NexaVM nDR User Guide

Product Version: 10.0.668.0

Document Version: V20250328

Copyright Statement

Trademark

NexaVM Technologies AG. reserves all rights to its trademarks, including, but not limited to NexaVM and other trademarks in connection with NexaVM Technologies AG. Other trademarks or registered trademarks presented in this document are owned or controlled solely by its proprietaries.

Notice

The products, services, or features that you purchased are all subject to the commercial contract and terms of NexaVM Technologies AG., but any part or all of the foregoing displayed in this document may not be in the scope of your purchase or use. Unless there are additional conventions, NexaVM Technologies AG. will disclaim any statement or warranty, whether implicit or explicit, on the contents of this document. In an event of product version upgrades or other reasons, the contents of this document will be irregularly updated and released. Unless there are additional conventions, this document, considered solely as a reference guide, will not make any warranty, whether implicit or explicit, on all the statements, information, or suggestions.

Table of Contents

1 Introduction

NDR is a hybrid cloud disaster recovery solution developed specifically for the NexaVM cloud platform. It supports a wide range of scenarios, including P2V, V2V, and Cloud-to-Cloud, all of which can be efficiently handled through the NDR platform. With its strong compatibility and architectural flexibility, NDR enables stable and high-performance disaster recovery to NexaVM, regardless of the source environment—be it physical infrastructure, application-specific setups, or various public and private clouds.

This document provides operational guidance for implementing a pure software-based disaster recovery solution using NDR on the NexaVM platform. It outlines each step in the process to help users effectively execute disaster recovery tasks.

A pure software solution refers to scenarios where NexaVM provides compute, storage, and network resources, and all data operations are managed at the software level through the cloud platform. NDR handles data acquisition, transmission, and historical snapshot management to ensure reliable protection.

Best Practices for Software-Only Disaster Recovery Configurations:

No.	DR Software Solution	DR Cloud Platform	Notes
1	NDR Software-Only	NexaVM Cloud + NSAN	Using NSAN enables snapshot rotation, allowing for more historical snapshots and high recall efficiency.
2	NDR Software-Only	NexaVM Cloud or NSSV + Backup Storage [1] Requires additional backup storage. [2] Backup license required.	Due to the external snapshot chain mechanism of qcow2, backup is needed to enable historical snapshot rotation.
3	NDR Software-Only	NSSV + Snapshots [1] NSSV version must be later than 4.10.7	Snapshot rotation is supported on NSSV starting from v 4.10.7.

1.1 Configuration Wizard

The configuration process is as follows:

1. **Prepare the management server:** The NDR management console is deployed on a Linux system by creating a virtual machine using the provided qcow2 image.
2. **Determine the disaster recovery architecture** (refer to Chapter 2).
3. **Configure the Source Server** (intermediate/proxy server) as needed, based on the selected architecture.
4. **Connect the Console with NexaVM Cloud**.
5. **Upload the BootImage** to the target NexaVM platform. The NDR platform provides BootImages for both Windows and Linux systems. Choose the appropriate image based on the source environment.
6. **Add the source machine:** agent-based or agentless method.
7. Configure protection process.
8. Configure the provisioning process.
9. Test the provisioning process.

1.2 Cloud Disk Storage and Snapshots

NexaVM supports historical point-in-time recovery through the cloud disk snapshot feature. Target disks can be created on both Ceph and non-Ceph storage types. Regardless of the storage type, NexaVM's backup functionality can be enabled to retain historical copies of target disks. All storage modes are fully compatible with provisioning features.

For Ceph storage, NexaVM supports snapshot rotation—when the number of snapshots reaches the configured retention limit, the system will automatically delete the oldest snapshot to maintain a rolling snapshot chain. In contrast, non-Ceph storage cannot support snapshot rotation due to the snapshot tree mechanism.

Primary Storage: Stores virtual machine disk files, including root and data disks, snapshots, and image cache. Supports two major categories of primary storage:

- **Local Storage:** Utilizes the physical disks of the host machine.
- **Shared Network Storage:** Includes NFS, Shared Mount Point, Ceph, Shared Block, Aliyun NAS, and Aliyun EBS.

- **NFS**: A standard network file system protocol.
- **Shared Mount Point**: Supports distributed file systems such as MooseFS, GlusterFS, OCFS2, and GFS2.
- **Ceph**: Distributed block storage.
- **Shared Block**: Shared block-level storage.

1.3 Installation Package and Components

The table below lists the components included in the installation package.

No.	Name	Purpose
1	Gateway_Windows_Server_(Treker)_xxx.exe Gateway_Linux_Server_(Treker)_xxx_fast_NDR.qcow2	Manages the console and data transmission. - Windows uses an installation package with a Management option. - Linux provides a Qcow2 image.
2	Agent_for_Windows_(Antenna)_xxx.exe	Windows source client agent.
3	Agent_for_Linux_(antenna)-10.0.xxx.xxx.tar.gz	Linux source client agent.
4	BootImage_for_Windows_(TrekerLite)_xxx.qcow2 BootImage_for_Windows_(TrekerLite)_xxx.iso	Windows base image file for pre-creating target instance. - Receives source machine data to write to the target system and data disks. - Performs system conversion tasks.
5	BootImage_for_Linux_(TrekerLite)_xxx.qcow2 BootImage_for_Linux_(TrekerLite)_xxx.iso	Linux base image file for pre-creating target instance. - Receives source machine data to write to the target system and data disks. - Performs system conversion tasks.
6	OfflineKit_xxx.vhd OfflineKit_xxx.iso	Windows base image file for offline synchronization from the source machine. Primarily used for legacy systems and physical machines. Applicable Scenarios: - Source client does not support agentless mode. - Source client cannot install an agent for

		any reason. - Source client has sufficient downtime to complete offline synchronization. - Source client can boot from an ISO.
7	FileAccess_kit_10_0_xxx.qcow2	File Access image, for creating a temporary recovery instance, enabling granular file-level recovery functionality.

1.3 Communication Ports

TCP Port	Purpose
80	Management Service
443	Management Service
20443	Management Service
20000	Server Port; Source Machine Access
20001	Server Port; Source Machine Access
20005	Source Machine Port
20010	Unidirectional Transmission Port from Source Machine to Target
50022	Linux BootImage & Linux Treker

1.4 Console Terminology

Term	Module	Description
Resources	Core Component Connections	Includes cloud, server, and source components. This module configures connections for migration components.
Cloud	Cloud	Supports API integration with NexaVM, OpenStack, and VMware for automated operations.
Server	Server	Handles data transmission, can act as both an intermediary and a target server.
Source	Source	Manages source machines, including agentless and offline hosts.
Protection	Protection	Manages data synchronization from source to cloud, including scheduled sync policies and transmission parameters.
Provision	Provision	Manages provisioning processes, ensuring target instances are booted to accordingly.
Diagnostic	Settings	Collects logs from servers and source machines for troubleshooting. Logs can be downloaded as packaged files.
Management	Settings	Manages communication and data transfer addresses between the

Address		console and components. When using multiple subnets, select all corresponding IP addresses.
Web Port	Settings	Configures management console and data synchronization ports. Port 20443 is recommended for internet transmission.
Security Code	Settings	Used for reverse connection authentication between source machines, servers, and target images.
UI Display Mode	Settings	Adjusts displayed information based on the selected view.
File Management	Settings	Preloads command files and related software as compressed packages into the console for protection tasks and migration cutovers.

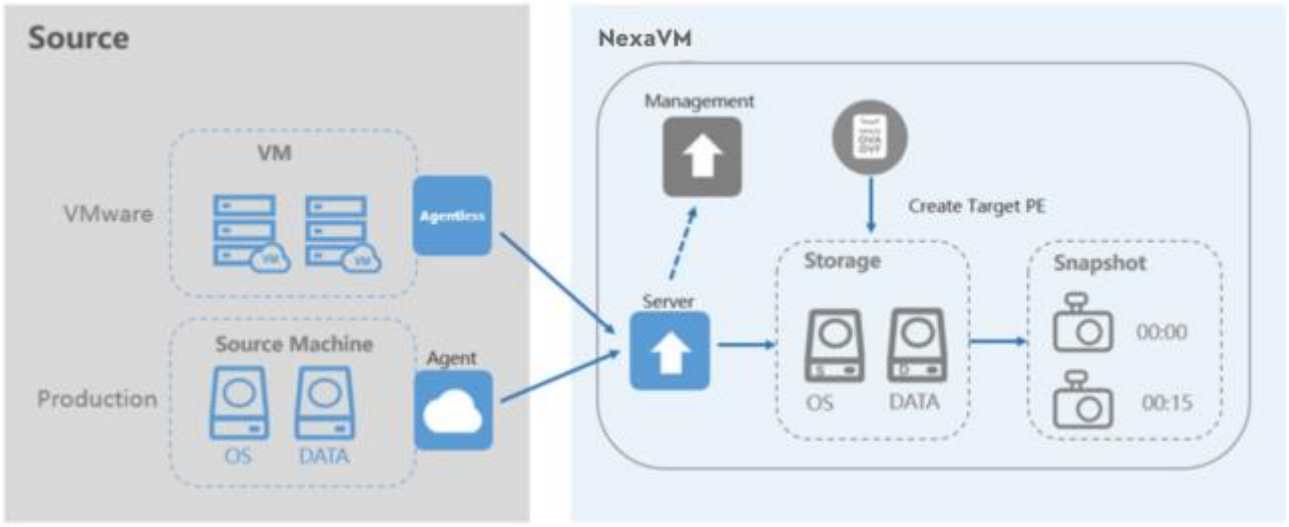
2 Architecture

This chapter outlines the architectural models and usage scenarios for disaster recovery, helping users identify the appropriate model based on their environment. It also provides best practices for each scenario.

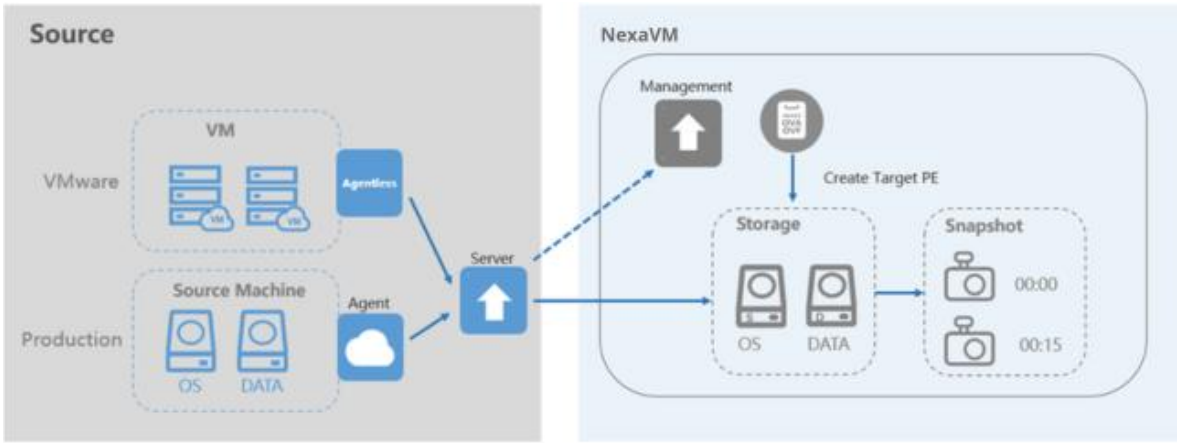
2.1 Architecture 1: Image Mode with Proxy Server

Topology Overview:

1. **Topology 1** - where the Server is deployed on the target side**.**



2. **Topology 2** - where the Server is Deployed on the source side.



While the Server service can theoretically be hosted on the same machine as the management console, deploying a dedicated Server is recommended to avoid affecting console access during data synchronization.

In this architecture, users must first upload the BootImage to the NexaVM platform and establish integration using an Access Key. Source machines are added to the console via agent or VMware API (agentless) methods. During synchronization, NDR automatically invokes NexaVM APIs to provision the target instance using the uploaded BootImage, attaching data disks accordingly.

Each source-to-target pair follows a one-to-one synchronization model. When configuring the synchronization task, users can select either Ceph or non-Ceph as the target disk storage type. Snapshot or backup functionality can also be enabled to retain historical copies with rolling retention.

Scenario Selection Guide:

Source Scenario	Server Deployment	Cloud Platform	Target Cloud Network	Notes
VMware Agentless	Deploy Target Server on the target cloud (Target cloud network must have direct access to the VMware VADP interface)	NexaVM	DHCP-enabled subnet (If the final target subnet lacks DHCP, migration can be completed using a DHCP subnet and switched later)	Refer to Topology 1
VMware Agentless	Deploy Source Server at the source (For network relay: When the source and target platforms cannot communicate directly, the Server at the source acts as an intermediary)	NexaVM		Refer to Topology 2
Agent Installed	Deploy Target Server on the target cloud (Target cloud network must have direct access to the source machine)	NexaVM	DHCP-enabled subnet (If the final target subnet lacks DHCP, synchronization can be completed using a DHCP	Refer to Topology 1
Agent Installed	Deploy Source Server at the source (For network relay:	NexaVM		Refer to Topology 2

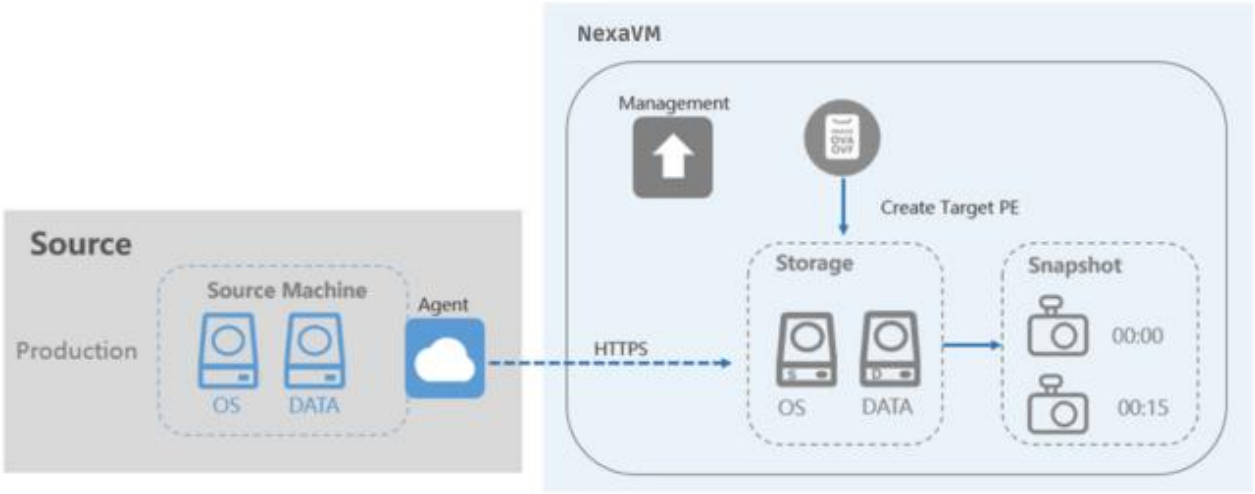
	When the source and target platforms cannot communicate directly, the Server at the source acts as an intermediary)		subnet and switched later	

Application Scenarios and Characteristics:

- Suitable for environments with private network connectivity and no one-way access restrictions. (For one-way access scenarios, refer to documentation on reverse connection methods.)
- The source environment uses VMware virtualization and supports agentless access via the VMware VADP interface.
- No agent installation is required to perform disaster recovery for VMware virtual machines to NexaVM.
- VMware agentless mode depends on VADP capabilities and supports limited concurrency, making it suitable for projects with flexible recovery schedules.
- The disaster recovery process requires a DHCP-enabled network on the NexaVM side. If the target network does not support DHCP, use a DHCP-enabled network during synchronization and switch to a static network configuration during cutover.
- Image mode supports multiple parallel cutovers, making it ideal for projects with high protection volume and limited cutover windows.

2.2 Architecture 2: Image Mode without Proxy Server

This image-based protection architecture does not require an intermediate server. The topology is as follows:



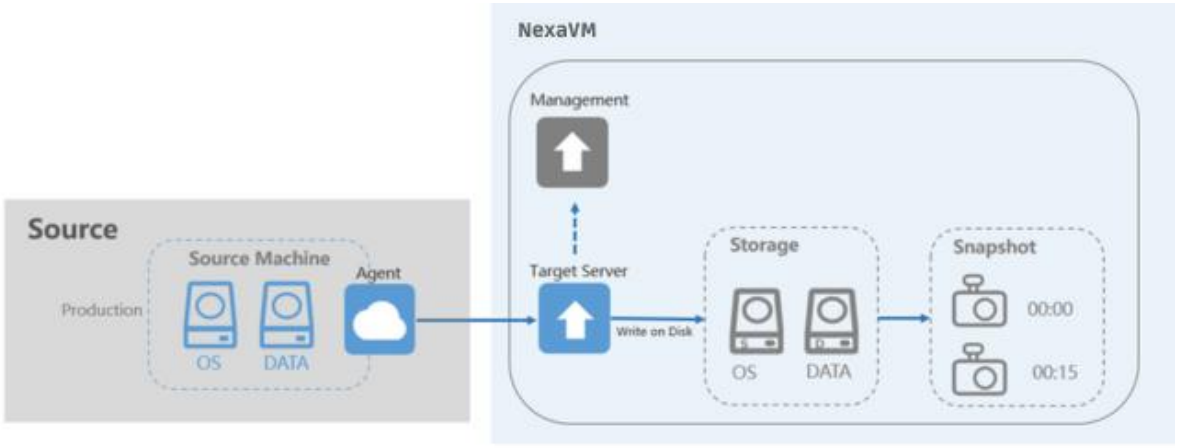
In this mode, users upload the BootImage to the NexaVM platform and connect via Access Key. The source machine establishes a direct protection task to the target cloud platform. Only reverse registration is supported for the source machine.

During protection, NDR automatically calls the NexaVM API to create and attach target disks to the target instance created based on the BootImage. Each protection task follows a one-to-one mapping between the source and target machine.

When configuring protection, users can select either Ceph or non-Ceph storage types for the target disk. Additionally, snapshot or backup features can be enabled for historical copy retention with rolling back capabilities.

2.3 Architecture 3: Disk-to-Disk Mode without Proxy Server

This architecture utilizes a direct disk-to-disk protection mode without using an intermediate server. The topology is as follows:



In this mode, there is no need to upload a BootImage. The NexaVM cloud platform is integrated using an Access Key. The source machine directly performs protection tasks to the target cloud platform by writing data to cloud disks through a Target Server. Both active and reverse registration modes are supported for the source machine.

During protection, the NDR platform automatically calls the NexaVM API to create and mount the necessary system and data disks on the target. This mode follows a many-to-one protection task structure between multiple source machines and a single Target Server.

Users can select either Ceph or non-Ceph storage types for target disk creation. Snapshot or backup features can be configured to retain historical copies with rolling retention, depending on the selected storage type.

Note: Disk-to-Disk mode without an intermediate server supports only scenarios where the Agent is installed on the source machine.

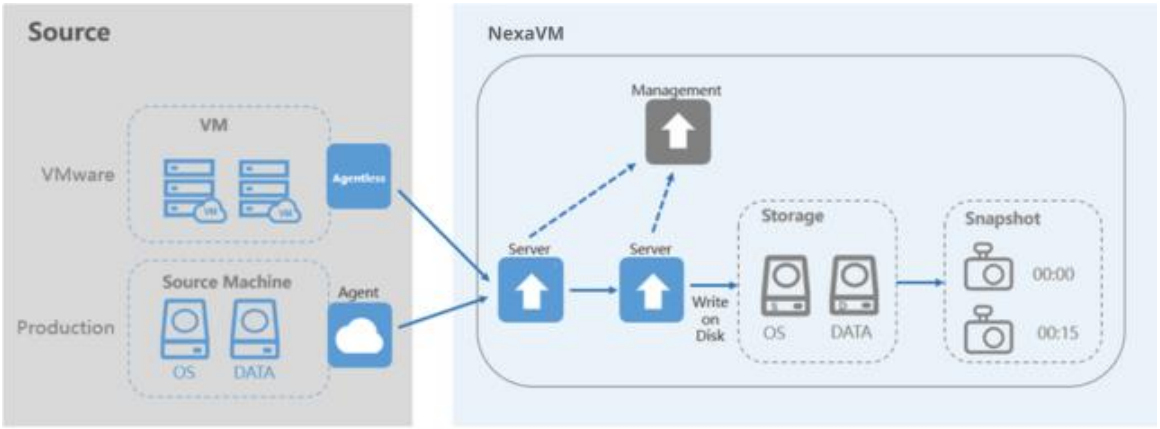
Scenario Selection Guide:

Source Scenario	Server Deployment	Cloud Platform	Target Cloud Network	Notes
Agent Installed	Target Server deployed inside NexaVM (required). No intermediate Server at source. Target cloud network can directly connect to the source machine.	NexaVM	DHCP not required	See topology diagram

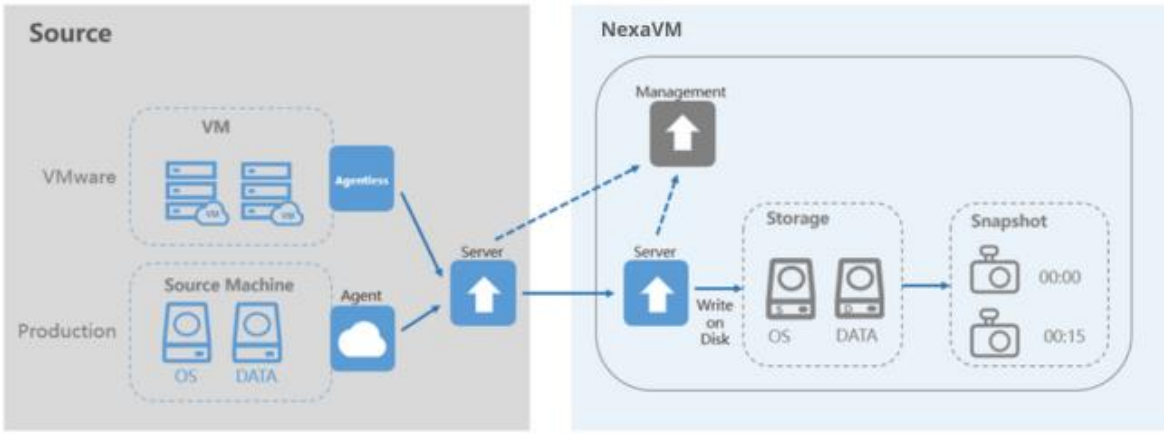
2.4 Architecture 4: Disk-to-Disk Mode with Proxy Server

This architecture utilizes a disk-to-disk protection mode with an intermediate server. The following diagrams illustrate the deployment topology:

1. **Topology 1** - where the Server is deployed on the target side.



2. **Topology 2** - where the Server is deployed on the source side.



While the Server service can be deployed on the same host as the management console, it is recommended to deploy a dedicated Server to avoid replication traffic impacting console access.

In this mode, there is no need to upload a BootImage. The NexaVM cloud platform is integrated using an Access Key. The source machine communicates through an intermediate Server for data replication. Both active and reverse registration modes are supported.

During synchronization, the NDR platform automatically calls the NexaVM API to create and attach system and data disks to the target instance. This architecture uses a many-to-one task structure, where multiple source machines send data to a single Server.

Target disk storage can be configured using Ceph or non-Ceph options. Snapshot or backup functions can be enabled for historical version retention, with support for rolling retention strategies based on storage type.

Note: This architecture supports disaster recovery cutover testing using replicated disk snapshots. Pre-cutover validation helps confirm configuration details and improve success rates during failover.

Scenario Selection Guide:

Source Scenario	Server Deployment	Cloud Platform	Target Cloud Network	Notes
VMware Agentless	Target Server deployed on the target NexaVM Intermediate server deployed within NexaVM (for VMware Agentless connection) Target cloud network must have direct access to the VMware VADP interface	NexaVM	DHCP not required	Refer to Topology 1
VMware Agentless	Target Server deployed on the target NexaVM Source intermediate server deployed at the source environment. For network relay: When the source and target platforms cannot communicate directly, the Server at the source acts as an intermediary	NexaVM		Refer to Topology 2
Agent Installed	Target Server deployed on the target NexaVM Target cloud network can directly connect to the source machine.	NexaVM	DHCP not required	Refer to Topology 1

Agent Installed	Target Server deployed on the target NexaVM Source intermediate server deployed at the source environment. For network relay: When the source and target platforms cannot communicate directly, the Server at the source acts as an intermediary	NexaVM		Refer to Topology 2

Applicable Scenarios and Characteristics

- Suitable for environments with private network connectivity and no one-way access restrictions. (For one-way access, reverse connection methods should be used—refer to related documentation.)
- The source environment is a VMware virtualization platform that supports agentless backup using the VMware VADP interface.
- VMware virtual machines can be protected without installing an agent.
- VMware agentless backup relies on VADP capabilities with limited concurrency, making it suitable for projects with flexible disaster recovery timelines.
- The disk-to-disk mode operates in a many-to-one structure, where multiple source machines write to the cloud platform through a single Server.
- Each Server deployed at the target should not exceed 23 mounted disks, in accordance with NexaVM’s per-instance disk mount limit.

2.5 Best Practices for VMware Agentless

1. **Optimizing Performance:**
    - Deploy one Server per ESXi host to optimize performance. Each Server should only handle migrations from its assigned ESXi host.
2. **Concurrency Limitations:**
    - By default, each Server can handle only one migration task per ESXi at a time. Additional tasks must wait to prevent performance impact on production workloads.
    - If multiple virtual machines reside on different ESXi hosts, concurrent migration is possible.
    - For specific needs, the concurrency limit can be adjusted via registry modifications on the Server, but it should not exceed 3. Refer to the knowledge base article *"VMware Agentless Mode Best Practices."*
    - If higher concurrency is required, consider using the agent-based migration mode.
3. **Compatibility Considerations:**
    - The Server communicates with ESXi and vCenter using VMware's VDDK component, which has version compatibility requirements. For upgrades or downgrades, refer to the knowledge base article *"Upgrading/Downgrading VDDK to a Specific Version."*
4. **Registering vCenter vs. ESXi Hosts:**
    - If there are many ESXi hosts (more than 20) or a large number of virtual machines (over 200), it is recommended to register each ESXi host individually.
    - If the number is smaller, registering the vCenter is sufficient.
5. **Disk Types Not Supported in Agentless Mode:**
    - RDM (Raw Device Mapping)
    - Independent - Persistent
    - Independent - Non-Persistent
    - SCSI bus-sharing disks

- Virtual machines using directly attached external storage

6. **Deployment for High-Performance Scenarios:**
   - In scenarios where high read speed from the source is critical, it is recommended to deploy the Server directly inside the source ESXi environment to maximize throughput.

3 Preparation

Based on the outlined preparation requirements, configure the necessary resources, install relevant software components, and initialize the configurations:

No.	Item	Details
1	Client Deployment	Install the agent(s) on the source machine(s).
2	Management	Create a Linux-based console via image and connect it to the NexaVM management network. Recommended specs: 4 vCPUs, 8 GB RAM, and at least 100 GB system disk.
3	Image Upload	Available formats: QCOW2, VHD, and more.
4	NexaVM AccessKey	Obtain keys to call the NexaVM API by either directly entering the AK/SK or adding them via account credentials.
5	Architecture Confirmation	Choose a suitable architecture based on the actual scenario.
6	License Activation	Activate solution license via online or manual.
7	Port Allowance	Open TCP Ports: 443, 20000-20001, 20005, 20443, 20010
8	NexaVM Platform	To use NexaVM's backup feature for retaining historical copies, ensure a NexaVM DR license is obtained in advance and appropriate backup storage resources are allocated.

3.1 Management Console Deployment

Create the Linux-based management console using a pre-provided image. Ensure that the console is connected to the NexaVM management network.

Recommended instance size: 4 vCPUs, 8 GB RAM or higher.

Best Practices:

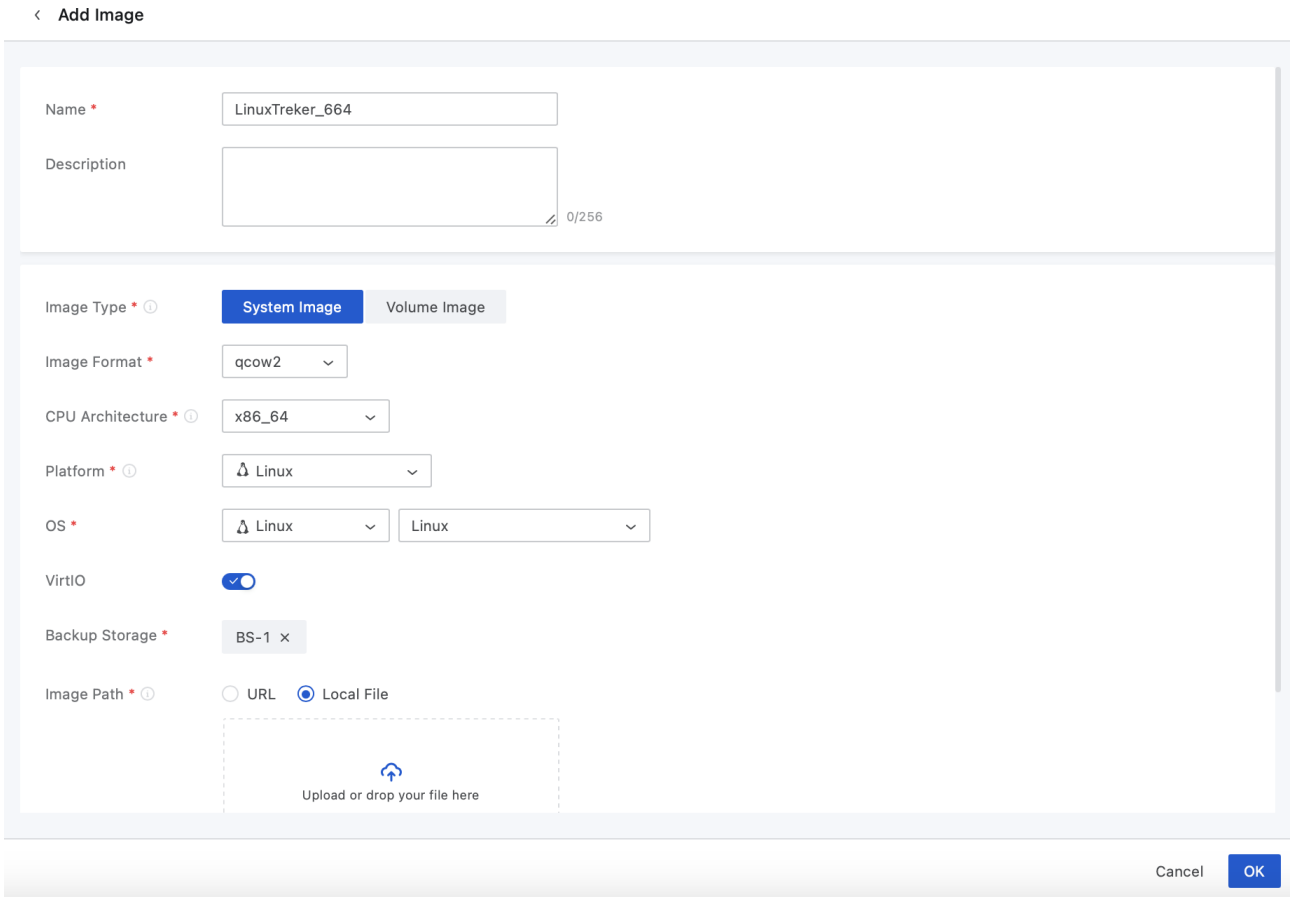
- If there are more than 5 source machines, deploy the management console and the Server separately. The management console should handle only management tasks, while the Server handles data transmission. Allocate high-performance disks and at least 4 vCPUs, 8 GB RAM, and 40 GB disk space for the console.

- The management console must be accessible by all Servers, BootImage instances, and agent-based source machines. For public network communication, a public IP is recommended.

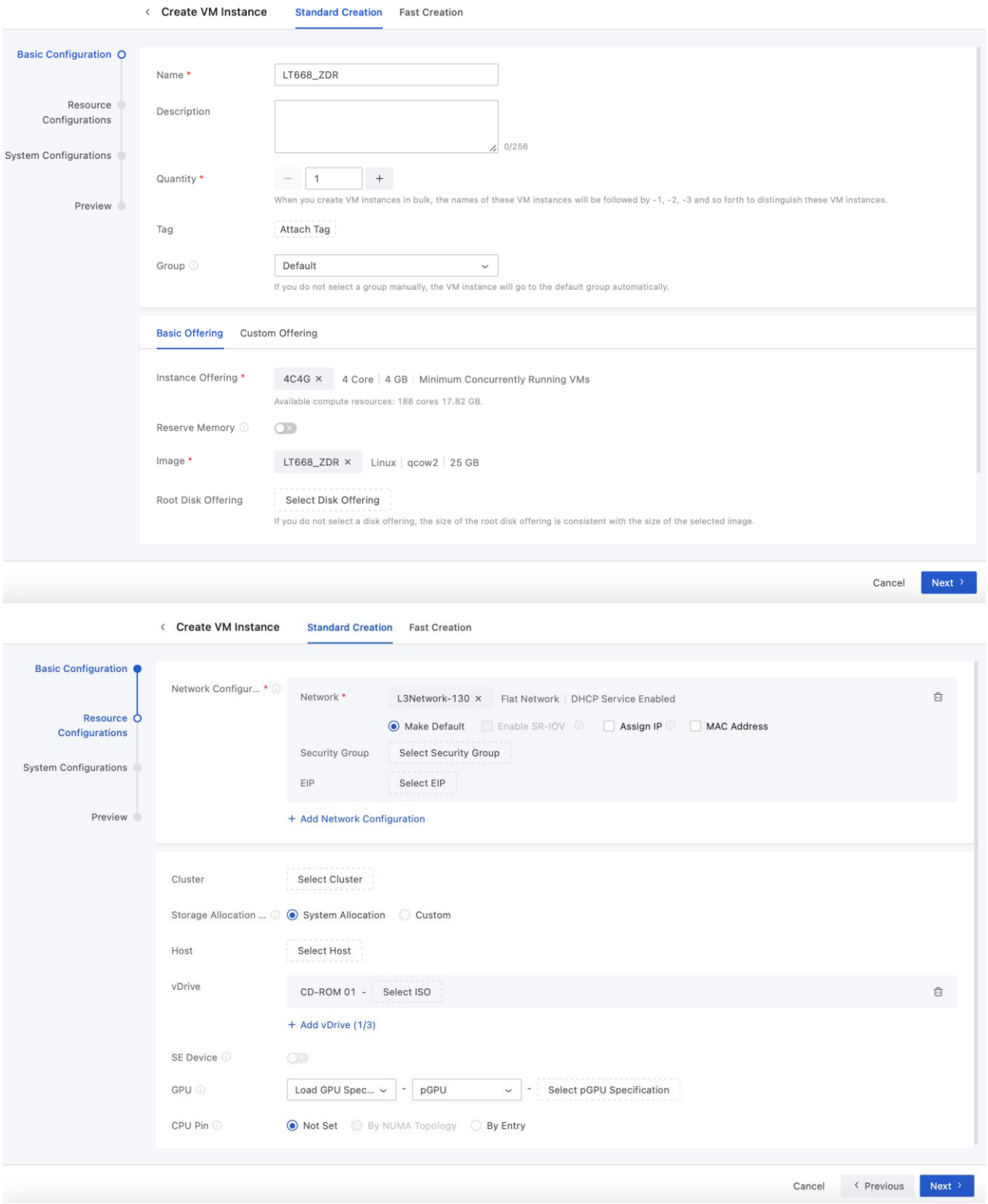
3.1.1 Deploy through Image

1. Find the following Linux server qcow2 image file from the NDR provided software: *NDR_Linux_Server_Gateway_(Treker)_637.qcow2*

2. Upload the image to the NexaVM cloud platform.

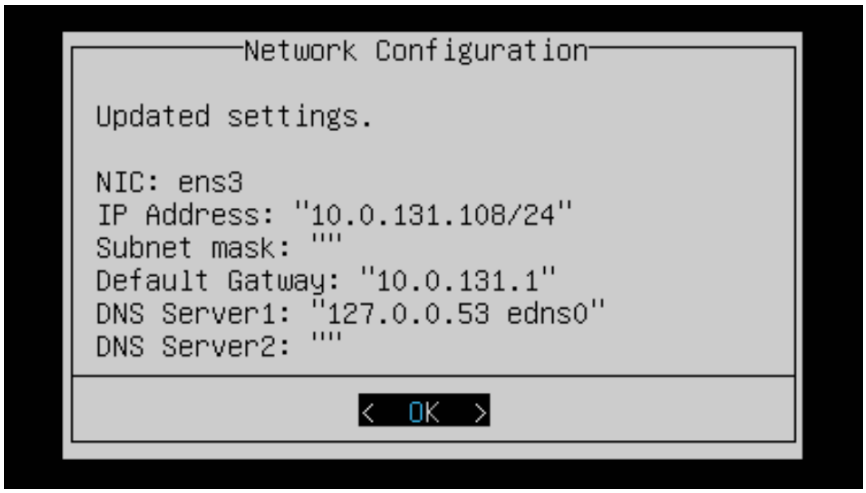


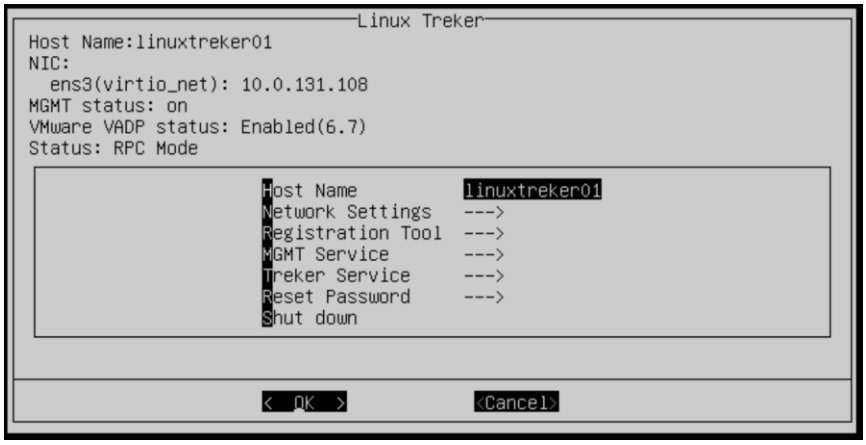
3. After the image upload is complete, create a VM instance. The recommended instance size is 4C8G or larger, with at least a 100GB system disk.



4. Once the virtual machine is created, the NDR service will start automatically. Users can access the management console by entering the instance's IP address in the browser.

5. Open the virtual machine console to see the menu below. The default menu password is "admin.”

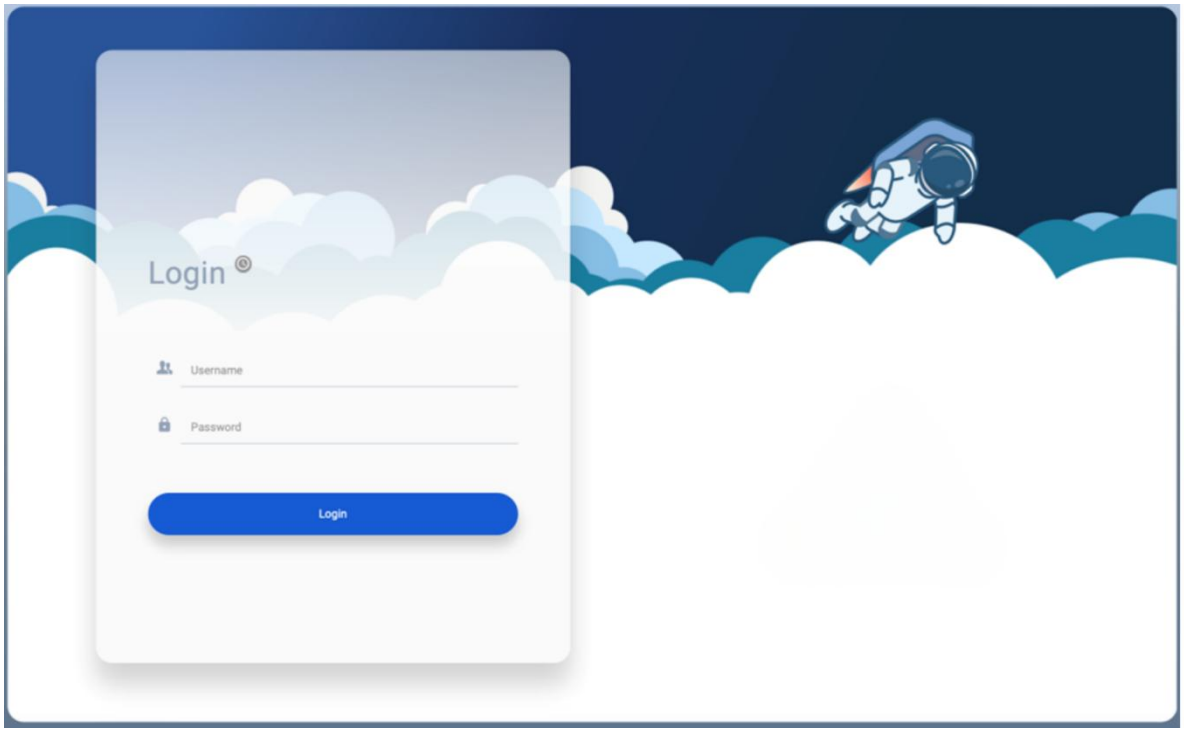




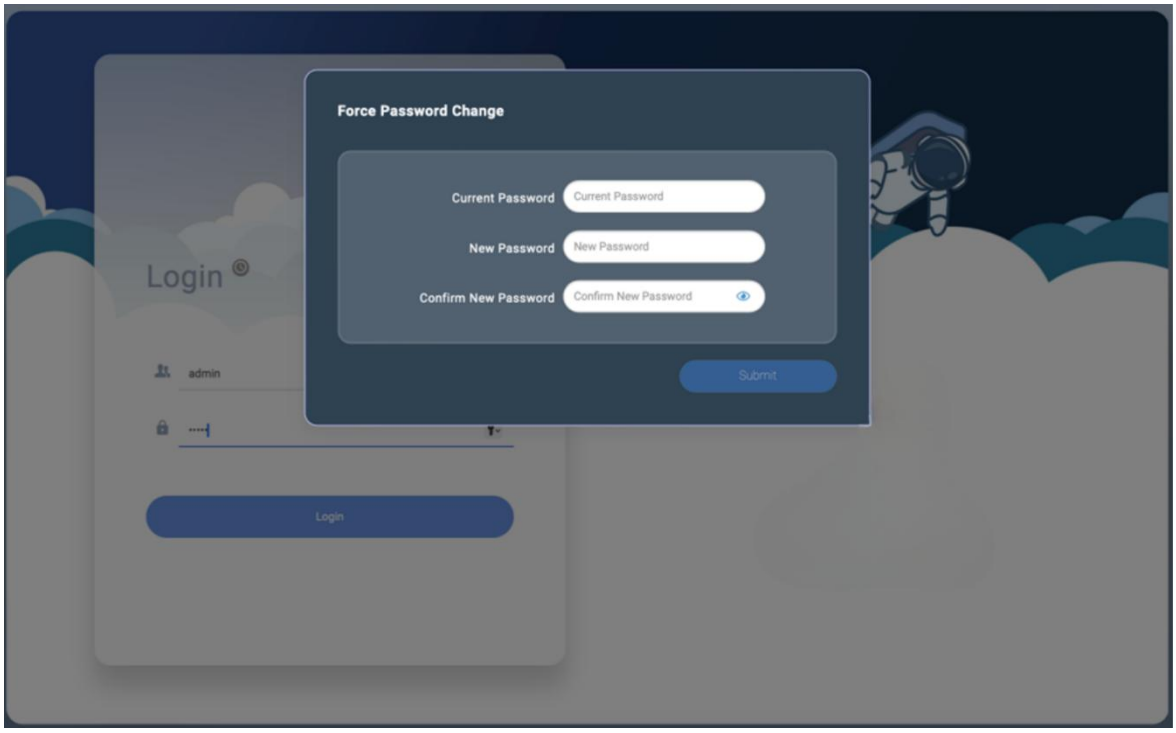
3.1.2 Log In to Management Console

Access the server where the management service is installed by entering its IP address or DNS name in a web browser. Use Chrome, Edge, or Firefox; Internet Explorer is not supported. Ensure that the NDR console server, NexaVM platform, and browser have synchronized system time, as time mismatches may cause login failures or synchronization errors. After logging in, you can update the management console settings.

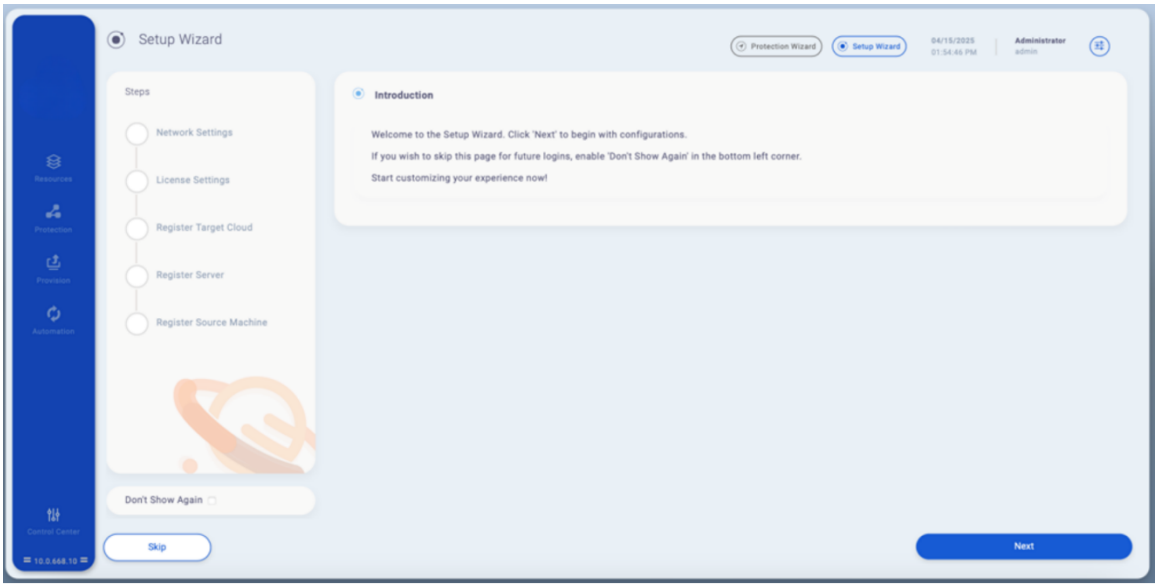
1. For the first login, enter the default username and password: admin/admin.



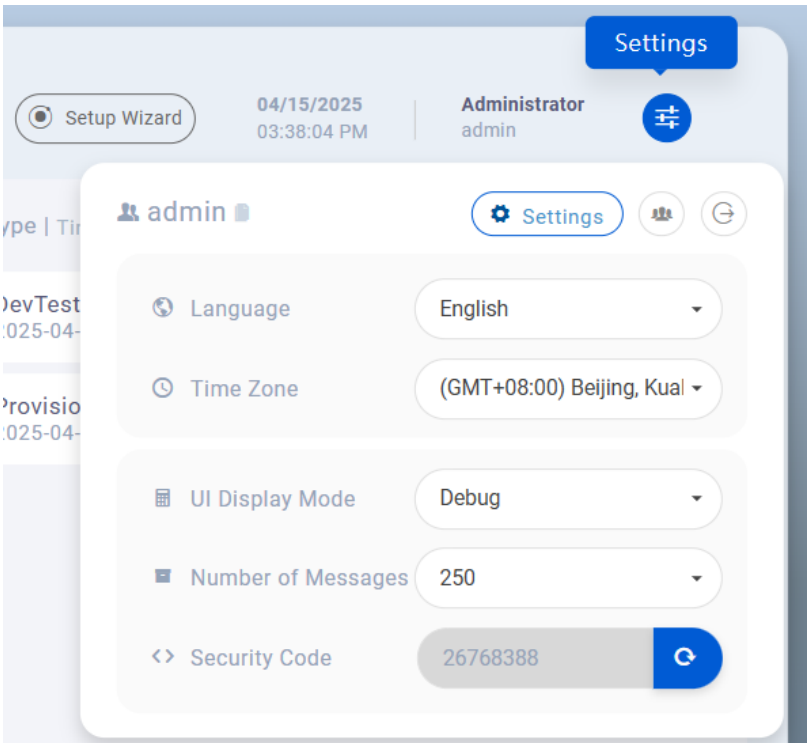
2. If prompted to change the password, enter the current password, “admin”, and configure a new login password.



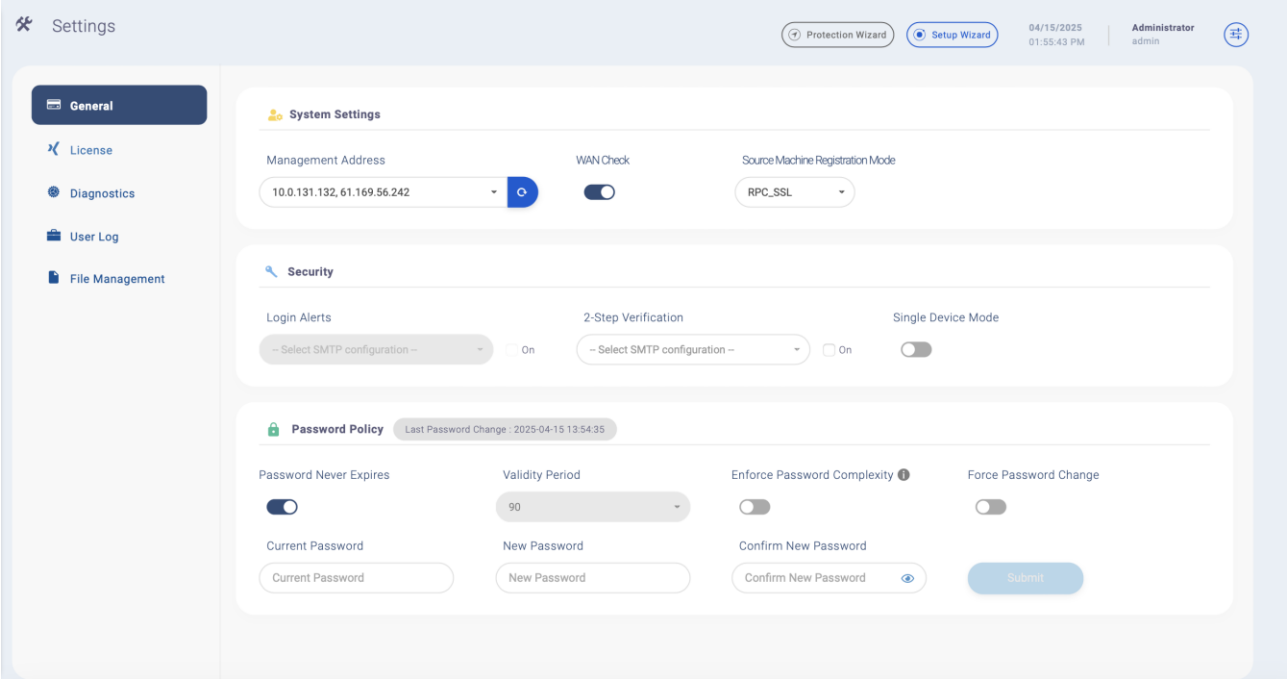
3. Upon logging in, the Setup Wizard page will open, guiding you through essential configurations for the protection and provisioning processes.
   To prevent this page from appearing during future logins, check the “Don’t Show Again” option at the bottom left. The wizard can be accessed at any time by clicking the “Setup Wizard” icon in the top-right corner.



4. During your initial login to the Management Console, begin with the basic configurations.



5. Under **Settings** > **General**, configure password policy, security measures, etc.



3.2 Source Server Deployment

For VMware agentless protection, a dedicated Source Server is required—either a Windows-based Server or a CentOS image-based Server—to connect with the VADP interface. Even when using the agent-based approach, deploying a separate Server helps minimize the load on the disaster recovery management console.

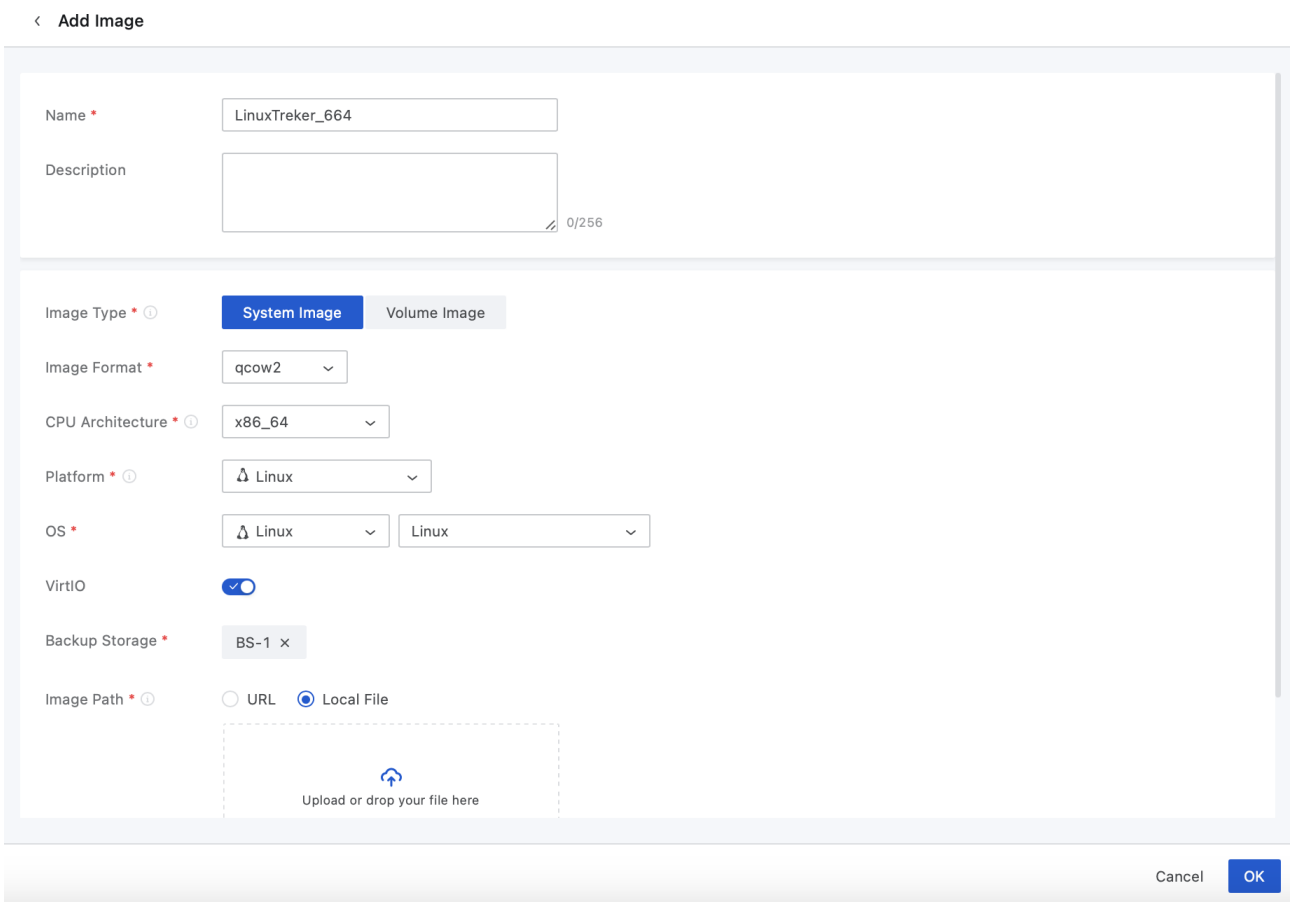
While the Server service can be co-deployed with the console, it is strongly recommended to set up a standalone Server for VMware integration to avoid performance impact from data replication traffic.

Deploy the Server by creating a Linux-based instance using the provided image. Ensure it is connected to the NexaVM management network.

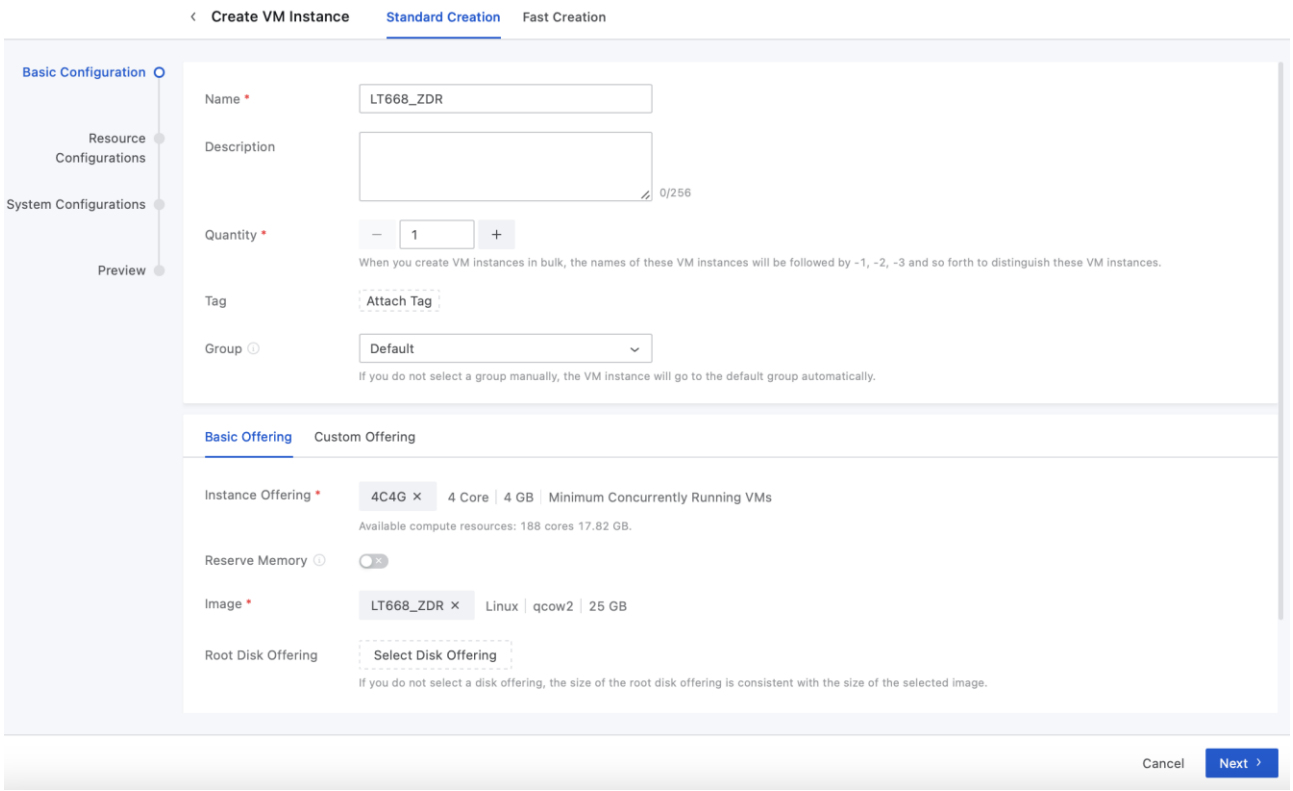
Recommended instance size: 4 vCPUs, 8 GB RAM or higher.

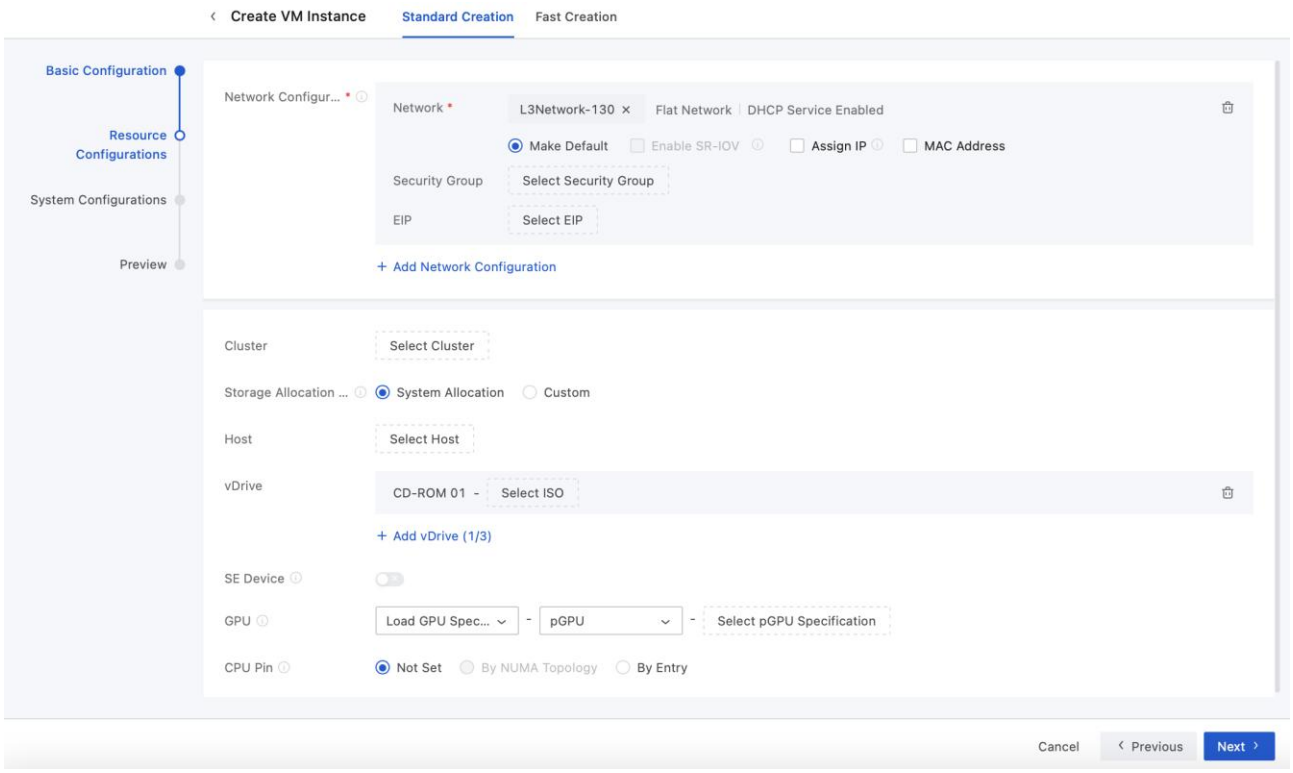
1. Find the following Linux server qcow2 image file from the NDR provided software: *NDR_Linux_Server_Gateway_(Treker)_637.qcow2*

2. Upload the image to the platform (using the NexaVM platform as an example).



3. After the image upload is complete, create a VM instance. The recommended instance size is 4C8G or larger, with at least a 100GB system disk.





4. Once the virtual machine is created, the NDR service will start automatically. Users can access the management console by entering the instance's IP address in the browser.

5. Open the virtual machine console to see the menu below. The default menu password is "admin."

3.3 License

3.3.1 About License Key

License Key Overview

- **Validity Period:** Unlimited source-to-target protection and provision within the valid period.
- **License Scope:** Limited by the number of source machines and disk capacity (not actual data volume).
- **License Components:**
    - Key: The license string.

  - Credits: Assigned to each key— based on the number of source machines, while capacity licenses are based on storage capacity.

- **Time Constraints:**
  - License activation validity period.
  - Time validity after activation and assignment.
  - Credits assigned to synchronization tasks follow the same validity period as the license type.
- **Official Capacity Licenses:**
  - Globally shared across management console.
  - Validity: Aligned with the main license duration upon credit deduction.
  - Minimum Unit: 1TB.

Test License

No.	Type	Protection Period	Included Capacity
1	Disaster Recovery Test	2 weeks	1TB

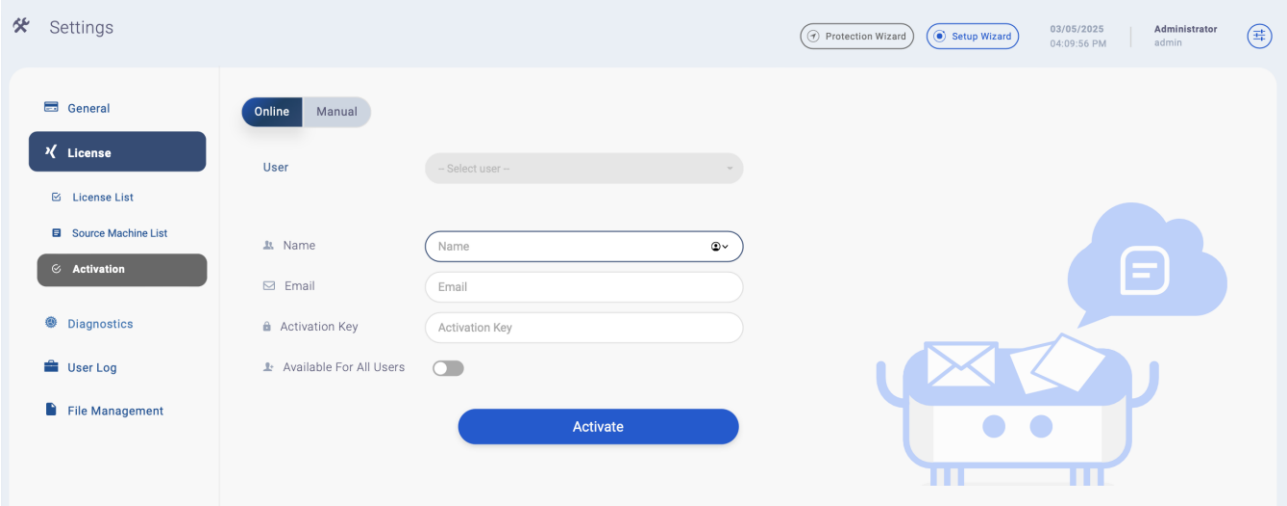
Official License

No.	Type	Protection Period	Included Capacity
1	Disaster Recovery (Subscription)	1 year	1TB
2	Disaster Recovery (Perpetual)	No expiration	1TB
3	Disaster Recovery - Capacity (Subscription)	Based on credit usage	N/A
4	Disaster Recovery - Capacity (Perpetual)	Based on credit usage	N/A
5	Cascaded/Parallel DR (Subscription)	1 year	1TB
6	Cascaded/Parallel DR (Perpetual)	No expiration	1TB
7	Cascaded/Parallel DR - Capacity (Subscription)	Based on credit usage	N/A
8	Cascaded/Parallel DR - Capacity (Perpetual)	Based on credit usage	N/A

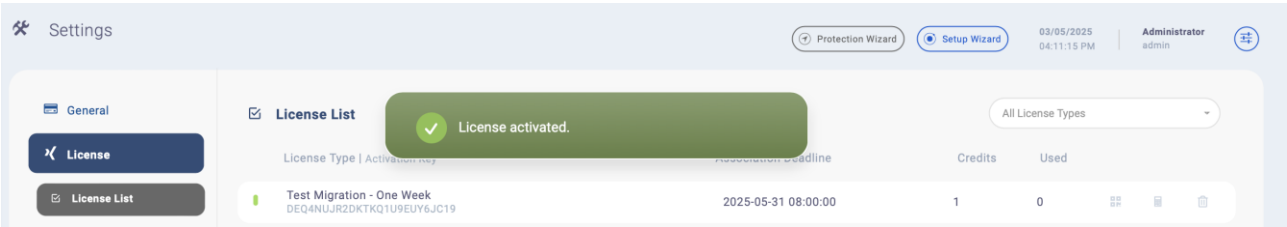
3.3.2 Online Activation

To activate the license, ensure that the Management Console has internet access and the correct DNS settings to query the activation server's IP address.

1. Navigate to the **Control Center** in the bottom-left corner and click License. Then click Activation. Enter the user details, including name, email, and activation key. If the key should be available to all users, enable the Available for All Users toggle. Click **Activate** to complete the process.



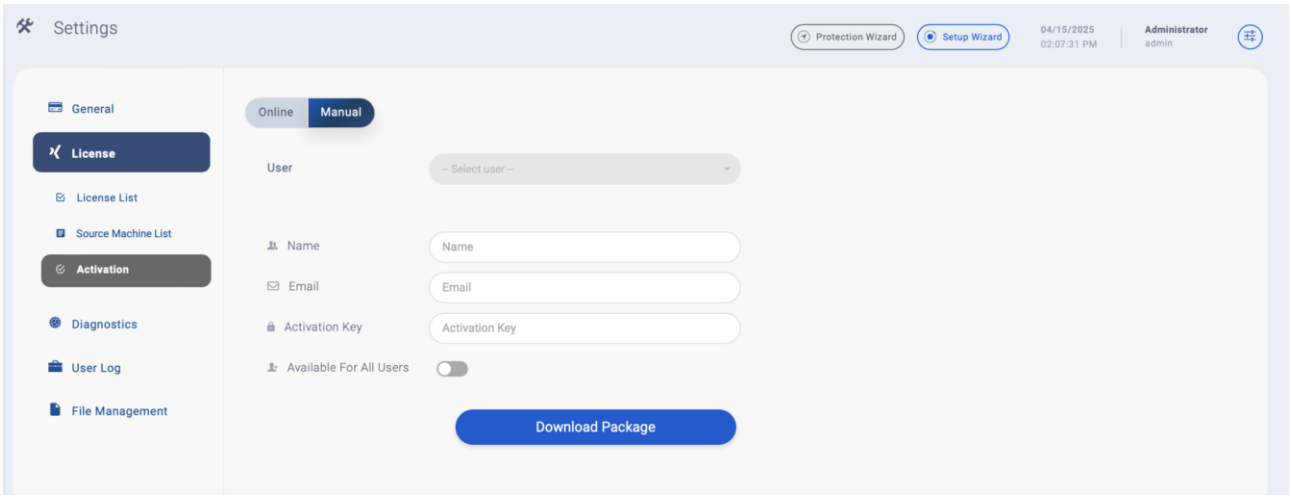
2. If the activation is successful, a pop-up message will appear confirming the activation with the statement "License activated." Additional details about the activated license can be viewed in the License List.



3.3.3 Manual Activation

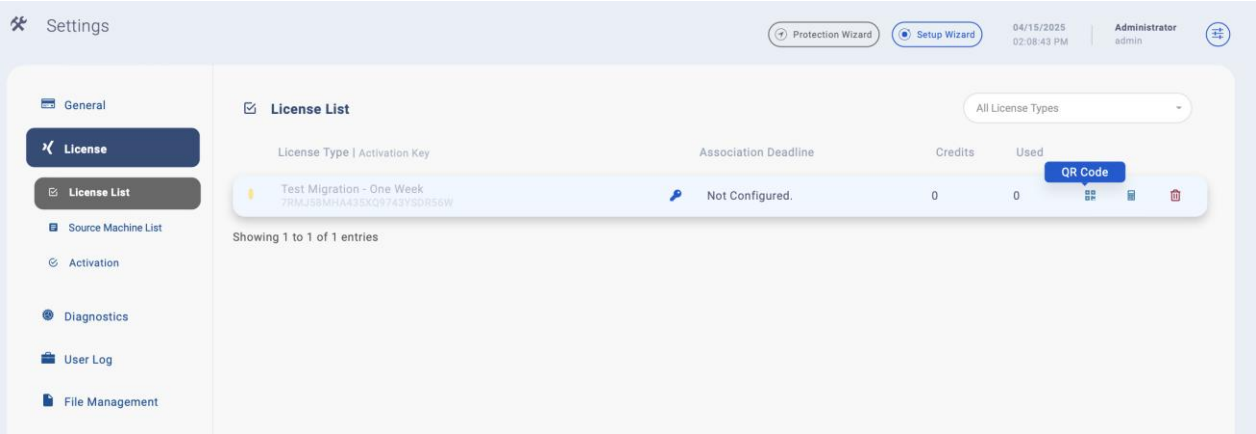
If the Management Console cannot access the internet or detect the correct DNS settings, download the activation file and provide it to technical support for assistance. Follow these steps to activate the license manually:

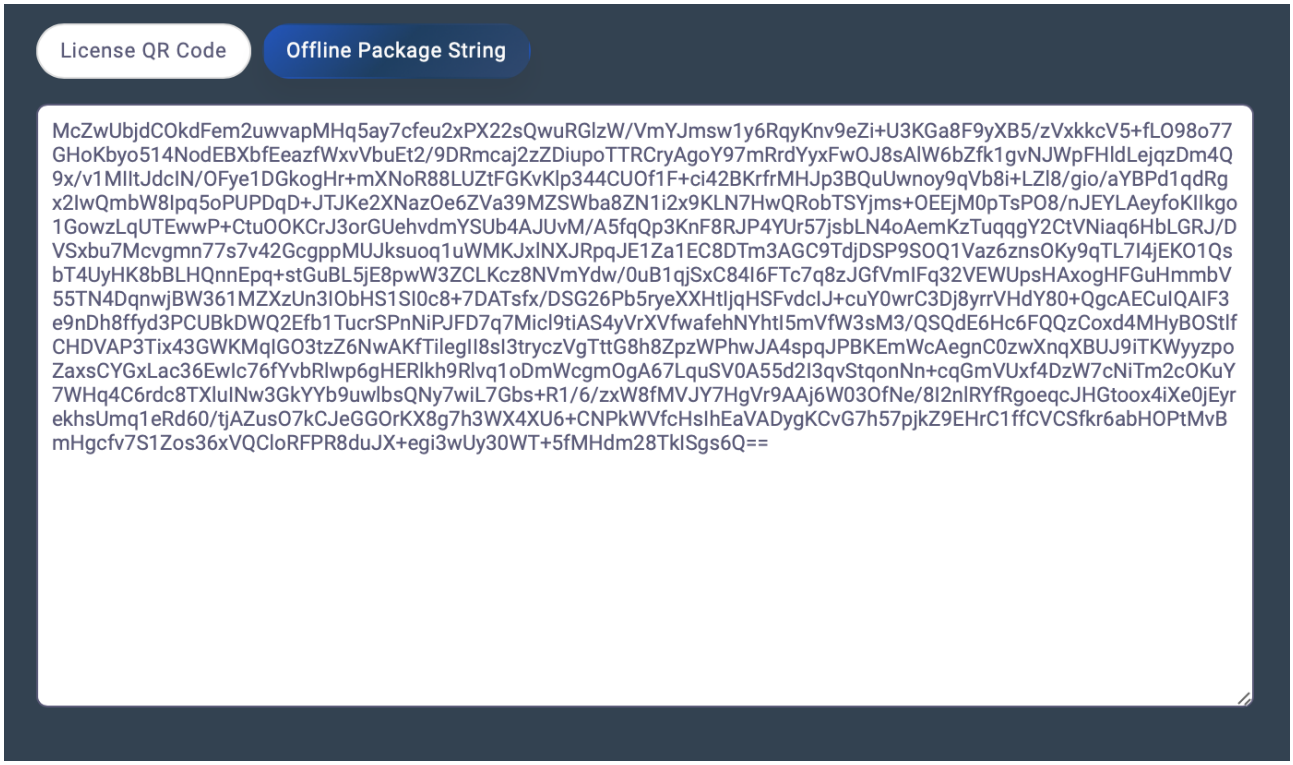
1. Visit the **License** page and click on **Activation**. Switch to the **Manual** tab. Enter the user details, including name, email, and activation key. Click **Download Package**.



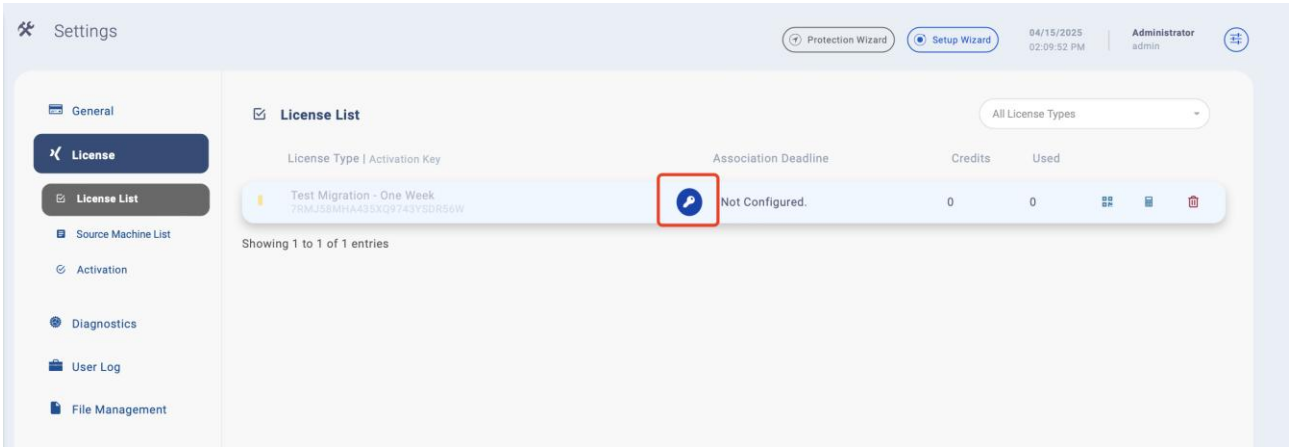
2. A file named *offline_activation.txt* will be downloaded. Send this file to your technical support contact for manual activation.

3. Alternatively, click the QR code icon next to the license key to scan the QR code or copy the activation string to obtain the activation code.

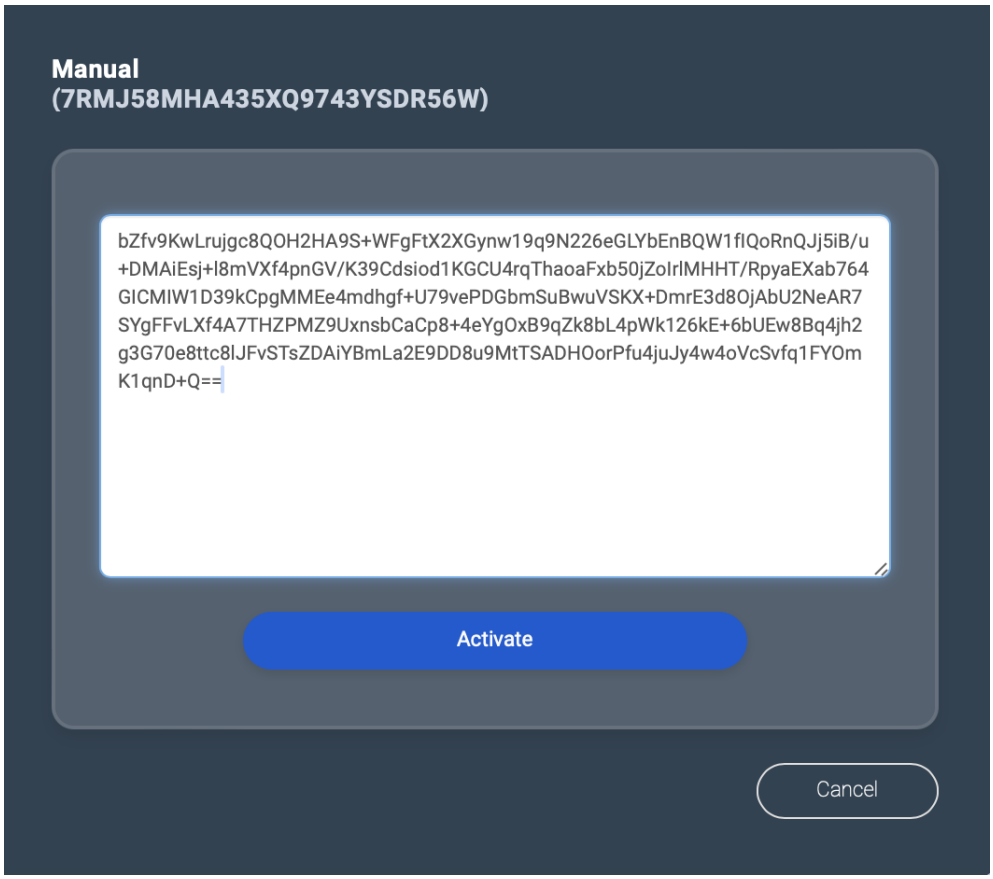




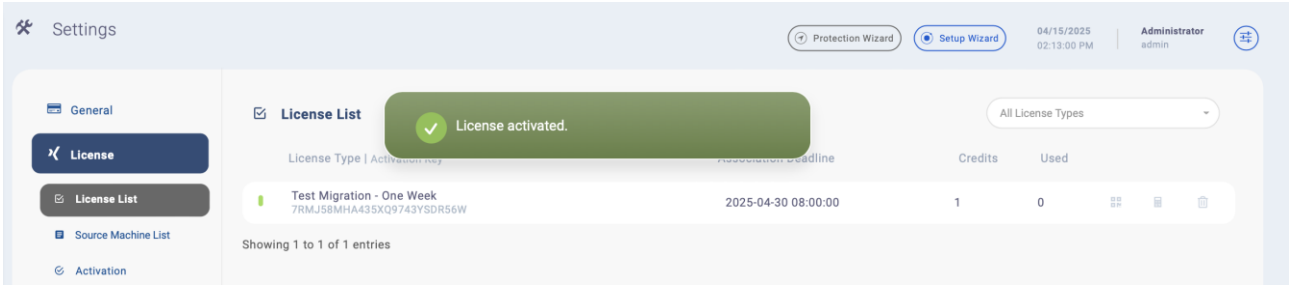
4. After receiving the activation string from technical support, click the “key” icon next to the corresponding license key.



5. Paste the activation string provided by technical support into the designated field. Click **Activate** to complete the activation process.



6. Once activation is successful, the manually activated license can be confirmed in the license list.



3.4 Upload BootImage to NexaVM

NDR provides a built-in feature for uploading images via the console, reducing manual operations. For detailed steps, refer to Appendix I.

1. **Add BootImage to NexaVM.**

   a) In NexaVM cloud platform, navigate to **Cloud Resource Pool** > **Image** > **Add Image**.

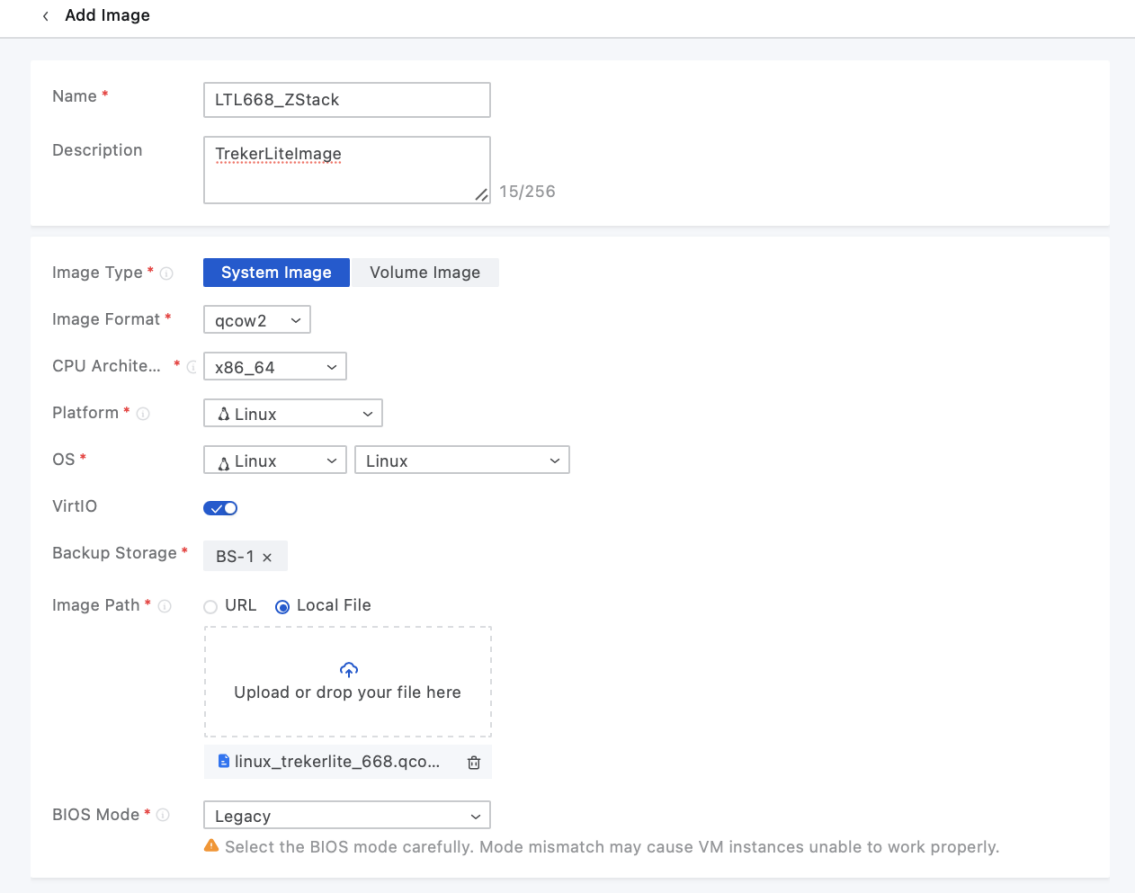
   b) Fill in the required fields based on the BootImage type, and upload the qcow2 image. Ensure the BootImage type and boot mode match the source machine's operating system:

   - Windows source machine → Windows BootImage.
   - Linux source machine → Linux BootImage.
   - BIOS boot mode source machine → Legacy BootImage
   - UEFI boot mode source machine → UEFI BootImage

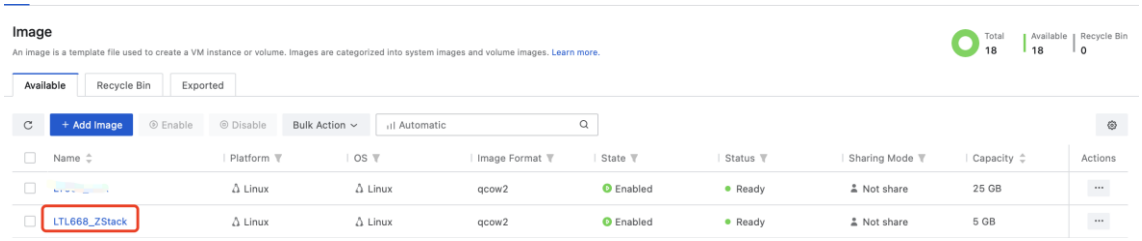
   Best Practices

   - To ensure compatibility, import the BootImage twice, each with a different boot mode: Legacy and UEFI versions.
   - If manually creating a BootImage (instead of API automation), ensure the system disk is at least 5GB larger than the source.
   - For cases where the target system disk size cannot be increased by 5GB, use the BootImage ISO version (manual process, see Appendix I).

c) Set the BootImage description to “**TrekerLiteImage**”, or it won’t appear in the protection configuration list.



2. Verify Image Status; “Ready” means it’s available for use.



3.5 Register Cloud API

NDR uses Access Key (AK) and Secret Key (SK) to automate processes, including creating target instances from BootImage, configuring networks, and attaching disks.

There are two ways to connect to the cloud platform, both relying on Access Key authentication:

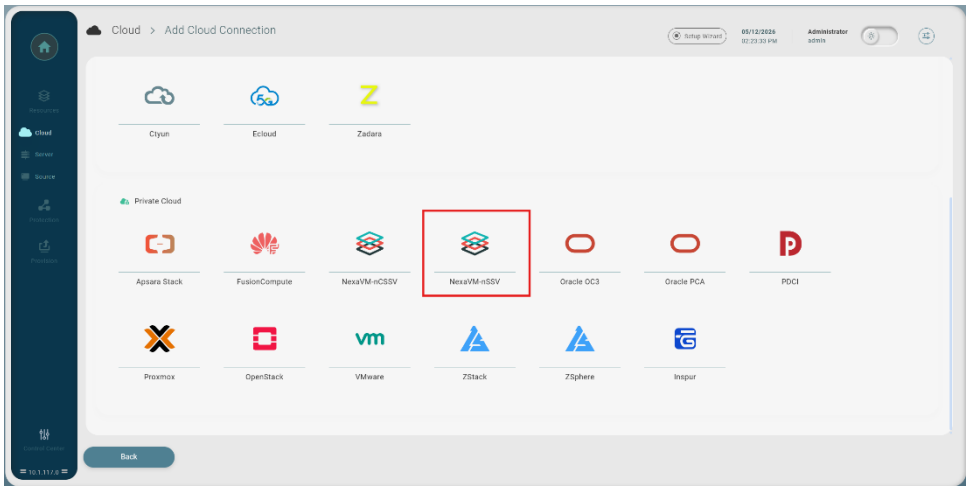
1. Using cloud platform credentials – NDR generates a new AK/SK via API.

2. Using an existing AK/SK – Directly connect with a pre-configured key.

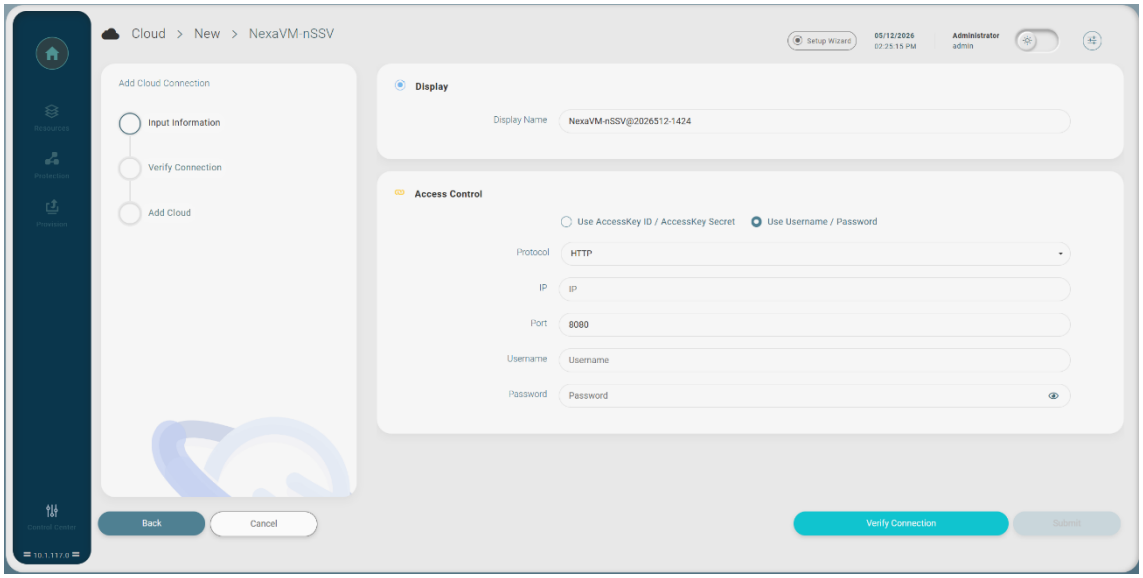
3.5.1 Method 1: Connect with Username and Password

1. Log in to the Management Console, navigate to Resources, under the Cloud page, click **Add** to create a new cloud connection.

2. Select **NexaVM** and click **Next**.



3. Select **Use Username/Password**, enter the NexaVM Cloud IP, and connect via port 8080. Enter the Username and Password, select the Time Zone based on the actual NexaVM Cloud environment, then click **Verify Connection**.



4. Once the verification is successful, click on **Submit** to save the settings.

5. The AccessKey created by the system will be visible in the NexaVM console.

3.5.2 Method 2: Connect with AccessKey / SecretKey

1. In NexaVM, navigate to **Operational Management** > **Access Control** to obtain an AccessKey.

2. Visit **Access Key Management** and generate a new AccessKey.

3. Copy the AccessKey ID and AccessKey Secret.

4. Log in to the Management Console, navigate to Resources, under the Cloud page, click **Add** to create a new cloud connection.

5. Select **NexaVM** and click **Next**.

6. Select **Use AccessKey ID / AccessKey Secret**, enter the NexaVM Cloud IP, and connect via port 8080. Enter the AccessKey ID and AccessKey Secret, select the Time Zone based on the actual NexaVM Cloud environment, then click **Verify Connection**.

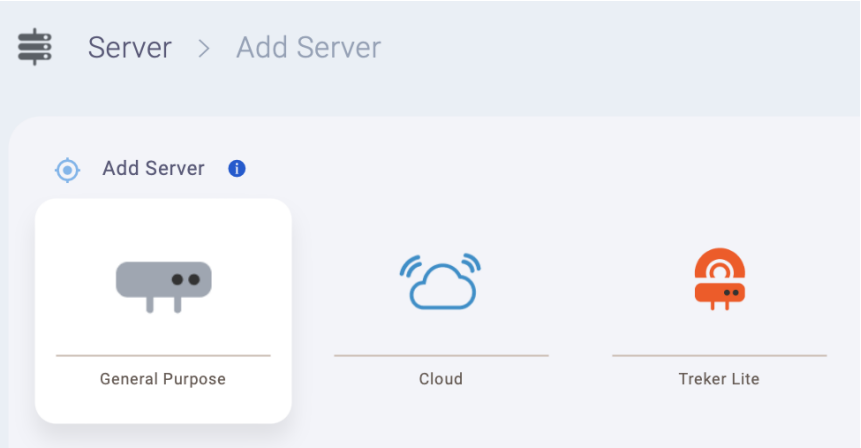
7. Once the verification is successful, click on **Submit** to save the settings.

8. Once registered, the new NexaVM cloud connection will be displayed.

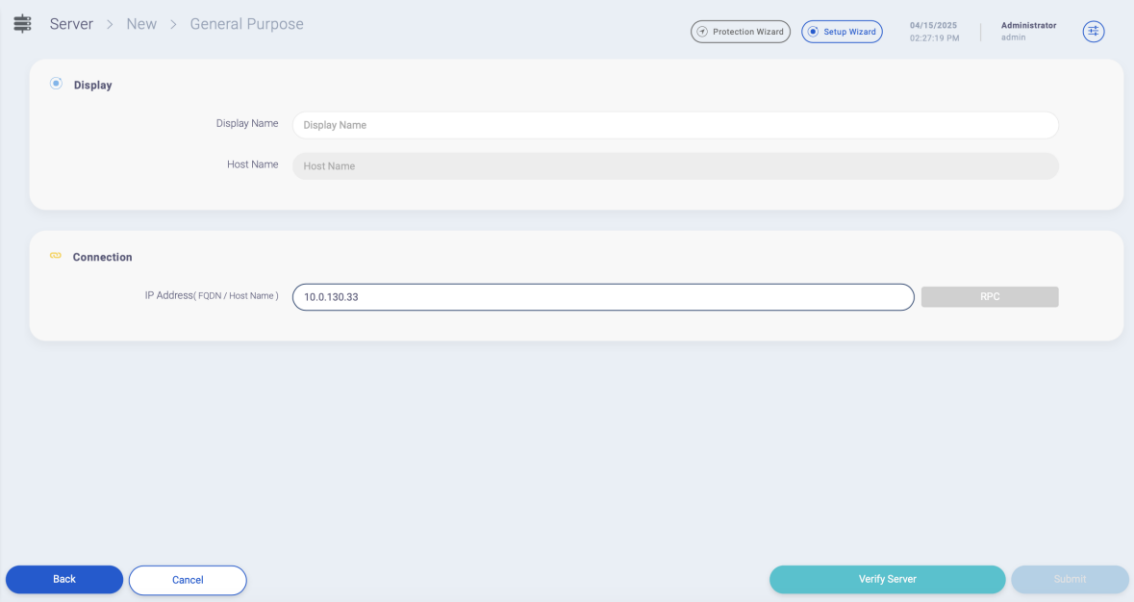
3.6 Register Source Server

1. Under **Resources**, visit the **Server** page and click **Add** to register a new server.

2. For server type, select **General Purpose**.



3. Enter the IP address of the server where the software is installed.



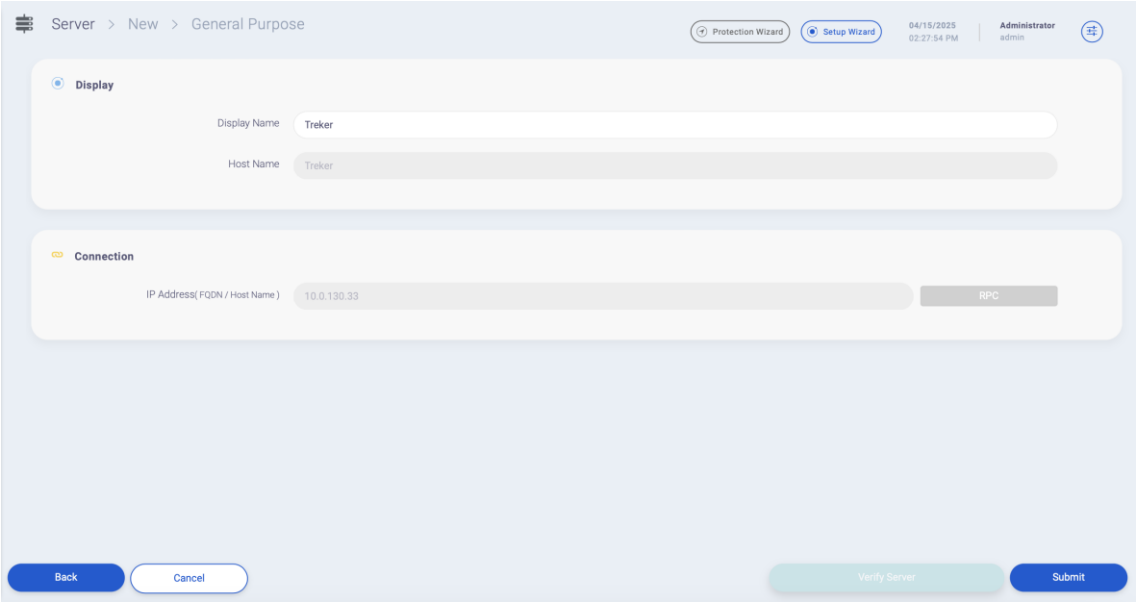
4. Click on **Verify Server**.
   If the IP address is unidentifiable, the browser will attempt verification for up to three minutes. If verification fails, check the following and re-enter the IP address.

   a) Ensure the server service software is properly installed.

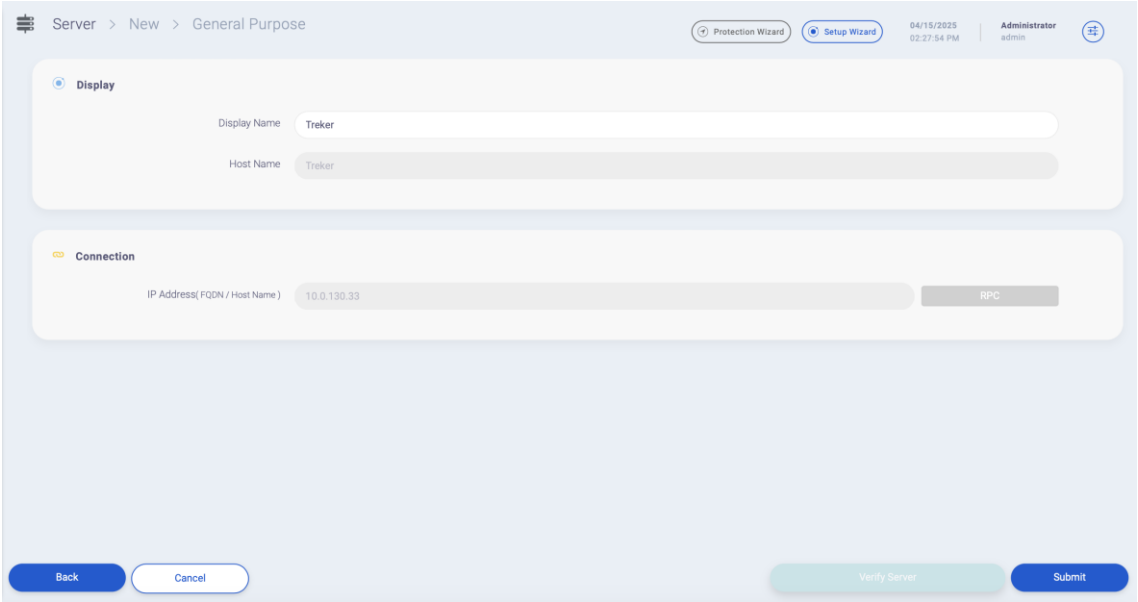
   b) Verify that the server service is running.

c) Confirm that the server is accessible via the internet.

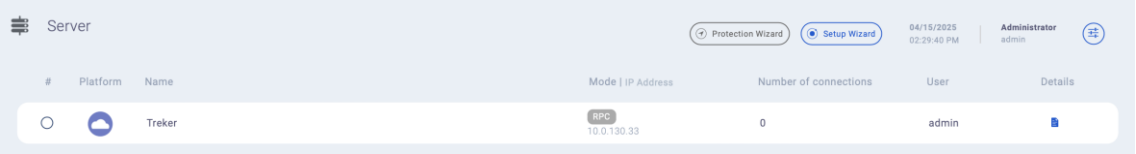
d) Check that TCP port 20001 is open.



5. Once the verification is complete, update the server display name if needed, then click **Submit** to save.



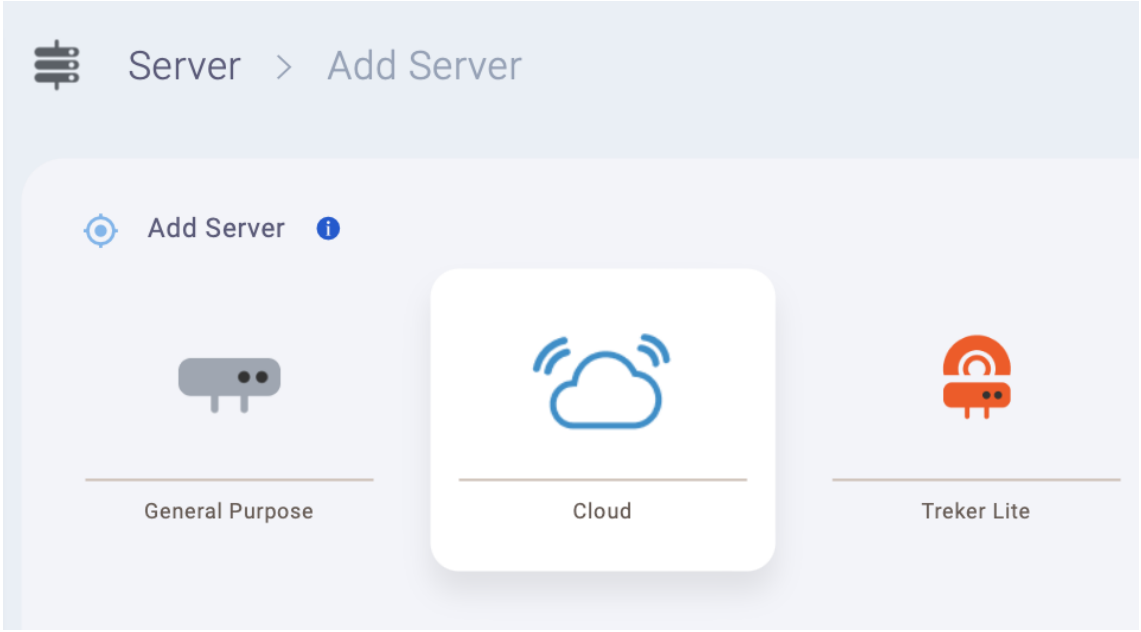
6. After successfully adding the server, it will be shown on the Server page.



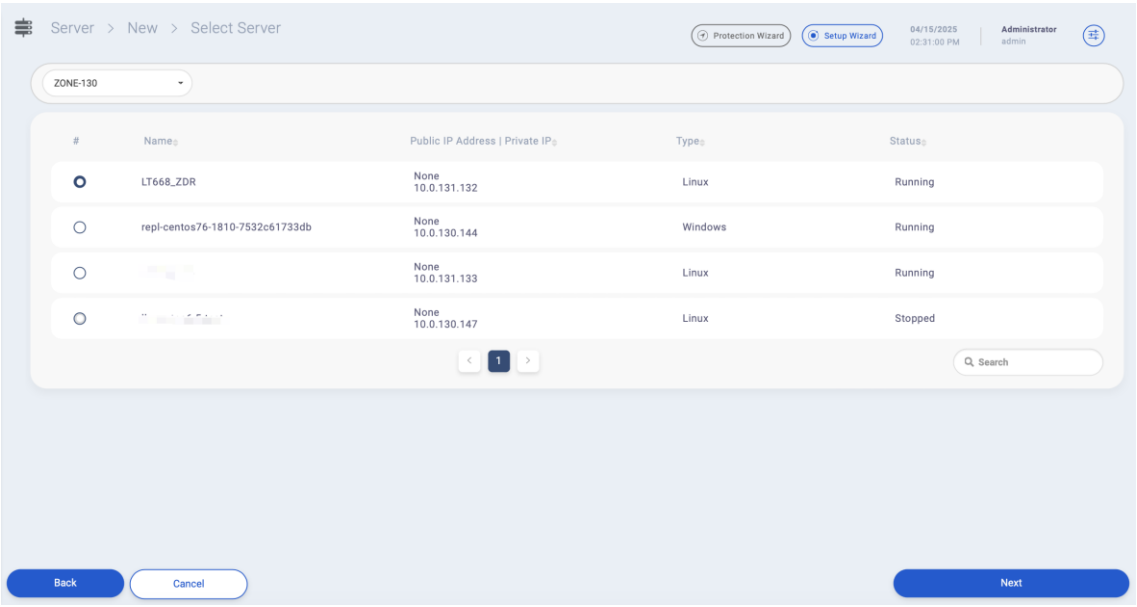
3.7 Register Target Server (Disk-to-Disk Mode)

If using Disk-to-Disk mode, follow the steps below to register a target server. If this mode is not in use, you may skip this section.

1. Under **Resources**, visit the **Server** page and click **Add** to register a new server.
2. For server type, select **Cloud**.

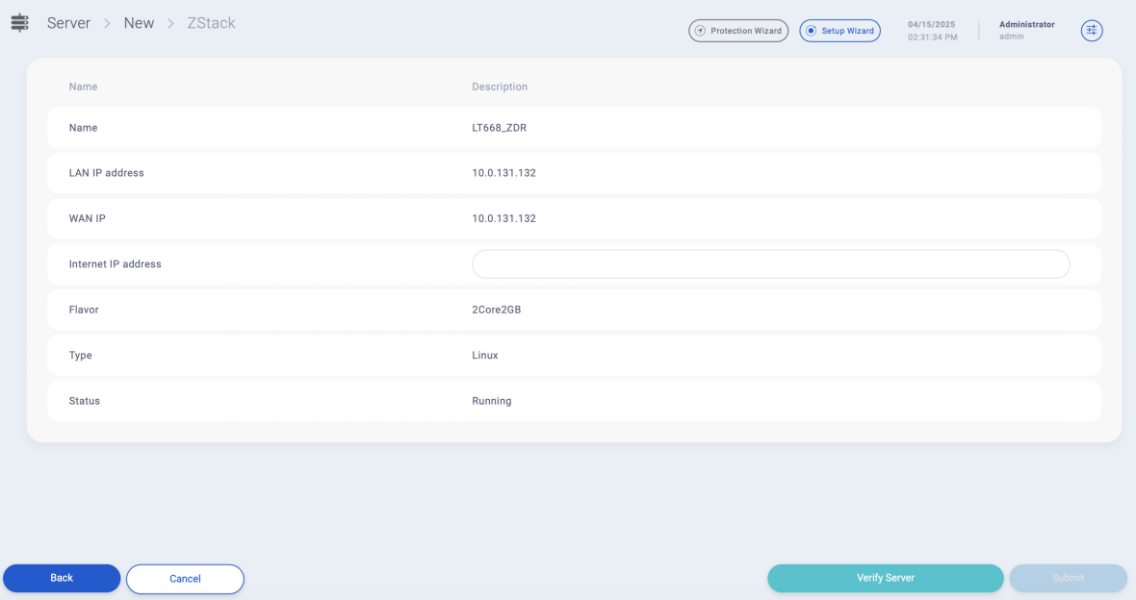


3. Select the target cloud connection and click **Next**.
4. Choose the server with the installed software and click **Next**.

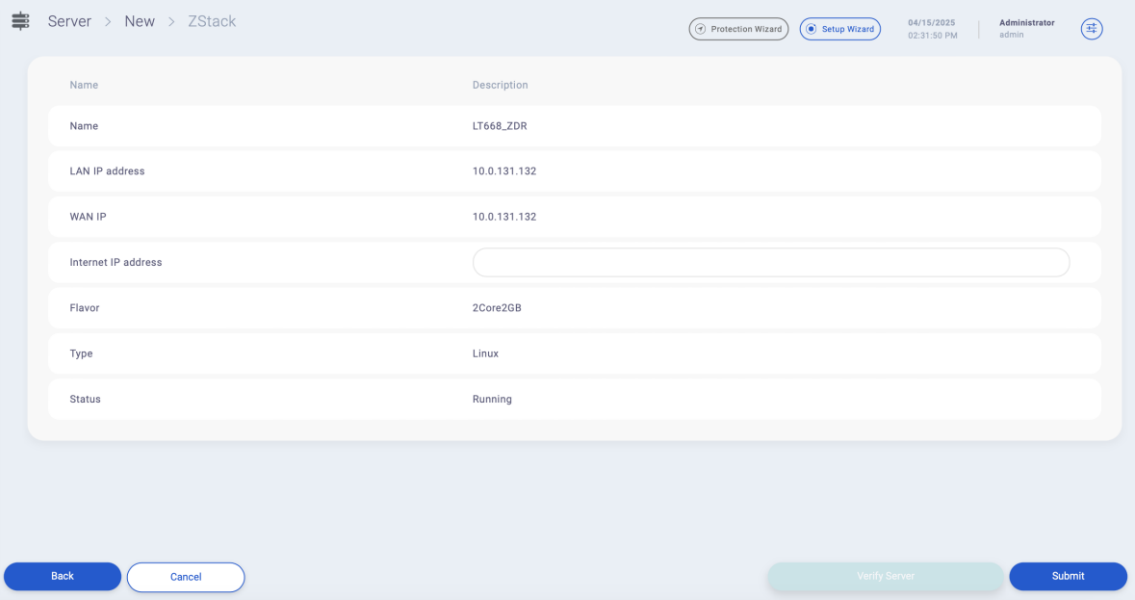


5. Click on **Verify Server**.

   If the IP address is unidentifiable, the browser will attempt verification for up to three minutes. If verification fails, check the server status and re-enter its IP address.



6. Once verification is complete, update the server display name if needed, then click **Submit** to save.



7. After successfully adding the server, it will be shown on the **Server** page.

4 Source Agent Installation and Registration

4.1 Windows Agent

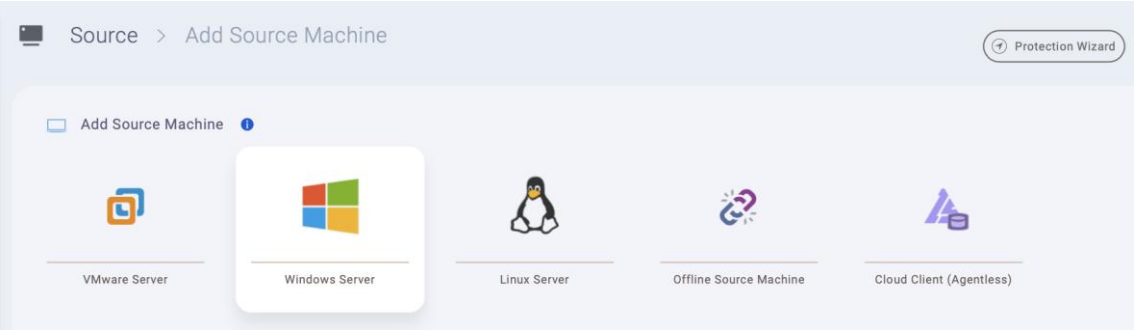
The Windows agent can be installed on Windows servers or source platforms. Its responsibility is to record IO changes on the source machine and execute synchronization and protection procedures to the target platform. Follow the steps below to complete the installation of the agent.

1. Log in to the source machine and run the agent installation file.
2. Follow the instructions on the installation wizard to complete the process.
3. Choose the installation folder and click **Next**. (The source agent only requires 50 to 100MB of hard disk space.)
4. Click **Install** to start the installation.
5. Wait for about one minute to finish the agent installation. Once completed, click **Finish** to exit the installation wizard.

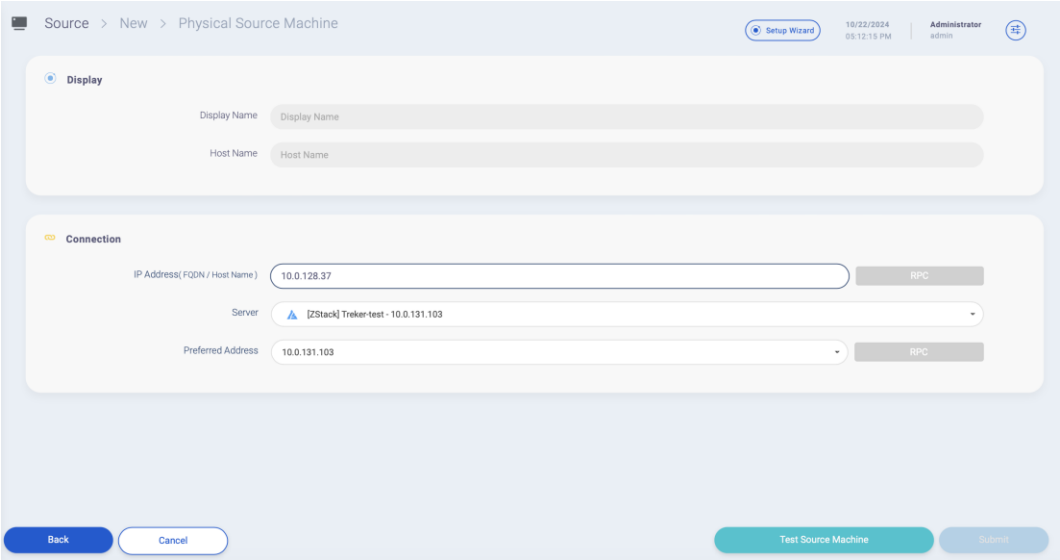
4.1.1 RPC Registration

If the Windows source machine has a public IP or an IP address obtained through FQDN (Fully Qualified Domain Name) resolution, use the RPC registration mode to register the source machine from the management console.

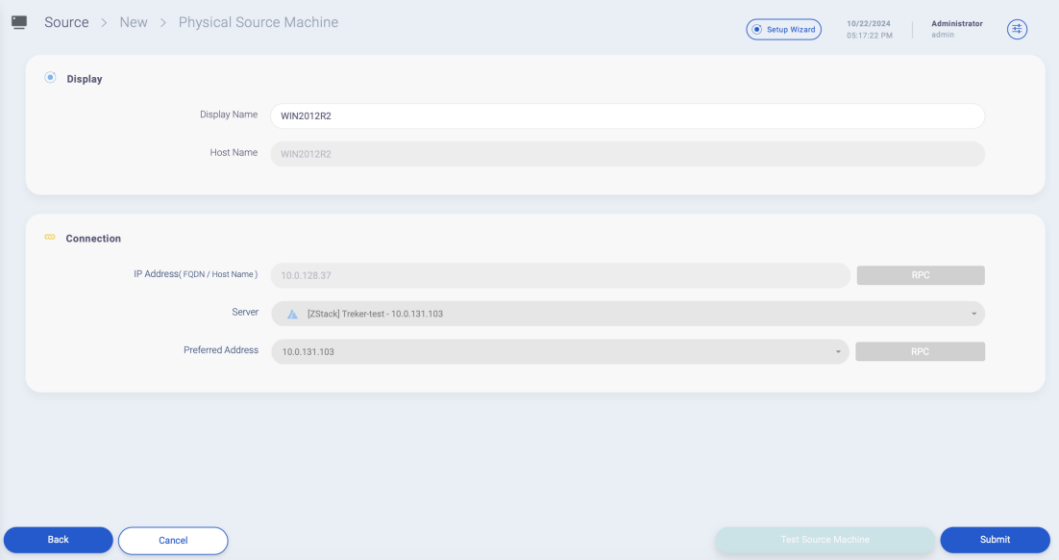
1. Under Resources, click **Source** to add a new source machine.
2. Under Source Machine Type, choose **Windows Server**.



3. Enter the IP address of the source machine where the source agent is installed into the IP address field.



4. Click **Test Source Machine** to verify the connection.

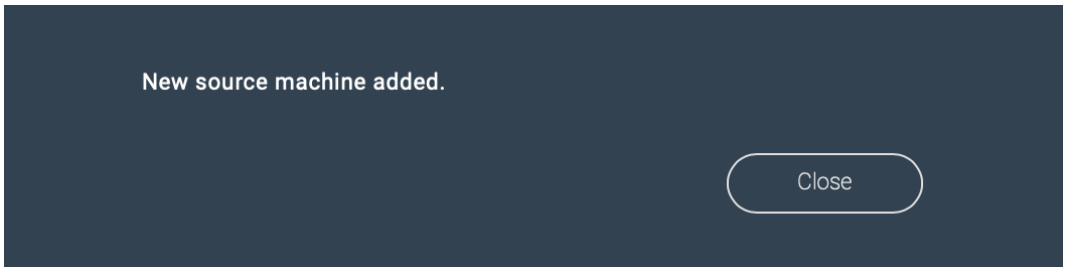


If the verification takes longer than three minutes, please check the following:

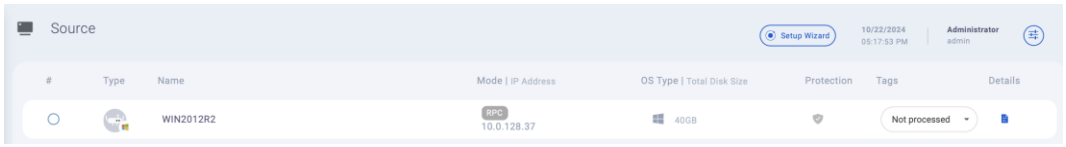
- Ensure the source agent is correctly installed on the source machine.
- Verify that the source agent is operating normally.
- Confirm that TCP: 20005 is enabled on the source machine.

After confirming the above, proceed to re-verify.

5. Once verified, options to modify the display name of the source machine will be enabled. Modify as needed and click **Submit**.



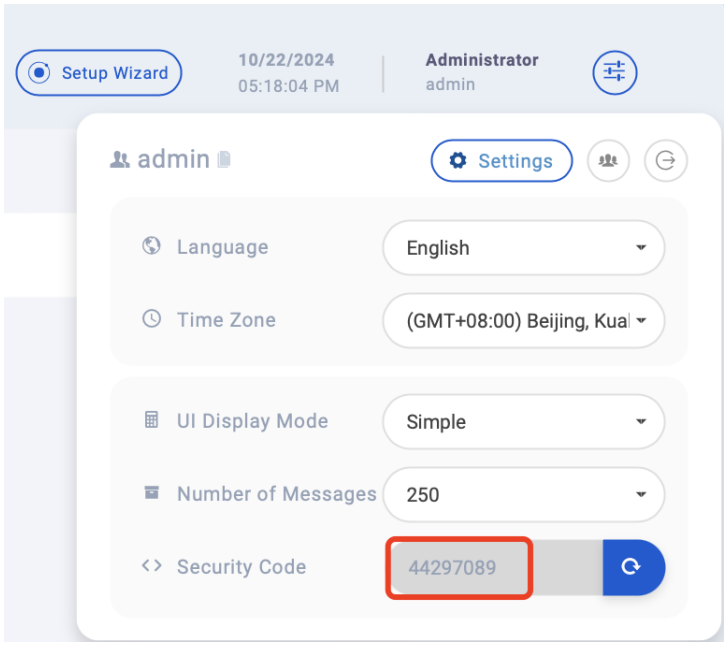
6. Once registered, the source machine will be displayed on the list.



4.1.2 HTTPS Registration

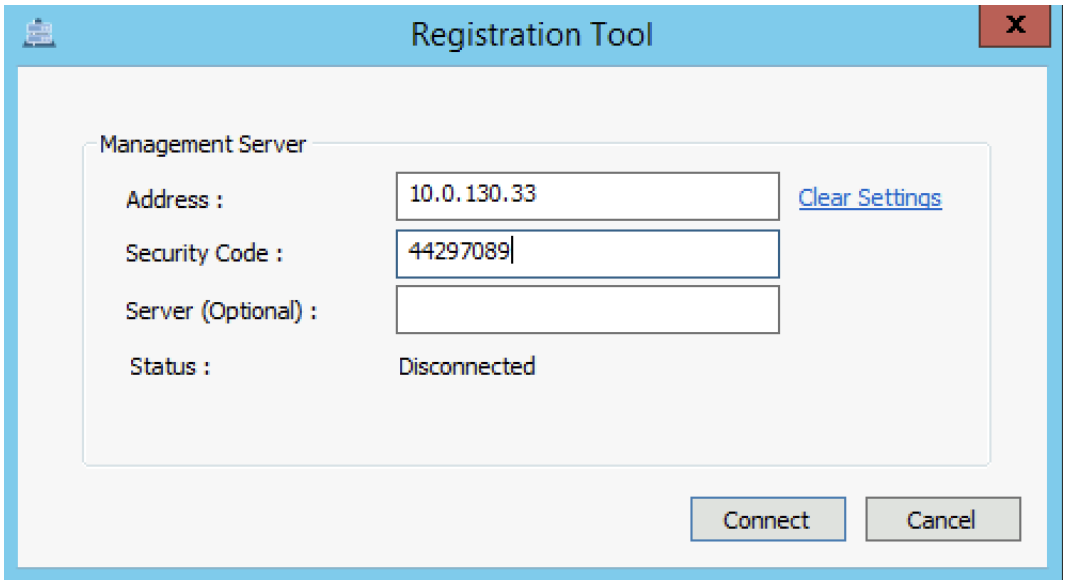
If the Windows source machine with the agent installed lacks a public IP, registration can be initiated through the HTTPS protocol, connecting the source machine to the Management Console.

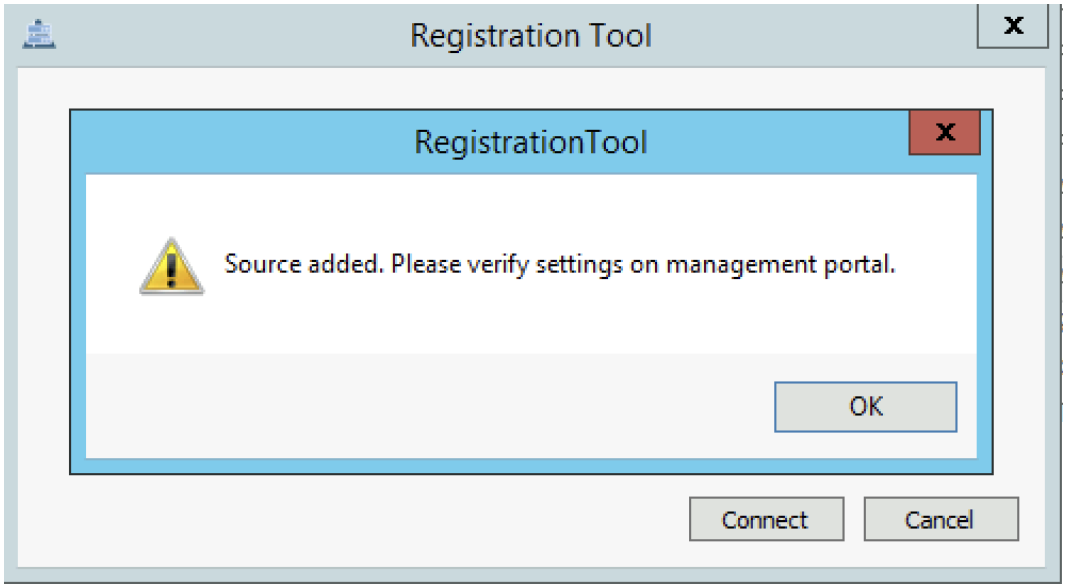
1. Obtain the security code from the **Settings** page located in the top right corner of the Management Console. If a new security code is needed, click the **refresh** icon next to the security code.



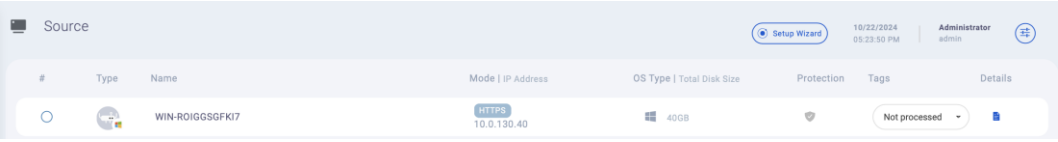
2. Log in to the source machine, locate the source agent installation directory, and click on **RegistrationTool.exe**.

3. Enter the IP address of the Management Console and the security code. If the Management Console port is 20443, append ":20443" to the end of the IP address. Click **Connect** to add the source machine to the Management Console. The registration process should complete within 10 to 30 seconds, depending on the network speed.





4. After registration, refresh the **Source** page of the Management Console to display the newly registered server.



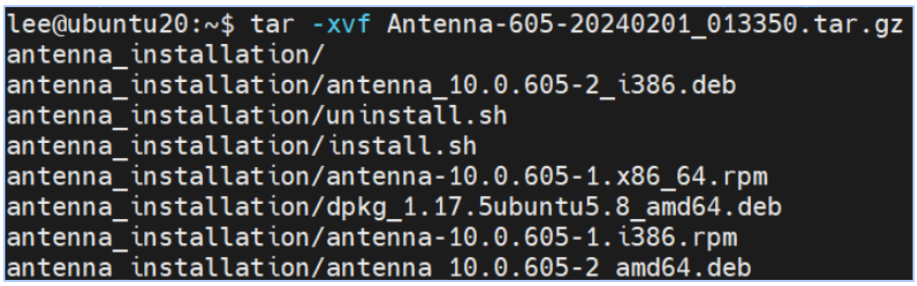
4.2 Linux Agent

The Linux agent is specifically designed for Linux systems. It is responsible for recording IO changes on the source machine and executing synchronization and protetion procedures to the target platform.

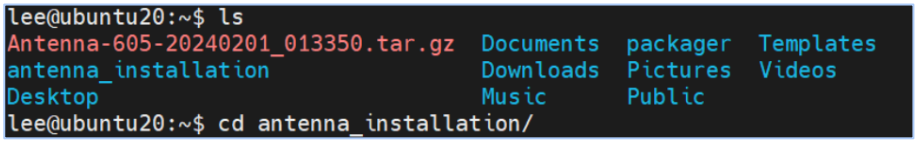
The installation package for Antenna for Linux must match with the source machine's Linux kernel version. To retrieve the correct kernel version, run the command "*uname -r*" on the Linux machine. This information is required for generating the appropriate Linux installation package and should be provided to your technical support contact.

Once you have the installation package, follow the instructions below:

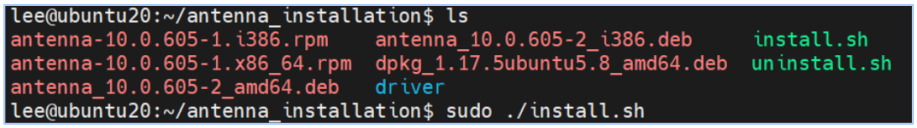
1. Upload the installation package (Antenna-version.releasedate.tar.gz) to the source machine and extract the installation files using the command: **tar -xvf Antenna-xxxxx.tar.gz.**



2. Change the installation directory using the command: **cd antenna_installation/**



3. Execute the command to begin the installation: **./install.sh**.

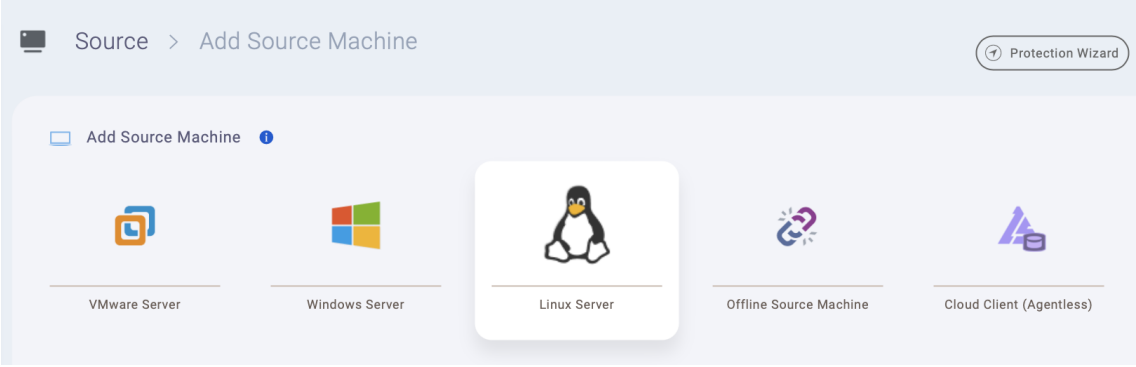


4.2.1 RPC Registration

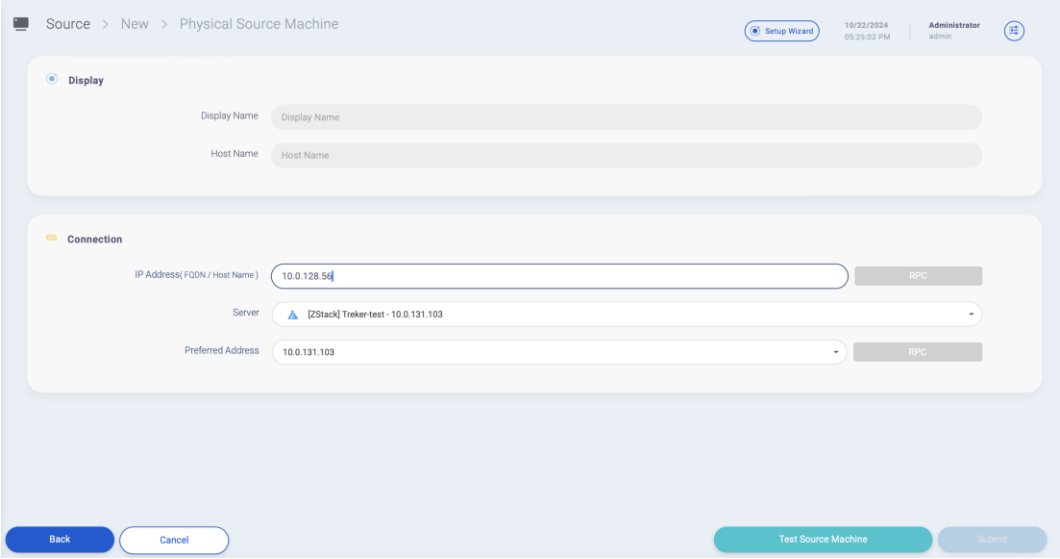
Once the Linux source machine is installed with the source agent, proceed to register it with the Management Console. If the source machine is accessible via a public IP, it can be registered using RPC mode.

1. Under Resources, click **Source** to add a new source machine.

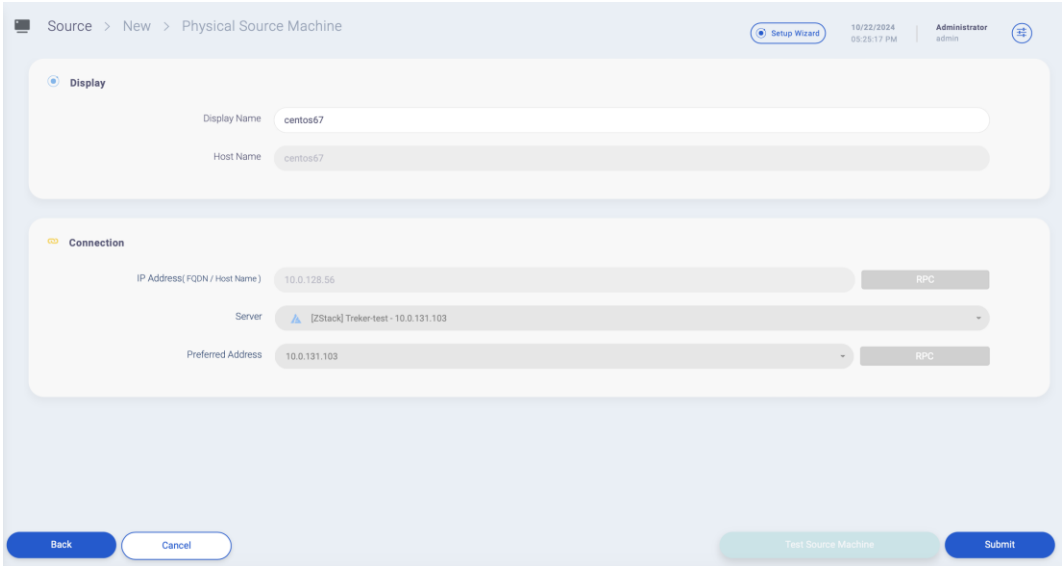
2. For Source Machine Type, select **Linux Server**.



3. Enter the IP address of the source machine where the source agent is installed into the IP address field.



4. Click **Test Source Machine** to verify the connection.

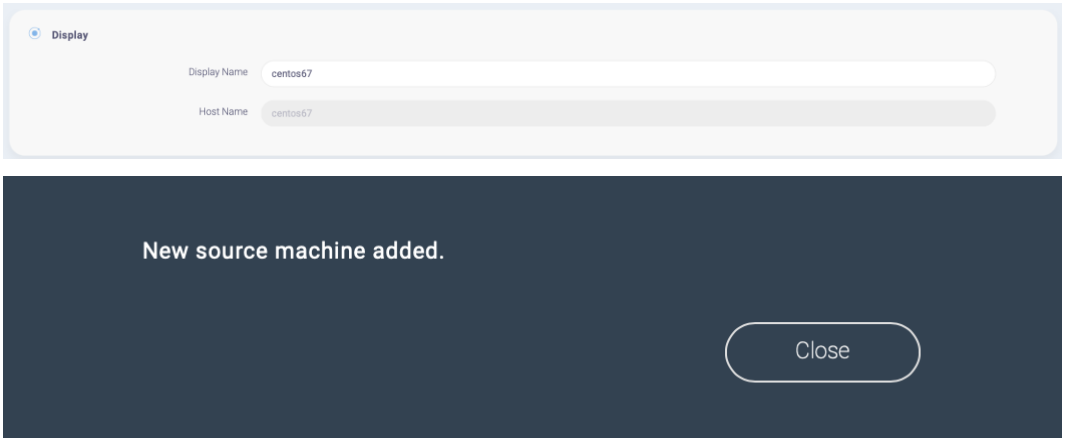


If the verification takes longer than three minutes, please check the following:

- Ensure the source agent is correctly installed on the source machine.
- Verify that the source agent is operating normally.
- Confirm that TCP: 20005 is enabled on the source machine.

After confirming the above, proceed to re-verify.

5. Once verified, options to modify the display name of the source machine will be enabled. Modify as needed and click **Submit**.

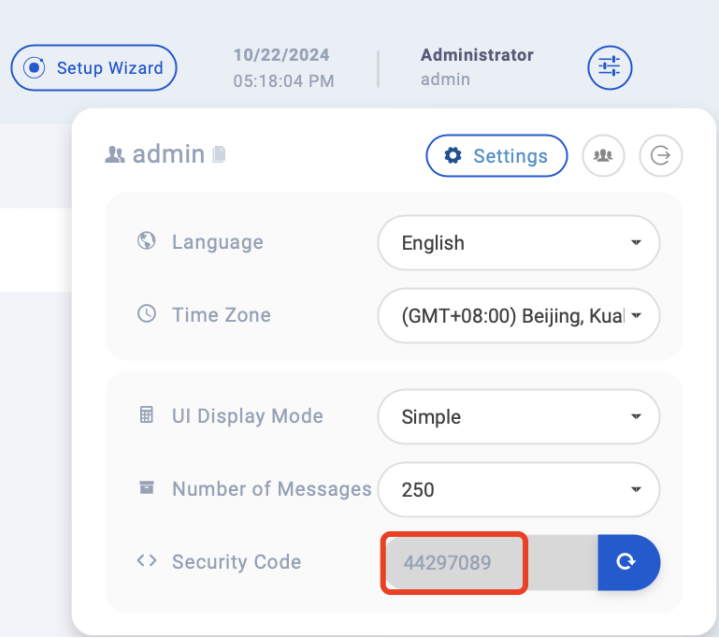


6. Once registered, the source machine will be displayed on the list.

4.2.2 HTTPS Registration

If the Linux source machine with the agent installed lacks a public IP, registration can be initiated through the HTTPS protocol, connecting the source machine to the Management Console.

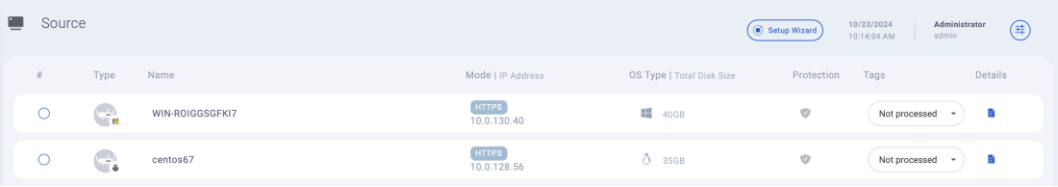
1. Obtain the security code from the **Settings** page located in the top right corner of the Management Console. If a new security code is needed, click the **refresh** icon next to the security code.



2. On the source machine, execute the command to run the registration: **/usr/local/antenna/antenna -t [Console IP] -c [Security Code]**.
   If the Management Console port is 20443, append ":20443" to the end of the IP address.
   For example:
   /usr/local/antenna/antenna -t 10.0.130.33 -c 44297089
   /usr/local/antenna/antenna -t 10.0.130.33:20443 -c 44297089

```
[root@centos67 ~]# /usr/local/antenna/antenna -t 10.0.130.33 -c 44297089
Source added. Please verify settings on management portal.
```

3. On the Source page of the Management Console, after registration, refresh the browser; the new source machine will be displayed.



4.3 VMware Agentless Registration

This section provides step-by-step guidance on adding a VMware platform and registering VMware virtual machines in the console via agentless mode. Before establishing a VMware API connection, ensure the following prerequisites are met:

- Prepare a Windows Treker Server or a Linux CentOS Treker Server in the source VMware environment
- If using vCenter, the Source Server must have connectivity to both vCenter and ESXi.
- Ensure ports 902 and 443 are open for communication with vCenter and ESXi.
- Use an admin account or an account with vStorage permissions and administrative access to the source virtual machines.
- The VMware agentless feature is only applicable to VMware to Cloud and Any to VMware scenarios.
- For more details, please refer to the official VMware documentation.

4.3.1 Register VMware Platform

There are two methods to add the VMware cloud connection.

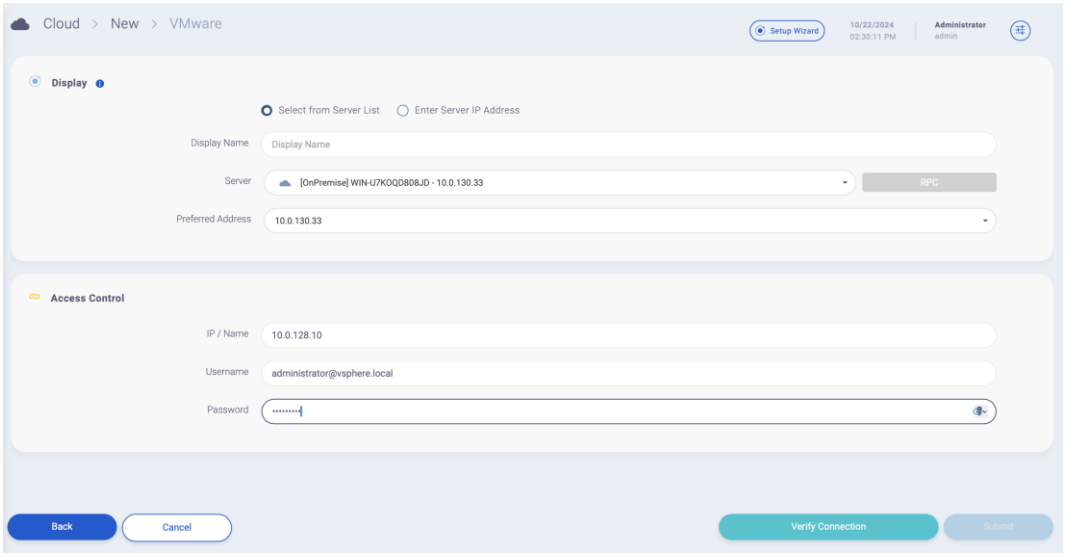
1. Under the Cloud page, click **Add** to create a new cloud connection.

2. Select **VMware** and click **Next**.

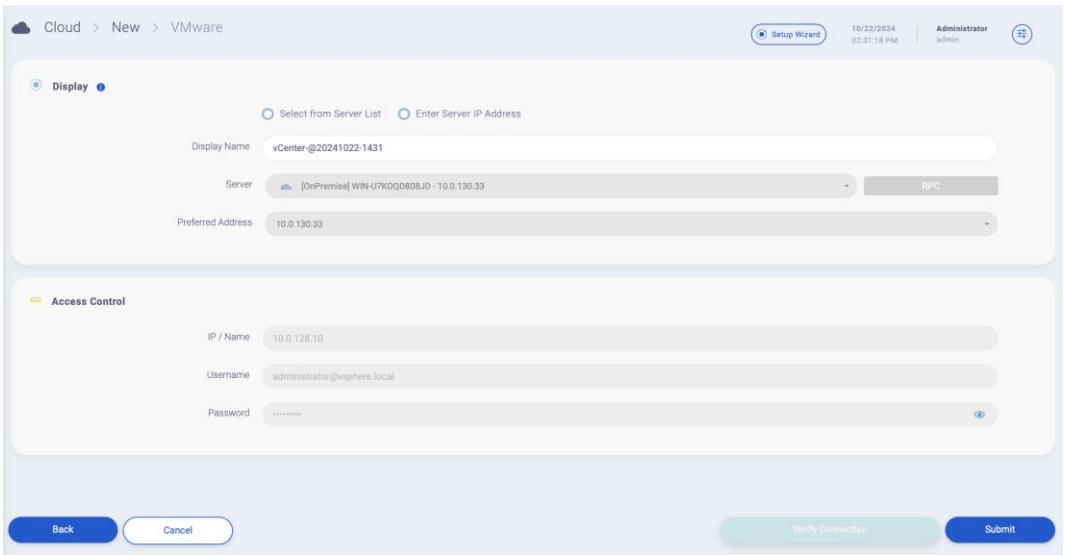
3. There are two methods to add cloud connection.

Method 1: Select from Server List

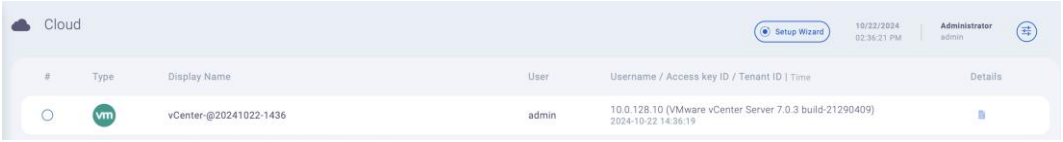
a) Choose Select from Server List and enter the ESXi IP/Name, ESXi Username, and ESXi Password, then click **Verify Connection**.



b) Once the verification is successful, click on **Submit** to save the settings.

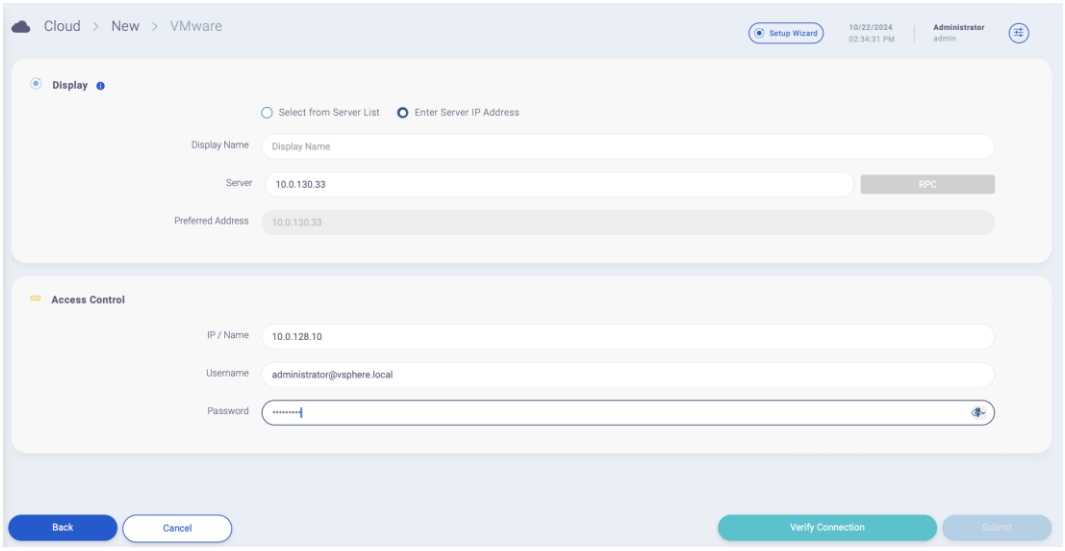


c) Once registered, the new VMware cloud connection will be displayed.

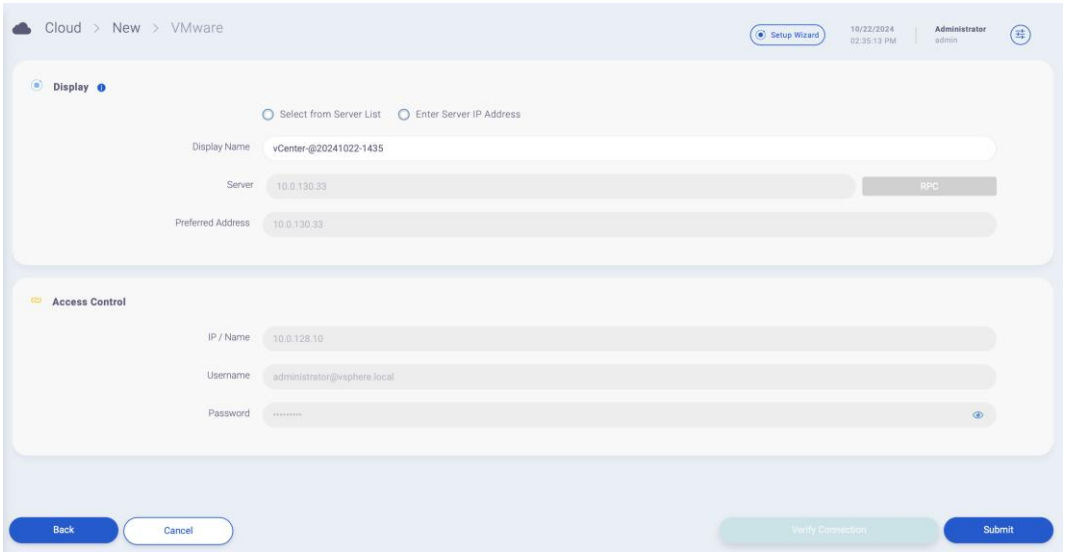


Method 2: Enter Server IP Address

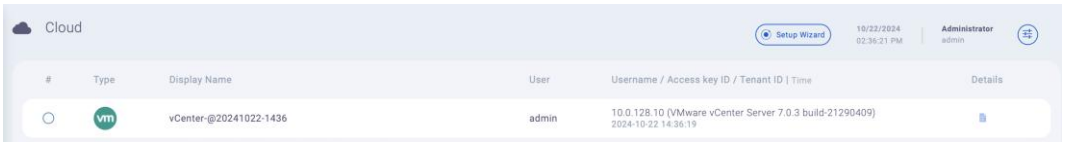
a) Choose Enter Server IP Address and enter the ESXi IP/Name, ESXi Username, and ESXi Password, then click **Verify Connection**.



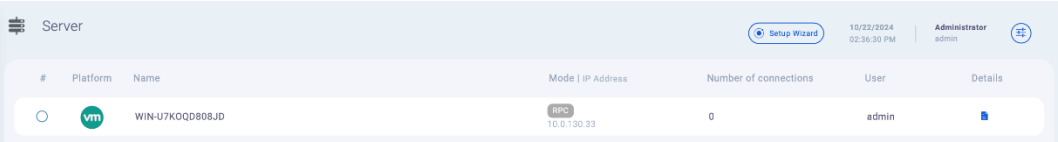
b) Once the verification is successful, click on **Submit** to save the settings.



c) Once registered, the new VMware cloud connection will be displayed.



4. Servers deployed under the registered VMware connection will be automatically added to the Management Console.



4.3.2 Register VMware VM

To deploy a disaster recovery scheme on a VMware virtual machine, select it as the source client for synchronization and protection tasks.

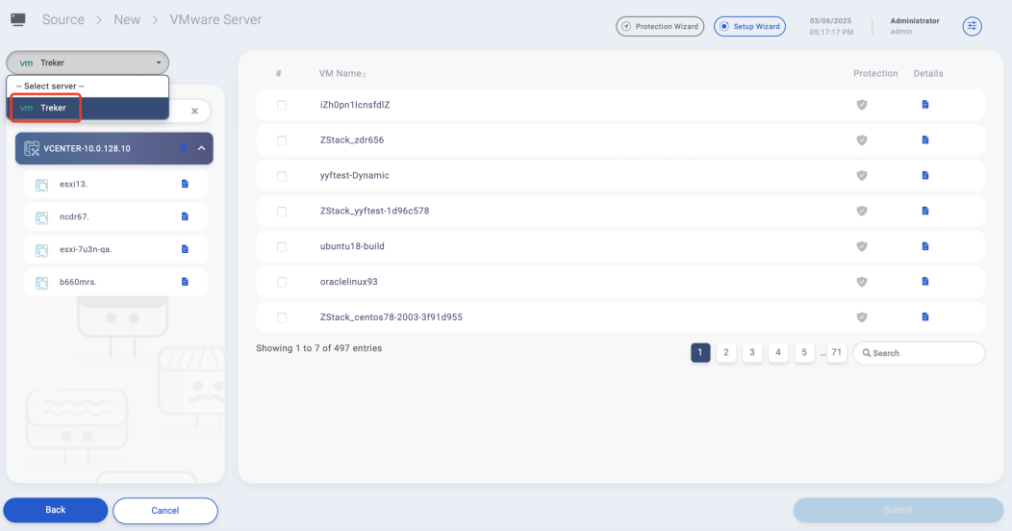
If planning to install an agent on the source VM, ensure a snapshot is taken beforehand. This allows quick rollback if issues arise.

Best Practice: Custom Naming for Source Hosts

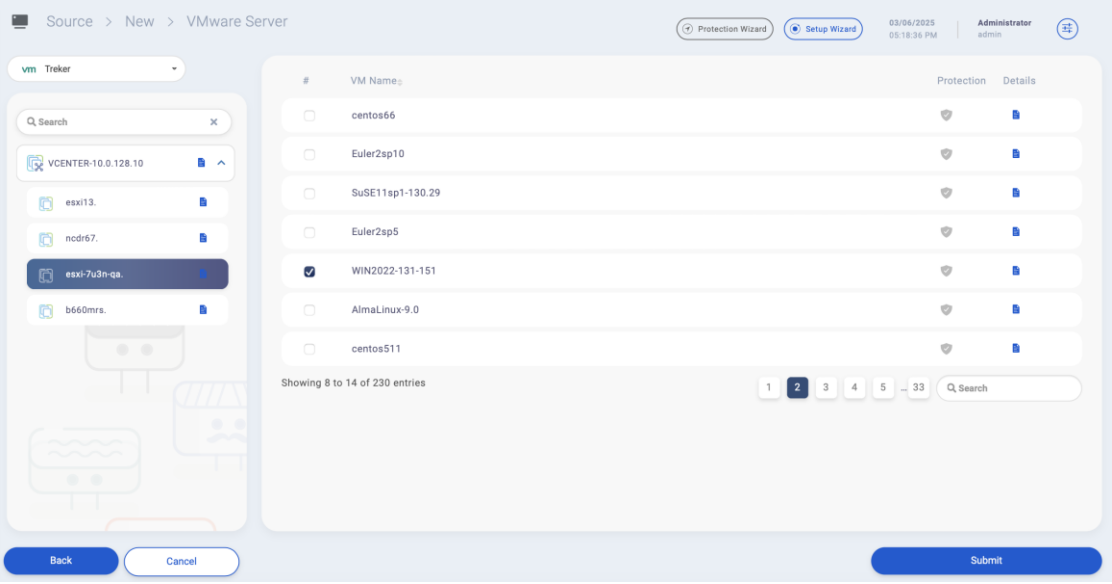
- It is recommended to customize the name of the registered source host.
- Append the IP address to the display name to maintain clarity.
- The migration display name will inherit the custom name of the source host.
- Example: *hostname.0.11*

1. Under **Resources**, select **Source** to add a new source machine. Choose **VMware Server** as the source machine type.

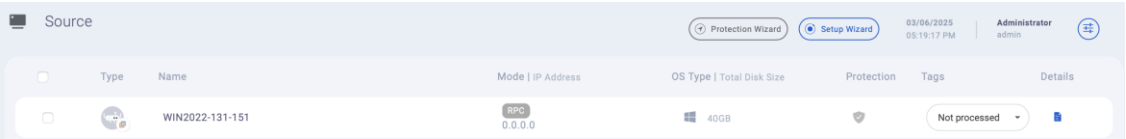
2. Choose the ESXi server from the drop-down list.



3. Select the desired virtual machine to register. Alternatively, enter a keyword to search for the VM. Choose the virtual machine to add and click **Submit**.



4. Once registered, the new source virtual machine will be displayed.

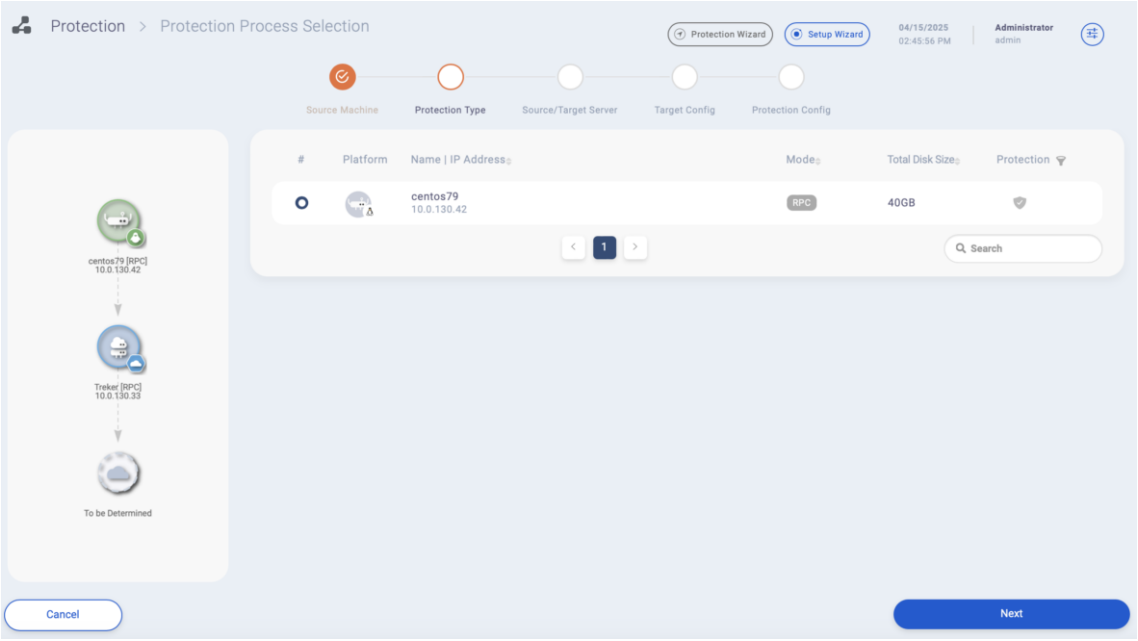


5 Create Protection Process

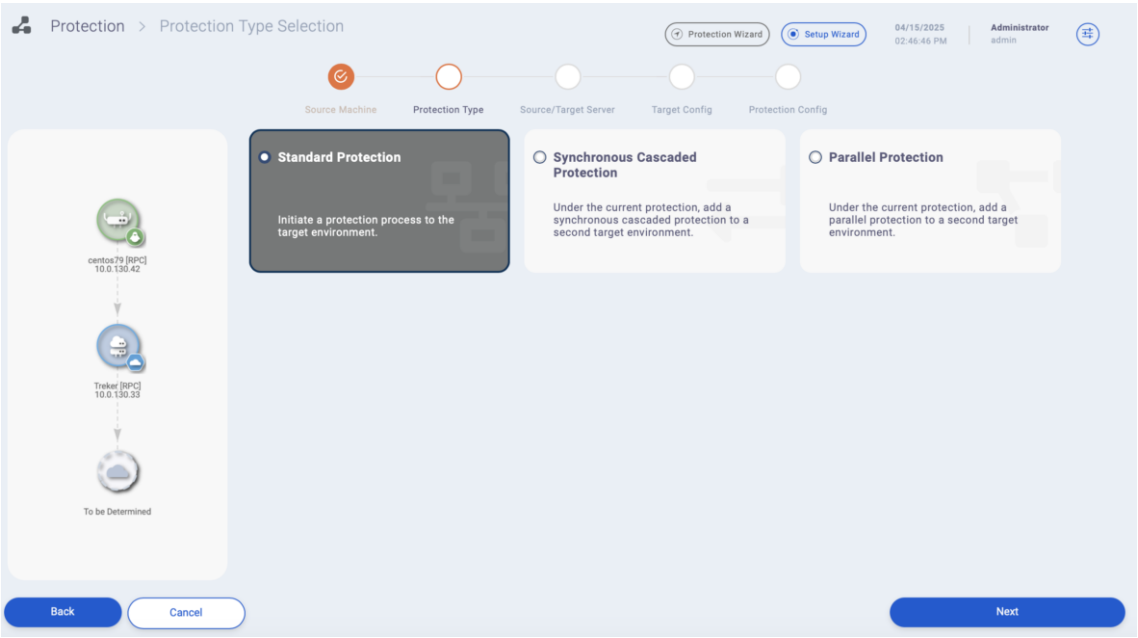
5.1 Architecture 1: Image Mode with Proxy Server

1. In the left-hand menu, click **Protection** and **Add**.

2. Select the source machine to protect and click **Next**.

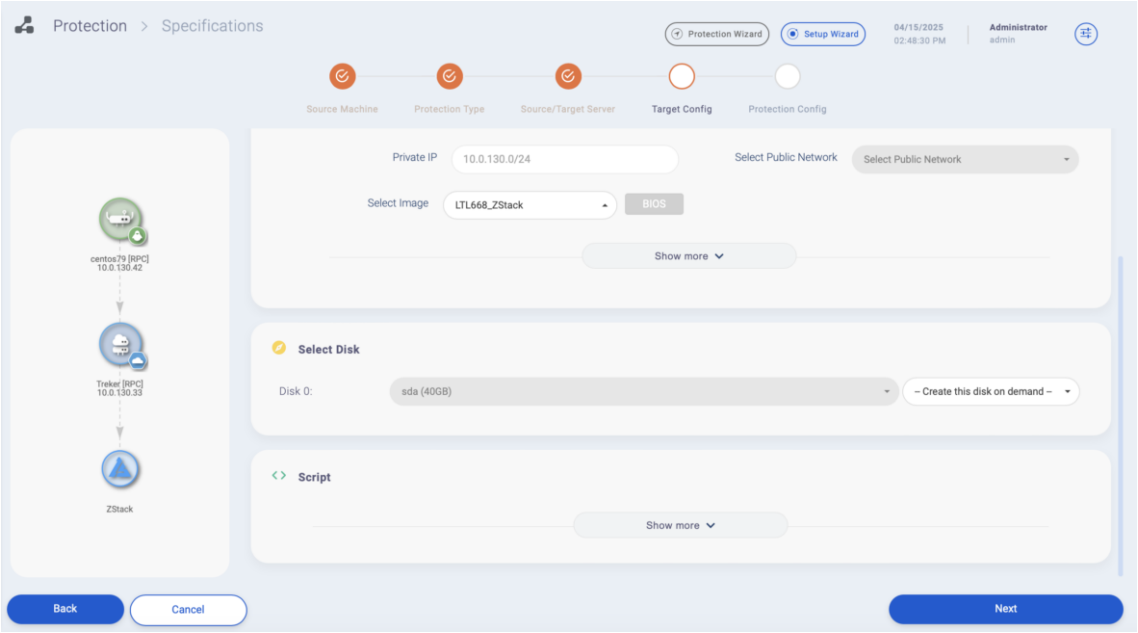


3. Choose the protection type: **Standard Protection**.

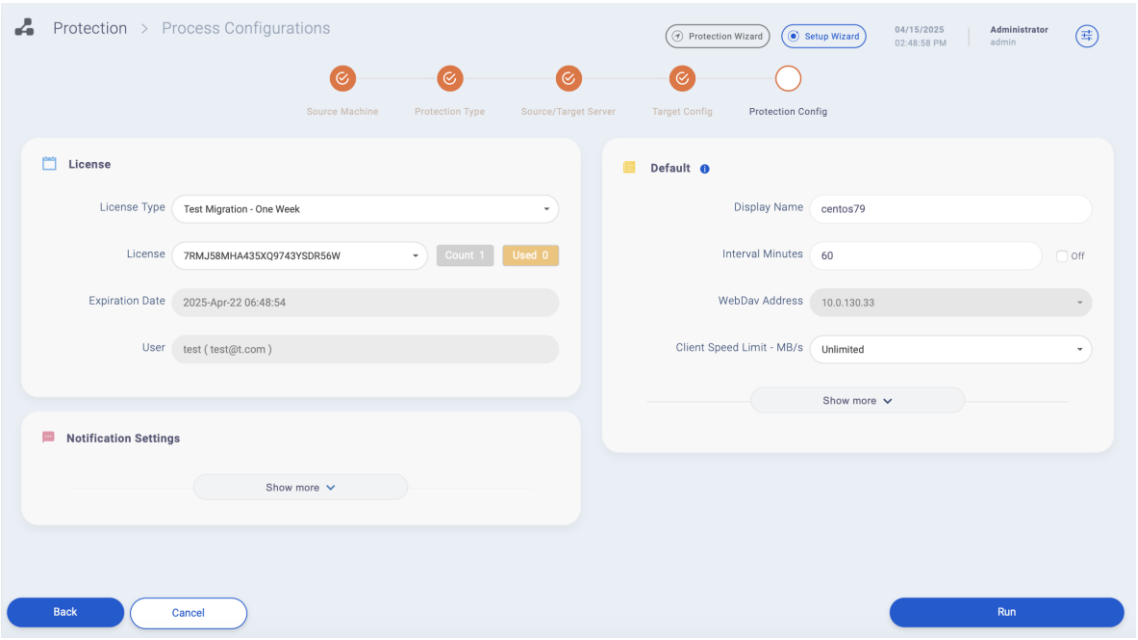


4. Select the Source and Target Server. For “Target Server”, choose the corresponding NexaVM target. If a Source Server was already bound during source machine registration, its IP address will be automatically displayed as the default Source Server.
5. Configure the target settings, including the NexaVM zone and primary storage for the source machine. Then specify the network, security group, image, CPU, memory, and replica storage type.

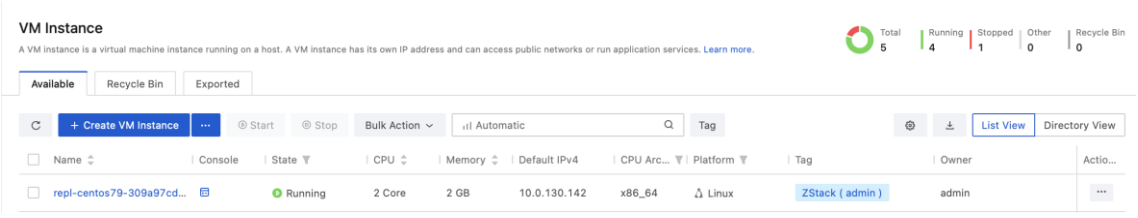
6. Select the disks to be protected.



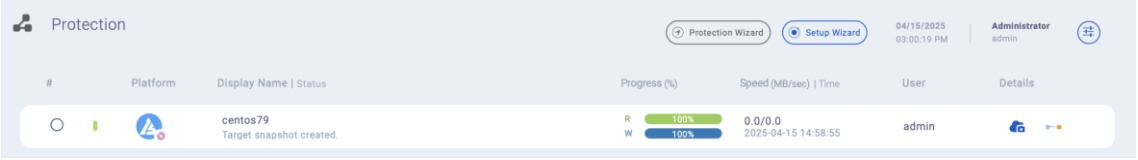
7. Configure the protection policy by selecting a license and optionally setting a custom name, synchronization frequency (in minutes), and the number of snapshots to retain. If the sync frequency is disabled, the system will perform only a one-time full protection. Disabling the snapshot count option will prevent any snapshots from being created. Click **Run** to initiate the protection process.



8. The target instance created from the image will appear in the NexaVM platform。

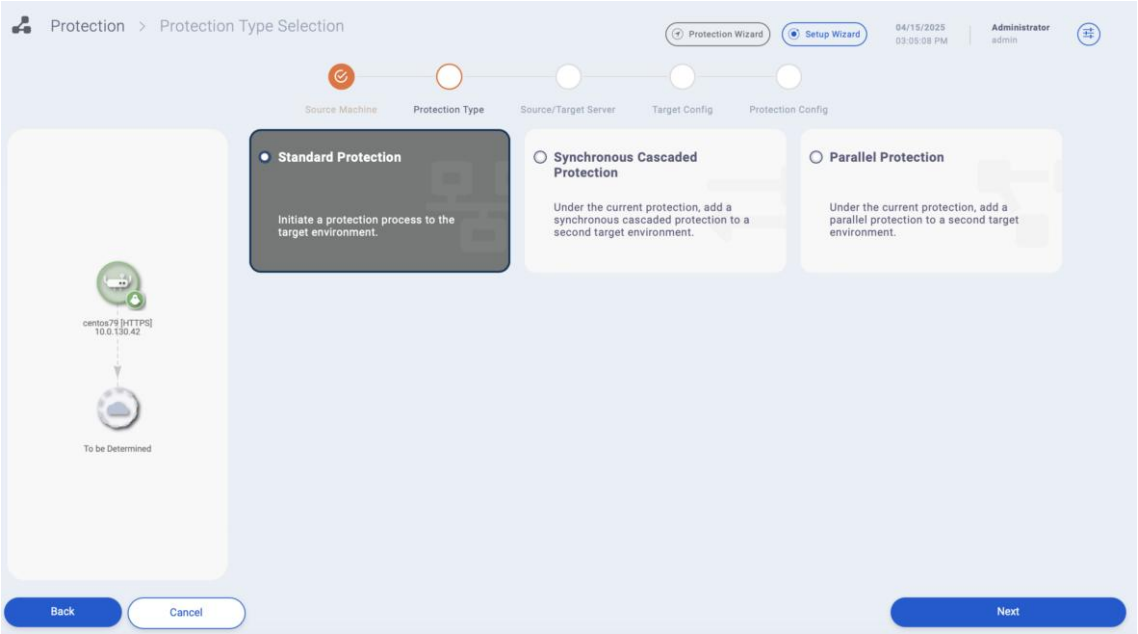


9. After synchronization is complete, the status displays: "Target snapshot created."

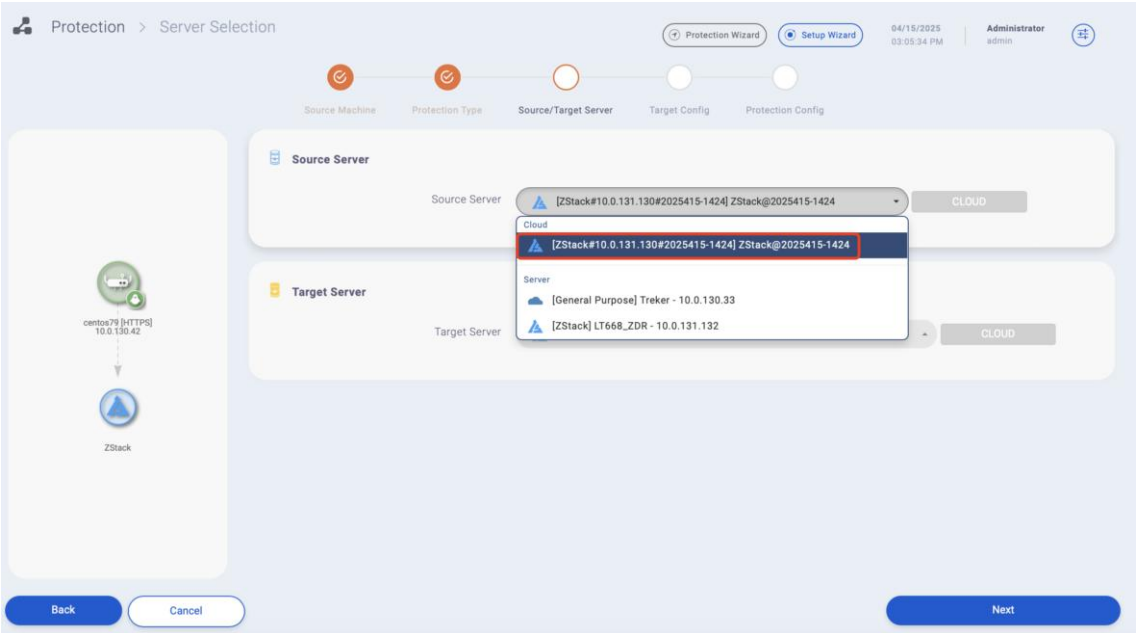


5.2 Architecture 2: Image Mode without Proxy Server

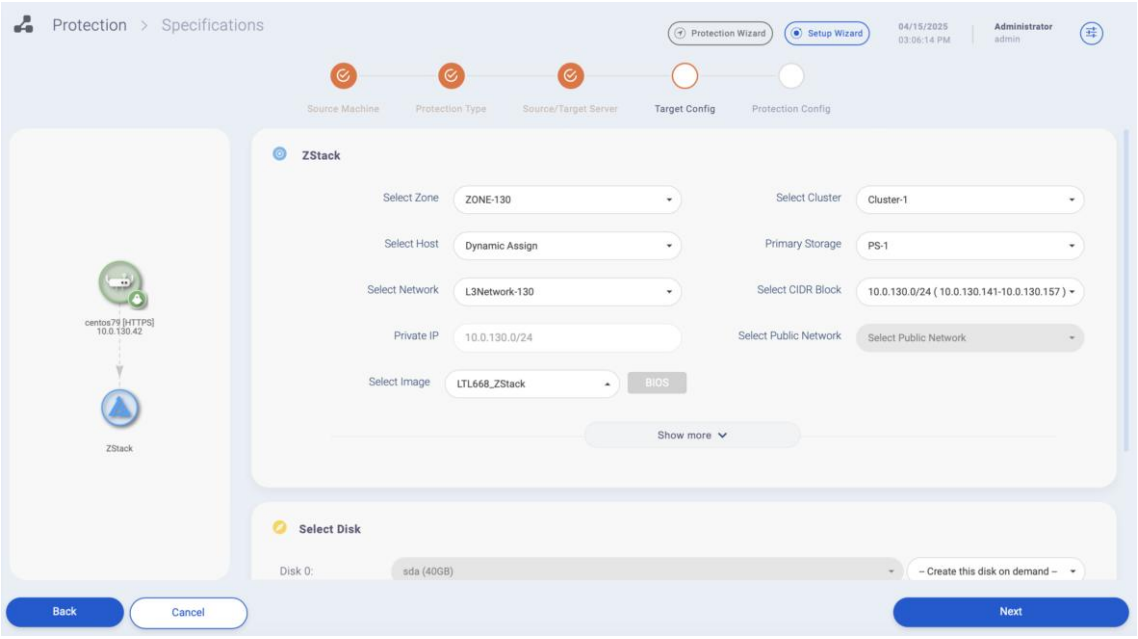
1. In the left-hand menu, click **Protection** and **Add**.
2. Select the source machine to protect and click **Next**.
3. Choose the protection type: **Standard Protection**.



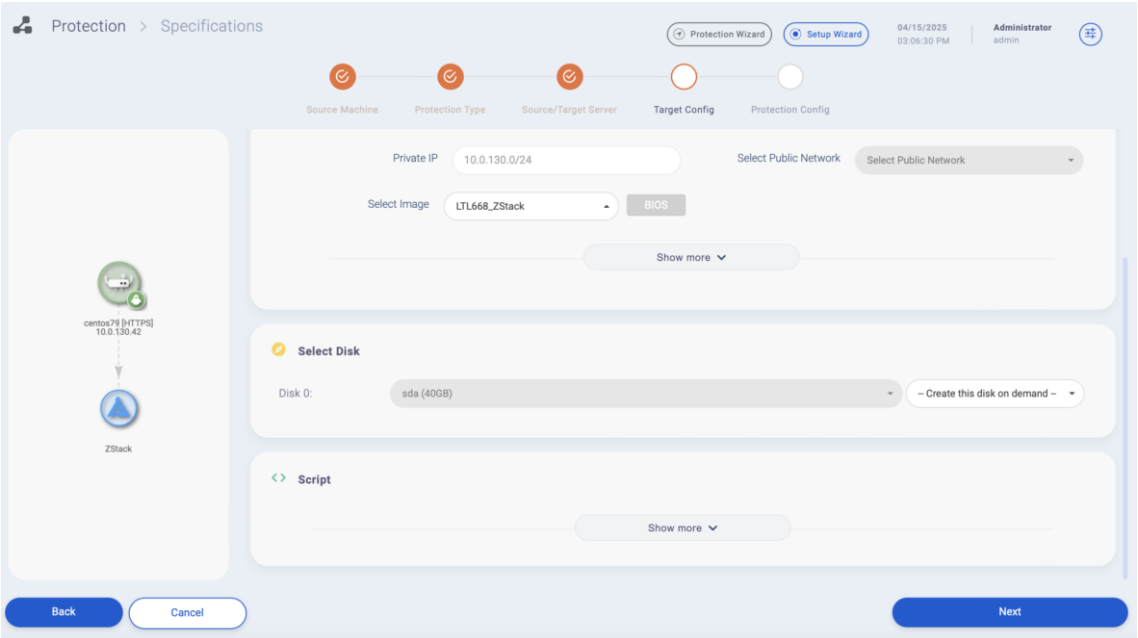
4. Select the Source and Target Server. Since no source server is deployed, select the target server deployed on NexaVM for both fields.



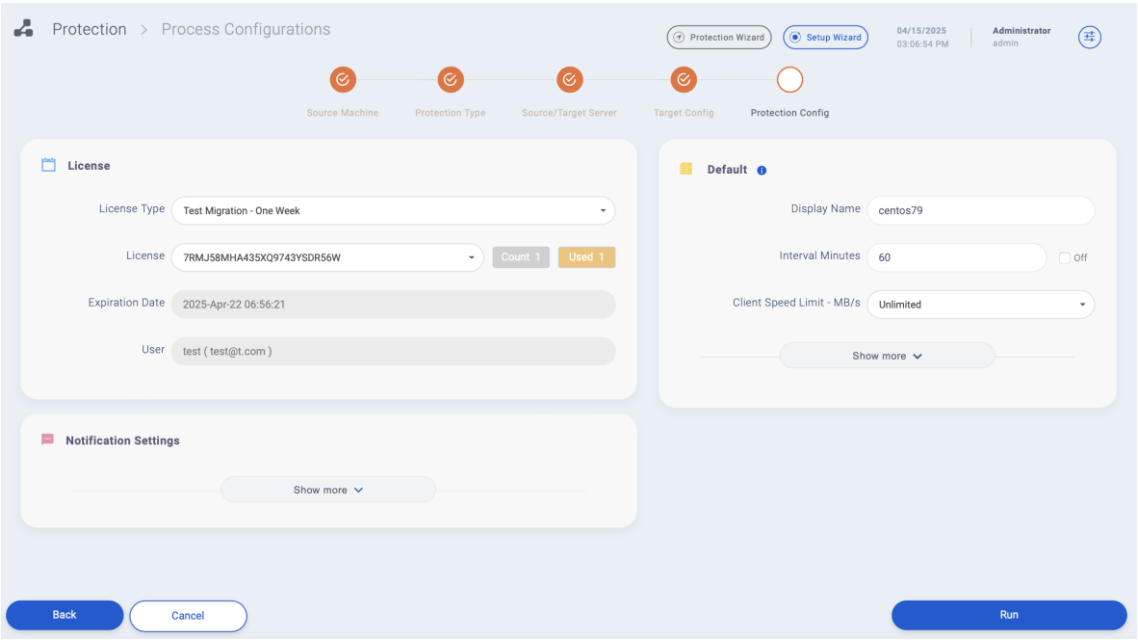
5. Configure the target settings, including the NexaVM zone and primary storage for the source machine. Then specify the network, security group, image, CPU, memory, and replica storage type.



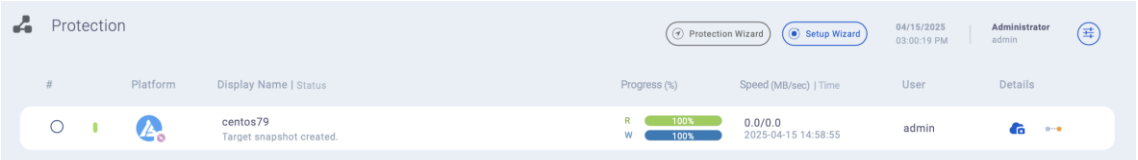
6. Select the disks to be protected.



7. Configure the protection policy by selecting a license and optionally setting a custom name, synchronization frequency (in minutes), and the number of snapshots to retain. If the sync frequency is disabled, the system will perform only a one-time full protection. Disabling the snapshot count option will prevent any snapshots from being created. Click **Run** to initiate the protection process.

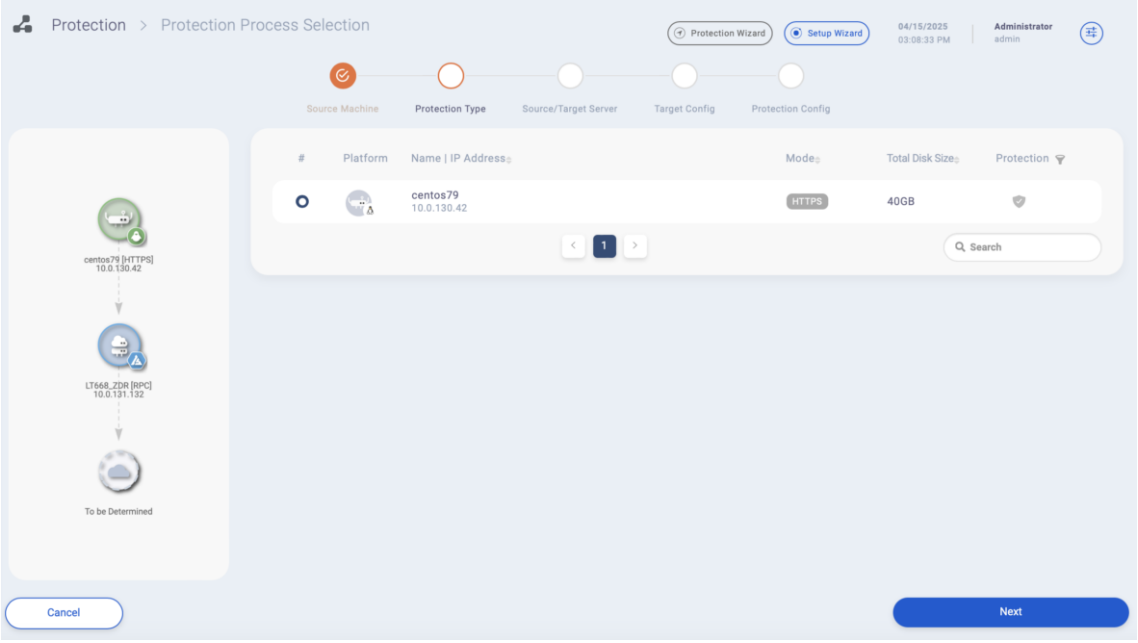


8. After synchronization is complete, the status displays: "Target snapshot created."

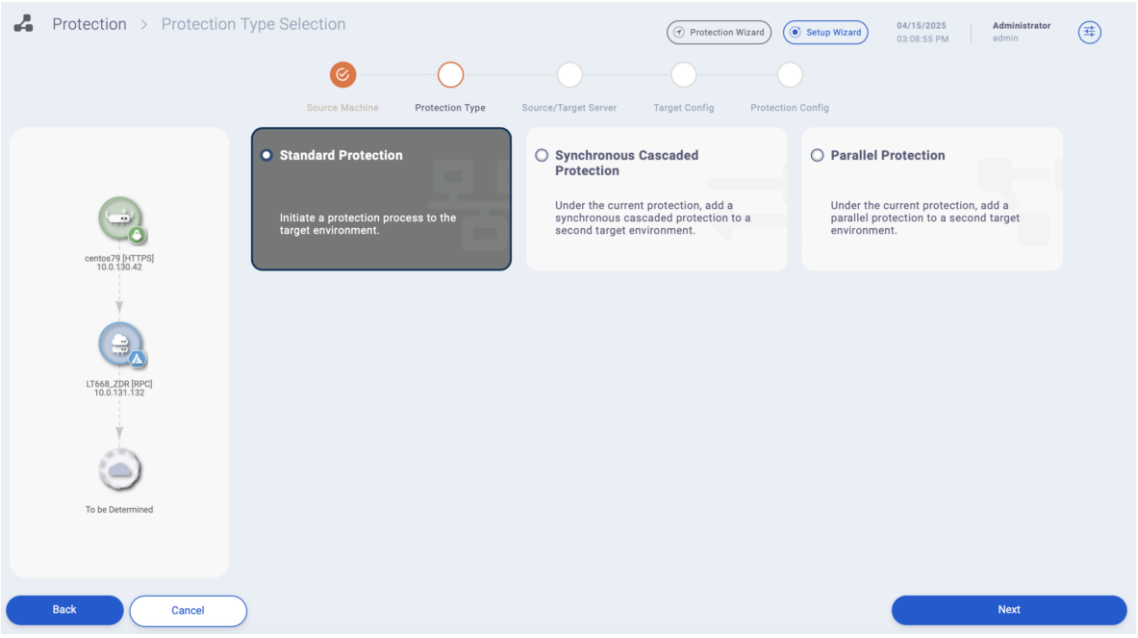


5.3 Architecture 3: Disk-to-Disk Mode without Proxy Server

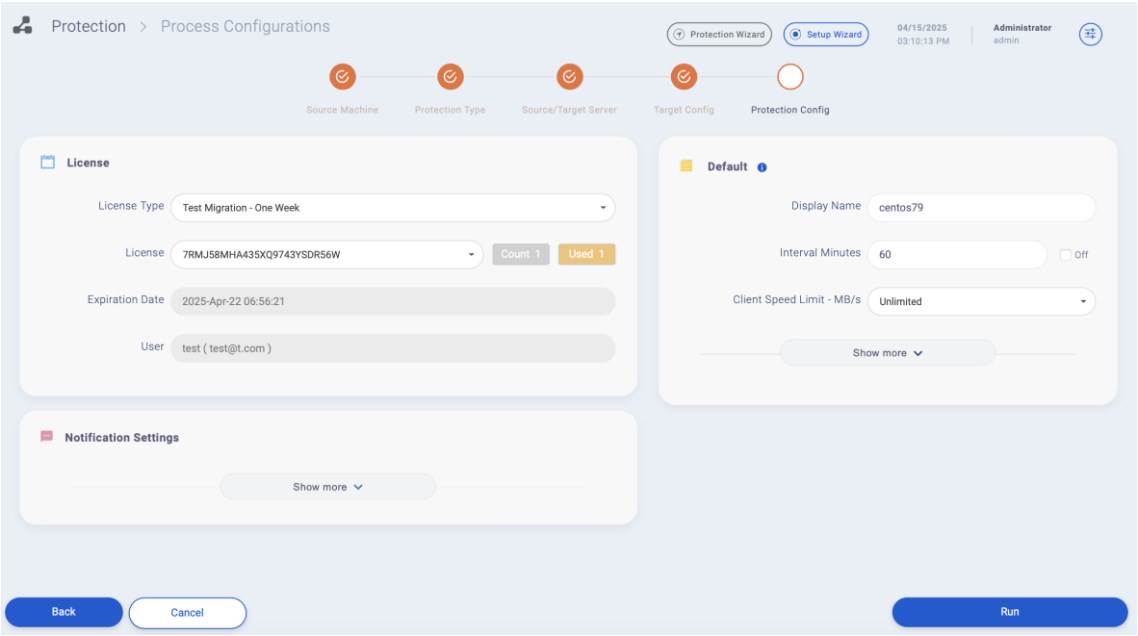
1. Click **Source**, select the added source machine, then click **Edit**. For the corresponding Server, select the one registered via the NexaVM Target.
2. Click to verify the client connection, if successful, click **Update**.
3. In the left-hand menu, click **Protection** and **Add**. Select the source machine to protect and click **Next**.



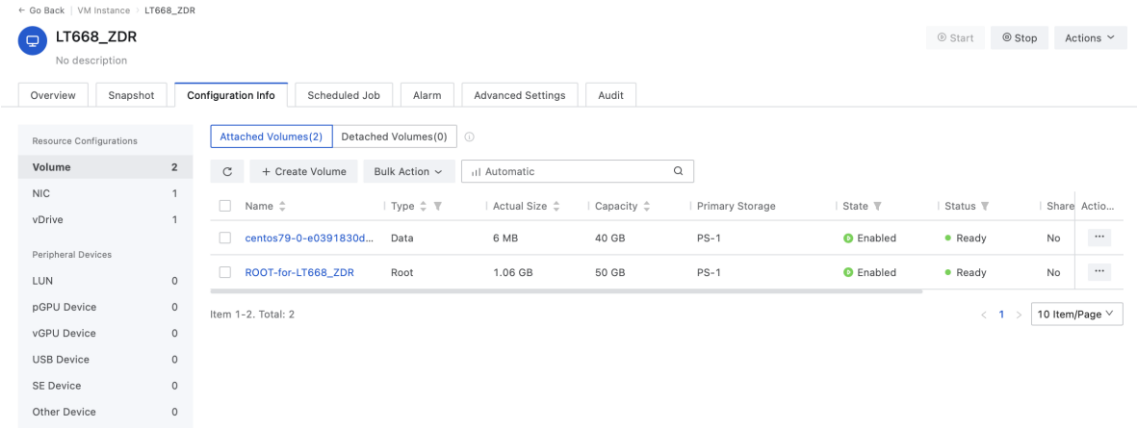
4. Choose the protection type: **Standard Protection**.



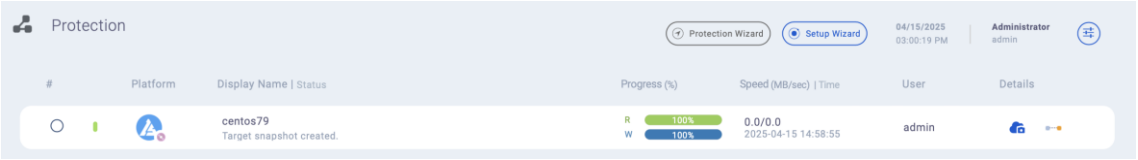
5. Select the Source and Target Server. Since no source server is deployed, select the target server deployed on NexaVM for both fields.
6. Configure the target settings, including the NexaVM zone and primary storage for the source machine. Then specify the network, security group, image, CPU, memory, and replica storage type. Select the disks to be protected.
7. Configure the protection policy by selecting a license and optionally setting a custom name, synchronization frequency (in minutes), and the number of snapshots to retain. If the sync frequency is disabled, the system will perform only a one-time full protection. Disabling the snapshot count option will prevent any snapshots from being created. Click **Run** to initiate the protection process.



8. The target server configuration in the NexaVM platform will display the mounted data disks, with both size and quantity matching those of the source machine

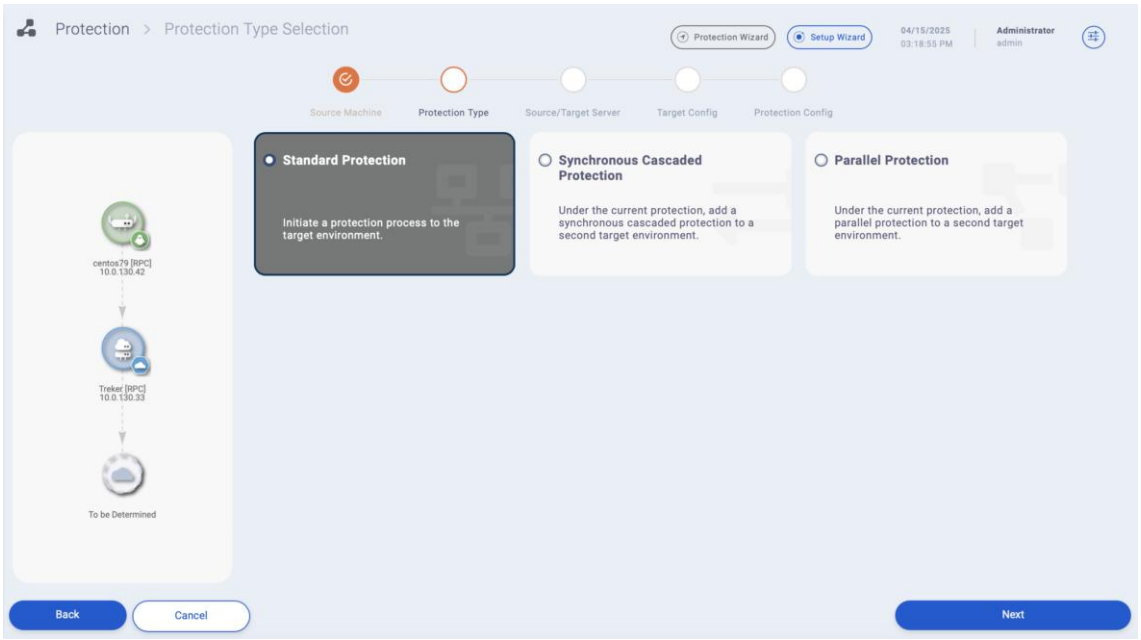


9. After synchronization is complete, the status displays: "Target snapshot created.”



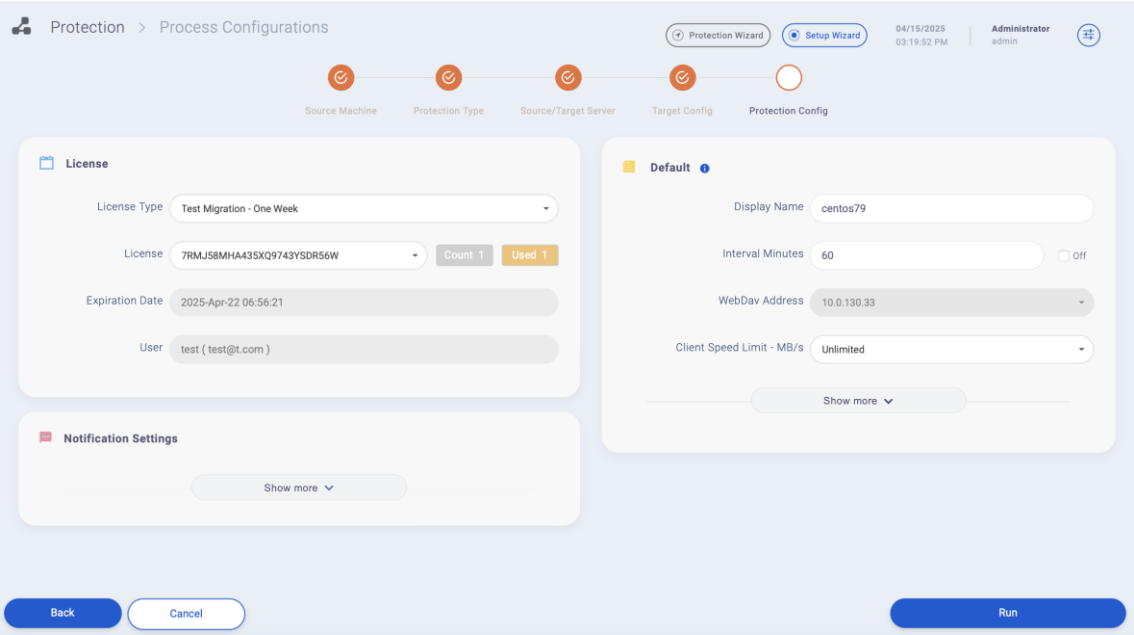
5.4 Architecture 4: Disk-to-Disk Mode with Proxy Server

1. Click **Source**, select the added source machine, then click **Edit**. For the corresponding Server, select the standard server registered for source proxy purpose.
2. Click to verify the client connection, if successful, click **Update**.
3. In the left-hand menu, click **Protection** and then **Add**. Select the source machine to protect and click **Next**.
4. Choose the protection type: **Standard Protection**.

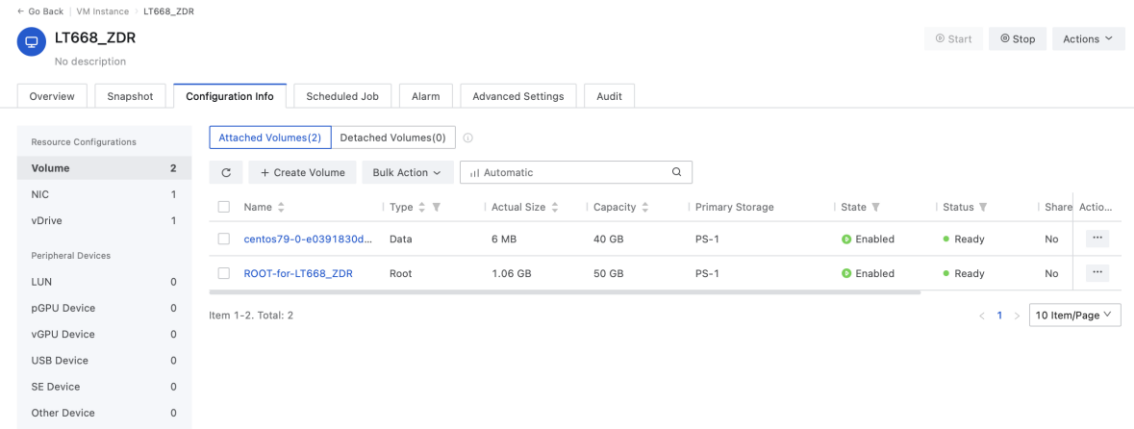


5. Define the protection route by selecting the Source and Target Server. For “Target Server”, choose the corresponding NexaVM target.
6. Configure the target settings, including the NexaVM storage type and select the source disks to be protected.

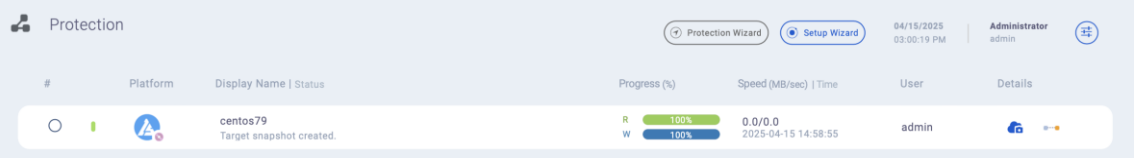
7. Configure the protection policy by selecting a license and optionally setting a custom name, synchronization frequency (in minutes), and the number of snapshots to retain. If the sync frequency is disabled, the system will perform only a one-time full protection. Disabling the snapshot count option will prevent any snapshots from being created. Click **Run** to initiate the protection process



8. The target server configuration in the NexaVM platform will display the mounted data disks, with both size and quantity matching those of the source machine



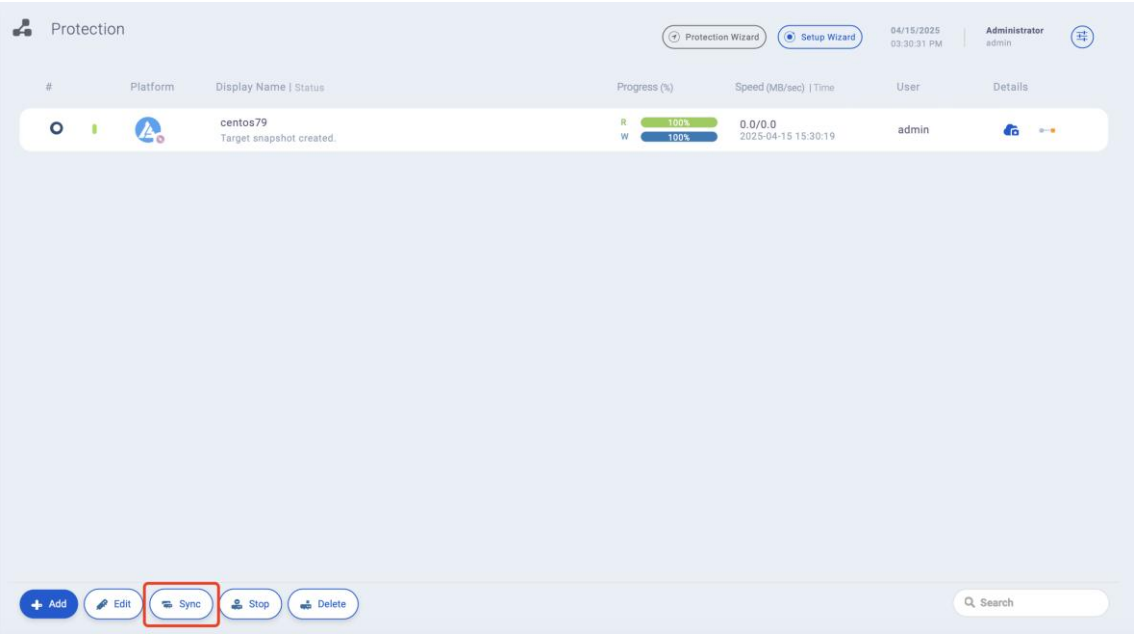
9. After synchronization is complete, the status displays: "Target snapshot created."



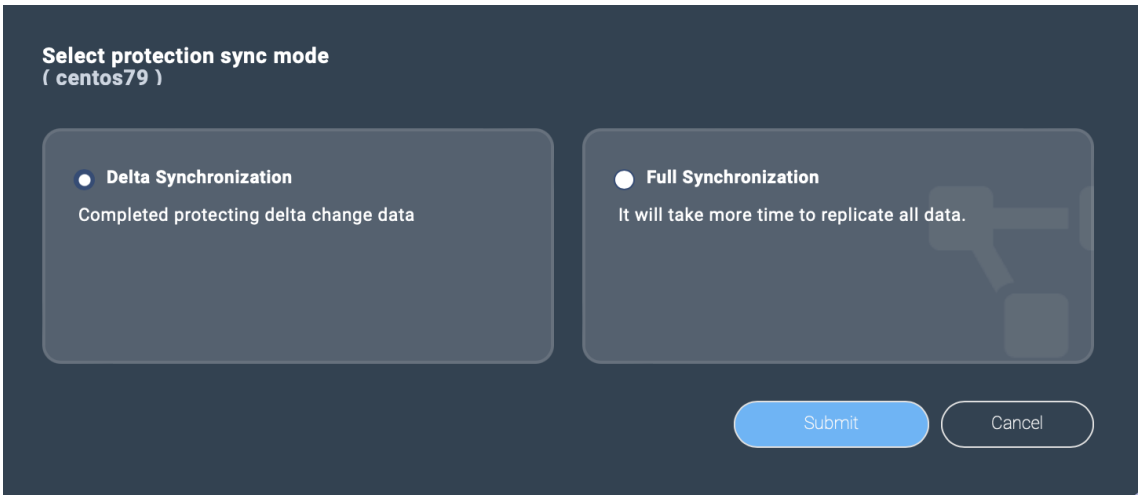
5.5 Delta Synchronization

After the first full protection from the source machine to the target platform, the system will perform synchronization based on the scheduled interval time. To manually trigger an incremental sync, follow these steps:

1. On the **Protection** page, select the process to perform delta synchronization and click **Sync**.



2. Choose **Delta Synchronization** and click **Submit**.



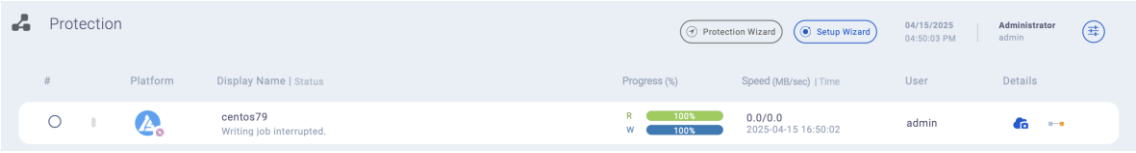
6 Create Provisioning Process

NDR offers four provisioning modes, each tailored to different disaster recovery scenarios:

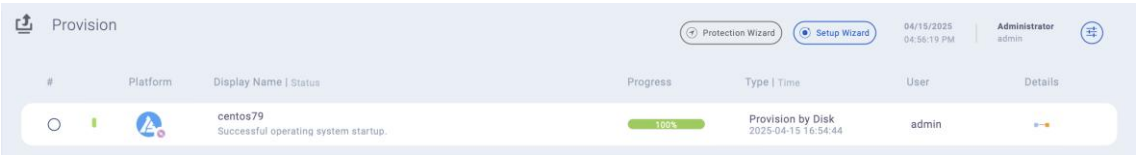
- **Provision by Disk** provisions the target instance directly using the protected system and data disks without creating additional disks, avoiding redundant resource usage. Before execution, the associated protection process is suspended to prevent further synchronization writes to the target disk undergoing system conversion. This mode is optimal for rapid cutover using the most up-to-date data.
- **Provision by Snapshot** initiates a new target instance using a selected target snapshot of the source machine. Users are prompted to choose a specific snapshot time point to generate new system and data disks. The associated protection task will be suspended during this operation to ensure data consistency.
- **DevTest by Snapshot** is intended for pre-cutover validation. A temporary test instance is created from a selected target snapshot, allowing verification of system functionality and necessary configuration adjustments before formal cutover. This mode operates without interrupting the active protection process and supports repeated testing without affecting ongoing data protection
- **File Access** enables quick access to individual files from protected disks through a web-accessible interface launched by a temporary instance. Users can browse the protected file structure, download specific files or folders, and access data via CIFS and NFS protocols. This mode is ideal for file-level recovery without provisioning a full server.

6.1 Provision by Disk

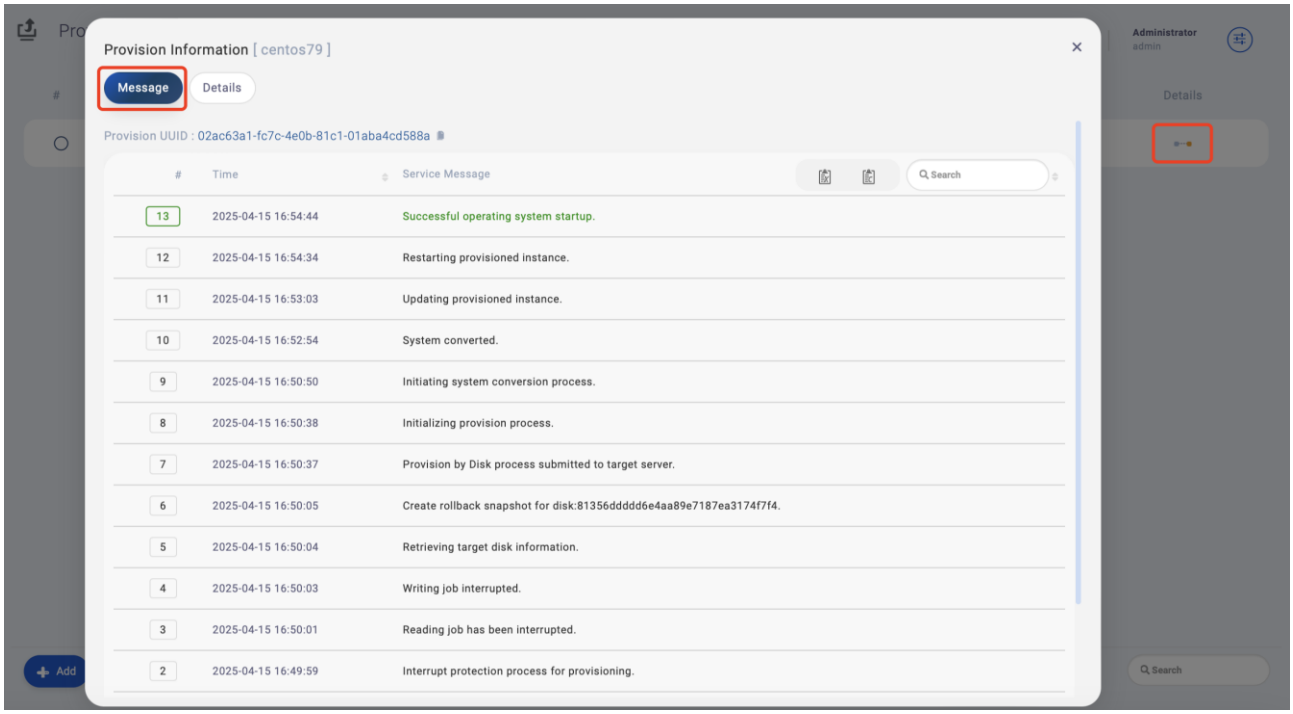
1. Within the left-hand menu, click on Provision and then **Add**. Select the protection process for provisioning.
2. Select the provisioning type: **Provision by Disk**.
3. Choose the disk from which to provision.
4. Configure the CPU, memory, and security group settings for the target instance.
5. Specify network configuration details for the instance, including IP address, subnet mask, gateway, and DNS server. Click **Submit** to proceed.
6. After clicking Submit, the provisioning process will initiate, and the task progress will be displayed. In Provision by Disk mode, the related protection process will be interrupted to ensure synchronization consistency



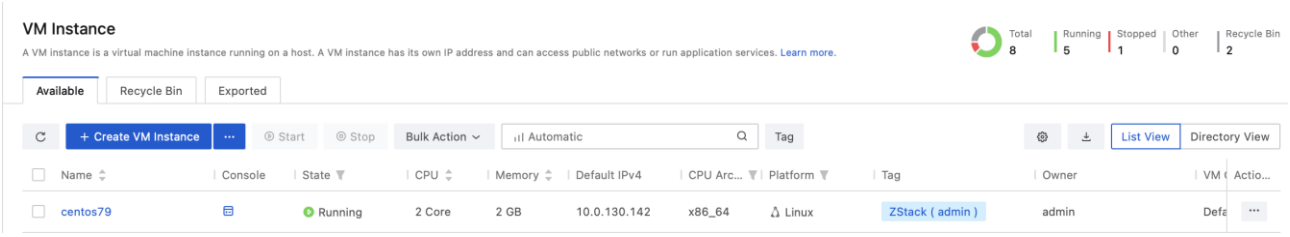
7. When the provisioning completes, the process status will be updated accordingly.



8. Click the **Details** button and select **Message** to view detailed logs of the provisioning process.

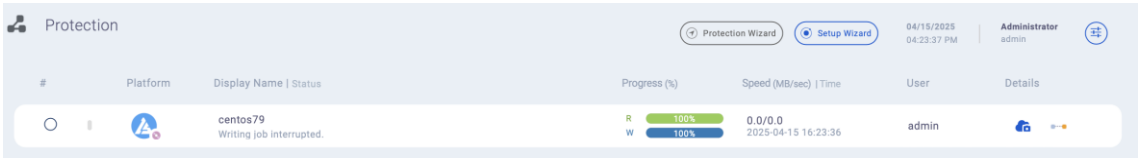


9. Click the **Details** tab to view the timeline, topology, associated Server, and detailed provisioning settings. The topology provides a visual representation of the data path between the protection and provisioning processes.
10. Log in to the NexaVM platform to verify that the target instance has been successfully created.

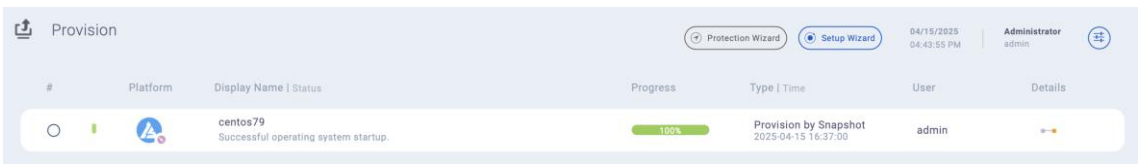


6.2 Provision by Snapshot

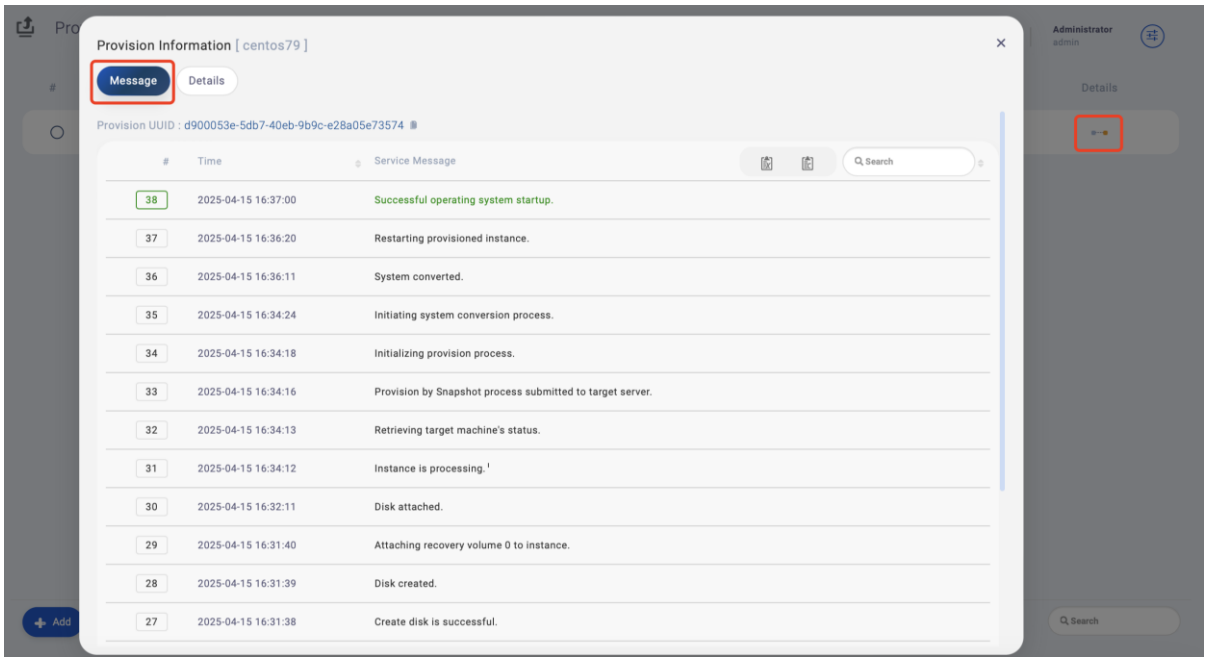
1. Within the left-hand menu, click on **Provision** and then **Add**. Select the protection process for provisioning.
2. Select the provisioning type: **Provision by Snapshot**.
3. Choose the disk snapshot time point from which to provision.
4. Configure the CPU, memory, and security group settings for the target instance.
5. Specify network configuration details for the instance, including IP address, subnet mask, gateway, and DNS server. Click **Submit** to proceed.
6. After clicking Submit, the provisioning process will initiate, and the task progress will be displayed. In Provision by Snapshot mode, the related protection process will be interrupted to ensure synchronization consistency.



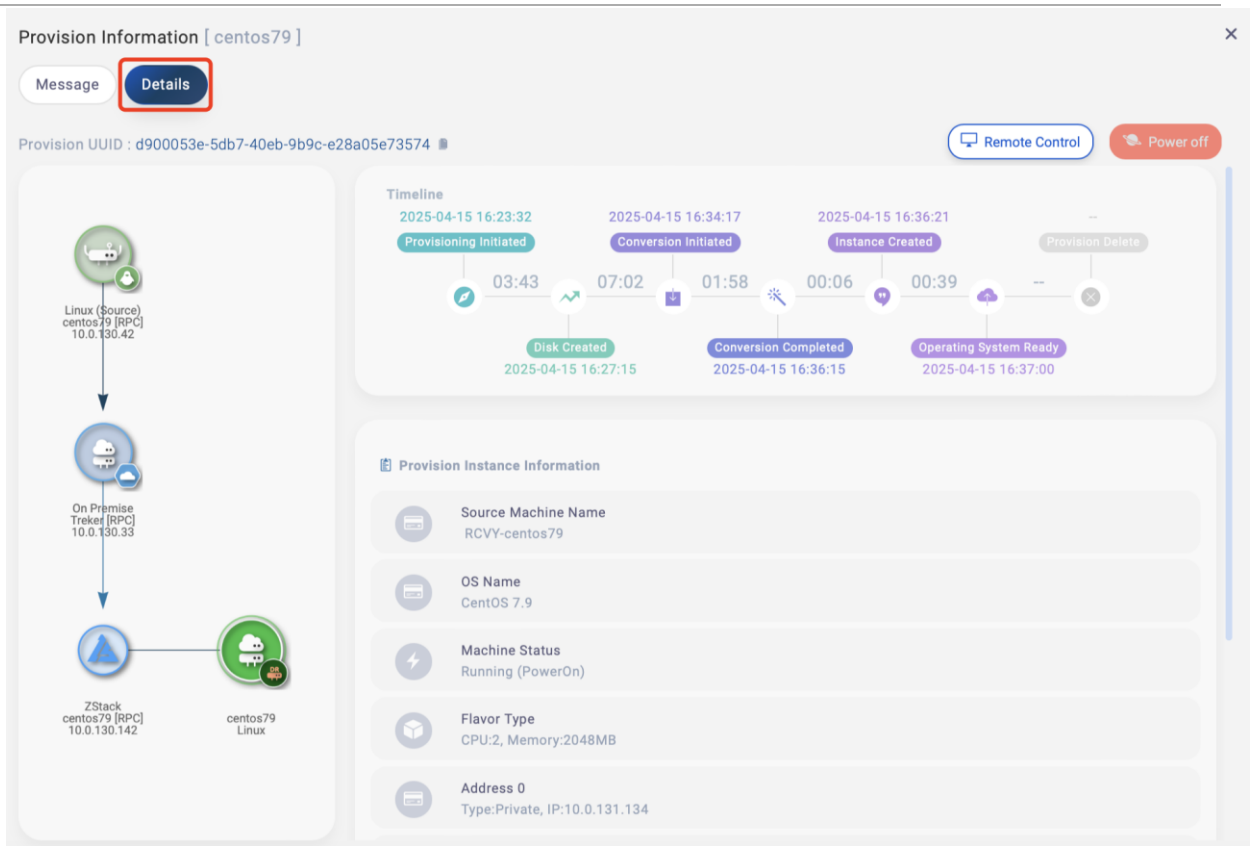
7. When the provisioning completes, the process status will be updated accordingly.



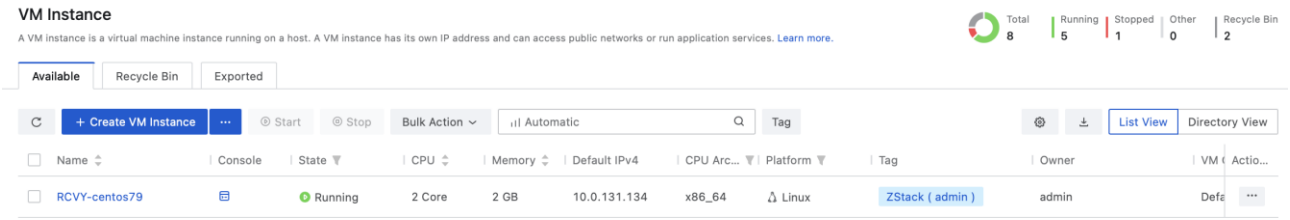
8. Click the **Details** button and select **Message** to view detailed logs of the provisioning process.



9. Click the **Details** tab to view the timeline, topology, associated Server, and detailed provisioning settings. The topology provides a visual representation of the data path between the protection and provisioning processes.

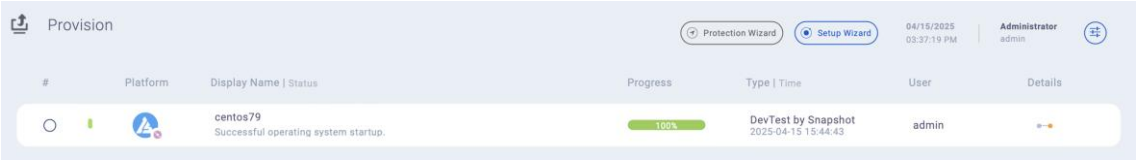


10. Log in to the NexaVM platform to verify that the target instance has been successfully created.

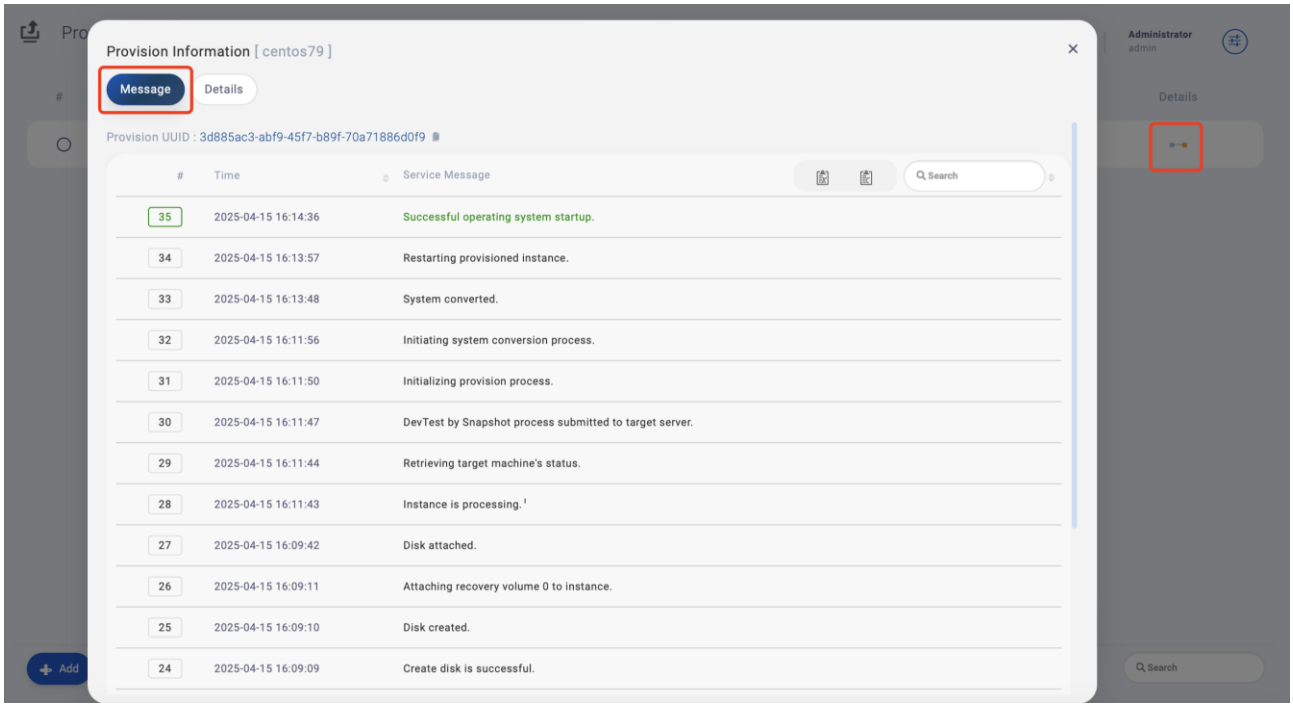


6.3 DevTest by Snapshot

1. Within the left-hand menu, click on **Provision** and then **Add**. Select the protection process for provisioning.
2. Select the provisioning type: **DevTest by Snapshot.**
3. Choose the disk snapshot time points from which to provision.
4. Configure the CPU, memory, and security group settings for the target instance.
5. Specify network configuration details for the instance, including IP address, subnet mask, gateway, and DNS server. Click **Submit** to proceed.
6. Under the DevTest by Snapshot provisioning mode, the related protection process will remain unaffected and synchronize as usual. After completing the provisioning, the process status on the provision page will display the successful message.

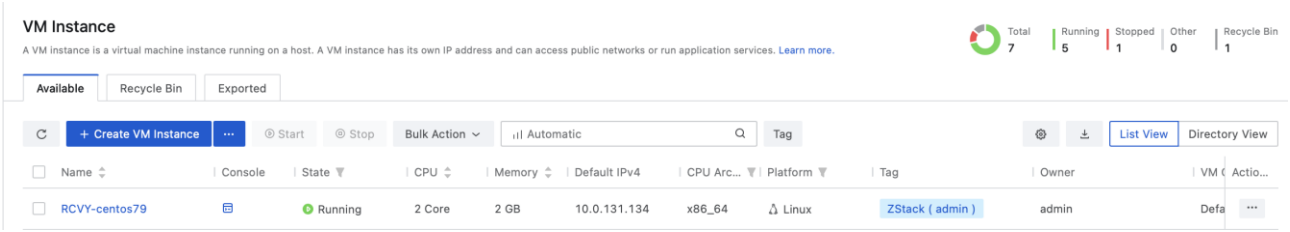


7. Click the **Details** button and select **Message** to view detailed logs of the provisioning process.



8. Click the **Details** tab to view the timeline, topology, associated Server, and detailed provisioning settings. The topology provides a visual representation of the data path between the protection and provisioning processes.

9. Log in to the NexaVM platform to verify that the target instance has been successfully created.



6.4 File Access

6.4.1 Upload File Access Image to NexaVM

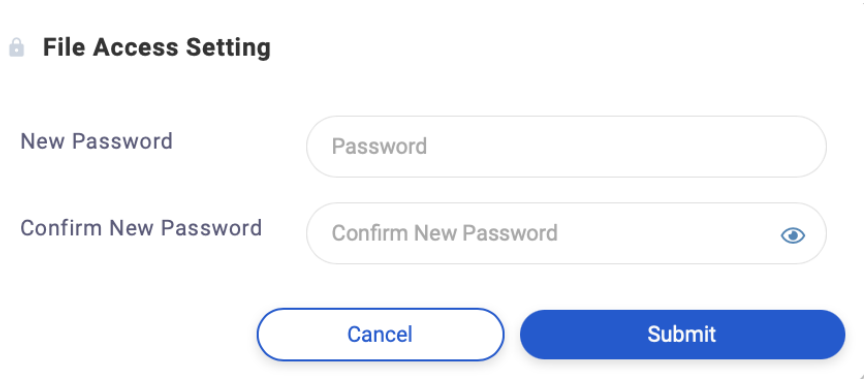
NDR provides the ability to upload images via the console, reducing manual operations. For detailed steps, refer to Appendix I.

1. In NexaVM cloud platform, navigate to **Cloud Resource Pool** > **Image** > **Add Image**. Note: The description must be set to “**FileAccessImage**”; otherwise, the image will not appear on the enablement page. The *FileAccessKit* package can be downloaded from the Package List.
2. After the image is added, check its status. When the status shows **Ready**, the image is available for use.

6.4.2 Create File Access Provisioning

1. Within the left-hand menu, click on **Provision** and then **Add**. Select the protection process for provisioning
2. Select the provisioning type: **File Access**.
3. Choose the disk snapshot time points from which to provision files from.
4. Configure the username, and password for the File Access Portal.
5. Once the File Access process completes, the message prompting for log in will be displayed.

6. On the **Details** page of the provisioning process, the username and password information configured can be found for the File Access Portal.
7. To reset the password, click on the blue icon next to the File Access Portal IP and select **Reset Password.**



8. To obtain the diagnosis of the File Access Portal, click on the **Diagnosis** option.

6.4.2 File Access Portal

Access the portal by clicking on the IP address displayed in the provisioning process status bar. After logging in, the portal will display a list of provisioned disks. Expanding these disks will reveal the folders and files they contain, aligning with the file structure of the client. Users have the option to download either a single file or multiple files. The following will sequentially explain the download process and other relevant configurations within the portal.

Download Single File

1. Click on name of a specific file to initiate the retrieval process.

Download Folder/Multiple Files

1. Select the desired files for retrieval and click **Download**.
2. A message will be prompted indicating that the zip and download process has started.
3. Click on **Downloads** in the left-hand menu options to view information about downloaded files. If you wish to delete the file copies saved in the File Access instance OS, select the corresponding files and click on **Delete File**.

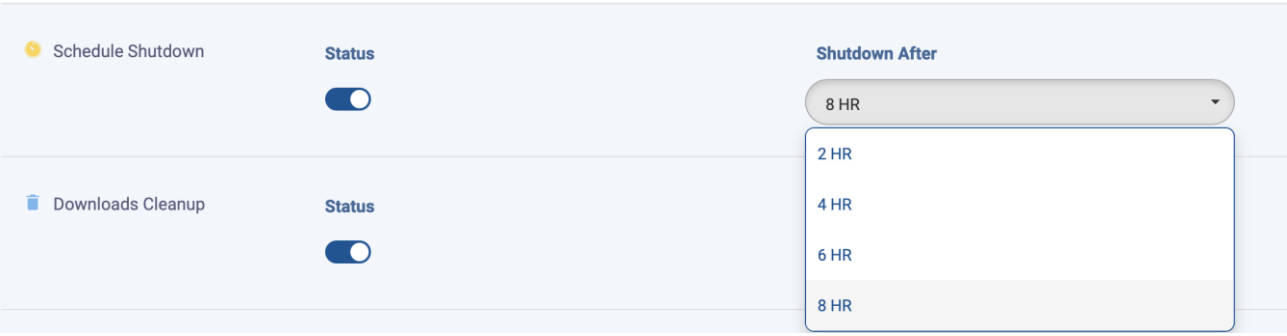
Search: If you need to find a specific file, enter the file name in the "Search" field at the top right corner. Then, select the file(s) and proceed to download.

Logs: The Logs tab in the left-hand menu is where to access all the activity logs of the File Access portal.

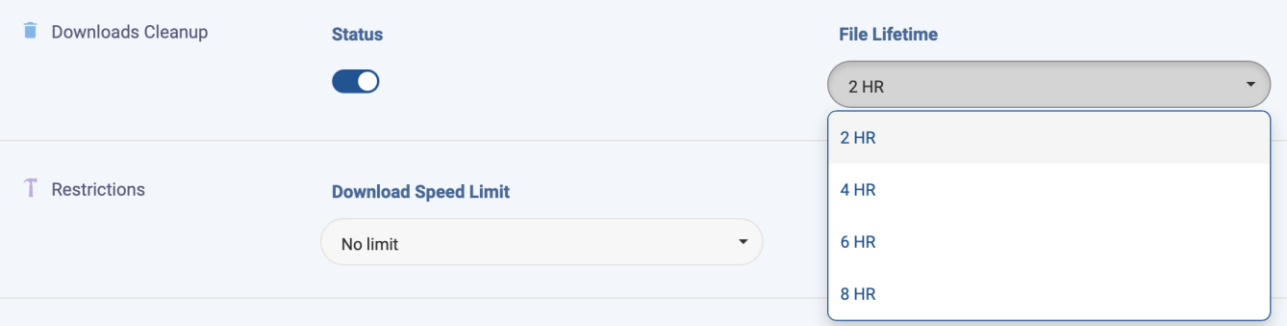
Settings: The Settings tab in the left-hand menu is where you can configure the File Access Portal.

General: Basic Configurations

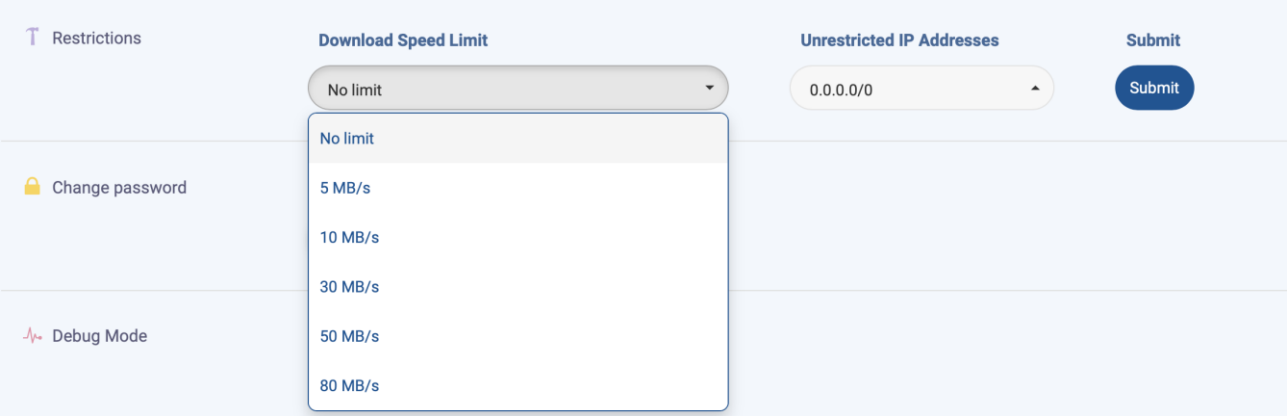
- **Time Zone & Language**: Change the displayed time zone and language.
- **Schedule Shutdown:** Automatically turn off the File Access instance by configuring the shutdown schedule.



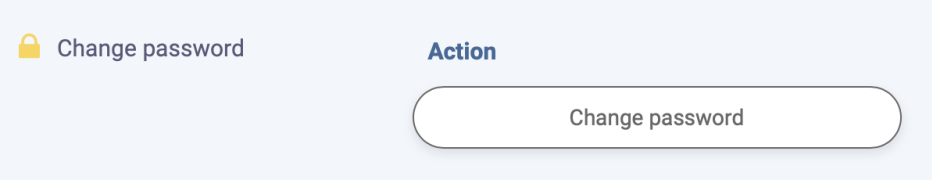
- **Downloads Cleanup**: Schedule the deletion of downloaded file copies and configure the duration for keeping them.

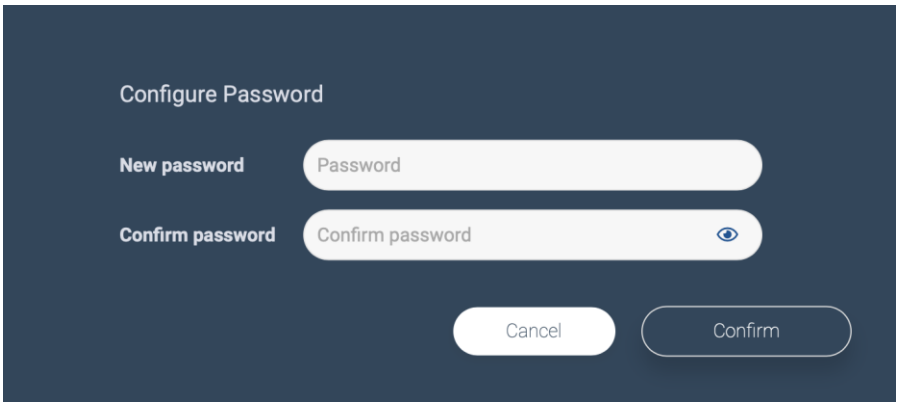


- **Restrictions:** Configure the maximum download speed and specify allowed IP addresses for portal access.

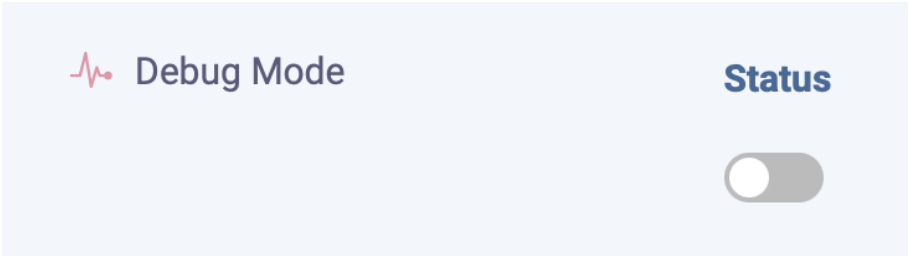


- **Change Password**: Modify the login password.

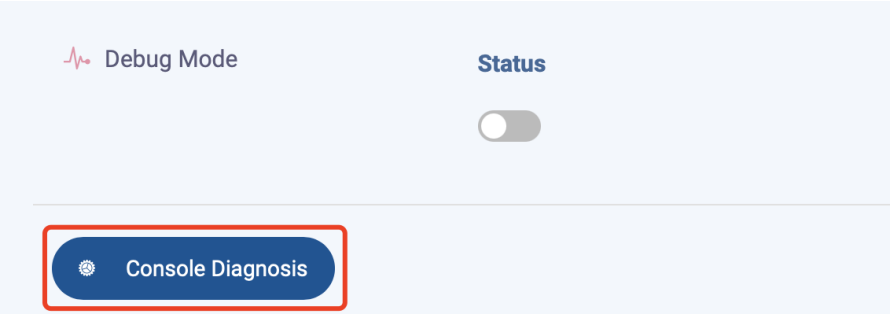




- **Debug Mode**:Enable Debug mode.



- **Console Diagnostics:** Collect console log information.



A. **File Sharing**: SMB and NFS file sharing are available. Set passwords and allowed IP addresses as needed to enable file access.

B. **MySQL Cloud Server**: If this feature is enabled, enter the SQL account information and configure the related settings. Click the **Access Link** button to access the connection.

6.5 Network Configuration Overview

1. When performing **Provision by Disk**, the network is typically set to **Clone Network Configuration**.
2. When performing **DevTest by Snapshot**, the network is typically set to **DHCP**.

7 Delete Provisioning Process

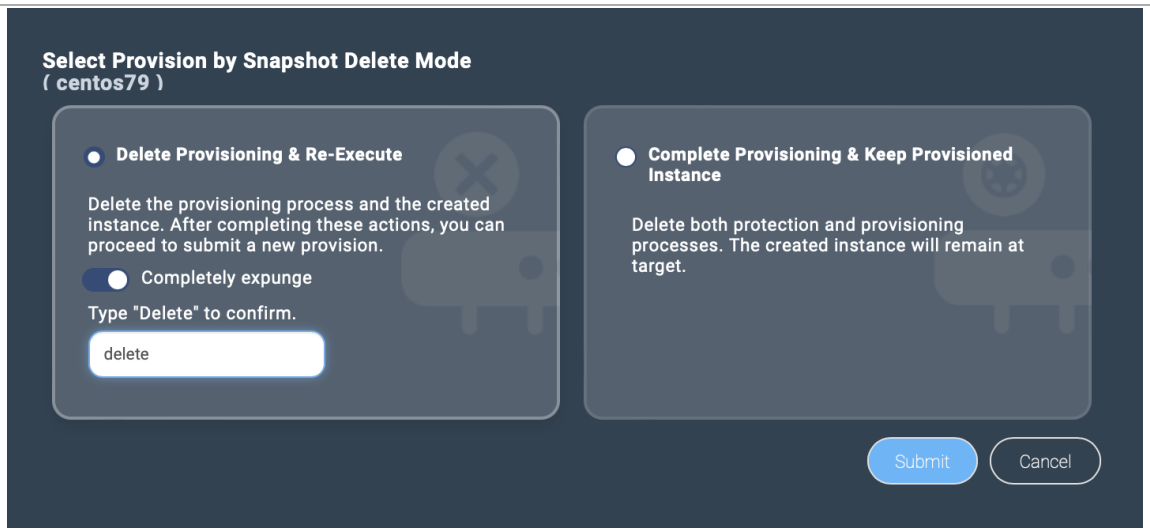
Delete Provision by Disk

1. On the Provision page, select the process to be deleted and click on **Delete**.
2. Select **Complete Provisioning & Keep Provisioned Instance**. Enter "**Delete**" and click to **Submit**.
3. **Important Note:** For official disaster recovery cutover, be sure to select **Keep the Provisioned Instance**. **DO NOT select** the first option. If **"Delete Provisioning & Re-**

Execute” is selected, it will immediately delete the provisioning task and the recovered instance on the NexaVM platform. This will result in the loss of recovered data. Please proceed with extreme caution.

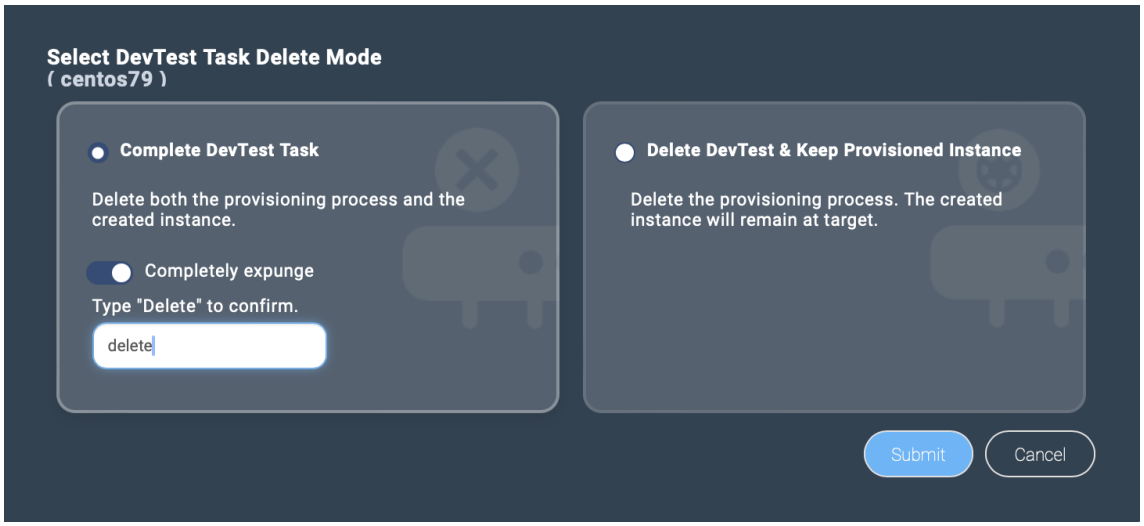
Delete Provision by Snapshot

1. On the Provision page, select the process to be deleted and click on **Delete.**
2. Select **Complete Provisioning & Keep Provisioned Instance**. Enter “**Delete**” and click to **Submit**.
3. When **Completely Expunge** is enabled, the provisioned cloud instance on NexaVM will be permanently removed from the recycle bin. When disabled, the instance will be moved to the recycle bin instead of being deleted immediately.
4. **Important Note:** This mode is **not recommended** for official migration cutovers.
   If **“Delete Provisioning & Re-Execute”** is selected, it will delete the provisioning task and the provisioned instance on the NexaVM platform. This will result in the loss of migrated data. Please proceed with extreme caution.



Delete DevTest by Snapshot

1. On the Provision page, select the process to be deleted and click on **Delete**.
2. Select **Complete DevTest Task**. Enter "**Delete"** and click to **Submit**.
3. When **Completely Expunge** is enabled, the provisioned cloud instance on NexaVM will be permanently removed from the recycle bin. When disabled, the instance will be moved to the recycle bin instead of being deleted immediately.
4. **Important Note:** This is a test recovery mode and is **not recommended** for official disaster recovery cutover.



8 Further Configuration Features

8.1 Download Diagnosis

Console Diagnosis

1. Click on **Control Center** and select **Diagnosis**.
2. Click on **Console Diagnosis** to download Management Console log information.

Protection Diagnosis

Method 1

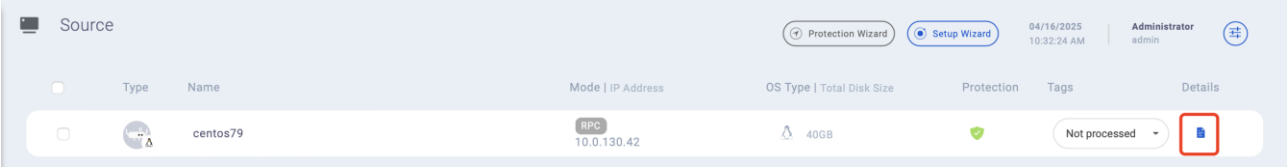
1. Click on the **Details** icon on the right side of the corresponding protection process.
2. Click on **Details** menu in the upper left corner, and click on **Diagnosis** to download the log information.

Method 2

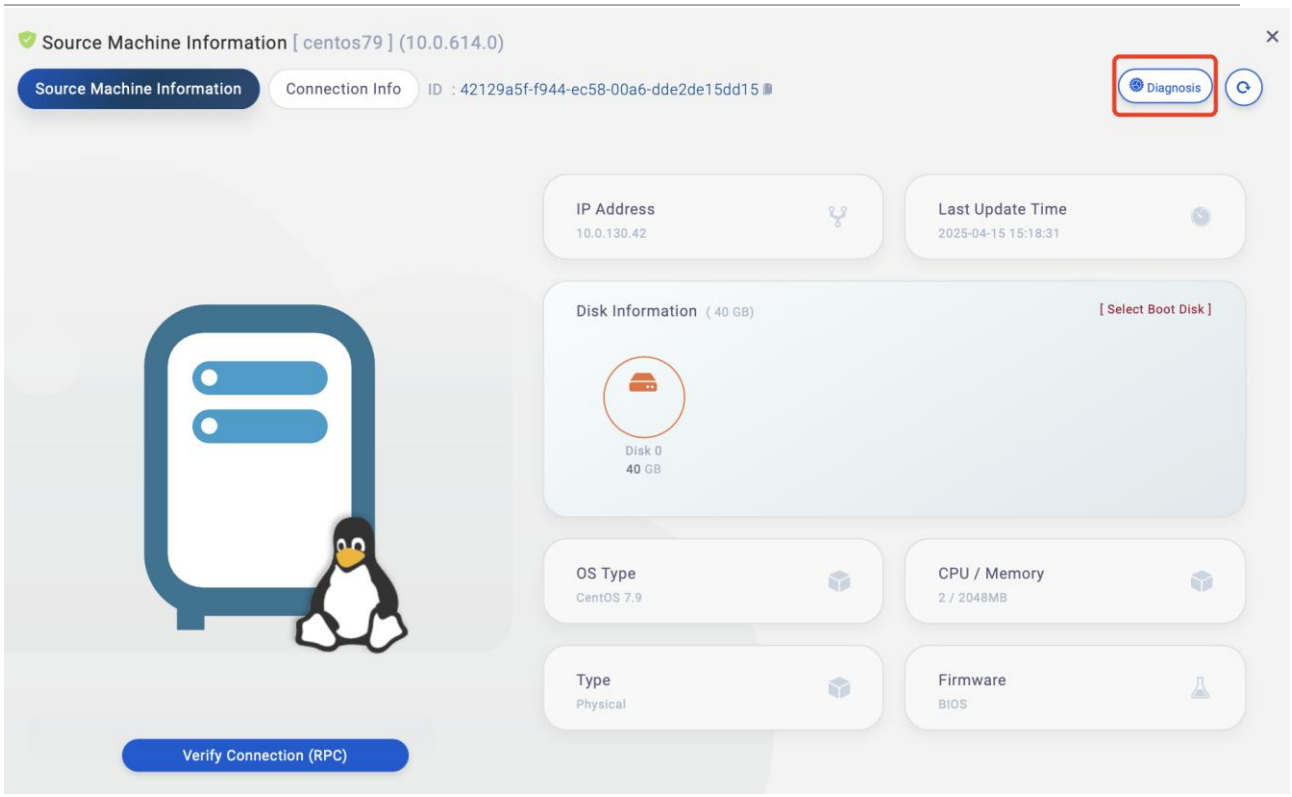
1. Click on **Control Center** and select **Diagnosis**.
2. On the **Protection** sub-page, select the protection process for which you want to obtain the diagnostic file, then click on **Protection Diagnosis** in the bottom right corner to download.

Source Machine Diagnosis

1. Click on **Control Center** and select **Diagnosis**.

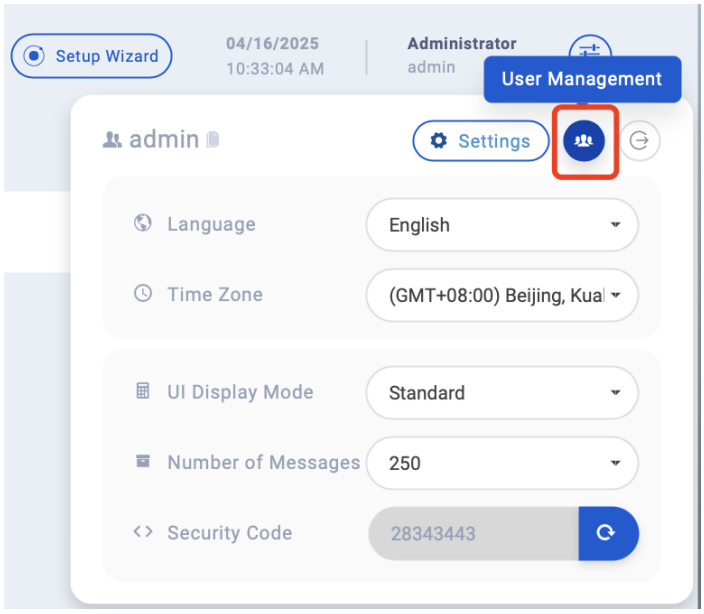


2. On the **Source** page, select the source machine for which you want to obtain the diagnostic file, then click on **Source Diagnosis** in the bottom right corner to download.

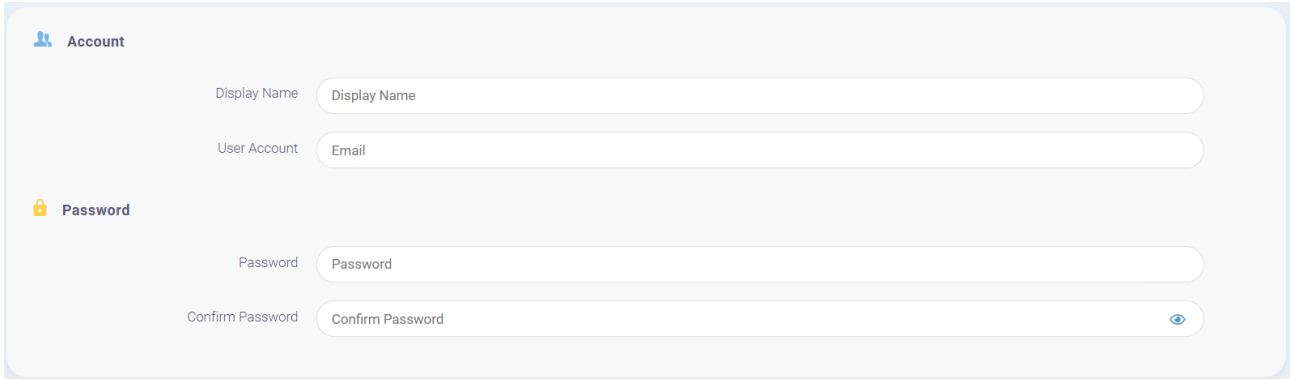


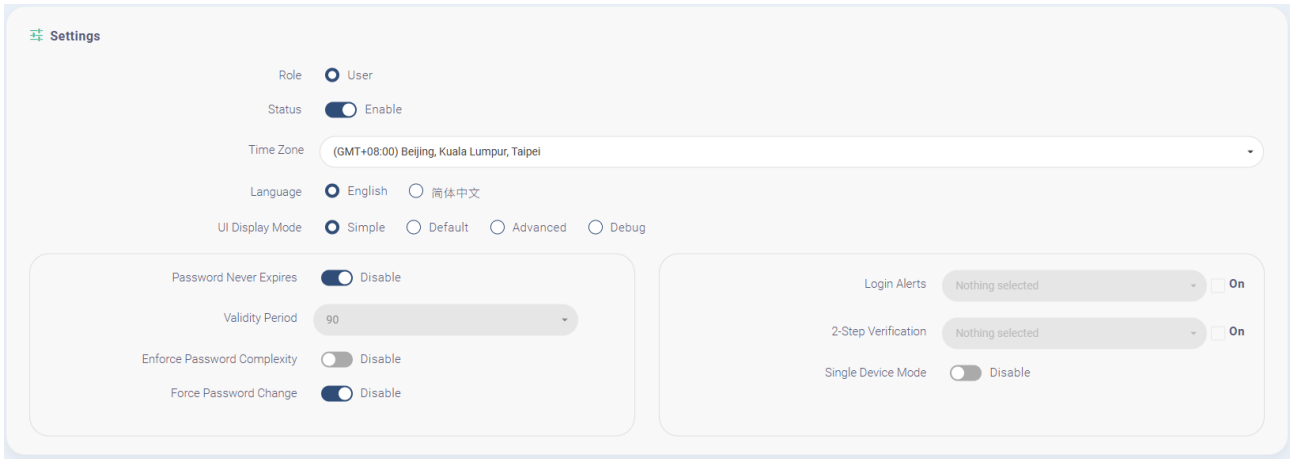
8.2 User Management

1. Click the **Settings** icon in the upper-right corner and navigate to the **User Management** icon.



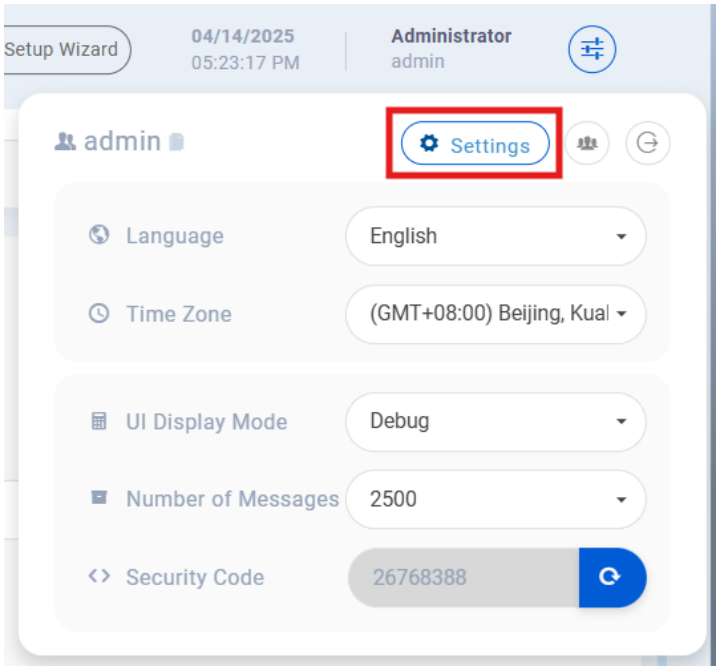
2. Click **Add** and fill in the required details including user account, password, time zone, language, UI display mode, etc. Then click **Submit**.



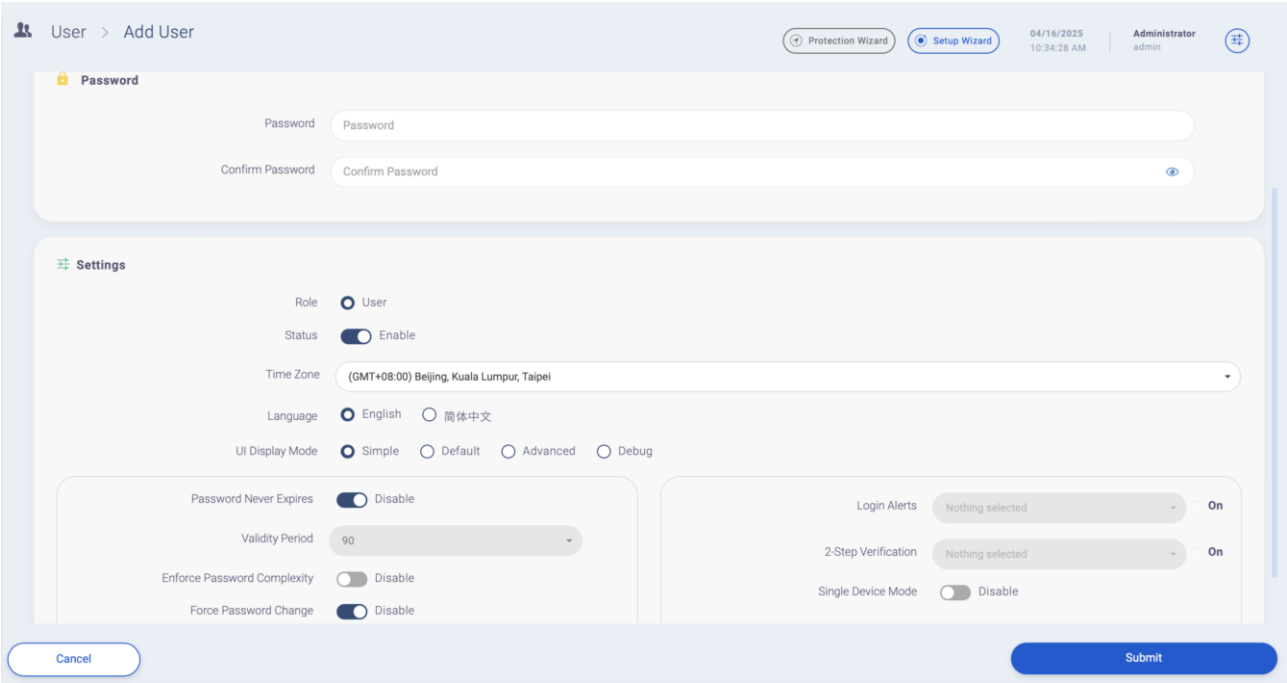


8.3 Password Settings

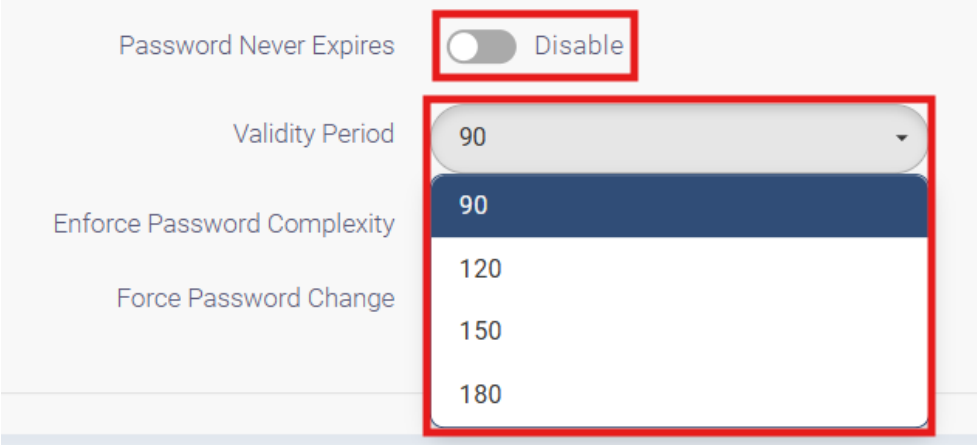
1. Click the "Settings" icon in the top-right corner to enter the settings page.



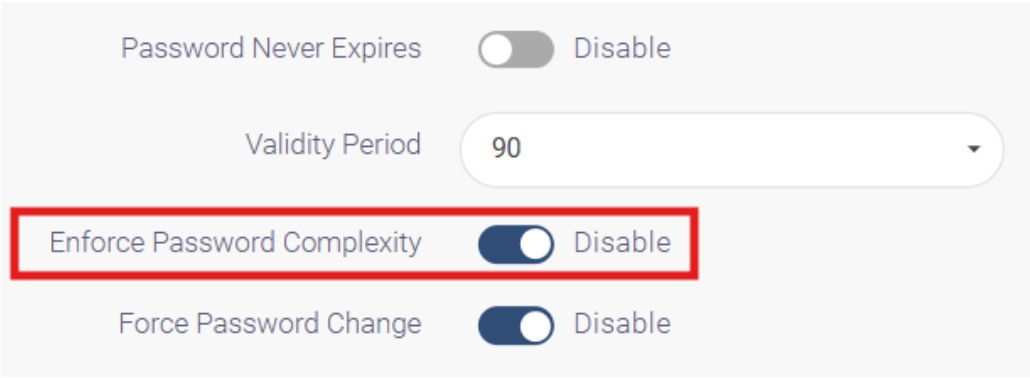
2. Navigate to **Password** section under **Settings**.



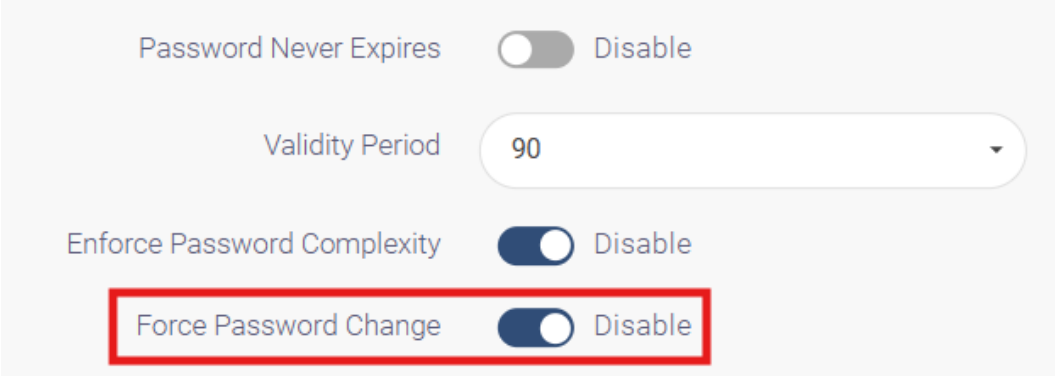
3. Disable the **Password Never Expires** option to set a password expiration period.



4. Enable the **Enforce Password Complexity** option to require users to meet complexity rules when setting a password.



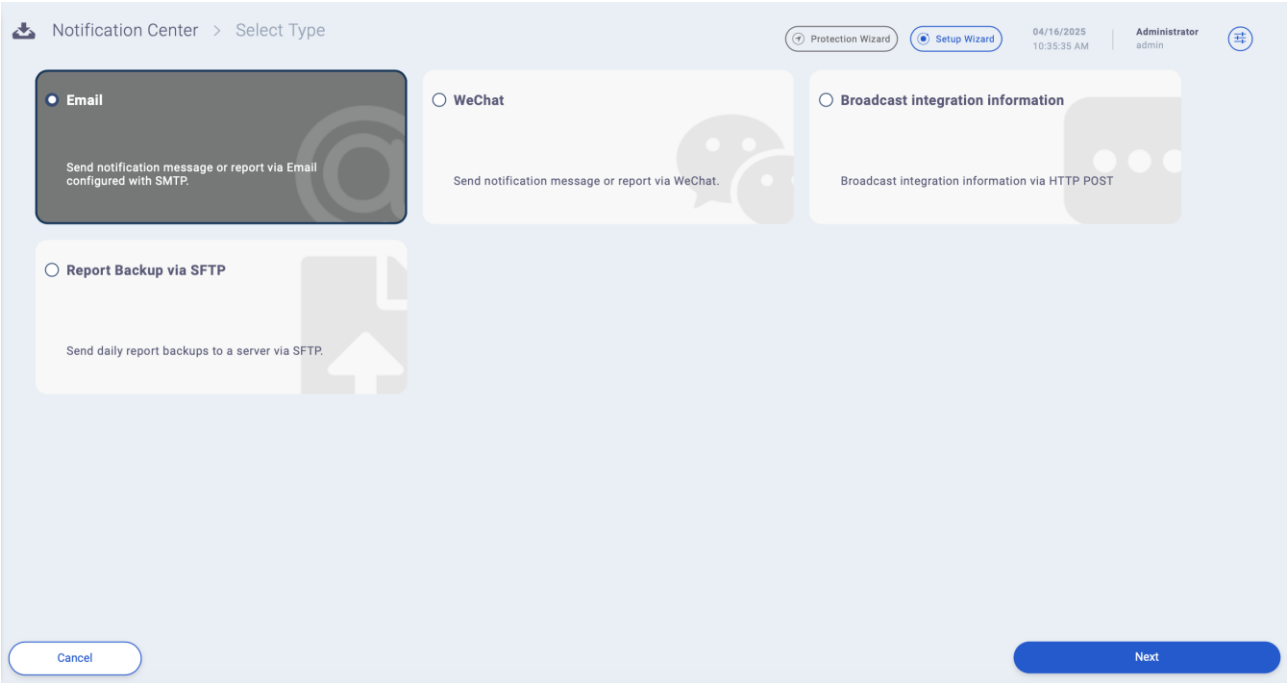
5. If required, enable the **Force Password Update** option to prompt users to change their login password upon next login.



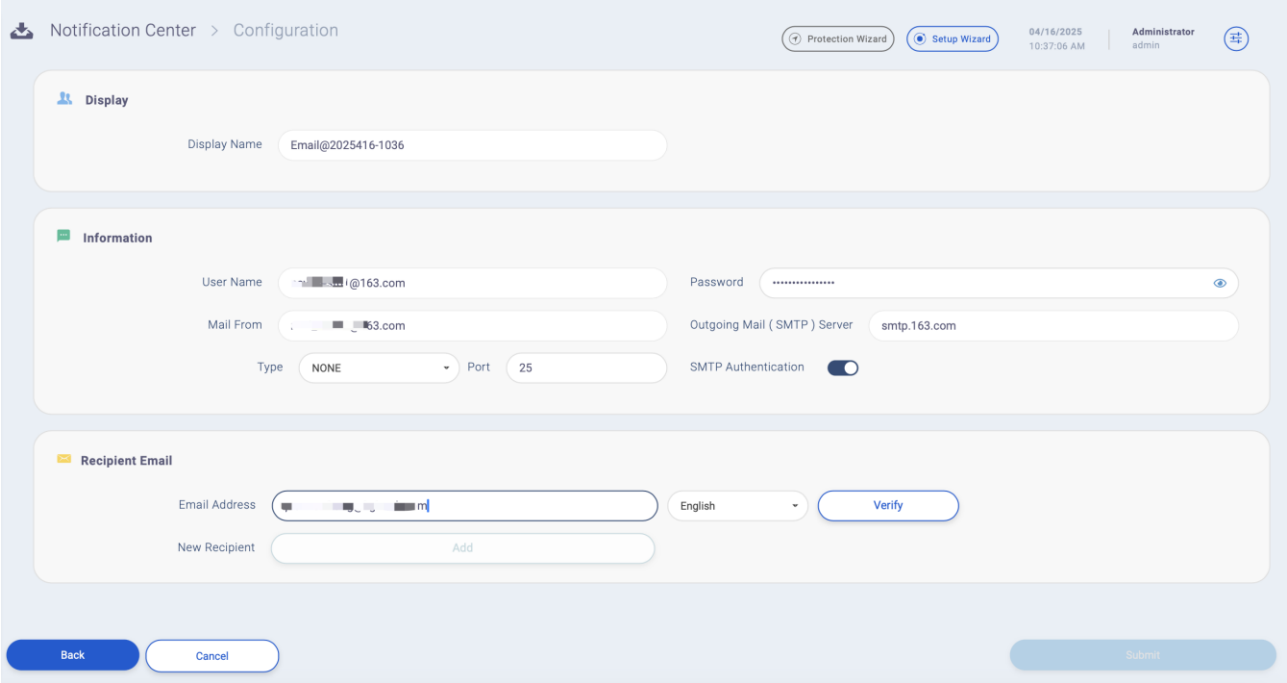
8.4 Notifications

Email

1. Click on **Control Center** and select **Notifications**.
2. Click **Add** and select **Email**.

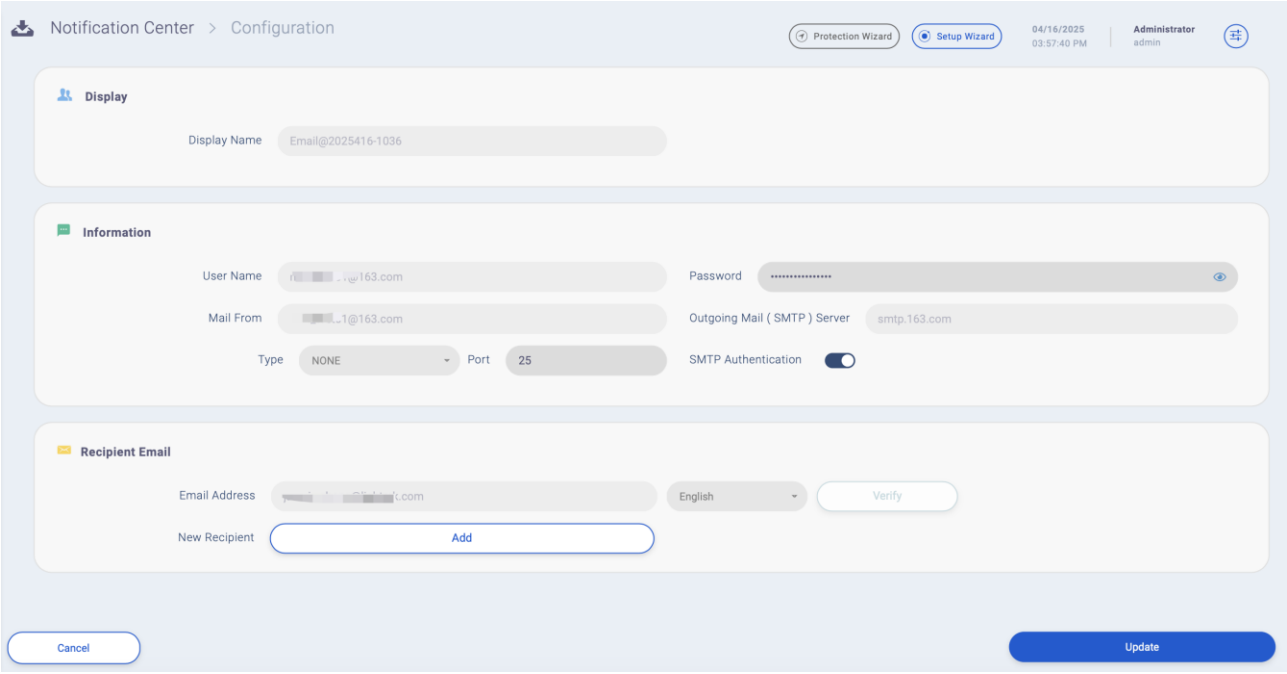


3. Input the details for email notification: display name, mail from, SMTP, recipient email, etc.

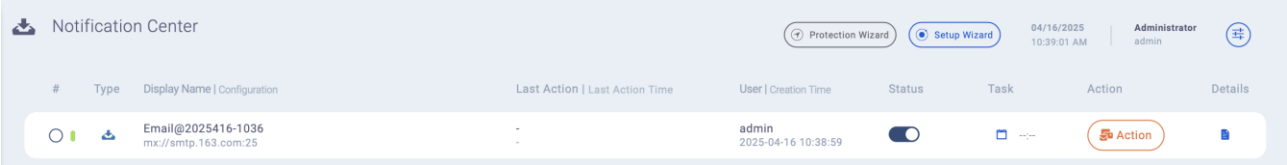


Note: User Name and Mail From need to have the same input.

4. Click **Submit** to save the settings.

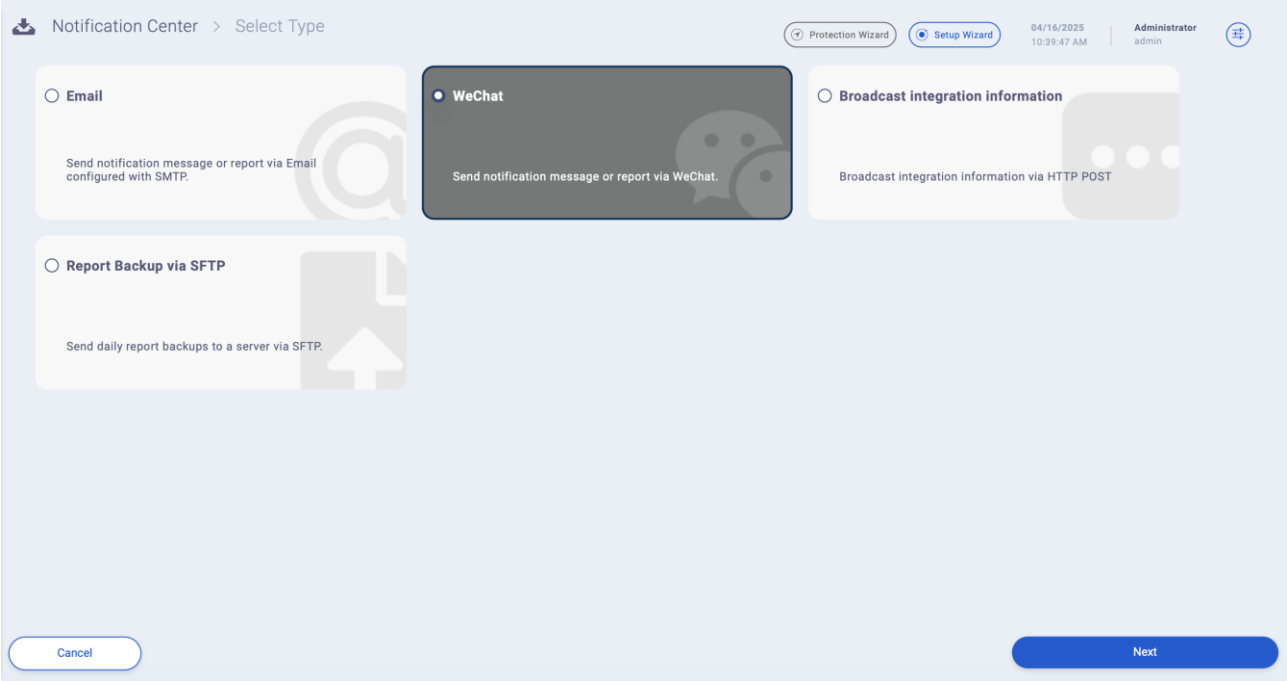


5. The new email notification module can be found in the list.

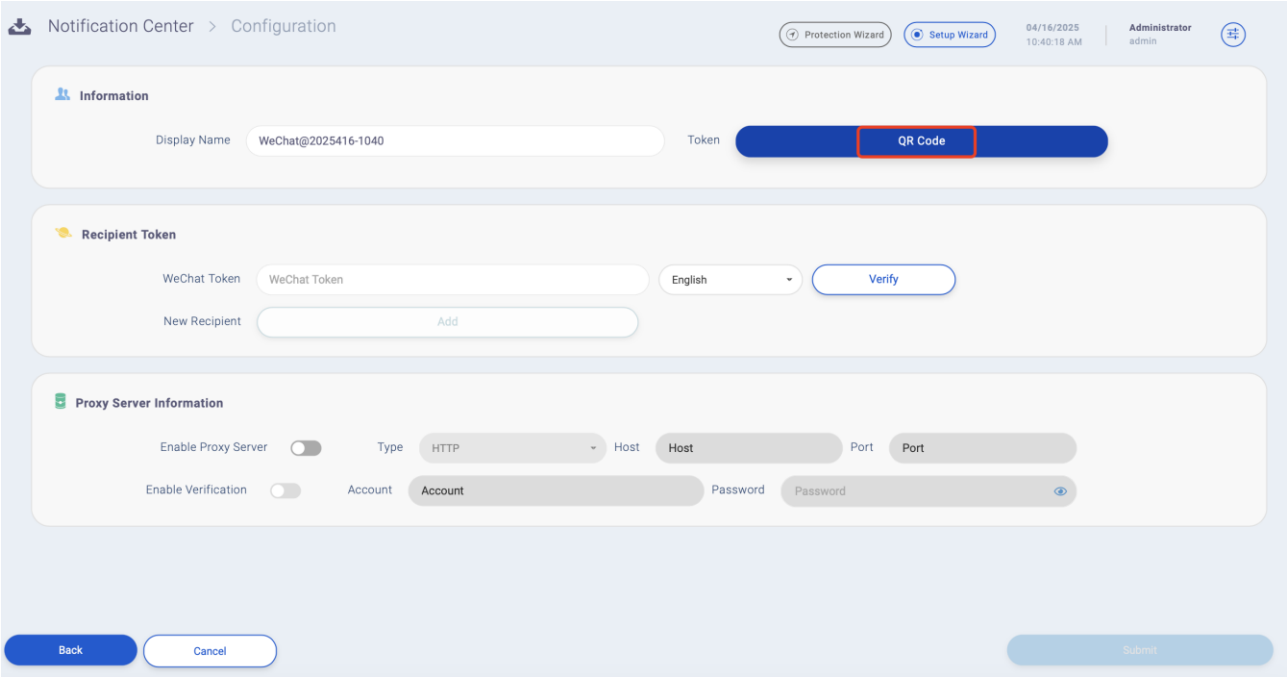


WeChat

1. Click on **Control Center** and select **Notifications**.
2. Click **Add** and select **WeChat**..



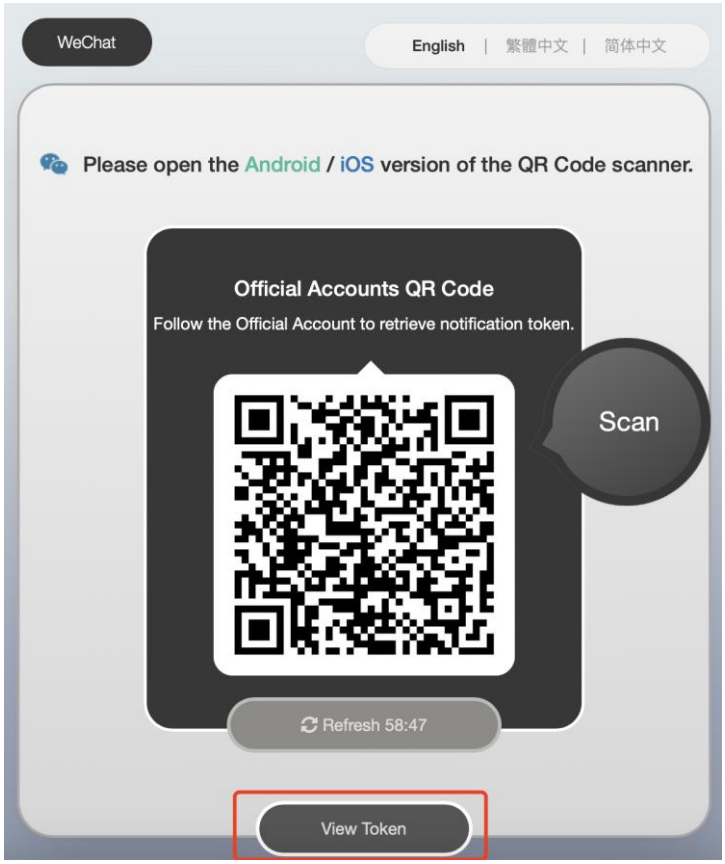
3. Enter a display name “WeChat” and click QR Code.



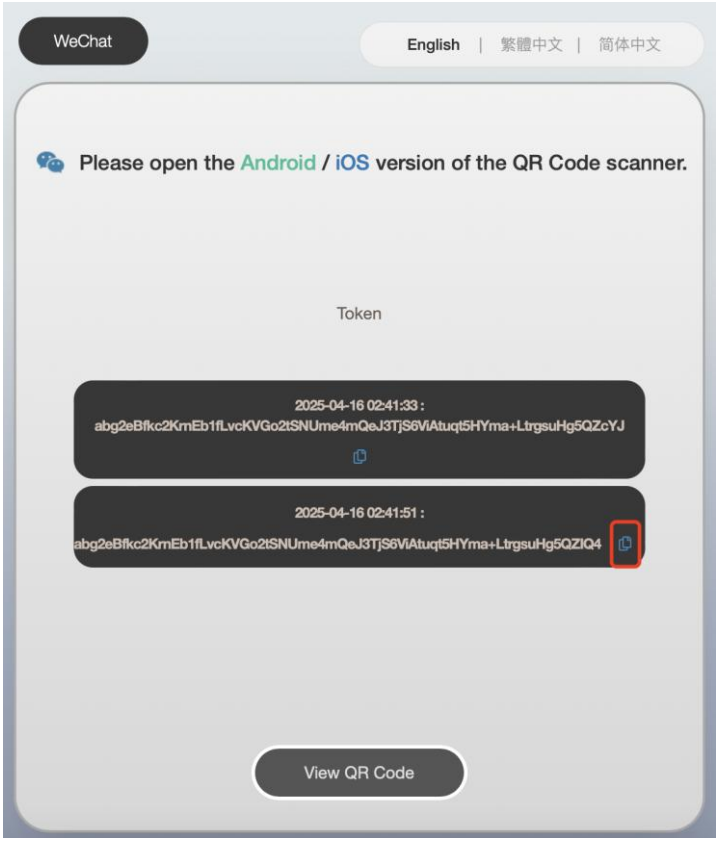
4. Scan the QR code to follow the official WeChat account.


WeChat
English | 繁體中文 | 简体中文
Please open the Android / iOS version of the QR Code scanner.
Official Accounts QR Code
Follow the Official Account to retrieve notification token.
Scan
Refresh 59:58
View Token

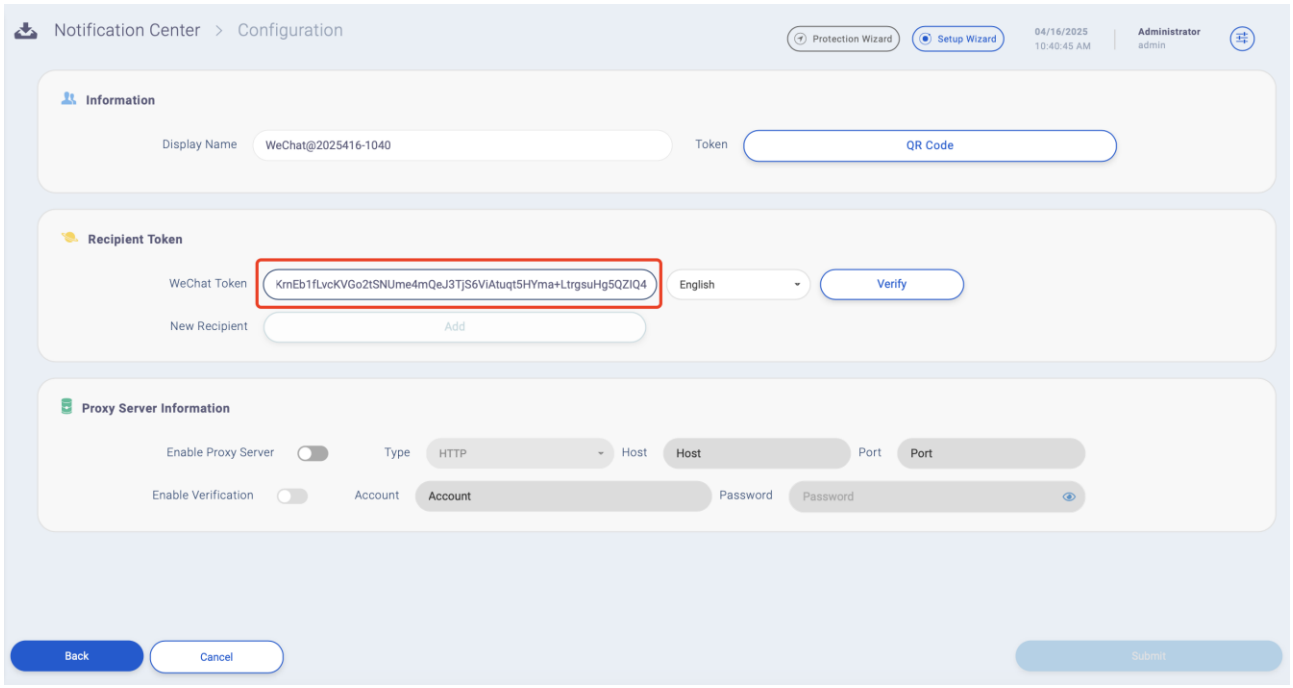
5. Click to view the authorization code.



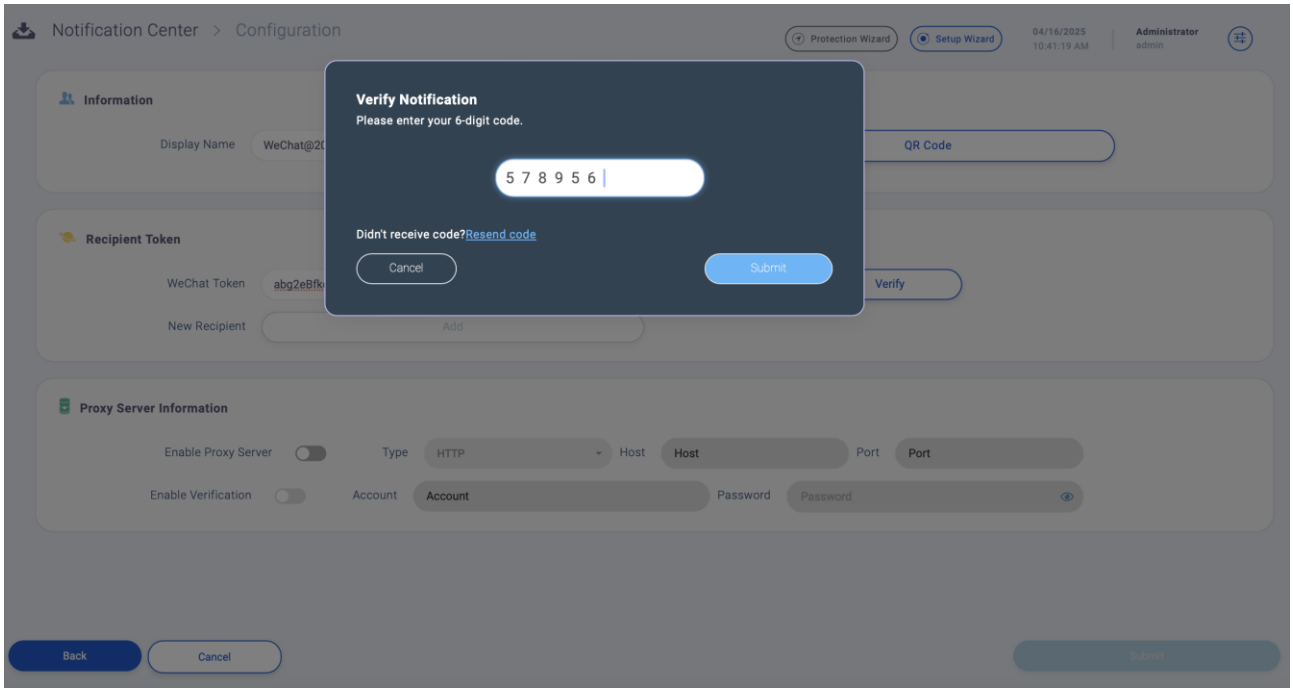
6. Copy the authorization code.



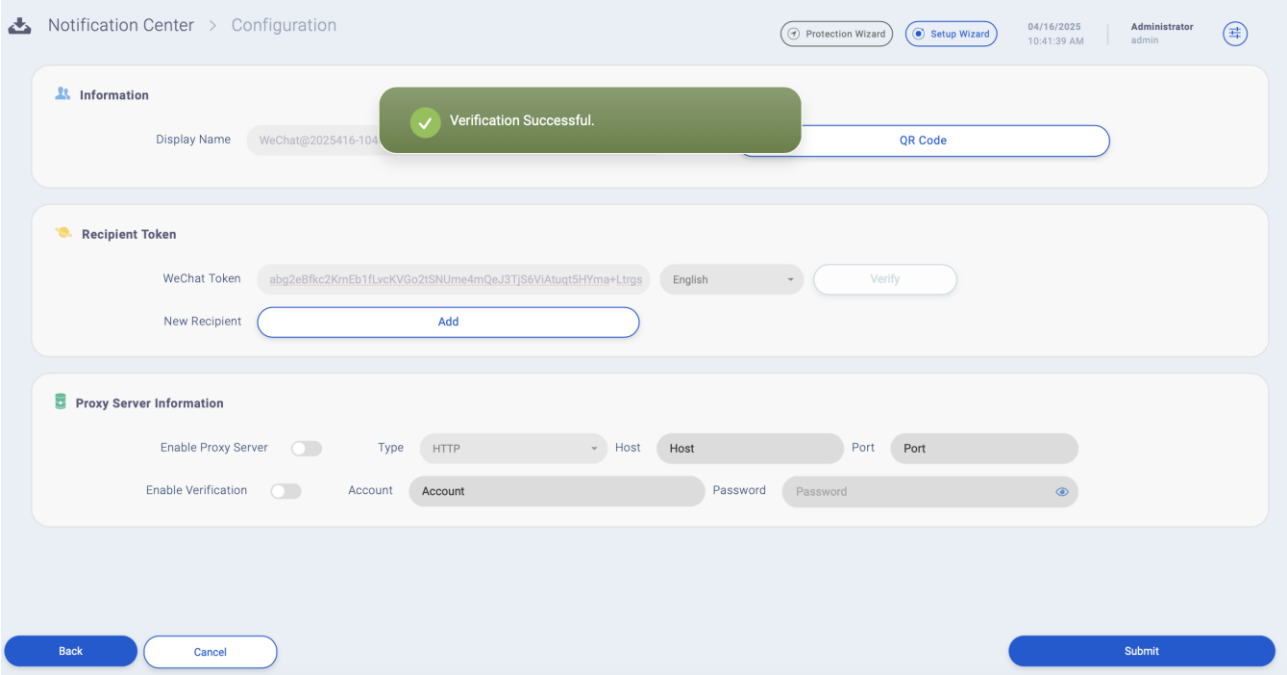
7. Return to the Management Console, enter the authorization code in the WeChat Token field, and click **Verify**.



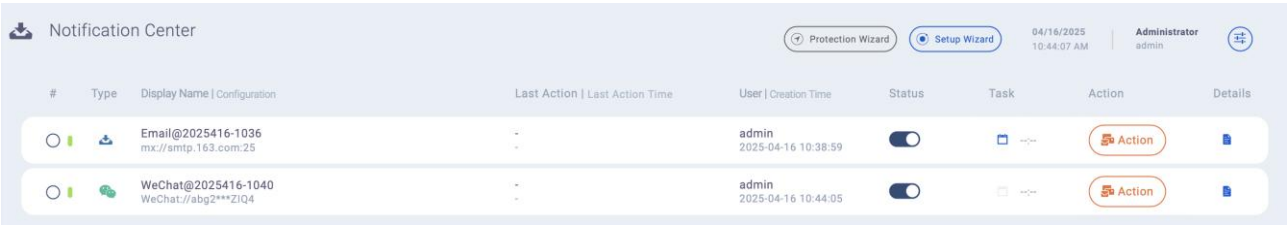
8. The system will prompt for a verification code. Check WeChat for the verification code, enter it in the provided field, and click **Submit**.



9. After verification, click **Submit** to save the settings.



10. The new email notification module can be found in the list.



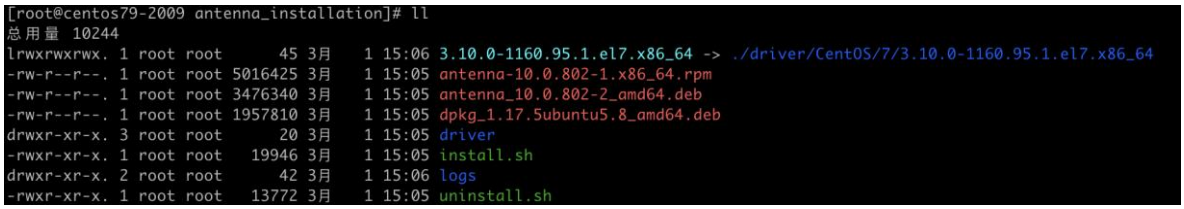
9 Uninstallation

9.1 Uninstalling Agent for Windows

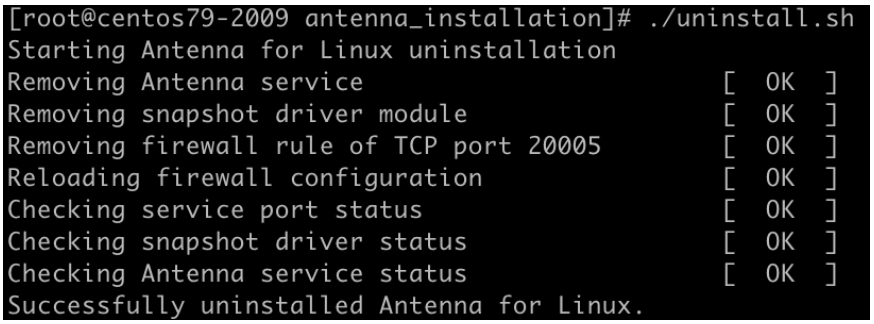
1. Double-click the ***NDR_Windows_Agent_(Antenna).exe*** installer and click **Next**.
2. Select **Remove**.
3. Click **Remove** to confirm. The system will delete all related files and settings.
4. Once the process is complete, click **Finish** to exit. The agent has now been successfully uninstalled.

9.2 Uninstalling Agent for Linux

1. Navigate to the directory containing the ***install.sh*** script.



2. Run the command ***./uninstall.sh***. The agent will be successfully uninstalled.



9.3 Uninstalling Windows Server

1. Double-click ***NDR_Windows_Server_Gateway_(Treker).exe*** installer and Click **Next**.

2. Select **Remove**.
3. Click **Remove** to confirm. The system will delete all related files and settings.
4. Once the process is complete, click **Finish** to exit. The Server has now been successfully uninstalled.

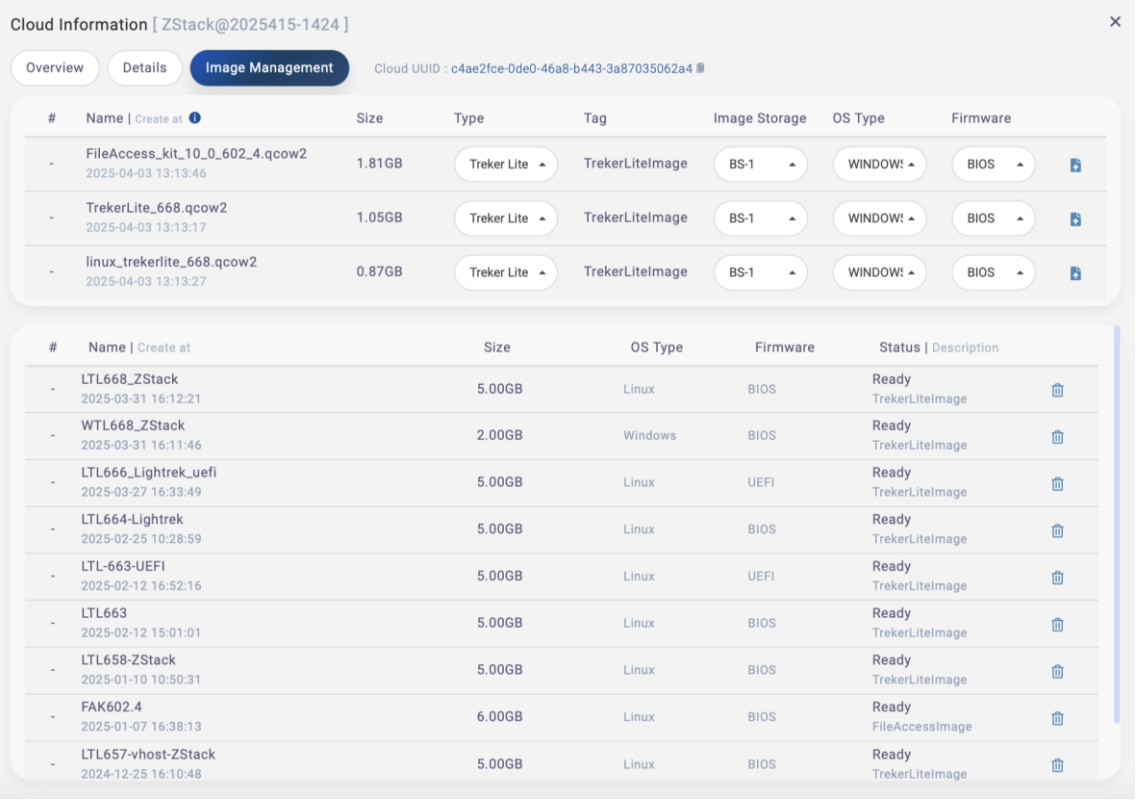
10 Appendix

This chapter provides an overview of the components related to NDR.

10.1 Appendix 1: Upload Server Image via Console

1. Add the NexaVM Cloud platform to the management console. Click the **Details** icon of the corresponding NexaVM platform.

2. Click the **Image Management** tab.

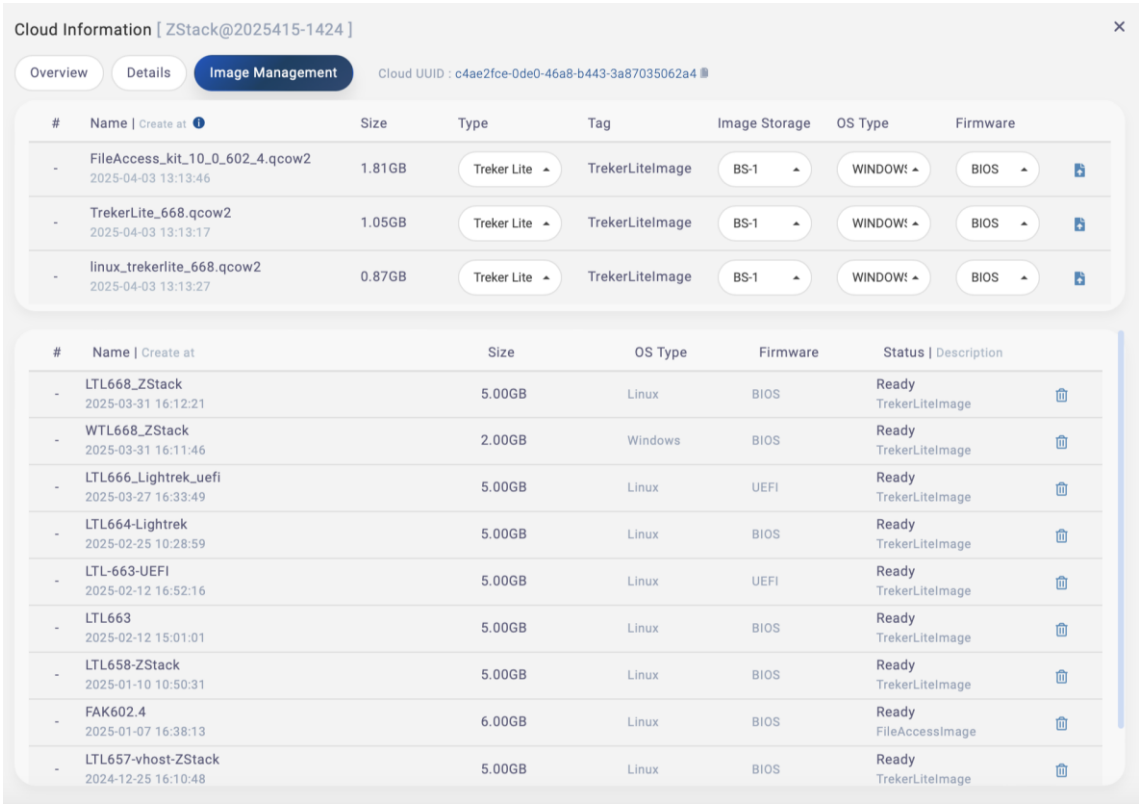


3. Place the image file in the designated directory.

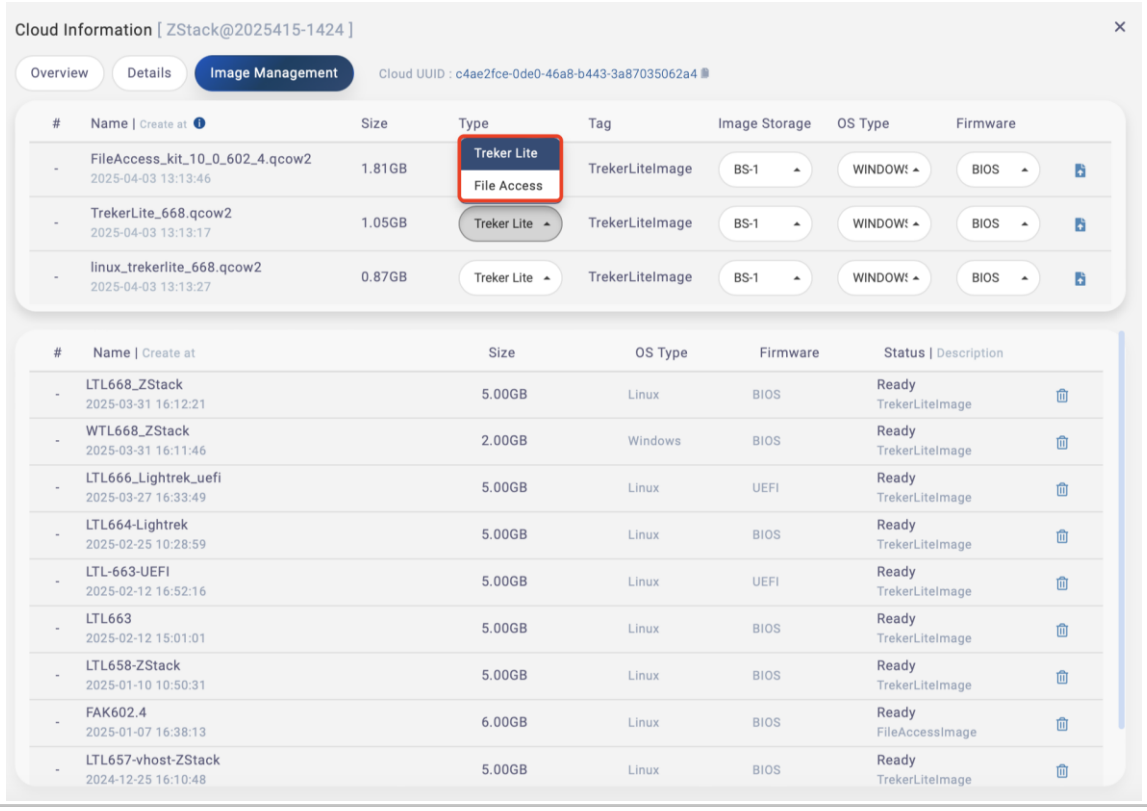
Note 1: For Windows, upload the image to the corresponding directory. The shortcut path is *C:\Program Files\NexaVM\Treker\packages*; the actual directory is shown in the screenshot below.

Note 2: The Linux Gateway image includes the BootImage by default.

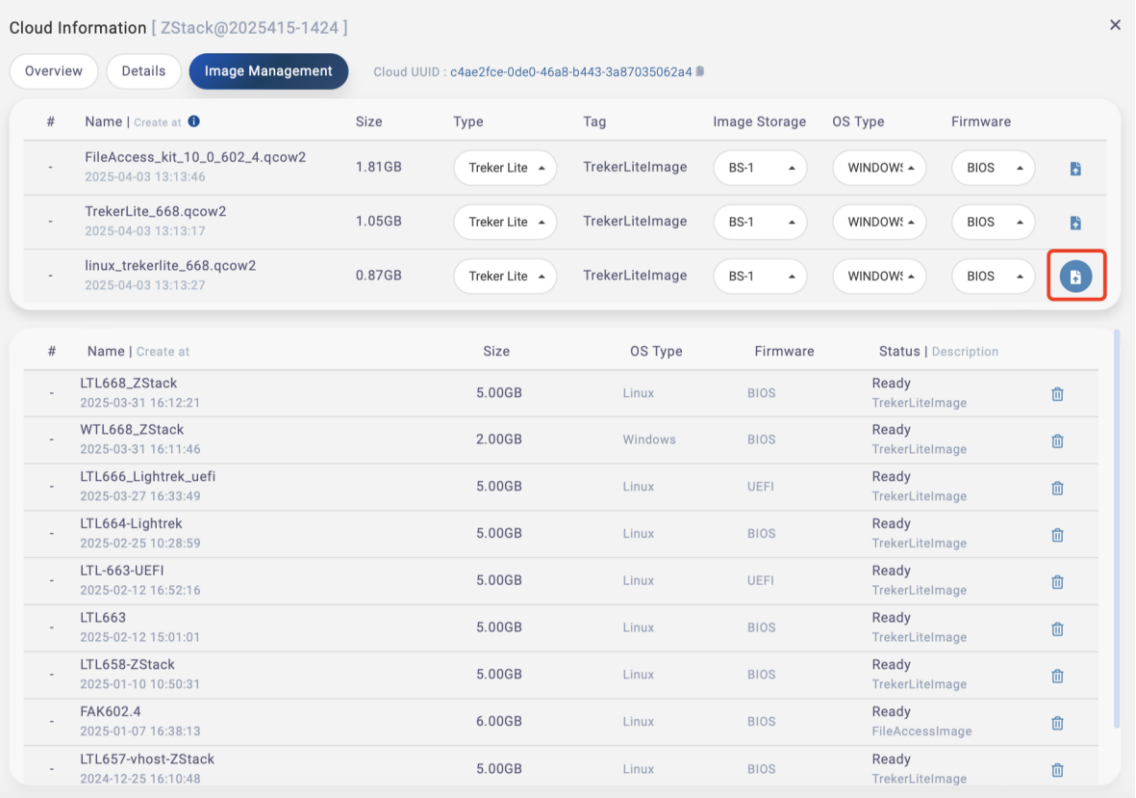
Note 3: The default compatibility mode for uploaded images is virtio.



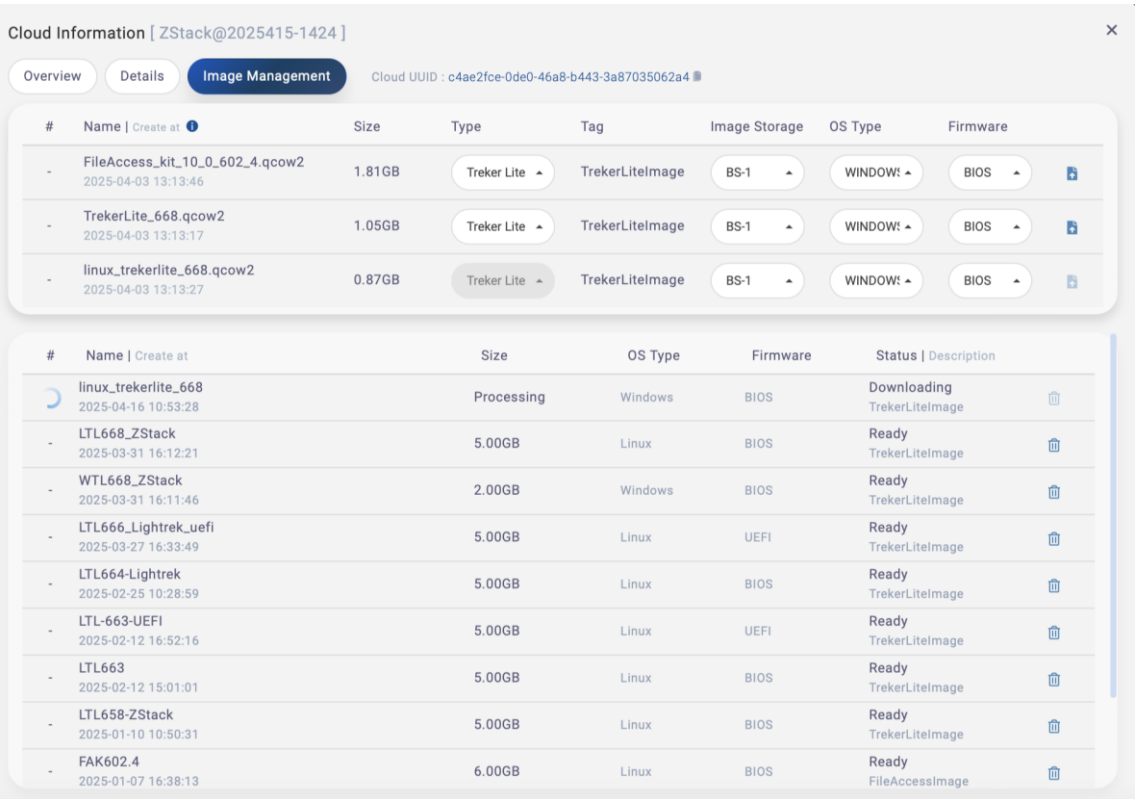
4. Specify the image type, target image server storage, OS type, and boot mode.



5. Click the Upload icon to upload the image.



6. In the lower pane, the upload progress will be displayed.



7. When the status of the image changes to "Ready", the image upload is complete.