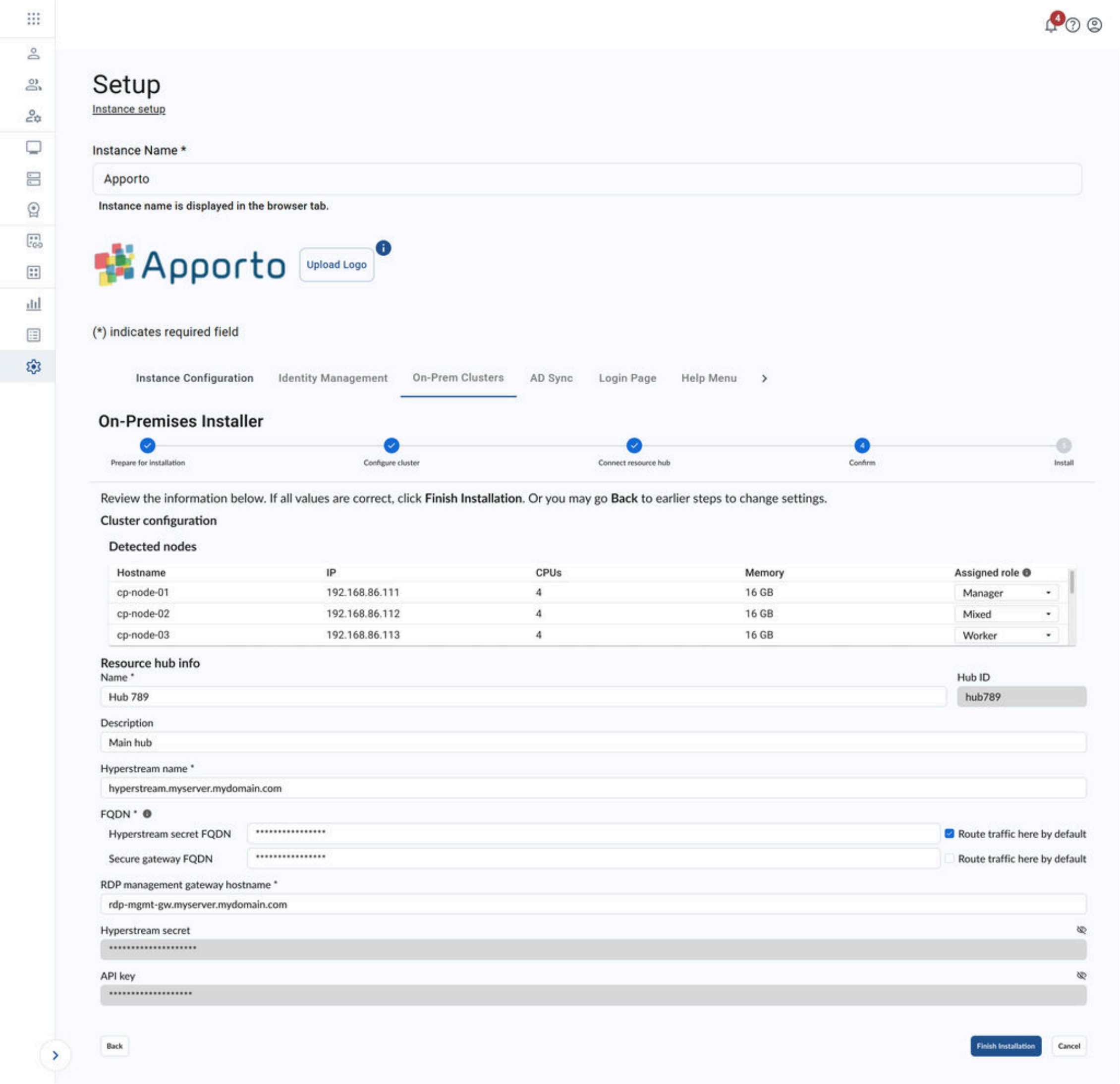
Once the form is filled in, click **Next** to advance to Step 4.

Step 4

Your node role assignments from Step 2 and resource hub values from Step 3 are displayed for confirmation. Review the settings, and go back to the earlier steps if anything needs to be altered.

⚠ Node role assignments cannot be edited once cluster registration is complete. If any Step 2 values are incorrect, contact Apporto Support for assistance.

If all settings are correct, click **Finish Installation**.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

On-Premises Installer

Review the information below. If all values are correct, click **Finish Installation**. Or you may go **Back** to earlier steps to change settings.

Cluster configuration

Detected nodes

Hostname	IP	CPUs	Memory	Assigned role
cp-node-01	192.168.86.111	4	16 GB	Manager
cp-node-02	192.168.86.112	4	16 GB	Mixed
cp-node-03	192.168.86.113	4	16 GB	Worker

Resource hub info

Name *: Hub 789

Hub ID: hub789

Description: Main hub

Hyperstream name *: hyperstream.myserver.mydomain.com

FQDN *

Hyperstream secret FQDN: •••••••••••••••• ☑ Route traffic here by default

Secure gateway FQDN: •••••••••••••••• □ Route traffic here by default

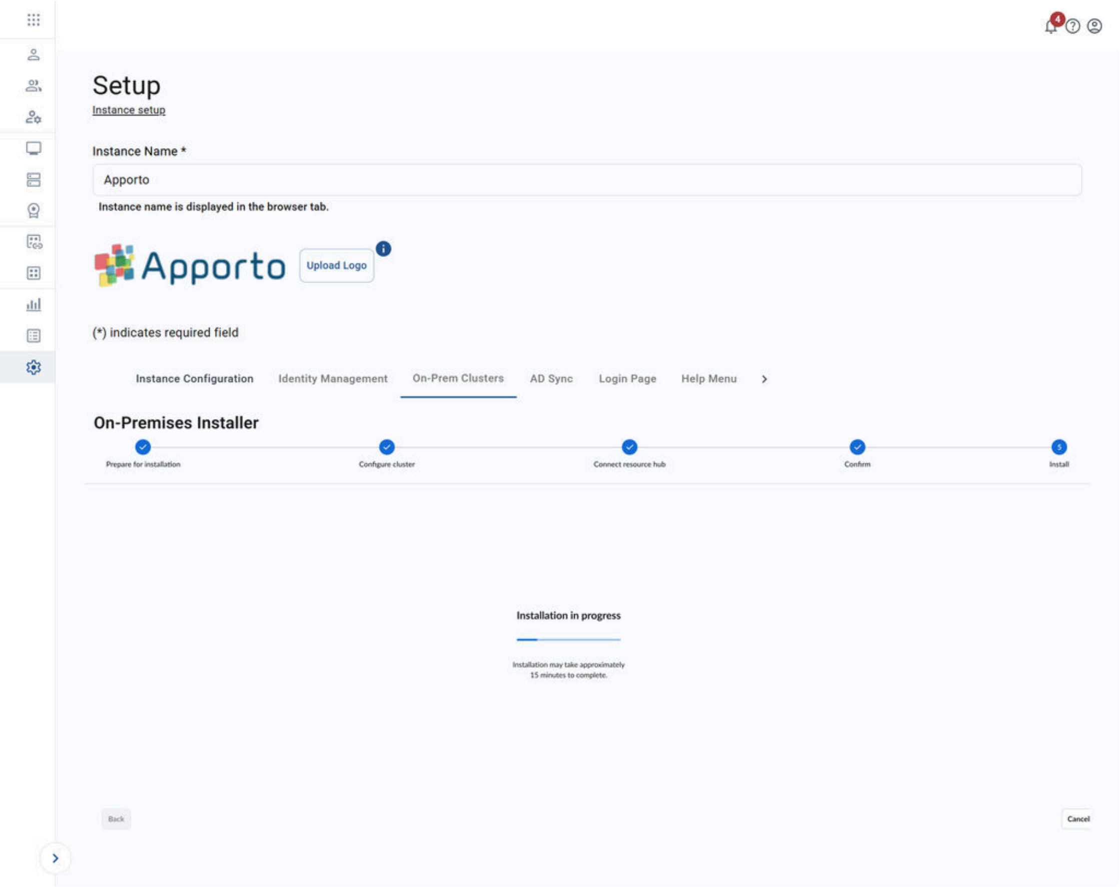
RDP management gateway hostname *: rdp-mgmt-gw.myserver.mydomain.com

Hyperstream secret: ••••••••••••••••••••

API key: •••••••••••••••••••

Step 5

The final step of installation pushes Apporto software and services down to the cluster. You will see a progress bar while the installation is running.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

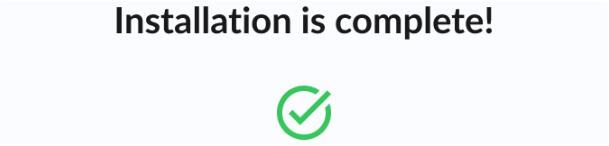
(*) indicates required field

On-Premises Installer

Installation in progress

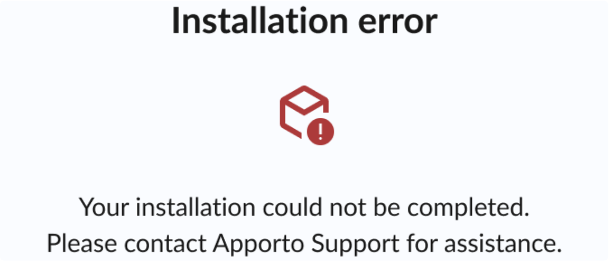
Installation may take approximately 15 minutes to complete.

Once installation has successfully completed, you will see a confirmation message. Click **Done** to return to the cluster list.



Installation is complete!

If there are any issues with the installation process, you will see an error message. Contact Apporto Support for assistance.



Installation error

Your installation could not be completed.
Please contact Apporto Support for assistance.

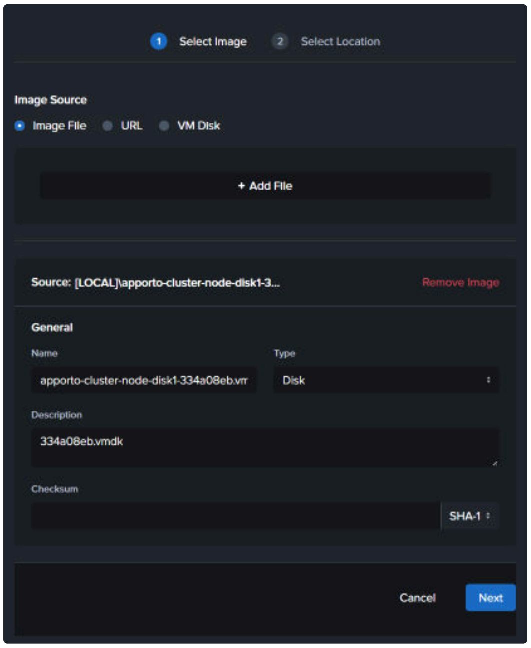
Hypervisor network configuration

Use the instructions below to add the Apporto VM to your hypervisor environment.

- Nutanix Prism
- VMware vSphere
- Proxmox Virtual Environment

Nutanix Prism

1. Download the Apporto VM file from Step 1 of the installer. Different file formats are available to meet the needs of various hypervisors. For Nutanix, download the .OVA image.
2. Unzip the file using 7Zip or another appropriate tool.
3. From the Nutanix Prism web console, import the .VMDK file.



1 Select Image 2 Select Location

Image Source

● Image File ○ URL ○ VM Disk

+ Add File

Source: [LOCAL]\apporto-cluster-node-disk1-3...

Remove Image

General

Name: apporto-cluster-node-disk1-334a08eb.vm

Type: Disk

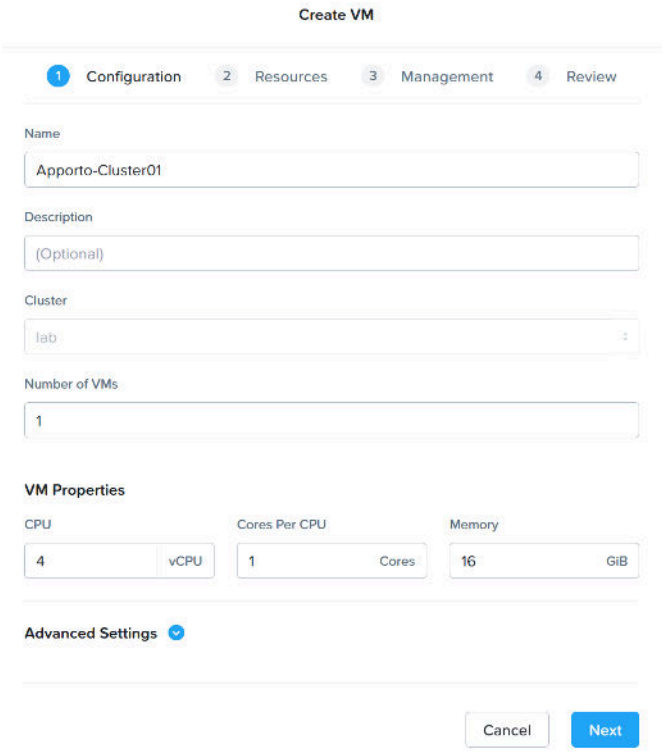
Description: 334a08eb.vmdk

Checksum: SHA-1

Cancel Next

We recommend you update the file name to something unique, in case a situation arises that warrants a new upload. Nutanix may not reference the correct file if the names are the same.

4. Create a new VM in Nutanix.



Create VM

1 Configuration 2 Resources 3 Management 4 Review

Name: Apporto-Cluster01

Description: (Optional)

Cluster: lab

Number of VMs: 1

VM Properties

CPU: 4 vCPU

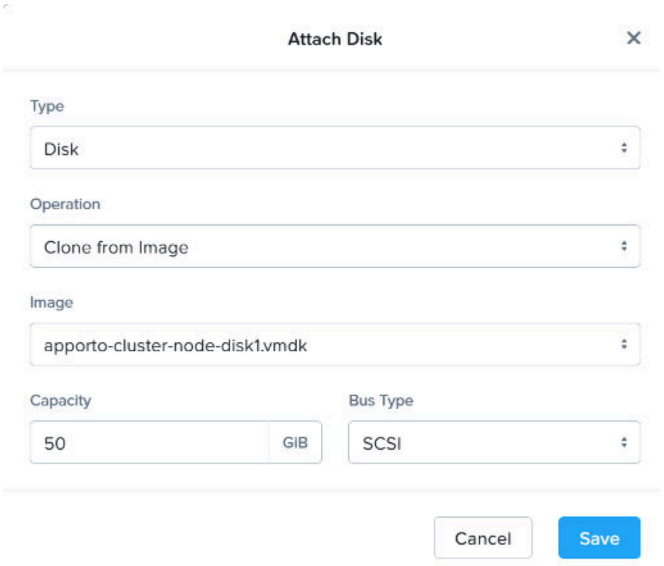
Cores Per CPU: 1 Cores

Memory: 16 GiB

Advanced Settings

Cancel Next

5. Attach the .VMDK image.



Attach Disk

Type: Disk

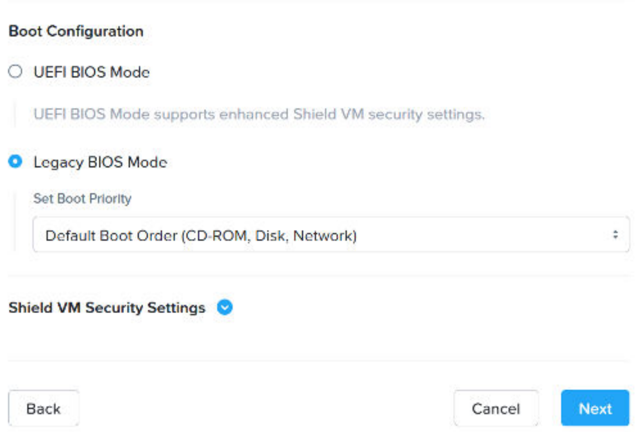
Operation: Clone from Image

Image: apporto-cluster-node-disk1.vmdk

Capacity: 50 GiB

Bus Type: SCSI

6. Adjust the BIOS mode.



Boot Configuration

○ UEFI BIOS Mode

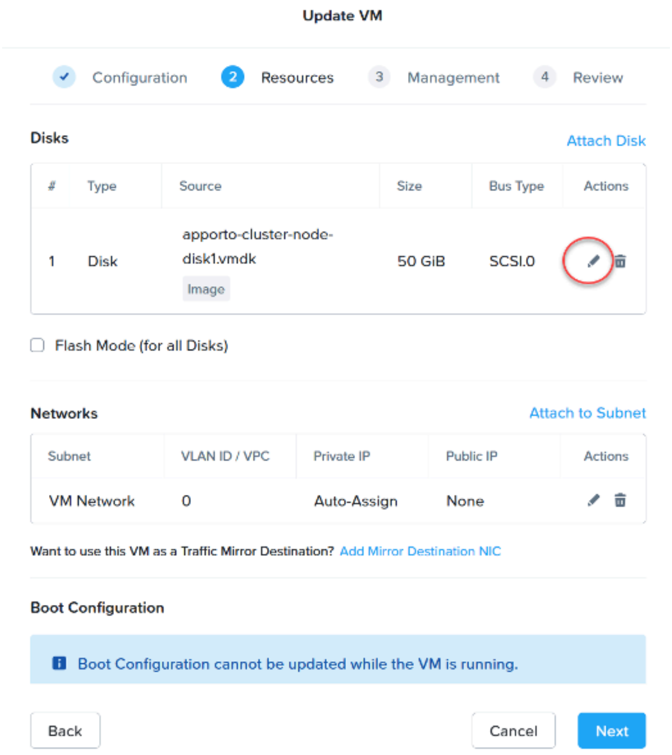
UEFI BIOS Mode supports enhanced Shield VM security settings.

● Legacy BIOS Mode

Set Boot Priority: Default Boot Order (CD-ROM, Disk, Network)

Shield VM Security Settings

7. Once the VM has been created, access the *Update Disk* screen.



Update VM

Disks

#	Type	Source	Size	Bus Type	Actions
1	Disk	apporto-cluster-node-disk1.vmdk Image	50 GiB	SCSI.0	

□ Flash Mode (for all Disks)

Networks

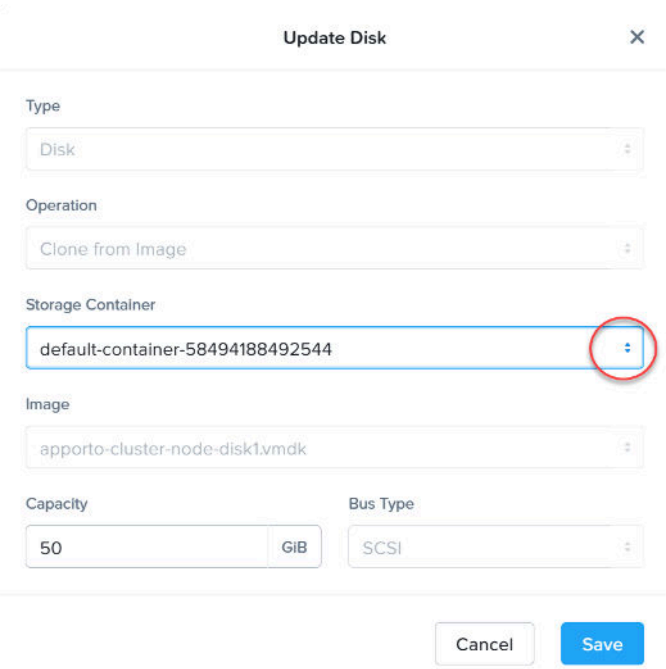
Subnet	VLAN ID / VPC	Private IP	Public IP	Actions
VM Network	0	Auto-Assign	None	

Want to use this VM as a Traffic Mirror Destination? Add Mirror Destination NIC

Boot Configuration

Boot Configuration cannot be updated while the VM is running.

8. Ensure that the .VMDK is pointing to the correct storage container.



Update Disk

Type: Disk

Operation: Clone from Image

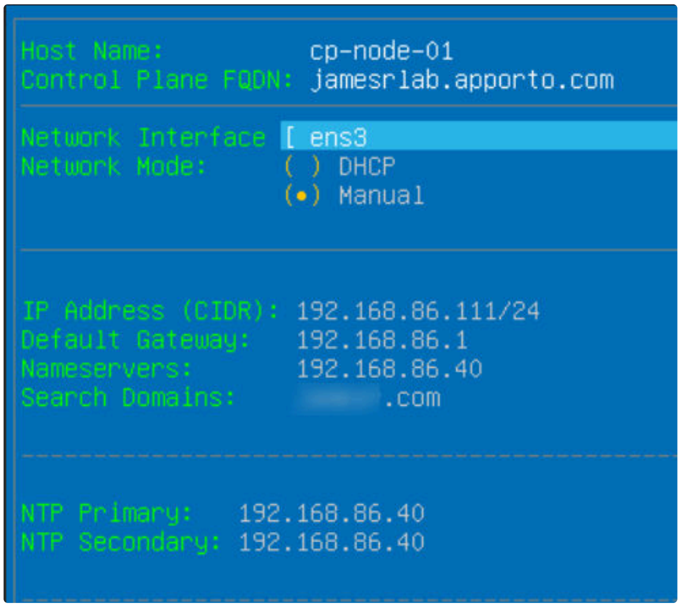
Storage Container: default-container-58494188492544

Image: apporto-cluster-node-disk1.vmdk

Capacity: 50 GiB

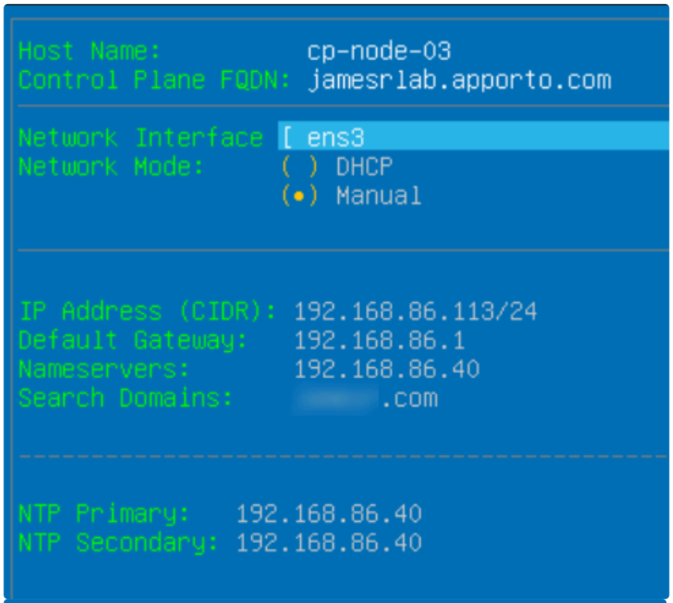
Bus Type: SCSI

9. Power on the first VM for your controller/manager to access the *Network Config* screen. Update the network config values to accommodate the Apporto VM, including the control plane FQDN (your Apporto instance domain). The image below shows sample values.

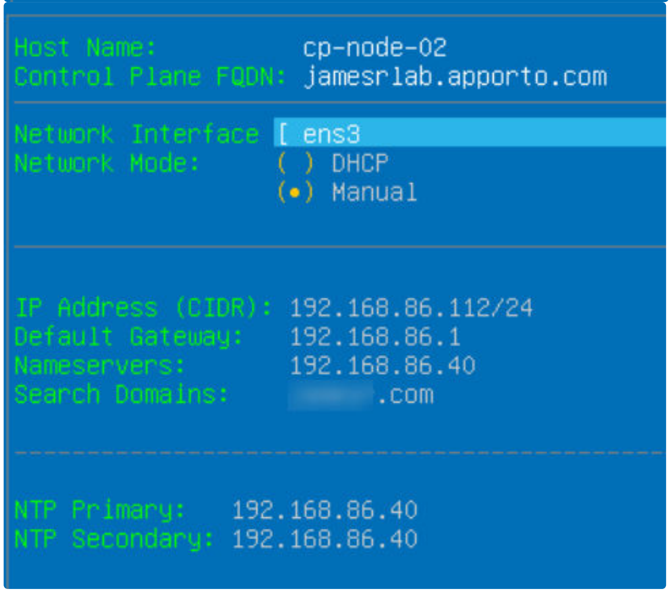


```
Host Name:           cp-node-01
Control Plane FQDN:  jamesrlab.apporto.com

Network Interface  [ ens3
Network Mode:       ( ) DHCP
                    (•) Manual

IP Address (CIDR):  192.168.86.111/24
Default Gateway:    192.168.86.1
Nameservers:        192.168.86.40
Search Domains:     [redacted].com

NTP Primary:    192.168.86.40
NTP Secondary:  192.168.86.40
```

a. Repeat the process for the additional nodes in your cluster. Most customers will have three nodes, where the first node is designated as the manager and the remaining nodes will serve as workers.



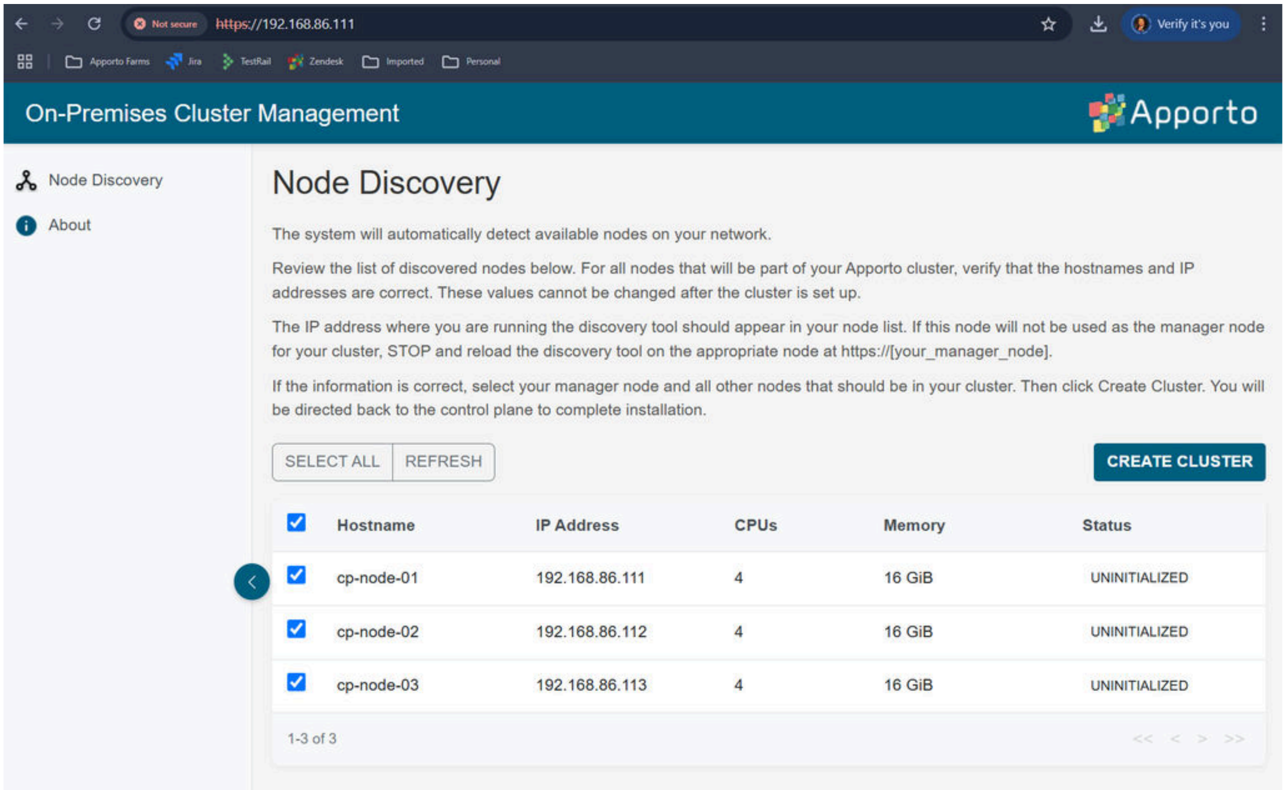
```
Host Name:            cp-node-03
Control Plane FQDN: jamesrlab.apporto.com

Network Interface [ ens3
Network Mode:       ( ) DHCP
                    (•) Manual

IP Address (CIDR): 192.168.86.113/24
Default Gateway:   192.168.86.1
Nameservers:       192.168.86.40
Search Domains:    [redacted].com

------------------------------------------

NTP Primary:   192.168.86.40
NTP Secondary: 192.168.86.40
```



```
Host Name:            cp-node-02
Control Plane FQDN: jamesrlab.apporto.com

Network Interface [ ens3
Network Mode:       ( ) DHCP
                    (•) Manual

IP Address (CIDR): 192.168.86.112/24
Default Gateway:   192.168.86.1
Nameservers:       192.168.86.40
Search Domains:    [redacted].com

------------------------------------------

NTP Primary:   192.168.86.40
NTP Secondary: 192.168.86.40
```

b. Click **Save** at the bottom of the screen.

10. Open https://[your_manager_node] in a browser window. This will launch the On-Premises Cluster Management tool that was included with the Apporto VM file.



Node Discovery

The system will automatically detect available nodes on your network.

Review the list of discovered nodes below. For all nodes that will be part of your Apporto cluster, verify that the hostnames and IP addresses are correct. These values cannot be changed after the cluster is set up.

The IP address where you are running the discovery tool should appear in your node list. If this node will not be used as the manager node for your cluster, STOP and reload the discovery tool on the appropriate node at https://[your_manager_node].

If the information is correct, select your manager node and all other nodes that should be in your cluster. Then click Create Cluster. You will be directed back to the control plane to complete installation.

SELECT ALL | REFRESH | CREATE CLUSTER

☑	Hostname	IP Address	CPUs	Memory	Status
☑	cp-node-01	192.168.86.111	4	16 GiB	UNINITIALIZED
☑	cp-node-02	192.168.86.112	4	16 GiB	UNINITIALIZED
☑	cp-node-03	192.168.86.113	4	16 GiB	UNINITIALIZED

1-3 of 3 << < > >>

Any nodes that are detected in your container will appear in the *Node Discovery* list.

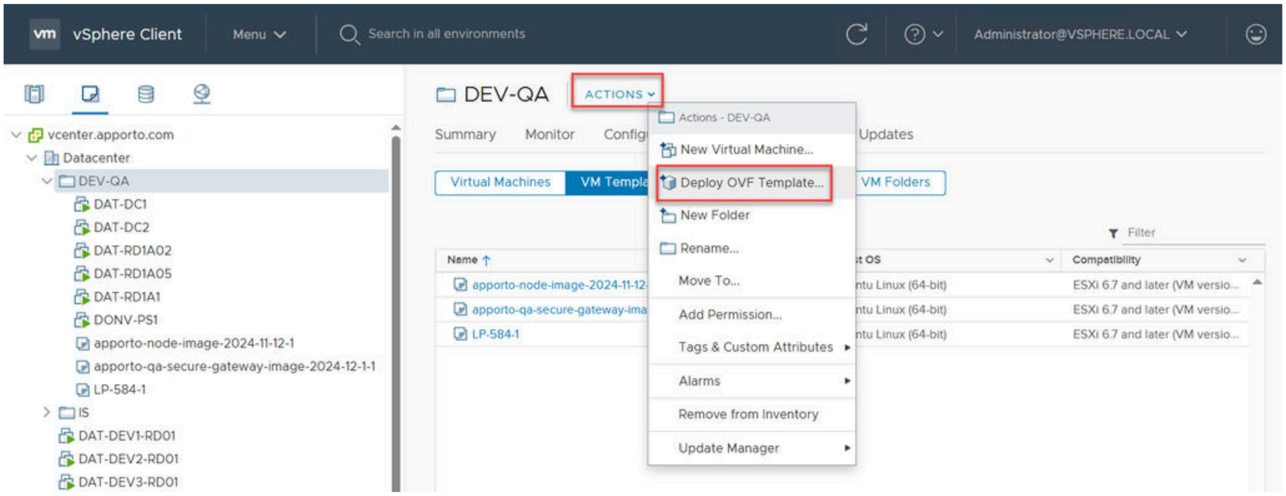
11. Select all nodes that you want to be connected to Apporto, then click **Create Cluster** to be transferred back to the Apporto NextGen control plane to continue cluster installation.

> Apporto recommends setting the NTP timeservers to be the same ones used by your local environment.

> If any nodes from your container do not appear in the list within a few minutes of loading the tool, you may want to click **Refresh**.

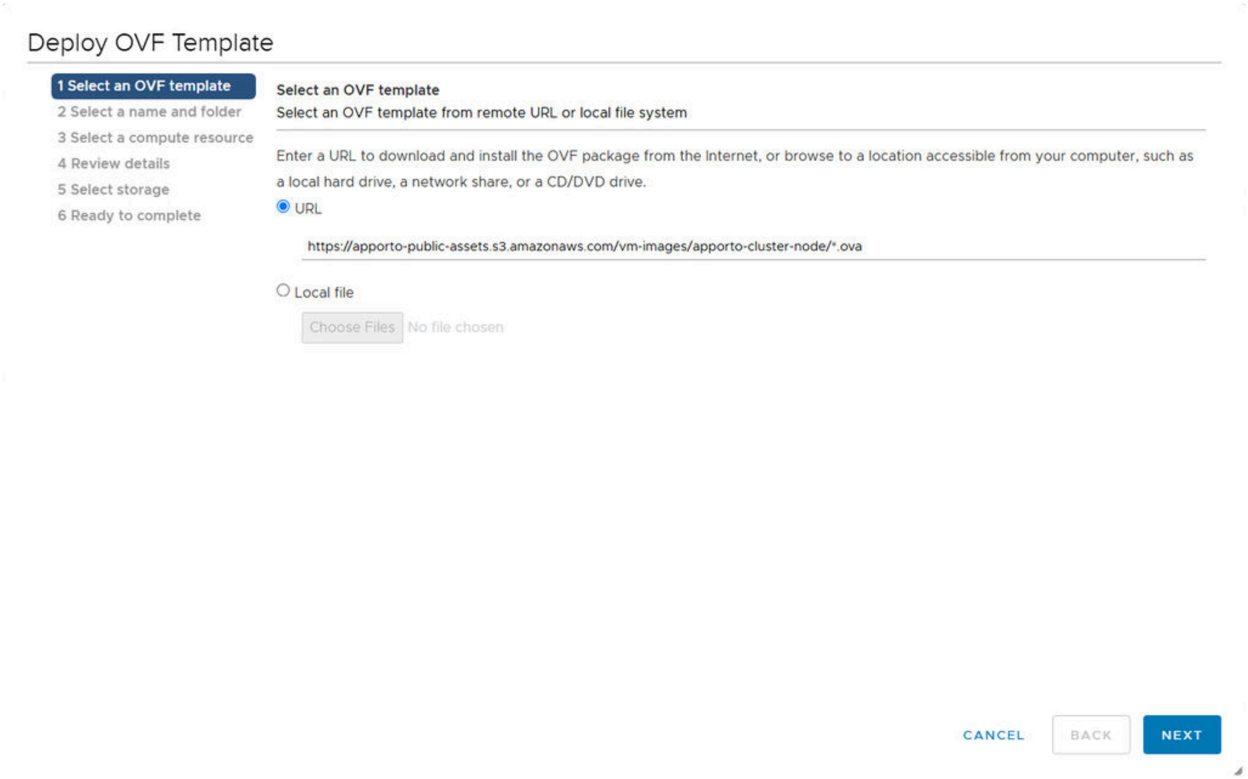
VMware vSphere

1. Download the Apporto VM file from Step 1 of the installer. Different file formats are available to meet the needs of various hypervisors. For VMware, download the .OVA image.
2. From the vSphere console, import the .OVA file as an OFV template. Alternatively, you can unzip the file and import the .VMDK disk image file.



Name ↑	t OS	Compatibility
apporto-node-image-2024-11-12-	ntu Linux (64-bit)	ESXi 6.7 and later (VM versio...
apporto-qa-secure-gateway-ima	ntu Linux (64-bit)	ESXi 6.7 and later (VM versio...
LP-584-1	ntu Linux (64-bit)	ESXi 6.7 and later (VM versio...

Both URL and local file options are provided onscreen. At this time, select the local file option to import the .OVA file. In the future, we may offer a public URL.



Deploy OVF Template

Select an OVF template

Select an OVF template from remote URL or local file system

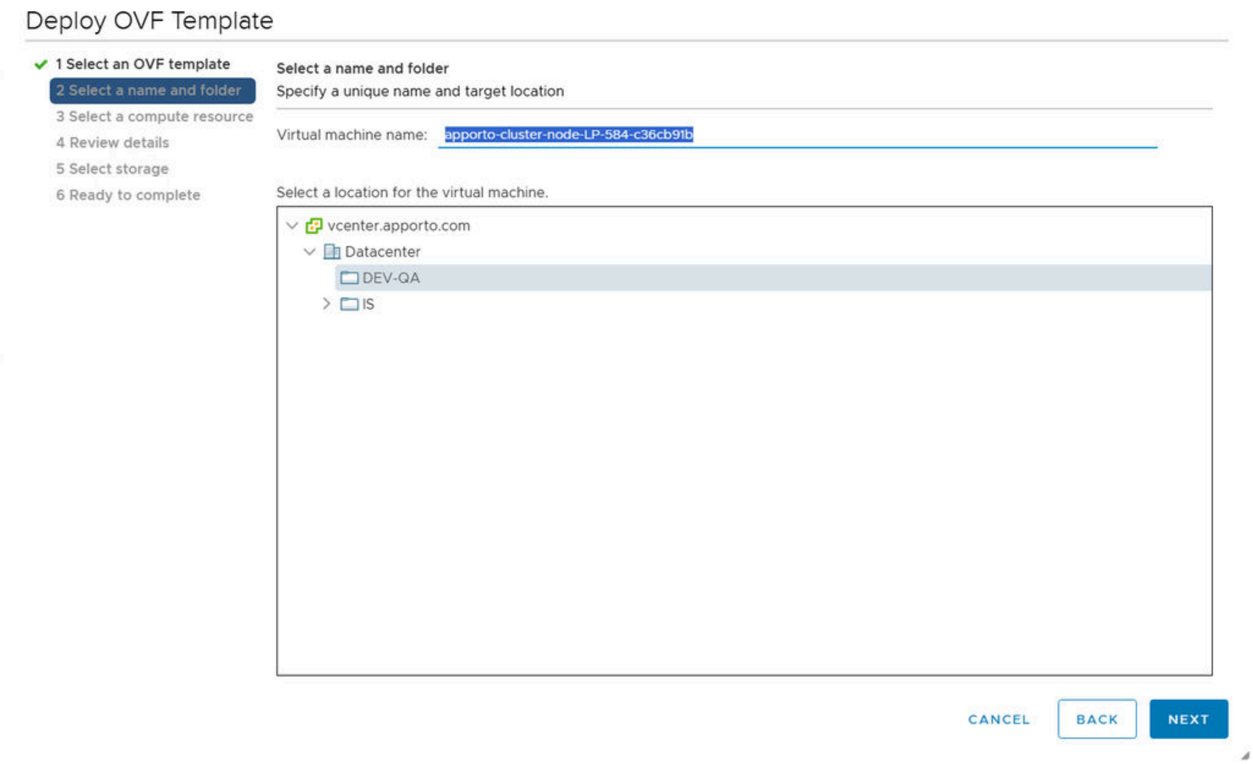
Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

https://apporto-public-assets.s3.amazonaws.com/vm-images/apporto-cluster-node/*.ova

○ Local file

3. Create a new VM in vSphere.



Deploy OVF Template

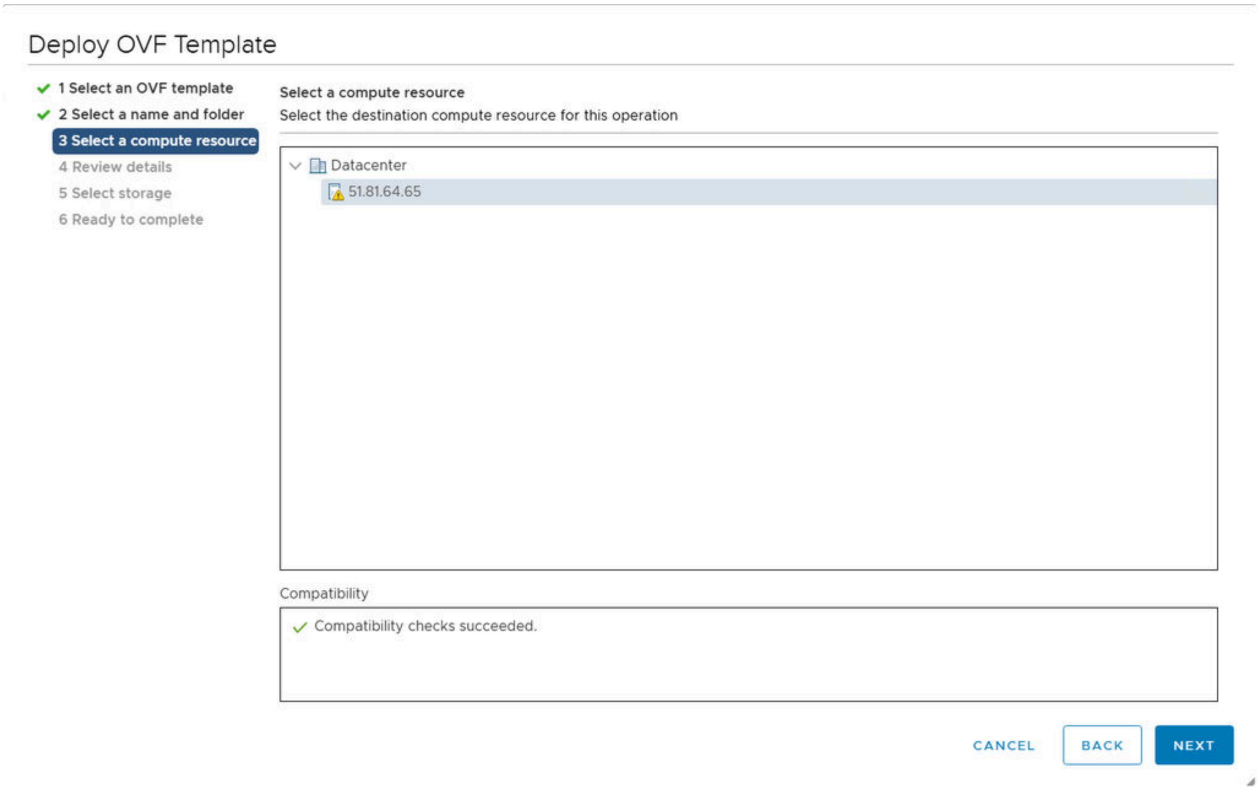
Select a name and folder

Specify a unique name and target location

Virtual machine name: apporto-cluster-node-LP-584-c36cb91b

Select a location for the virtual machine.

4. Select the appropriate compute resource.


Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

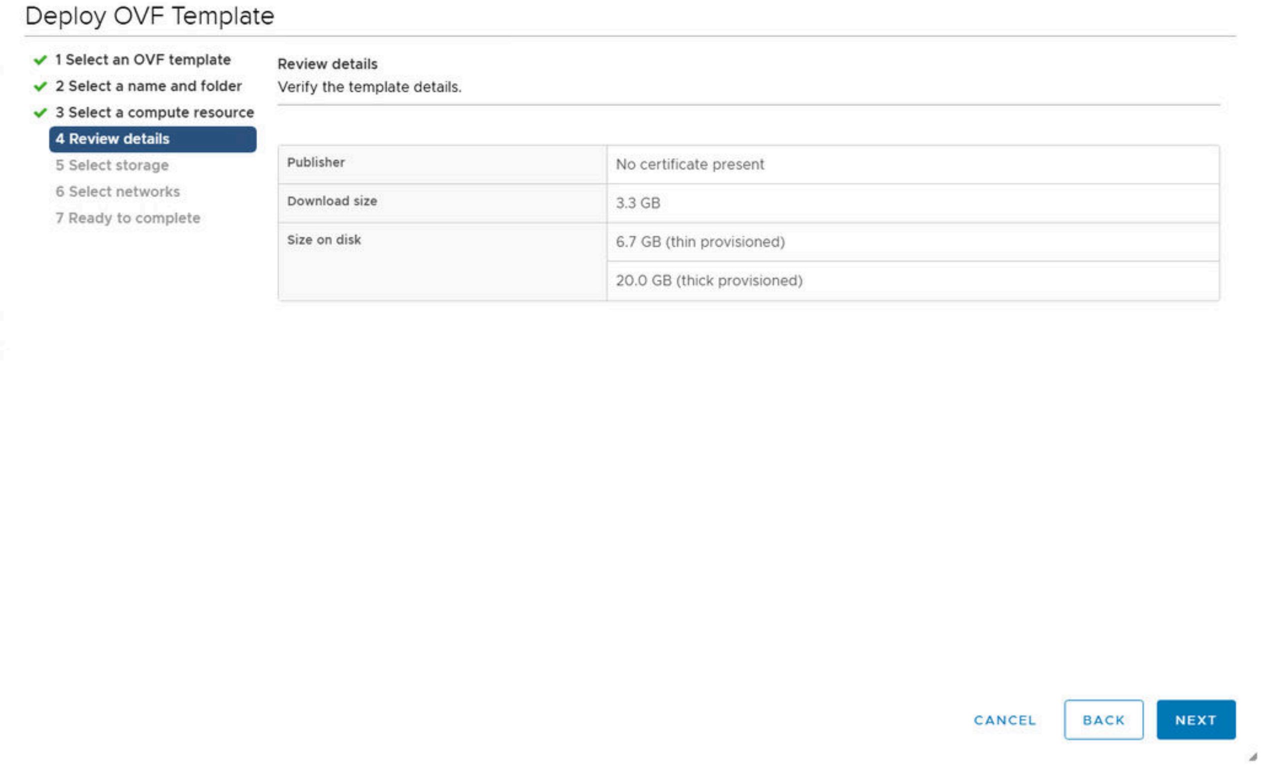
Select a compute resource

Select the destination compute resource for this operation

Compatibility

✓ Compatibility checks succeeded.

5. Review and confirm the template details.


Deploy OVF Template

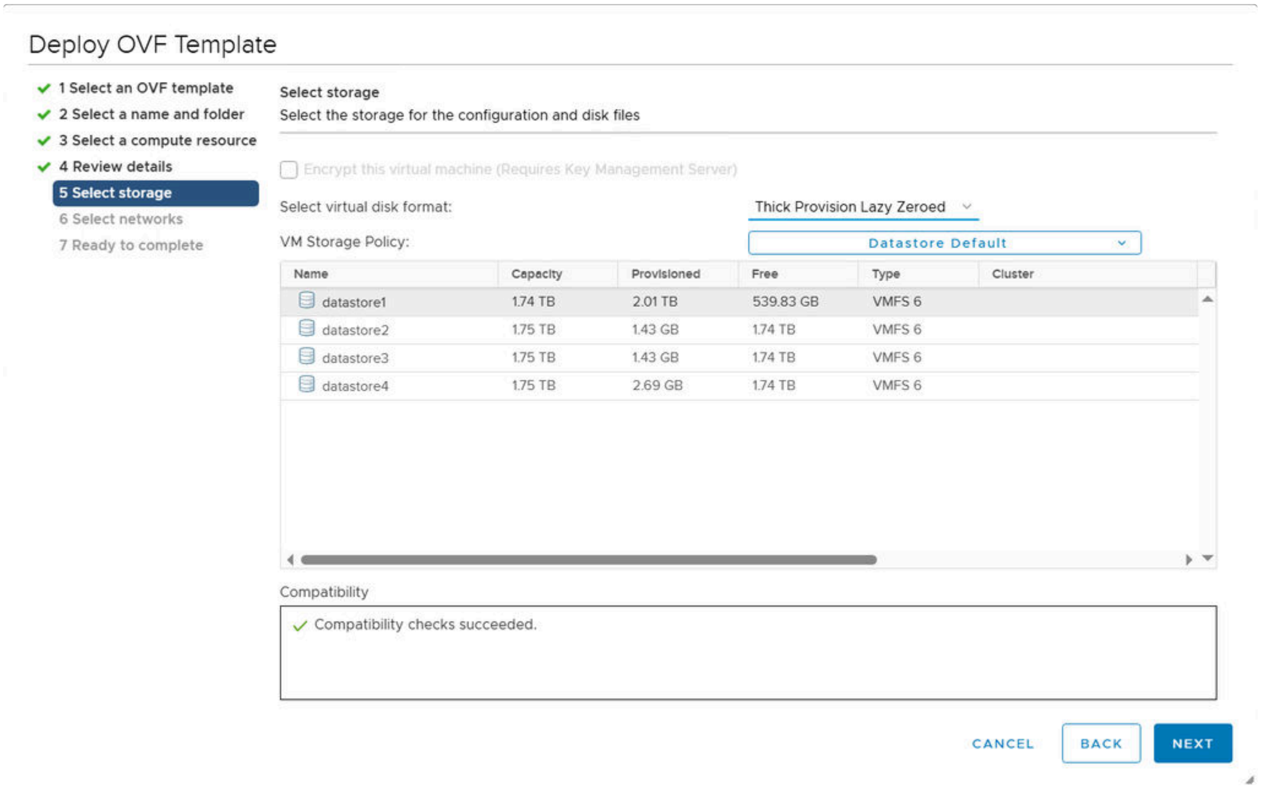
✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Review details

Verify the template details.

Publisher	No certificate present
Download size	3.3 GB
Size on disk	6.7 GB (thin provisioned)
	20.0 GB (thick provisioned)

6. Select the appropriate storage container.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

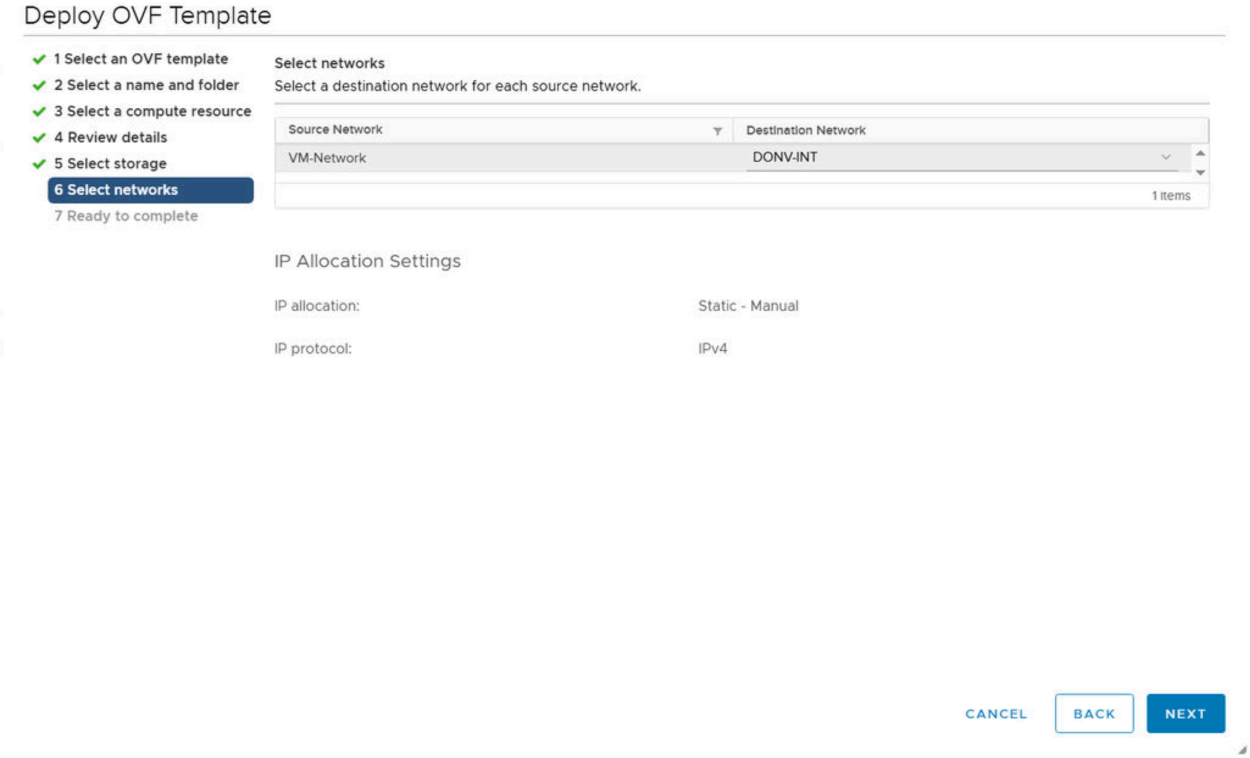
VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore1	1.74 TB	2.01 TB	539.83 GB	VMFS 6	
datastore2	1.75 TB	1.43 GB	1.74 TB	VMFS 6	
datastore3	1.75 TB	1.43 GB	1.74 TB	VMFS 6	
datastore4	1.75 TB	2.69 GB	1.74 TB	VMFS 6	

Compatibility

✓ Compatibility checks succeeded.

7. Select your destination network.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks
- 7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM-Network	DONV-INT

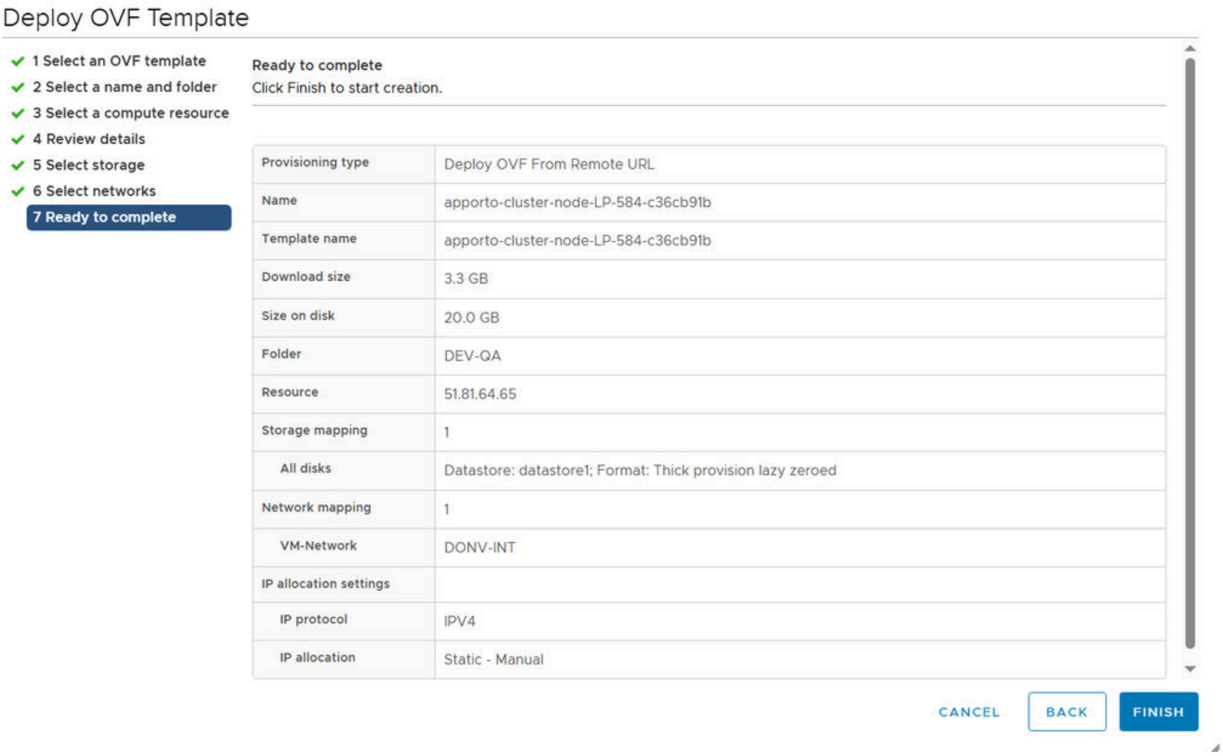
1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

8. Confirm all values, and click **Finish** to deploy the template.



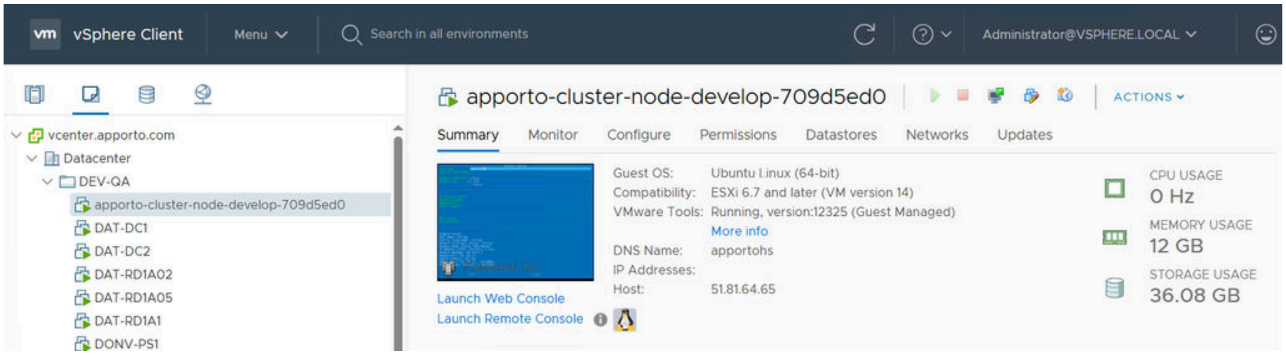
Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 Select storage
✓ 6 Select networks
7 Ready to complete

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	apporto-cluster-node-LP-584-c36cb91b
Template name	apporto-cluster-node-LP-584-c36cb91b
Download size	3.3 GB
Size on disk	20.0 GB
Folder	DEV-QA
Resource	51.81.64.65
Storage mapping	1
All disks	Datastore: datastore1; Format: Thick provision lazy zeroed
Network mapping	1
VM-Network	DONV-INT
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

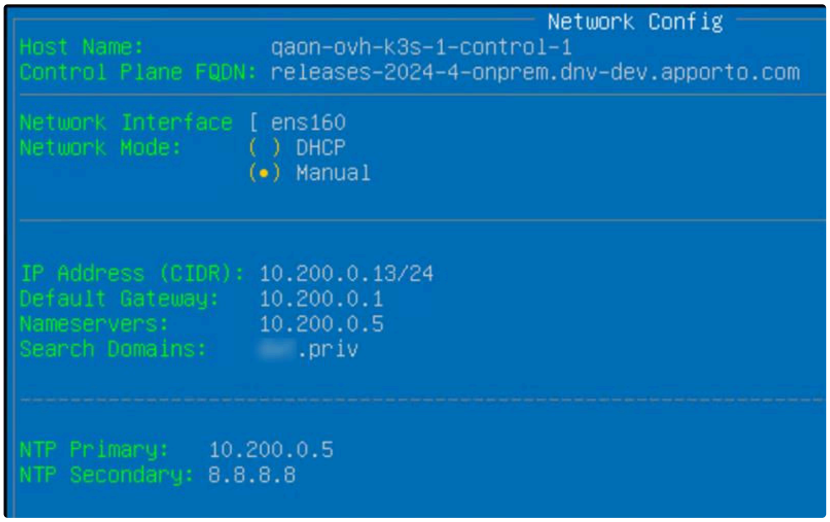
9. Once the VM has been created, view its details from your resource list.



Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:12325 (Guest Managed)
More info
DNS Name: apportohs
IP Addresses:
Host: 51.81.64.65

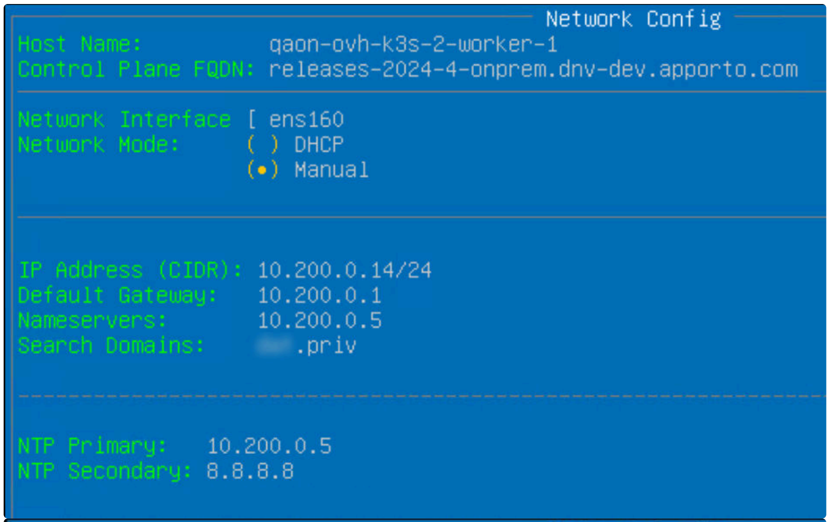
CPU USAGE 0 Hz
MEMORY USAGE 12 GB
STORAGE USAGE 36.08 GB

10. Power on the first VM for your controller/manager to access the *Network Config* screen. Update the network config values to accommodate the Apporto VM, including the control plane FQDN (your Apporto instance domain). The image below shows sample values.

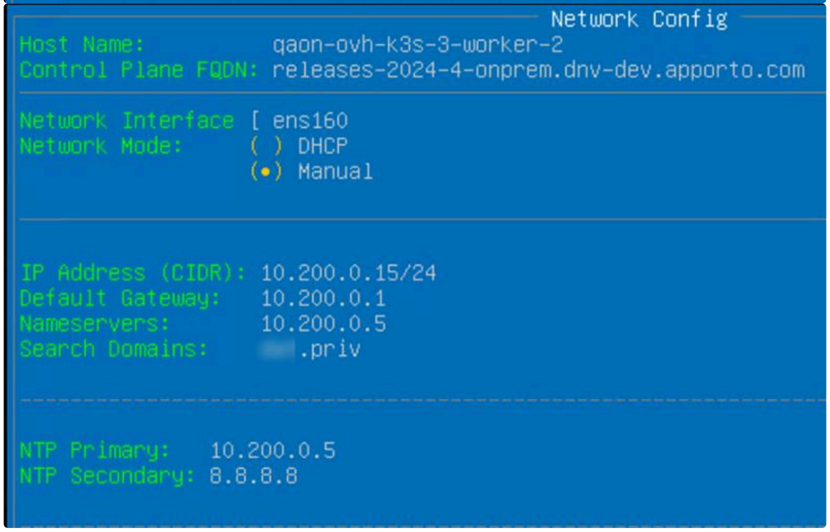


```
                                Network Config
Host Name:         qaon-ovh-k3s-1-control-1
Control Plane FQDN: releases-2024-4-onprem.dnv-dev.apporto.com

Network Interface [ ens160
Network Mode:      ( ) DHCP
                   (•) Manual


IP Address (CIDR): 10.200.0.13/24
Default Gateway:   10.200.0.1
Nameservers:       10.200.0.5
Search Domains:    [redacted].priv


NTP Primary:   10.200.0.5
NTP Secondary: 8.8.8.8
```

a. Repeat the process for the additional nodes in your cluster. Most customers will have three nodes, where the first node is designated as the manager and the remaining nodes will serve as workers.



```
                                          Network Config
Host Name:           qaon-ovh-k3s-2-worker-1
Control Plane FQDN: releases-2024-4-onprem.dnv-dev.apporto.com

Network Interface [ ens160
Network Mode:       ( ) DHCP
                    (•) Manual

IP Address (CIDR): 10.200.0.14/24
Default Gateway:   10.200.0.1
Nameservers:       10.200.0.5
Search Domains:    [redacted].priv

NTP Primary:   10.200.0.5
NTP Secondary: 8.8.8.8
```

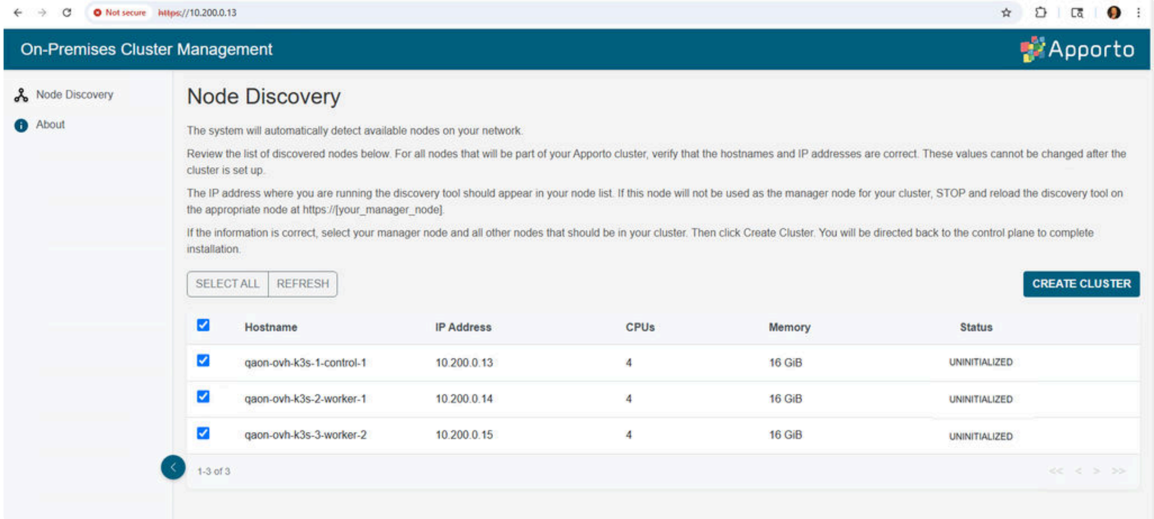


```
                                          Network Config
Host Name:           qaon-ovh-k3s-3-worker-2
Control Plane FQDN: releases-2024-4-onprem.dnv-dev.apporto.com

Network Interface [ ens160
Network Mode:       ( ) DHCP
                    (•) Manual

IP Address (CIDR): 10.200.0.15/24
Default Gateway:   10.200.0.1
Nameservers:       10.200.0.5
Search Domains:    [redacted].priv

NTP Primary:   10.200.0.5
NTP Secondary: 8.8.8.8
```

b. Click **Save** at the bottom of the screen.

11. Open https://[your_manager_node] in a browser window. This will launch the On-Premises Cluster Management tool that was included with the Apporto VM file.

    Any nodes that are detected in your container will appear in the *Node Discovery* list.



Not secure https://10.200.0.13
On-Premises Cluster Management
Apporto
Node Discovery
About

Node Discovery

The system will automatically detect available nodes on your network.

Review the list of discovered nodes below. For all nodes that will be part of your Apporto cluster, verify that the hostnames and IP addresses are correct. These values cannot be changed after the cluster is set up.

The IP address where you are running the discovery tool should appear in your node list. If this node will not be used as the manager node for your cluster, STOP and reload the discovery tool on the appropriate node at https://[your_manager_node].

If the information is correct, select your manager node and all other nodes that should be in your cluster. Then click Create Cluster. You will be directed back to the control plane to complete installation.

☑	Hostname	IP Address	CPUs	Memory	Status
☑	qaon-ovh-k3s-1-control-1	10.200.0.13	4	16 GiB	UNINITIALIZED
☑	qaon-ovh-k3s-2-worker-1	10.200.0.14	4	16 GiB	UNINITIALIZED
☑	qaon-ovh-k3s-3-worker-2	10.200.0.15	4	16 GiB	UNINITIALIZED

1-3 of 3

12. Select all nodes that you want to be connected to Apporto, then click **Create Cluster** to be transferred back to the Apporto NextGen control plane to continue cluster installation.

Apporto recommends setting the NTP timeservers to be the same ones used by your local environment.

Proxmox Virtual Environment

COMING SOON

Adding a gateway or load balancer

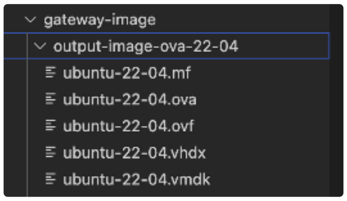
Apporto requires the use of a secure gateway or load balancer appliance in conjunction with your on-premises cluster. If you do not have your own preferred appliance, use the information below to set up the Apporto gateway appliance.

Build

1. SSH into a node in your Apporto container.
2. Download the gateway image from https://apporto-public-assets.s3.amazonaws.com/vm-images/apporto-secure-gateway/releases/2025-1-0-BETA1/apporto-secure-gateway-2025-1-0-BETA1.ova.
3. Copy the contents of the gateway folder to gateway-image on your node.
4. cd into the gateway-image, and execute the following command:

```
packer build -var="ssh_password=ubuntu" -var="env=qa" -force virtualbox-ova-ova.pkr.hcl
```

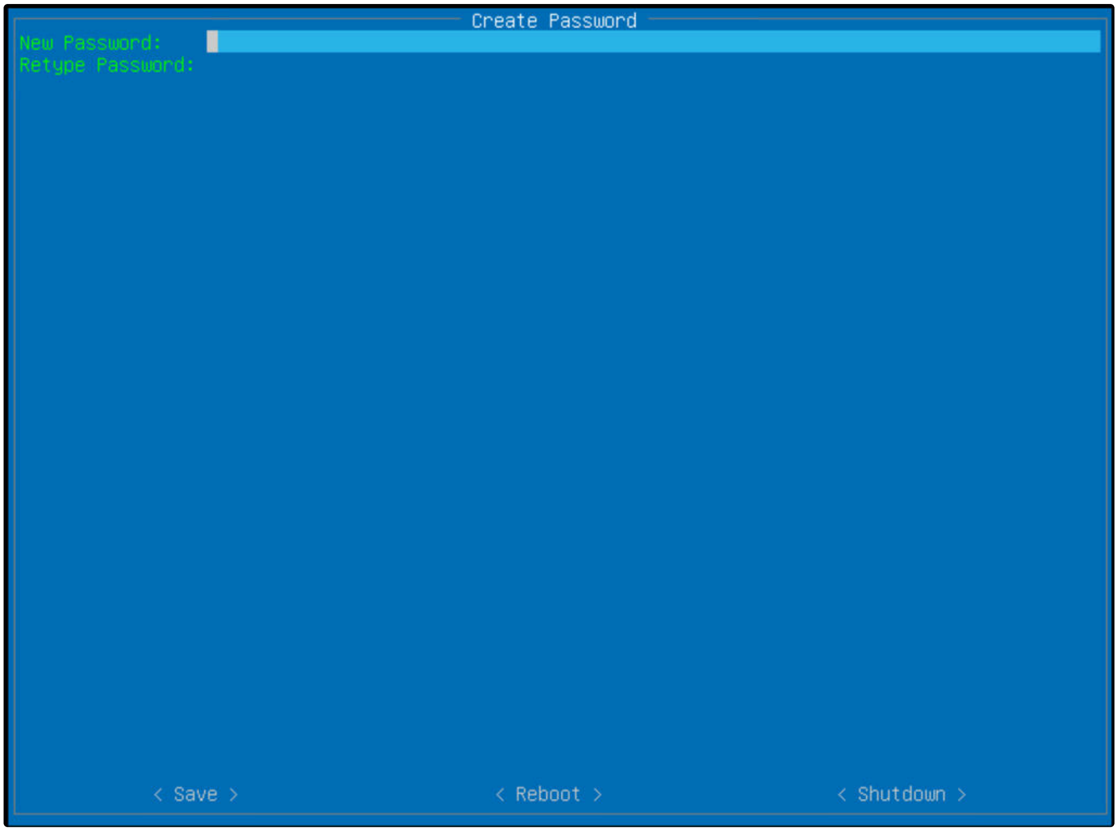
5. Once the image has successfully built, you can find the different format output images in the output-image-ova-22-04 directory.



```
gateway-image
  output-image-ova-22-04
    ubuntu-22-04.mf
    ubuntu-22-04.ova
    ubuntu-22-04.ovf
    ubuntu-22-04.vhdx
    ubuntu-22-04.vmdk
```

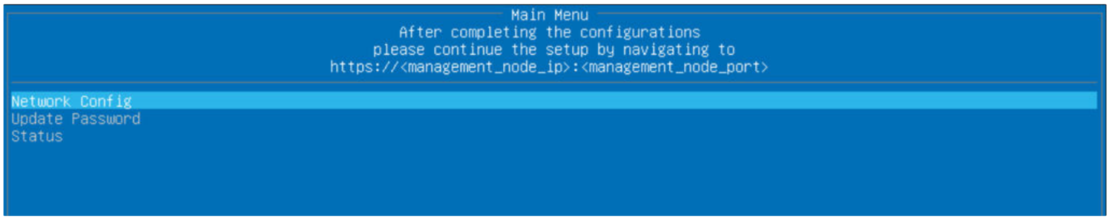
Deployment and testing

1. Create 2 VMs from the image.
2. After turning them on, you will be asked to set up a new password for the *apporto* user. Enter your new password value and select **Save**.



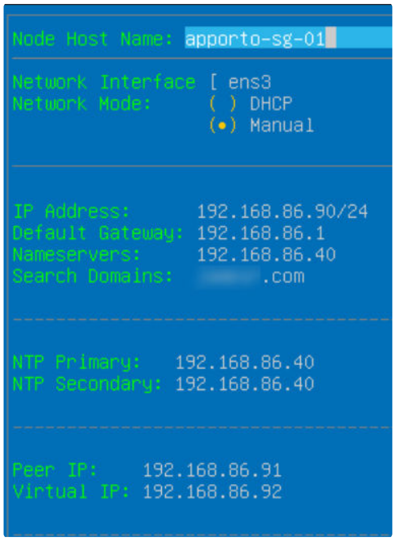
```
                         Create Password
New Password:
Retype Password:

        < Save >            < Reboot >            < Shutdown >
```

3. From the *Main Menu*, select the **Network Config** option.

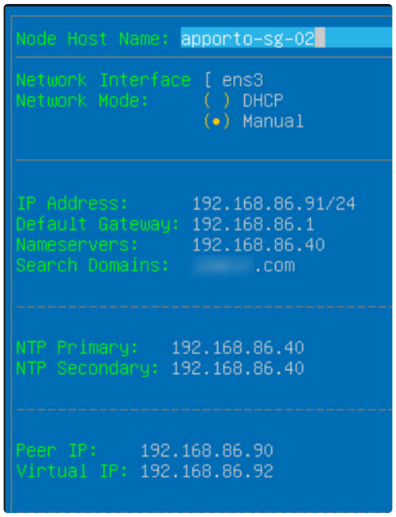


```
                              Main Menu
                     After completing the configurations
                    please continue the setup by navigating to
              https://<management_node_ip>:<management_node_port>

Network Config
Update Password
Status
```

4. Configure the gateway's network settings. Complete this step for each of the 2 nodes.



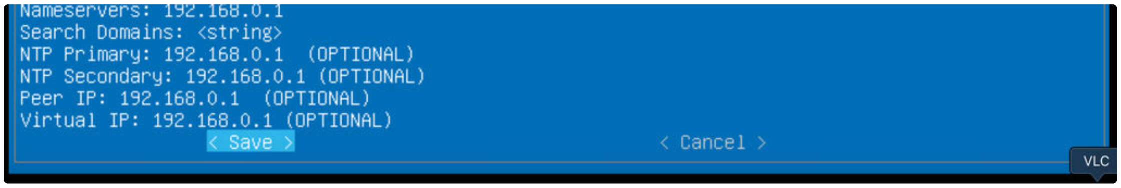
```
Node Host Name: apporto-sg-01

Network Interface [ ens3
Network Mode:      ( ) DHCP
                   (•) Manual

IP Address:      192.168.86.90/24
Default Gateway: 192.168.86.1
Nameservers:     192.168.86.40
Search Domains:  [redacted].com

------------------------------------

NTP Primary:   192.168.86.40
NTP Secondary: 192.168.86.40

------------------------------------

Peer IP:    192.168.86.91
Virtual IP: 192.168.86.92

------------------------------------
```



```
Node Host Name: apporto-sg-02

Network Interface [ ens3
Network Mode:      ( ) DHCP
                   (•) Manual

IP Address:       192.168.86.91/24
Default Gateway:  192.168.86.1
Nameservers:      192.168.86.40
Search Domains:   [redacted].com

NTP Primary:   192.168.86.40
NTP Secondary: 192.168.86.40

Peer IP:    192.168.86.90
Virtual IP: 192.168.86.92
```

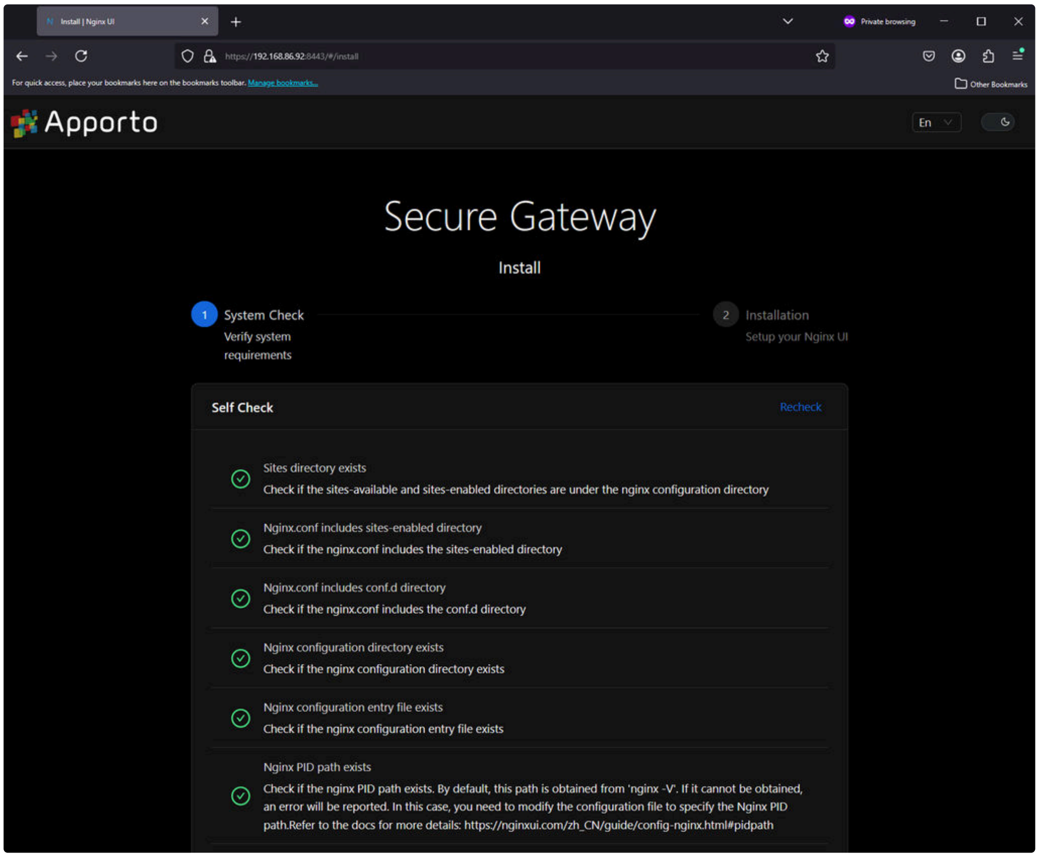
a. The virtual IP value should be set to a floating IP address, which should be configured in your DNS to access the application/UI. Once this is complete, you access the VIP IP address to continue the setup using port 8443 - https://192.168.86.92:8443/#/dashboard/server. b. The peer IP value should be the address of the second node.

5. Once you are done with network configuration, go to the bottom of the screen and select **Save**.



```
Nameservers: 192.168.0.1
Search Domains: <string>
NTP Primary: 192.168.0.1  (OPTIONAL)
NTP Secondary: 192.168.0.1 (OPTIONAL)
Peer IP: 192.168.0.1  (OPTIONAL)
Virtual IP: 192.168.0.1 (OPTIONAL)
              < Save >                         < Cancel >
```

6. You will be returned to the *Main Menu* screen. Select the **Quit** button.
7. The provisioning status will display. When provisioning completes, visit the displayed link to set up the gateway application.
8. The secure gateway application will run a system check to verify that all system requirements for installation are met.



Install | Nginx UI
Private browsing
https://192.168.86.92:8443/#/install
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Other Bookmarks
Apporto
En

Secure Gateway

Install

1 System Check
Verify system requirements

2 Installation
Setup your Nginx UI

Self Check — Recheck

Sites directory exists
Check if the sites-available and sites-enabled directories are under the nginx configuration directory

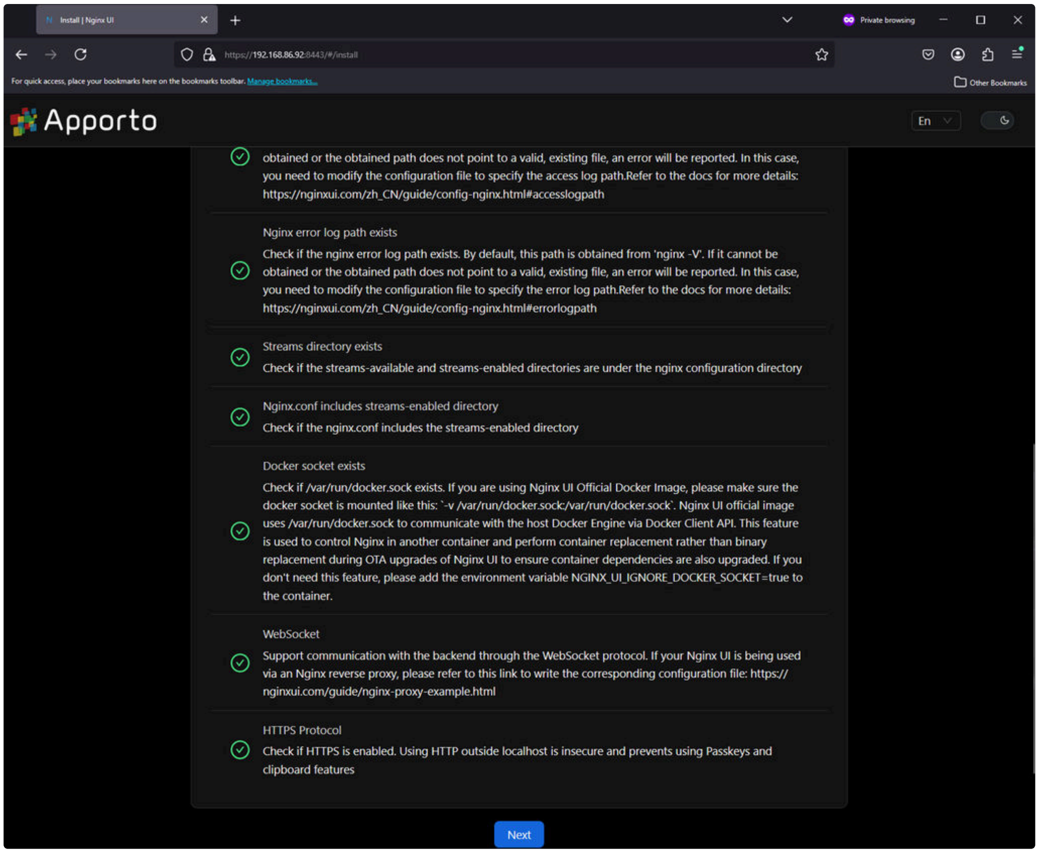
Nginx.conf includes sites-enabled directory
Check if the nginx.conf includes the sites-enabled directory

Nginx.conf includes conf.d directory
Check if the nginx.conf includes the conf.d directory

Nginx configuration directory exists
Check if the nginx configuration directory exists

Nginx configuration entry file exists
Check if the nginx configuration entry file exists

Nginx PID path exists
Check if the nginx PID path exists. By default, this path is obtained from 'nginx -V'. If it cannot be obtained, an error will be reported. In this case, you need to modify the configuration file to specify the Nginx PID path.Refer to the docs for more details: https://nginxui.com/zh_CN/guide/config-nginx.html#pidpath


Install | Nginx UI
Private browsing
https://192.168.86.92:8443/#/install
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Other Bookmarks
Apporto
En

obtained or the obtained path does not point to a valid, existing file, an error will be reported. In this case, you need to modify the configuration file to specify the access log path.Refer to the docs for more details: https://nginxui.com/zh_CN/guide/config-nginx.html#accesslogpath

Nginx error log path exists

Check if the nginx error log path exists. By default, this path is obtained from 'nginx -V'. If it cannot be obtained or the obtained path does not point to a valid, existing file, an error will be reported. In this case, you need to modify the configuration file to specify the error log path.Refer to the docs for more details: https://nginxui.com/zh_CN/guide/config-nginx.html#errorlogpath

Streams directory exists

Check if the streams-available and streams-enabled directories are under the nginx configuration directory

Nginx.conf includes streams-enabled directory

Check if the nginx.conf includes the streams-enabled directory

Docker socket exists

Check if /var/run/docker.sock exists. If you are using Nginx UI Official Docker Image, please make sure the docker socket is mounted like this: `-v /var/run/docker.sock:/var/run/docker.sock`. Nginx UI official image uses /var/run/docker.sock to communicate with the host Docker Engine via Docker Client API. This feature is used to control Nginx in another container and perform container replacement rather than binary replacement during OTA upgrades of Nginx UI to ensure container dependencies are also upgraded. If you don't need this feature, please add the environment variable NGINX_UI_IGNORE_DOCKER_SOCKET=true to the container.

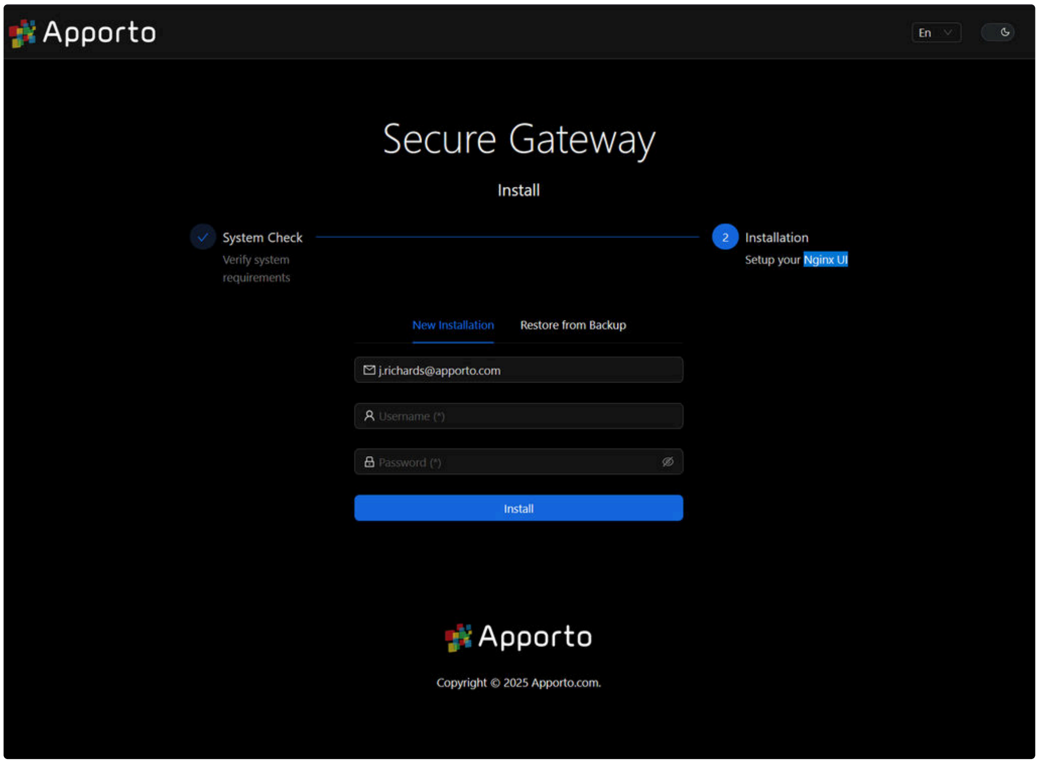
WebSocket

Support communication with the backend through the WebSocket protocol. If your Nginx UI is being used via an Nginx reverse proxy, please refer to this link to write the corresponding configuration file: https://nginxui.com/guide/nginx-proxy-example.html

HTTPS Protocol

Check if HTTPS is enabled. Using HTTP outside localhost is insecure and prevents using Passkeys and clipboard features

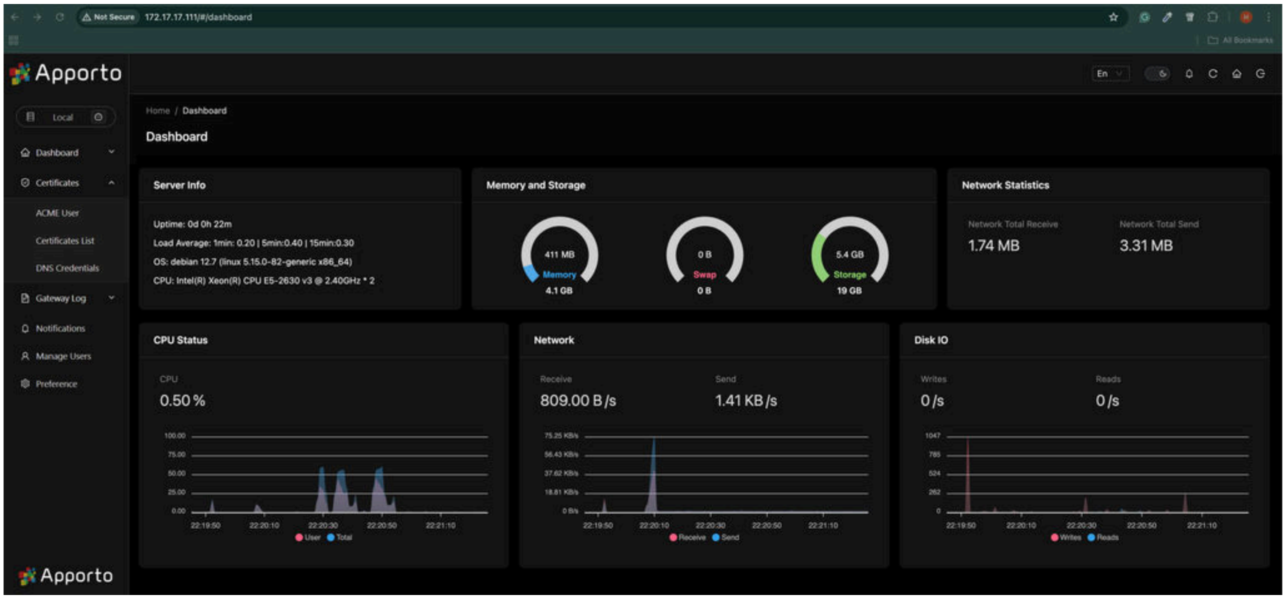
9. If you pass the system check, click **Next** to proceed to installation.
10. For a new installation, fill in the values listed below.



j.richards@apporto.com

    a. Enter your email, username, and password.
    b. Leave the database field blank.
    c. Click **Install**.

11. Once the installation is complete and you are signed in, you will see the gateway dashboard.



Dashboard

Server Info

Uptime: 0d 0h 22m
Load Average: 1min: 0.20 | 5min:0.40 | 15min:0.30
OS: debian 12.7 (linux 5.15.0-82-generic x86_64)
CPU: Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz * 2

Memory and Storage

Memory	Swap	Storage
411 MB	0 B	5.4 GB
4.1 GB	0 B	19 GB

Network Statistics

Network Total Receive	Network Total Send
1.74 MB	3.31 MB

CPU Status

CPU 0.50 %

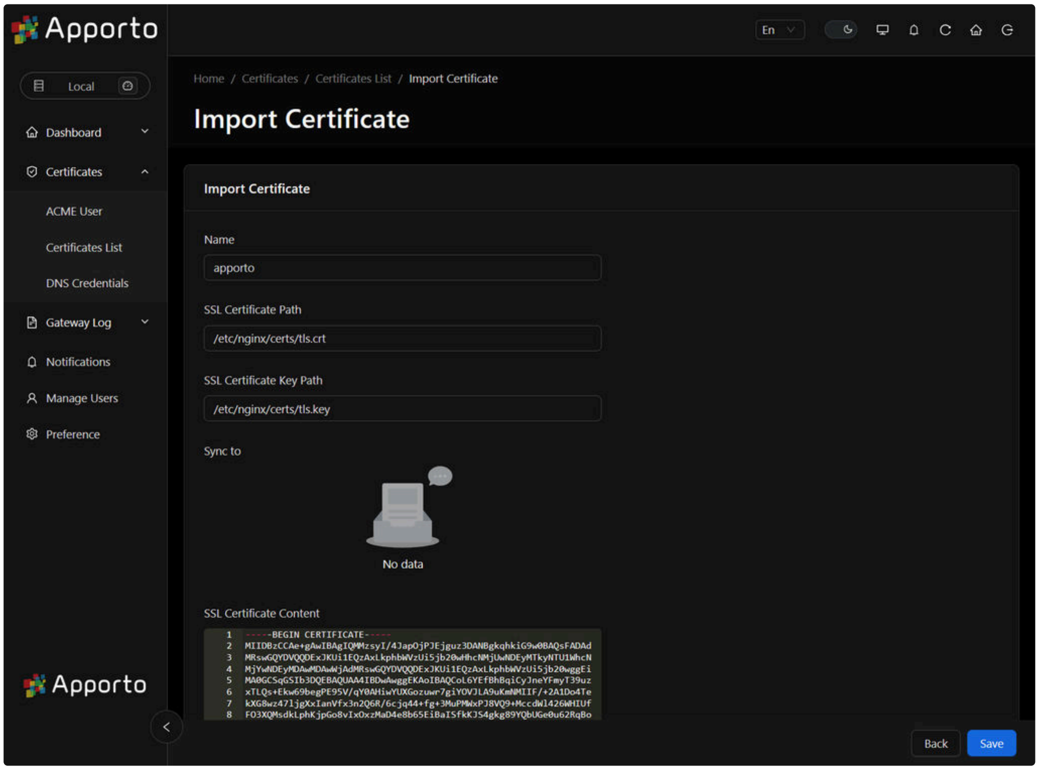
Network

Receive 809.00 B/s Send 1.41 KB/s

Disk IO

Writes 0 /s Reads 0 /s

12. To add a certificate, visit the *Certificates List* screen and select the **Import** feature. After entering all necessary values, click **Save**.



Import Certificate

Import Certificate

Name: apporto

SSL Certificate Path: /etc/nginx/certs/tls.crt

SSL Certificate Key Path: /etc/nginx/certs/tls.key

Sync to

SSL Certificate Content

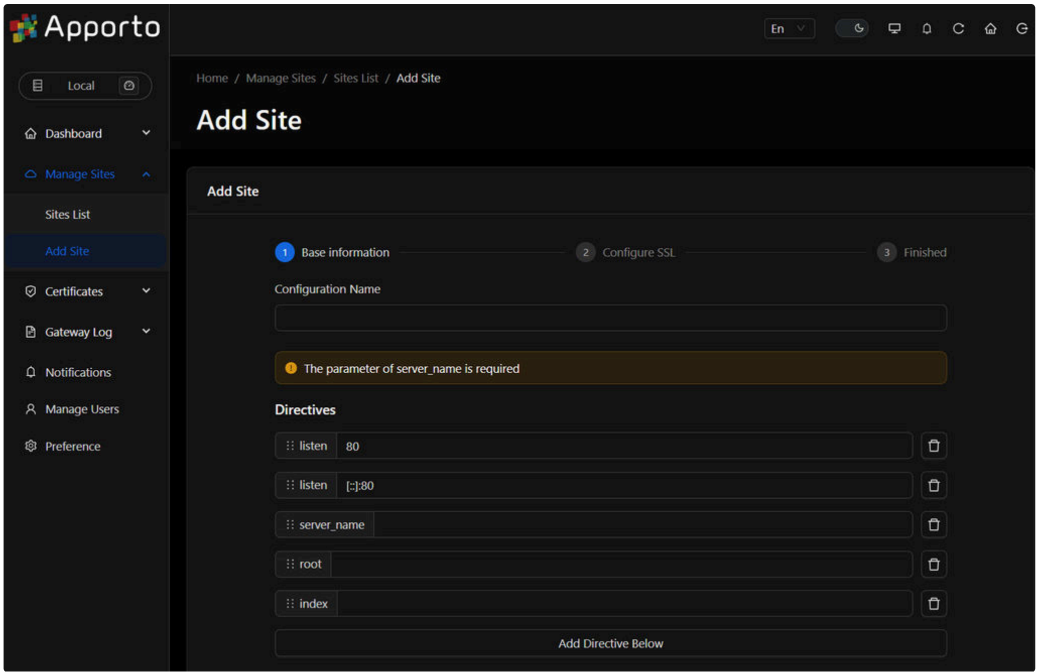
```
-----BEGIN CERTIFICATE-----
MIIDBzCCAe+gAwIBAgIQMMzsyI/4JapOjPJEjguz3DANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJKUi1EQzAxLkphbWVzUi5jb20wHhcNMjUwNDEyMTkyNTU1WhcN
MjYwNDEyMDAwMDAwWjAdMRswGQYDVQQDExJKUi1EQzAxLkphbWVzUi5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCoL6YEfBhBqiCyJneYFmyT39uz
xTLQs+Ekw69begPE95V/qY0AHiwYUXGozuwr7giYOVJLA9uKmNMIIF/+2A1Do4Te
kXG8wz47ljgXxIanVfx3n2Q6R/6cjq44+fg+3MuPMWxPJ8VQ9+MccdWl426WHIUf
FO3XQMsdkLphKjpGo8vIxOxzMaD4e8b65EiBaISfkKJS4gkg89YQbUGe0u62RqBo
```

a. Cert name = “apporto”

b. SSL cert path = /etc/nginx/certs/tls.crt

c. SSL cert key path = /etc/nginx/certs/tls.key

13. To add a site, visit the *Add Site* screen. Enter the values listed below.



Add Site

Add Site

1 Base information — 2 Configure SSL — 3 Finished

Configuration Name

The parameter of server_name is required

Directives

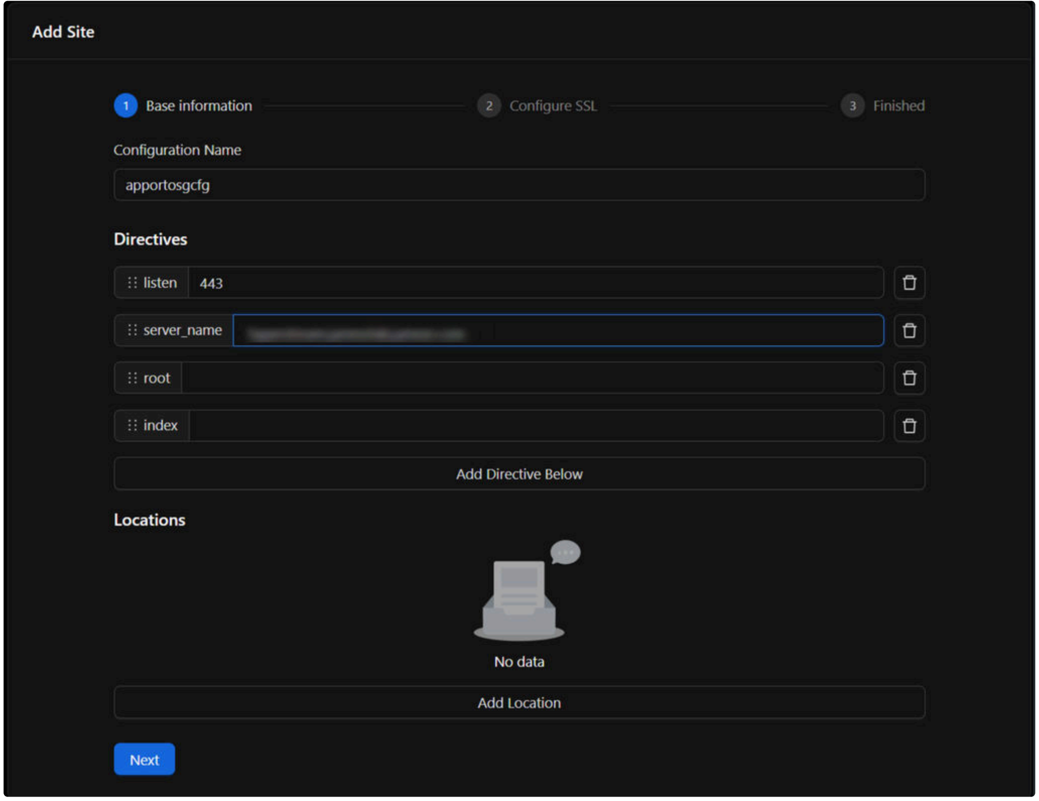
listen 80

listen [::]:80

server_name

root

index


Add Site

1 Base information — 2 Configure SSL — 3 Finished

Configuration Name: apportosgcfg

Directives

listen 443

server_name [redacted]

root

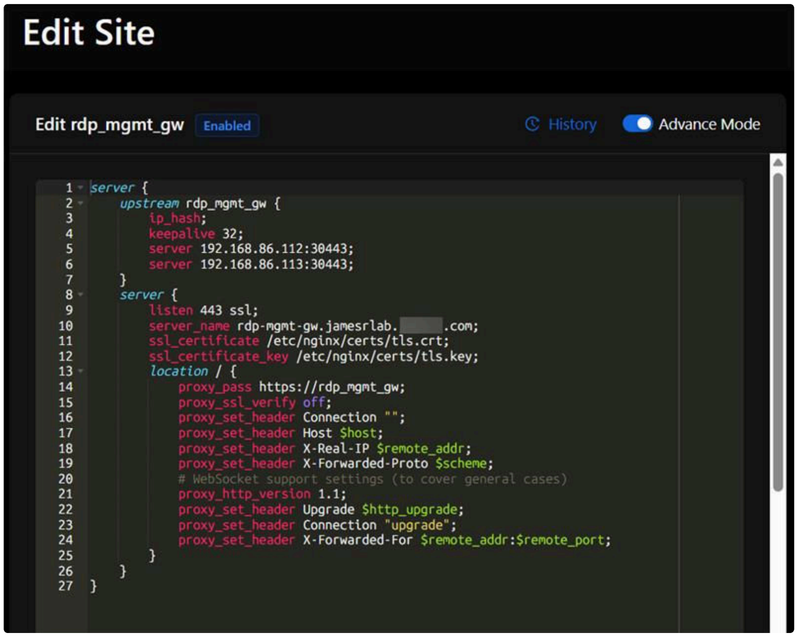
index

Locations

No data

   a. ConfigurationName
   b. Directive = “server_name”
      i. Your hostname must be all lowercase.
   c. Click **Next**.

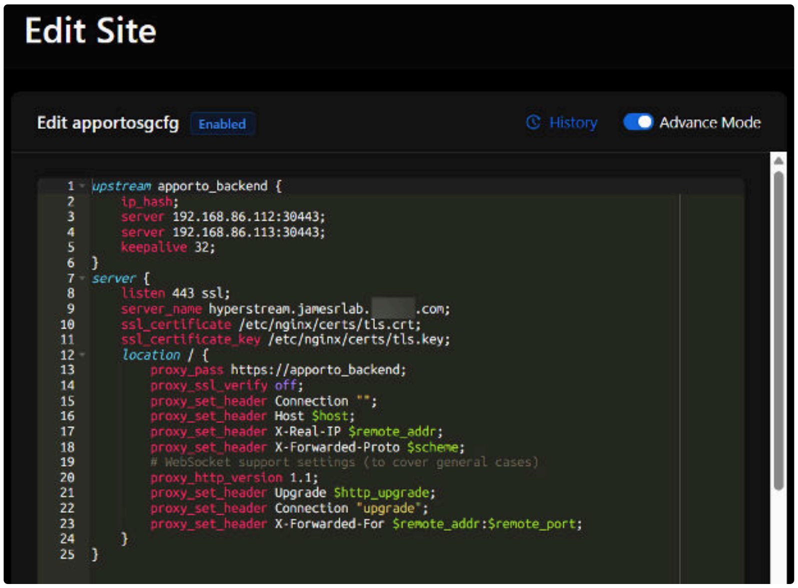
14. Skip the second step in the wizard by clicking **Next** again.
15. Click **Modify Config**. The *Edit Site* screen will now load.
16. Toggle on the “Advance mode” setting to convert from basic mode to advanced mode. This will allow you to add any needed multi-lines.
   a. The sample below is for rdp-mgmt-gateway. This should be configured on an internal load balancer and will be visible to the Apporto service. And the server name (hostname) value must be all lowercase.



```
server {
    upstream rdp_mgmt_gw {
        ip_hash;
        keepalive 32;
        server 192.168.86.112:30443;
        server 192.168.86.113:30443;
    }
    server {
        listen 443 ssl;
        server_name rdp-mgmt-gw.jamesrlab.[redacted].com;
        ssl_certificate /etc/nginx/certs/tls.crt;
        ssl_certificate_key /etc/nginx/certs/tls.key;
        location / {
            proxy_pass https://rdp_mgmt_gw;
            proxy_ssl_verify off;
            proxy_set_header Connection "";
            proxy_set_header Host $host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-Proto $scheme;
            # WebSocket support settings (to cover general cases)
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "upgrade";
            proxy_set_header X-Forwarded-For $remote_addr:$remote_port;
        }
    }
}
```

```
server {
    upstream rdp_mgmt_gw {
        ip_hash;
        keepalive 32;
upstream apporto_backend {
    ip_hash;
    server REPLACE_WITH_IP_OF_WORKER_NODE2:30443;
    server REPLACE_WITH_IP_OF_WORKER_NODE3:30443;
    keepalive 32;
}
server {
    listen 443 ssl;
    server_name REPLACE_WITH_HOSTNAME_OF_HYPERSTREAM;
    ssl_certificate /etc/nginx/certs/tls.crt;
    ssl_certificate_key /etc/nginx/certs/tls.key;
    location / {
        proxy_pass https://apporto_backend;
        proxy_ssl_verify off;
        proxy_set_header Connection "";
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-Proto $scheme;
        # WebSocket support settings (to cover general cases)
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header X-Forwarded-For $remote_addr:$remote_port;
    }
}
    }
    server {
        listen 443 ssl;
        server_name rdp-mgmt-gw.jamesrlab.??????.com;
        ssl_certificate /etc/nginx/certs/tls.crt;
        ssl_certificate_key /etc/nginx/certs/tls.key;
        location / {
            proxy_pass https://rdp_mgmt_gw;
            proxy_ssl_verify off;
            proxy_set_header Connection "";
            proxy_set_header Host $host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-Proto $scheme;
            # WebSocket support settings (to cover general cases)
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "upgrade";
            proxy_set_header X-Forwarded-For $remote_addr:$remote_port;
        }
    }
}
```

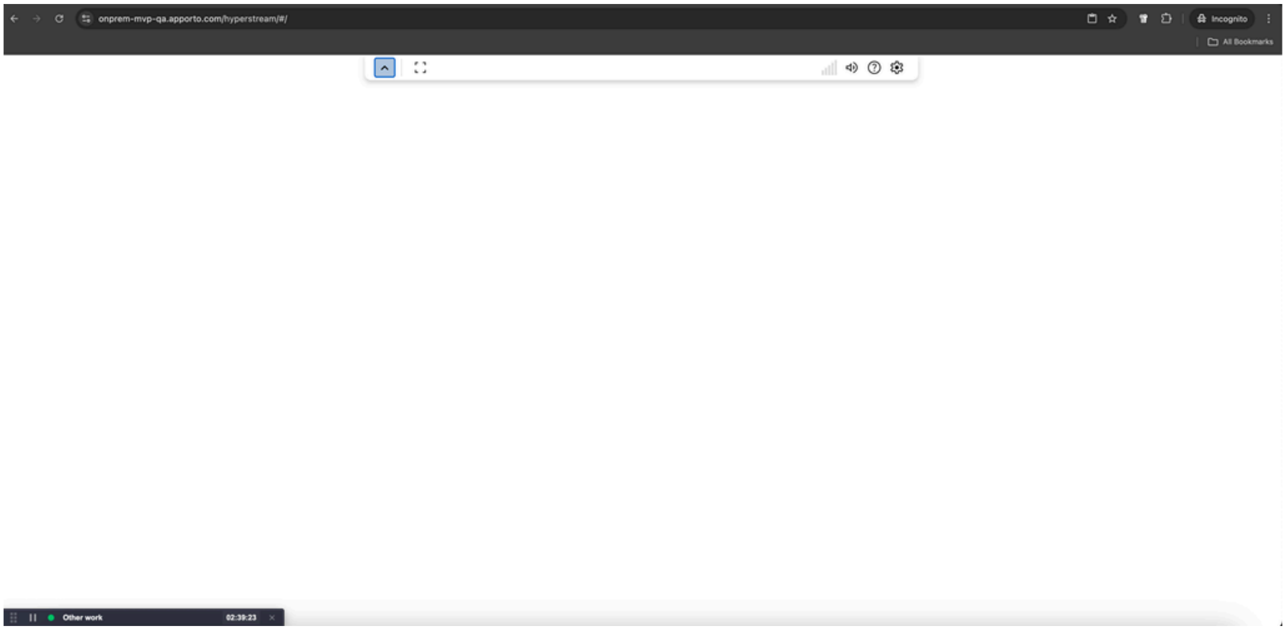
b. The sample below is for the hyperstream hostname. The value must be all lowercase.



```
upstream apporto_backend {
    ip_hash;
    server 192.168.86.112:30443;
    server 192.168.86.113:30443;
    keepalive 32;
}
server {
    listen 443 ssl;
    server_name hyperstream.jamesrlab.[redacted].com;
    ssl_certificate /etc/nginx/certs/tls.crt;
    ssl_certificate_key /etc/nginx/certs/tls.key;
    location / {
        proxy_pass https://apporto_backend;
        proxy_ssl_verify off;
        proxy_set_header Connection "";
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-Proto $scheme;
        # WebSocket support settings (to cover general cases)
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header X-Forwarded-For $remote_addr:$remote_port;
    }
}
```

```
upstream apporto_backend {
    ip_hash;
    server REPLACE_WITH_IP_OF_WORKER_NODE2:30443;
    server REPLACE_WITH_IP_OF_WORKER_NODE3:30443;
    keepalive 32;
}
server {
    listen 443 ssl;
    server_name REPLACE_WITH_HOSTNAME_OF_HYPERSTREAM;
    ssl_certificate /etc/nginx/certs/tls.crt;
    ssl_certificate_key /etc/nginx/certs/tls.key;
    location / {
        proxy_pass https://apporto_backend;
        proxy_ssl_verify off;
        proxy_set_header Connection "";
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-Proto $scheme;
        # WebSocket support settings (to cover general cases)
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header X-Forwarded-For $remote_addr:$remote_port;
    }
}
```

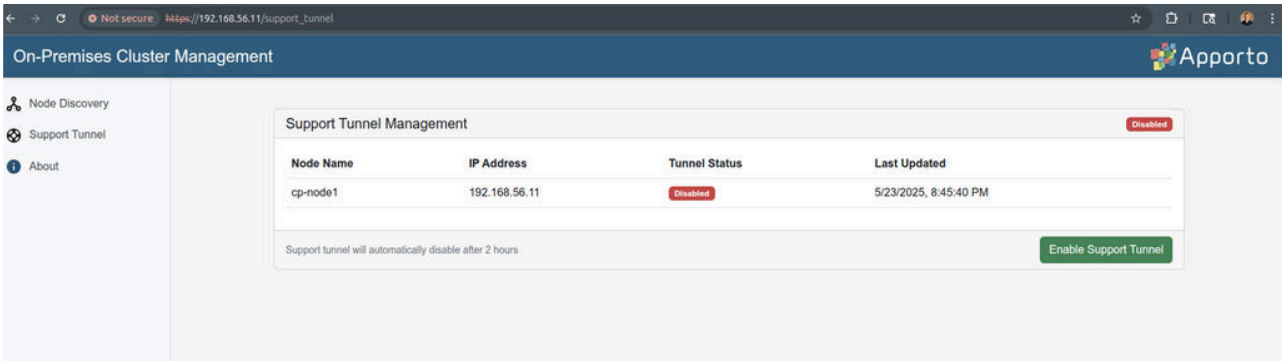
17. Click **Save** to commit the site edits.
18. For hyperstream, verify the changes by browsing to https://server_name/hyperstream/#.



Setting up the support tunnel

In case of any issues with your environment, Apporto Support can troubleshoot by accessing your cluster through a support tunnel. To enable the support tunnel, follow the steps below.

1. Return to https://[your_manager_node] in a browser window. Click on **Support Tunnel** to view the *Support Tunnel Management* screen.


Not secure ~~https~~://192.168.56.11/support_tunnel
On-Premises Cluster Management
Apporto
Node Discovery
Support Tunnel
About
Disabled
Enable Support Tunnel

Support Tunnel Management

Node Name	IP Address	Tunnel Status	Last Updated
cp-node1	192.168.56.11	Disabled	5/23/2025, 8:45:40 PM

Support tunnel will automatically disable after 2 hours

2. The current status of the support tunnel on the manager node will display.
3. If the tunnel is disabled, click **Enable Support Tunnel**.
4. The tunnel will auto-disable after 2 hours. It can be re-enabled if needed by repeating the steps above.

Administration

Outside of the cluster deployment process, the Apporto NextGen control plane houses the configuration of users, servers, desktops/applications, and all other major parts of the platform. Details related to on-premises deployment are described below. For additional details, visit the Apporto Help Center.

> Configuration updates (hyperstream or RDP management gateway hostnames, encryption or API keys, SSO to the desktop settings, etc.) can take up a few minutes to sync down to the on-prem cluster.

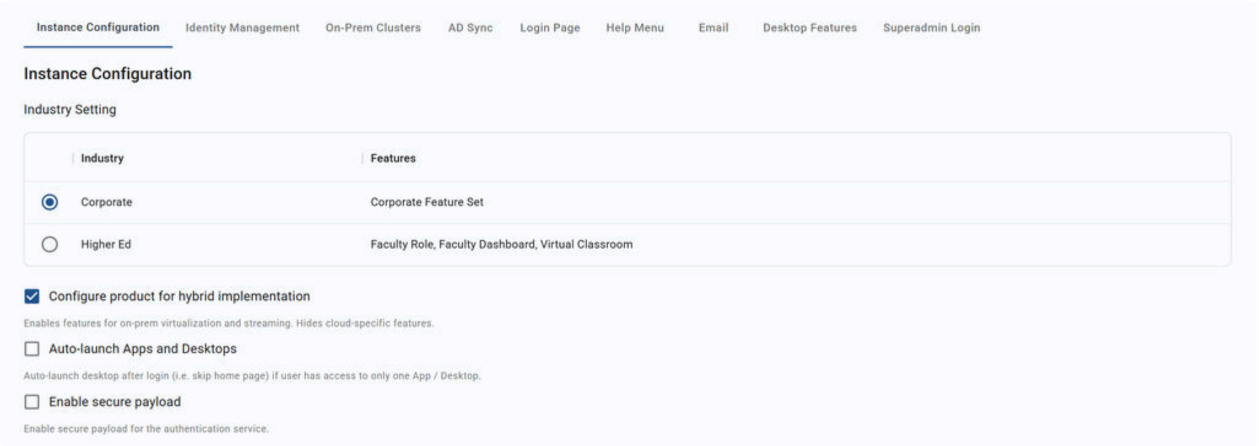
Setup

The *Setup* section provides configuration options for look and feel, identity management and authentication, desktop features, and more.

Instance configuration

For on-premises installations, the “Configure product for hybrid implementation” setting must be checked.

> ⚠ There will also be a subscription value that is hidden once the hybrid checkbox is checked. Fill this field with “Apps” prior to checking the hybrid implementation checkbox to ensure that your user account is recognized during installation.



Instance Configuration

Industry Setting

	Industry	Features
●	Corporate	Corporate Feature Set
○	Higher Ed	Faculty Role, Faculty Dashboard, Virtual Classroom

☑ Configure product for hybrid implementation

Enables features for on-prem virtualization and streaming. Hides cloud-specific features.

☐ Auto-launch Apps and Desktops

Auto-launch desktop after login (i.e. skip home page) if user has access to only one App / Desktop.

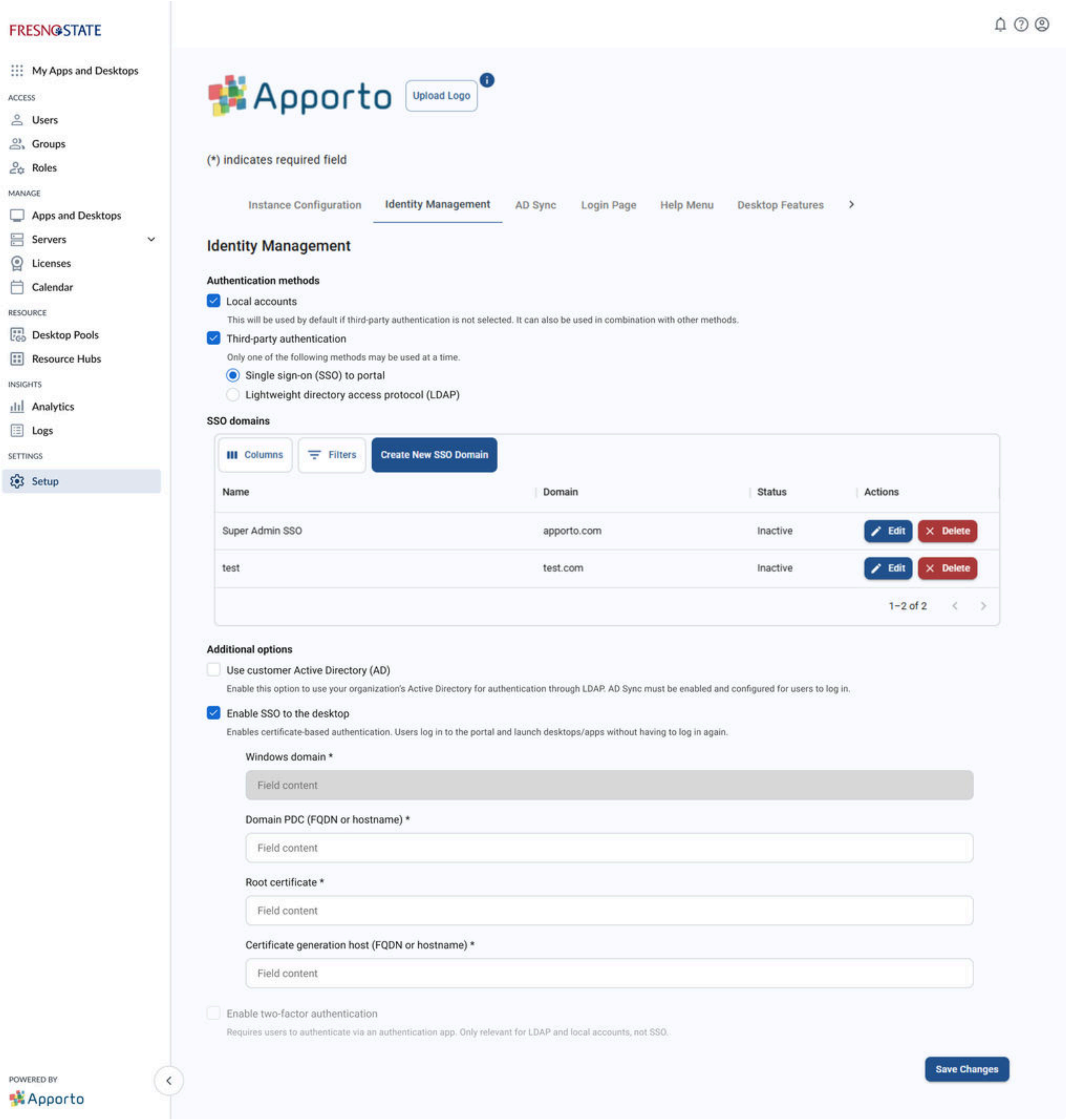
☐ Enable secure payload

Enable secure payload for the authentication service.

> ⚠ Do not uncheck this checkbox. Doing so would hide the “On-Prem Clusters” tab and the cluster installer.

Identity management

The “Identity Management” tab provides your instance’s authentication method settings.



(*) indicates required field

Identity Management

Authentication methods

☑ Local accounts

This will be used by default if third-party authentication is not selected. It can also be used in combination with other methods.

☑ Third-party authentication

Only one of the following methods may be used at a time.

● Single sign-on (SSO) to portal

○ Lightweight directory access protocol (LDAP)

SSO domains

Name	Domain	Status	Actions
Super Admin SSO	apporto.com	Inactive	Edit Delete
test	test.com	Inactive	Edit Delete

1–2 of 2

Additional options

☐ Use customer Active Directory (AD)

Enable this option to use your organization's Active Directory for authentication through LDAP. AD Sync must be enabled and configured for users to log in.

☑ Enable SSO to the desktop

Enables certificate-based authentication. Users log in to the portal and launch desktops/apps without having to log in again.

Windows domain *

Field content

Domain PDC (FQDN or hostname) *

Field content

Root certificate *

Field content

Certificate generation host (FQDN or hostname) *

Field content

☐ Enable two-factor authentication

Requires users to authenticate via an authentication app. Only relevant for LDAP and local accounts, not SSO.

Users can be authenticated through the following methods:

- Local accounts (email address & password)
- Single sign-on (SSO) to the control plane
- Lightweight directory access protocol (LDAP)

> If you desire to use LDAPS in this beta version, we recommend first attempting LDAP and then updating your configuration to LDAPS after obtaining the root certificate.

There are additional options for:

- Using your organization’s Active Directory (AD)
  - If customer AD is selected for either SSO to the control plane or LDAP, the “AD Sync” tab will be visible.
- Single sign-on (SSO) being passed from the control plane to the desktop

- If SSO to the desktop is enabled, certificate values are required. See the Apporto Help Center article on generating SSO certificates for more information.

Field	Datatype	Required?	Notes
Windows domain	String	System-generated	This value will be inserted by the system.
Domain PDC (FQDN or hostname)	String	Yes	Primary domain controller
Root certificate	String	Yes	Enter the full string of the certificate. In a future version, file upload may be made available.
Certificate generation host (FQDN or hostname)	String	Yes	

- Two-factor authentication (2FA)

If you desire to use SSO to the desktop in this beta version, we recommend the following order of operations:

1. Use local accounts for initial setup.
2. Configure LDAP and AD sync settings. Verify that AD users are able to authenticate into Apporto.
3. Update your LDAP settings to LDAPS by adding your root certificate and updating your LDAP server port(s).
4. Enable SSO to the desktop and fill in its related values.

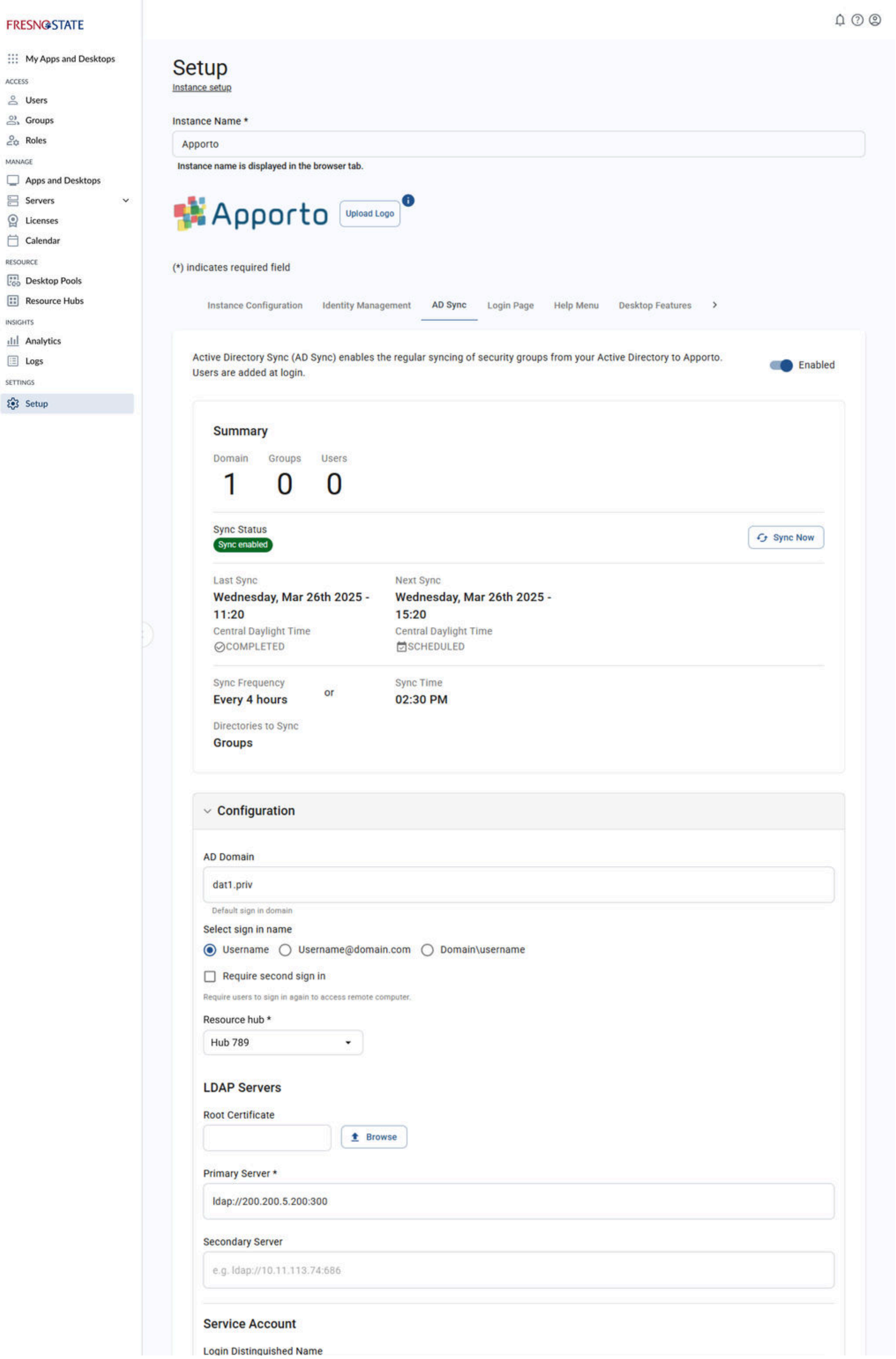
For information on how to configure authentication methods, visit the Apporto Help Center.

On-prem clusters

Information about this tab is available above in the Deployment section.

AD sync

This tab provides configuration options for Active Directory (AD) and LDAP sync.



Setup

Instance setup

Instance Name *

Apporto

Instance name is displayed in the browser tab.

(*) indicates required field

Active Directory Sync (AD Sync) enables the regular syncing of security groups from your Active Directory to Apporto. Users are added at login.

Enabled

Summary

Domain	Groups	Users
1	0	0

Sync Status
Sync enabled

Last Sync	Next Sync
Wednesday, Mar 26th 2025 - 11:20	Wednesday, Mar 26th 2025 - 15:20
Central Daylight Time	Central Daylight Time
COMPLETED	SCHEDULED

Sync Frequency
Every 4 hours

or

Sync Time
02:30 PM

Directories to Sync
Groups

Configuration

AD Domain

dat1.priv

Default sign in domain

Select sign in name

● Username ○ Username@domain.com ○ Domain\username

□ Require second sign in

Require users to sign in again to access remote computer.

Resource hub *

Hub 789

LDAP Servers

Root Certificate

Primary Server *

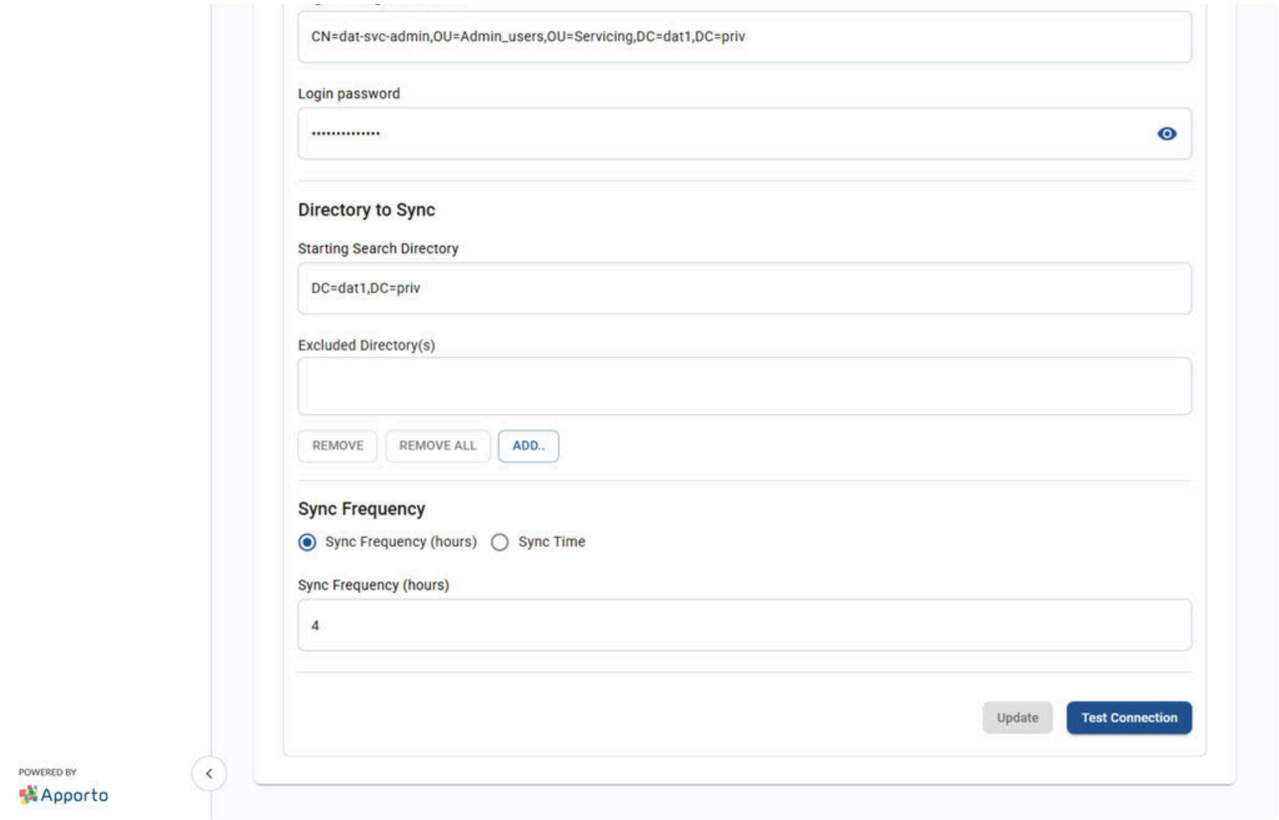
ldap://200.200.5.200:300

Secondary Server

e.g. ldap://10.11.113.74:686

Service Account

Login Distinguished Name



CN=dat-svc-admin,OU=Admin_users,OU=Servicing,DC=dat1,DC=priv

Login password

••••••••••••••

Directory to Sync

Starting Search Directory

DC=dat1,DC=priv

Excluded Directory(s)

Sync Frequency

● Sync Frequency (hours) ○ Sync Time

Sync Frequency (hours)

4

For on-premises deployments, the resource hub that houses the sync server must be selected. More information is available in the AD sync section of the Help Center.

In the beta version of the installer, Apporto Support will need to manually connect LDAP to a resource hub. The field shown above will be added in an upcoming release. Please inform Support which resource hub houses your LDAP sync server.

Currently, the automated AD/LDAP sync schedules (by hours or by time) are not working for on-prem customers. After saving your settings, click on the **Sync Now** button at the top of the screen whenever you need to update the sync.

Desktop features

The “Desktop Features” tab allows you to manage the features a user will see when in an active virtual desktop session. This list will change as new features are added. And there may be some differences in availability between cloud-based and on-premises instances.

For more details, visit the article on desktop features in the Help Center.

User accounts

Managing users

You will have an initial admin account created for you by Apporto staff. You may create additional user accounts based on your identity management selections. For information on how to manage users, visit the Apporto Help Center.

Forgot password

If you are unable to sign in to the initial admin account, use the “forgot password” function to reset your credentials.

1. From the Apporto instance *Sign In* page, click on **Forgot Password**.
2. Enter the email address associated with the user account and click **Send Password Reset Email**.
3. Password reset instructions will be sent to the email address provided. Click on the reset link in the email.

4. You will be directed to the *Reset Password* page. Enter and submit your desired password.
5. Once you receive a confirmation message, you can sign in with your new password.

Resources

Resource hubs

You will have at least 1 resource hub configured by the time you've completed cluster installation. However, the settings that are defined during installation are only the minimum hub values needed for the installation process. You will need to return to the *Resource hubs* section to fill in the remaining values. See the Apporto Help Center articles on creating and managing resource hubs for more information.

⚠ For this beta version, if you need to delete a resource hub and recreate it, you will need to use a different hub name to prevent errors.

Desktop pools

Additional configuration can be made for handling multiple server pools as if they were a single virtual desktop. The Apporto Help Center articles on creating and managing desktop pools will help you configure these entities.

Servers and virtual machines

To provide app/desktop sessions to users, configure the multi-session and single-session servers that reside within your resource hub. There are a few Apporto Help Center articles that provide details on how to set up your servers. Visit the overview page on managing servers and VMs to get further instructions.

Applications and virtual desktops

Apporto customers can serve both applications and desktops to end users. The Apporto Help Center article on creating apps and desktops will explain how to get these items set up for your users.

Known issues

The following list addresses items that are present in the Beta version but are planned for resolution in upcoming releases:

- Cluster installer
  - The Apporto VM download link in the Step 1 screen will be updated soon. For now, please open https://apporto-public-assets.s3.amazonaws.com/vm-images/apporto-cluster-node/releases/2025-1-0-BETA1/apporto-cluster-node-2025-1-0-BETA1.ova in a browser window.
- Resource hubs
  - Apporto Support will need to manually connect LDAP to a resource hub. Inform Apporto Support which resource hub houses your LDAP sync server.
  - For your cluster's resource hub, the hyperstream and RDP management gateway hostnames must be all lowercase.
  - If you need to delete a resource hub and recreate it, you will need to use a different hub name to prevent errors.
  - Configuration updates (hyperstream or RDP management gateway hostnames, encryption or API keys, etc.) can take up a few minutes to sync down to the on-prem cluster.
- Instance configuration
  - There is a subscription value in the "Instance Configuration" tab of *Setup* that is hidden once the hybrid checkbox is checked. Fill this field with "Apps" prior to checking the hybrid implementation checkbox to ensure that your user account is recognized during installation.
- Identity management & AD/LDAP sync

- SSO to the desktop is currently creating two certs for each request. This should not impede deployment, but you may see it in certificate logs.
- SSO to the desktop is generating temporary files in the hyperstream tmp directory. These will be cleaned up in a future release.
- Configuration updates (SSO to the desktop settings, etc.) can take up a few minutes to sync down to the on-prem cluster.
- The automated AD/LDAP sync schedules (by hours or by time) are not working for on-prem customers. After saving your settings, click on the **Sync Now** button at the top of the *AD Sync* screen whenever you need to update the sync.