LOC-A Core Framework User Guide (Version 3.3)

Date: 2024-12-9

Table of Contents

Summary of Statement

This document is intended for both professional services engineers and end users. It describes how to deploy the LOC-A Core Framework and use the LOC-A Core Framework to deploy and manage cloud clusters and bare metal systems at edge sites.

LOC-A Core Framework Overview

Lenovo Open Cloud Automation (LOC-A) Core Framework is a modular automation framework designed to enable Lenovo's customers to easily deploy and manage cloud solutions and workloads on Lenovo hardware. It is intended to be:

- An **OPEN** lightweight automatic deployment engine that can be extended to support various cloud offerings.
- An **Enterprise** solution for edge-site cloud life cycle management.

The LOC-A Core Framework appliance provides a self-contained image, for quick installation, that contains all the services required to do the automated cloud deployment and management for edge sites. The services within the image run as services on top of a built-in K3S cluster. The following components are included:

- **Inventory Service (LIS)**
  The Inventory service is the source-of-truth for the infrastructure that handles planning data and edge site resources, including sites, IP addresses and VLANs, cloud services, network services, and the cloud objects, such as tenants and clusters. The metadata for resources can be imported or created by users in the planning phase.

- **Configuration Service (LCS)**
  The Configuration service is an execution orchestrator built on AWX. LOC-A LCS is configured with pre-defined automation workflows and job templates that make managing the infrastructure easy and efficient.

- **Hardware Management Service (LMS)**
  The Hardware Management service helps to provision hardware and performs hardware management operations during the lifecycle of Lenovo servers. LOC-A includes Confluent and Lenovo OneCli as components of its Hardware Management Service. LMS is responsible for:
  - Server inventory
  - Server power operations
  - Server operating system deployment
  - Server firmware updates
  - Server configuration

Installation and Upgrade

Installation and configuration

Environment requirements

The following requirements need to be met to deploy LOC-A Core Framework and use it to deploy cloud clusters to edge sites.

- An ESXi host must be available to run the LOC-A Core Framework software appliance. The following resources are required by the virtual machine:
  - 8 CPU cores
  - 32 GB memory
  - 300 GB disks

- Make sure that you have vCenter installed to manage this ESXi host.

- Two networks are essential for LOC-A to be able to deploy and manage cloud clusters:
  - **OOB Management Network(BMC/XCC).**
    An Out-of-band management network for the BMC(XCC) of each server in the cluster, and optionally, switch discovery and management

  - **Cloud/OS Networks(Management).**
    In-band cloud-specific data and management networks. The cloud network topology may vary for different cloud offering types that LOC-A supports. Among cloud networks, an operating system (OS)/cloud management network is mandatory for in-band OS deployment and management.

    Note: The Management network is the OS/Cloud management network that is essential to central management of all cloud platform flavors.

- The LOC-A Core Framework appliance must have layer 3 access to the out-of-band (OOB) network used to access the BMCs of the edge-site nodes. It also must have layer 3 access to the OS/Cloud management network for the configuration and deployment of the target edge-site nodes.

- Secured and reliable connectivity between the LOC-A Core Framework appliance and the edge sites must exist. OOB and OS/Cloud management networks for the edge sites must be global layer 3 networks; network address translation (NAT) is assumed not to be used.

- The LOC-A Core Framework also supports Bare Metal OS deployment of a number of operating systems:
  - CentOS
  - Ubuntu
  - ESXi
- The cloud flavors (cloud types) supported by the LOC-A Core Framework appliance are:
  - VMware ThinkAgile VX Cluster(vSAN)
  - Red Hat OpenShift Container Platform (RHOCP)

The server types and supported cloud flavors matrix is as follows:

	VMware ThinkAgile VX Cluster(vSAN)	Red Hat OpenShift Container Platform (RHOCP)
ThinkSystem SE350 (MT: 7Z46)	Yes	Yes
ThinkSystem SR630 (MT: 7X02)	Yes	Yes
ThinkSystem SR650 (MT: 7X06)	Yes	Yes
ThinkEdge SE450 (MT: 7D8T)	N/A	Yes
ThinkEdge SE360 V2 (MT:7DAM)	N/A	Yes
ThinkEdge SE350 V2 (MT: 7DA9)	N/A	Yes
ThinkEdge SE455 V3 (MT: 7DBY)	N/A	Yes

Table 1: Cloud flavors support matrix

The server types and supported OS flavors version matrix is:

	Ubuntu	CentOS	ESXi
ThinkSystem SE350 (MT: 7Z46)	18.04.6,20.04.6,22.04.3,22.04.4, 22.04.5	7.9, 8.3	7.0.3d, 7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c
ThinkSystem SR630 (MT: 7X02)	18.04.6,20.04.6,22.04.3, 22.04.4,22.04.5	7.9, 8.3	7.0.3d, 7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c
ThinkSystem SR650 (MT: 7X06)	18.04.6,20.04.6,22.04.3, 22.04.4,22.04.5	7.9, 8.3	7.0.3d, 7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c
ThinkEdge SE450 (MT: 7D8T)	20.04.6,22.04.3, 22.04.4,22.04.5	N/A	7.0.3d, 7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c
ThinkEdge SE360 V2 (MT:7DAM)	22.04.3, 22.04.4,22.04.5	N/A	7.0.3k,7.0.3m, 7.0.3n, 8.0.1c
ThinkEdge SE350 V2 (MT: 7DA9)	22.04.3, 22.04.4,22.04.5	N/A	7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c
ThinkEdge SE455 V3 (MT: 7DBY)	20.04.6,22.04.3,22.04.4,22.04.5	N/A	7.0.3d, 7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c

Table 2: OS flavors support matrix

Each target node must have appropriate licensing to support the attachment of remote media. Ensure that the following two licenses are enabled on the target nodes:

- Lenovo xClarity Controller Enterprise Upgrade
- Lenovo xClarity Controller Advanced Upgrade

If the target node is using XCC2 (on SE350 V2, SE360 or newer system) the above two packages have been combined into an XCC 2 Platinum License.

Redfish support must be enabled on the target systems for the deployment to work.

Note: On systems shipped from the factory, this is enabled by default

See the Release Notes for a full list of supported cloud types. See *Cloud deployment* on page 91 for more requirements and details on each supported cloud type.

Sample network configuration

Figure 1 shows the typical network topology for the LOC-A Core Framework appliance and edge sites:

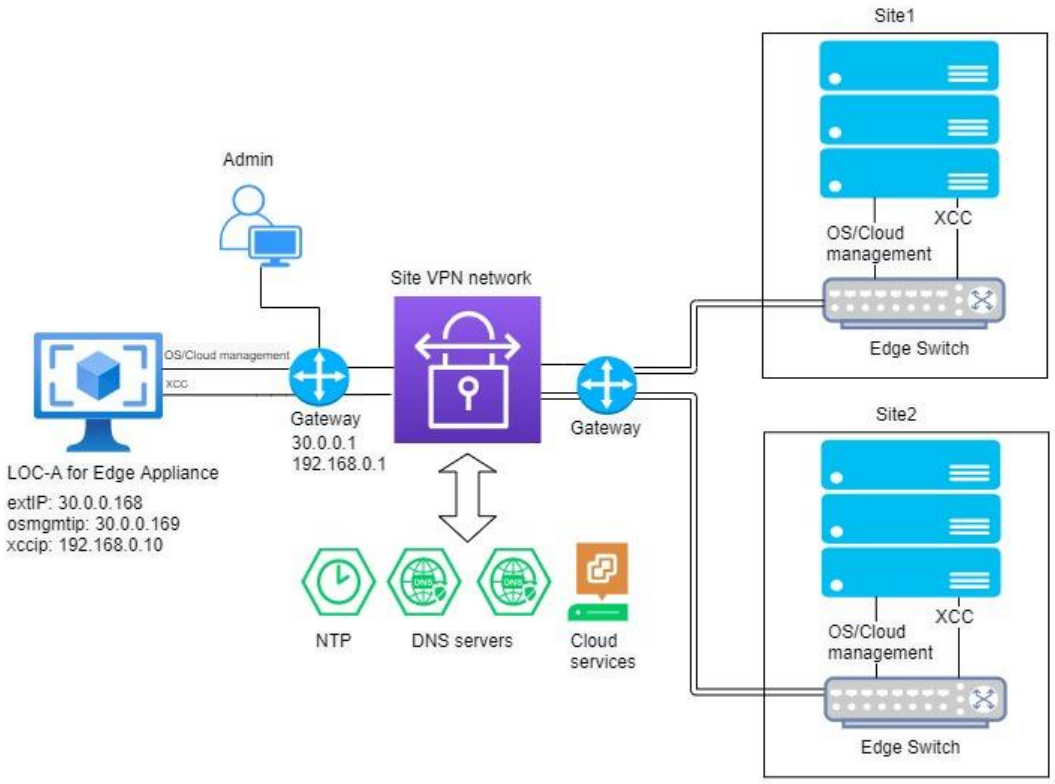


Figure 1: Network topology of LOC-A Core Framework

The LOC-A Core Framework supports either a dedicated edge OOB network separated from cloud networks, or a layer 3 network on which OOB and cloud networks can be shared.

Step-by-step LOC-A Core Framework appliance installation

1. Prepare the network of the ESXi host that will be used to host the LOC-A Core Framework appliance. A network is required to access the OS/cloud management network of edge sites. If your OOB and OS/cloud management networks are separated by VLANs, you will also need to create a BMC port group for LOC-A Core Framework to access the target network.

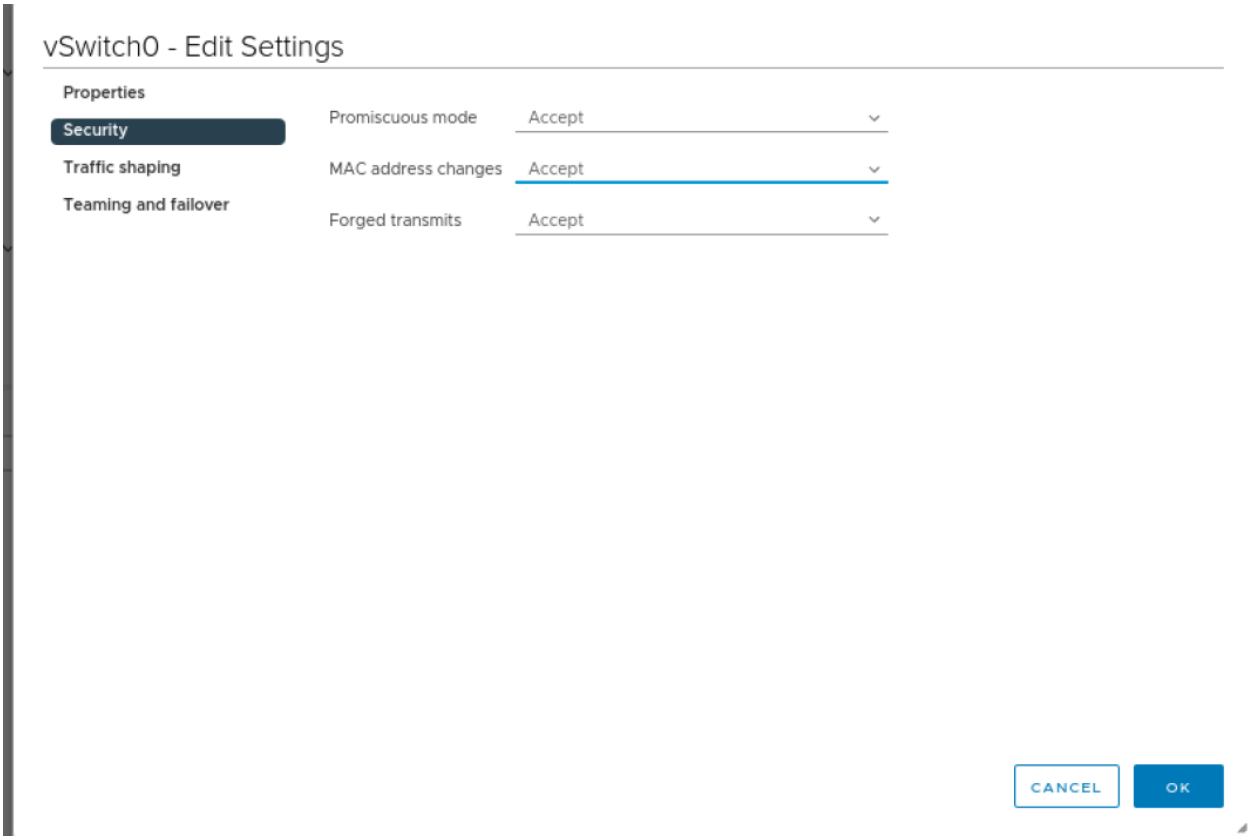


Figure 2: ESXi host network setting

2. Download the LOC-A Core Framework software appliance image from Lenovo to a system that can access the target vCenter vSphere client for your environment.

3. Deploy the OVA to the ESXi host:
    a. From vSphere, go to **VMs and Templates.** Then right click on the Datacenter of the target ESXi host and click **Deploy OVF Template**.
    b. Click **Local file** and then **UPLOAD FILES** to select the OVA file that was downloaded from Lenovo. Click **Next**.
    c. Give the virtual machine a name and a folder. Click **Next.**
    d. Choose the ESXi host for the compute resource and click **Next**.
    e. Review the template details and click **Next**.
    f. Choose the type of disk provisioning and click **Next**.
    g. Ensure that the network mappings are configured properly.
        - The external network should correspond to the network to access the OS/cloud management network.
        - The XCC network should correspond to the dedicated BMC(XCC) network. If the XCC network is shared, you can specify the same network as the first network.

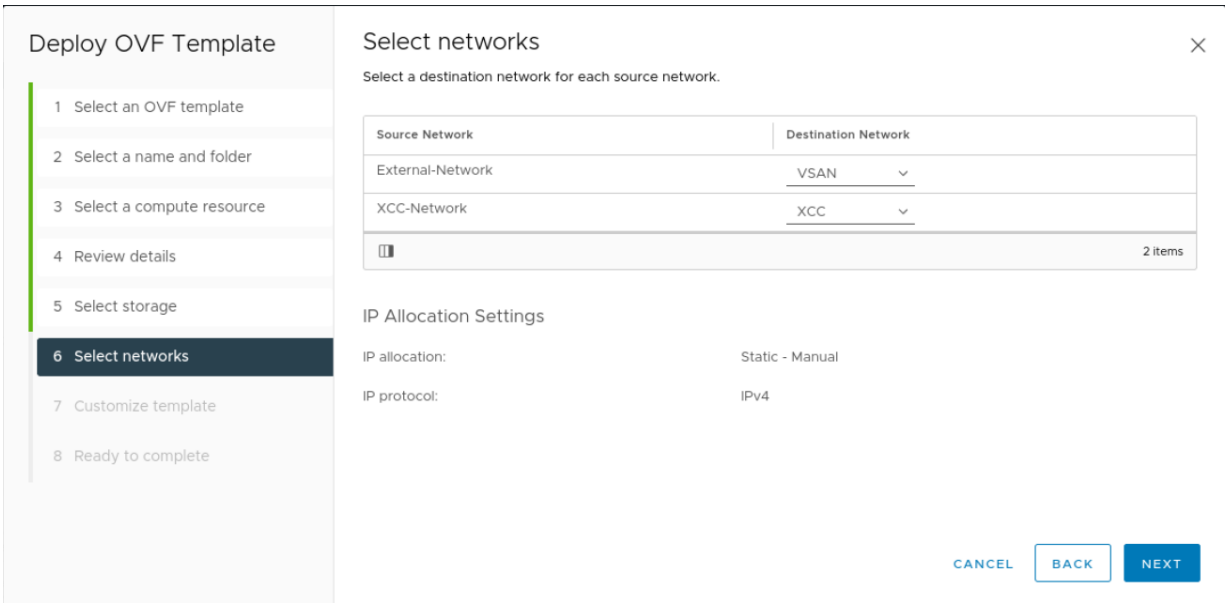


Figure 3: Example of network selection

h. In Customize Template, enter the network configuration of the LOC-A Core Framework appliance. Table 1 lists the parameters and descriptions.

Parameter	Mandatory	Description	Sample Value
Hostname	Yes	Hostname of the LOC-A appliance. Hostname must respect the following rules: • Must be 253 characters or less. • Can only contain letters(a-z,A-Z), digits(0-9), hyphen('-') and dots('.'). • Cannot start or end with a dot or hyphen.	Loca-edge
External Network IP	Yes	External IPv4 address of the LOC-A appliance portal. You can then access the portal GUI via https://[*External Network IP*] This is also the interface for the appliance to access the DNS servers and vCenters in OS/cloud management network for the edge sites.	30.0.0.168
External Network Netmask	Yes	Netmask of the subnet for external network interface.	255.255.255.0
External Network Gateway	Yes	The gateway of the external network interface.	30.0.0.1
XCC Network IP	No	If the edge-site nodes BMC(XCC) network is not accessible through an	192.168.0.10

Parameter	Mandatory	Description	Sample Value
		external network IP address, you MUST specify the XCC network interface with its IPv4 address. This is used for server management. If edge nodes XCC network is accessible through external network IP, you MUST NOT specify the IP and the netmask/gateway of XCC network interface.	
XCC Network Netmask	No	Netmask of the subnet for XCC network interface.	255.255.255.0
XCC Network Gateway	No	The gateway of the XCC network interface.	192.168.0.1
OS management Network IP	Yes	An extra IPv4 address in the OS/cloud management network for LOC-A to perform OS deployment. This IP address is usually in the same subnet of the External Network IP address, and it needs to be a different from IP the External Network IP.	30.0.0.169
OS management Network Netmask	Yes	Netmask of the subnet for the OS/cloud management network interface.	255.255.255.0
OS management Network Gateway	Yes	The gateway of the OS/cloud management network interface.	30.0.0.1
DNS Server #1	Yes	Primary DNS server for the appliance. **Note:** This does not need to be the DNS server used by the edge sites. You can plan and import the settings for the DNS servers for the edge site later through LOC-A portal web interface.	8.8.8.8
DNS Server #2	No	Secondary DNS server for the appliance.	114.114.114.114

Table 3: LOC-A deployment properties

Figure 4 and Figure 5 show two examples of the input for a dedicated XCC network and a shared XCC network:

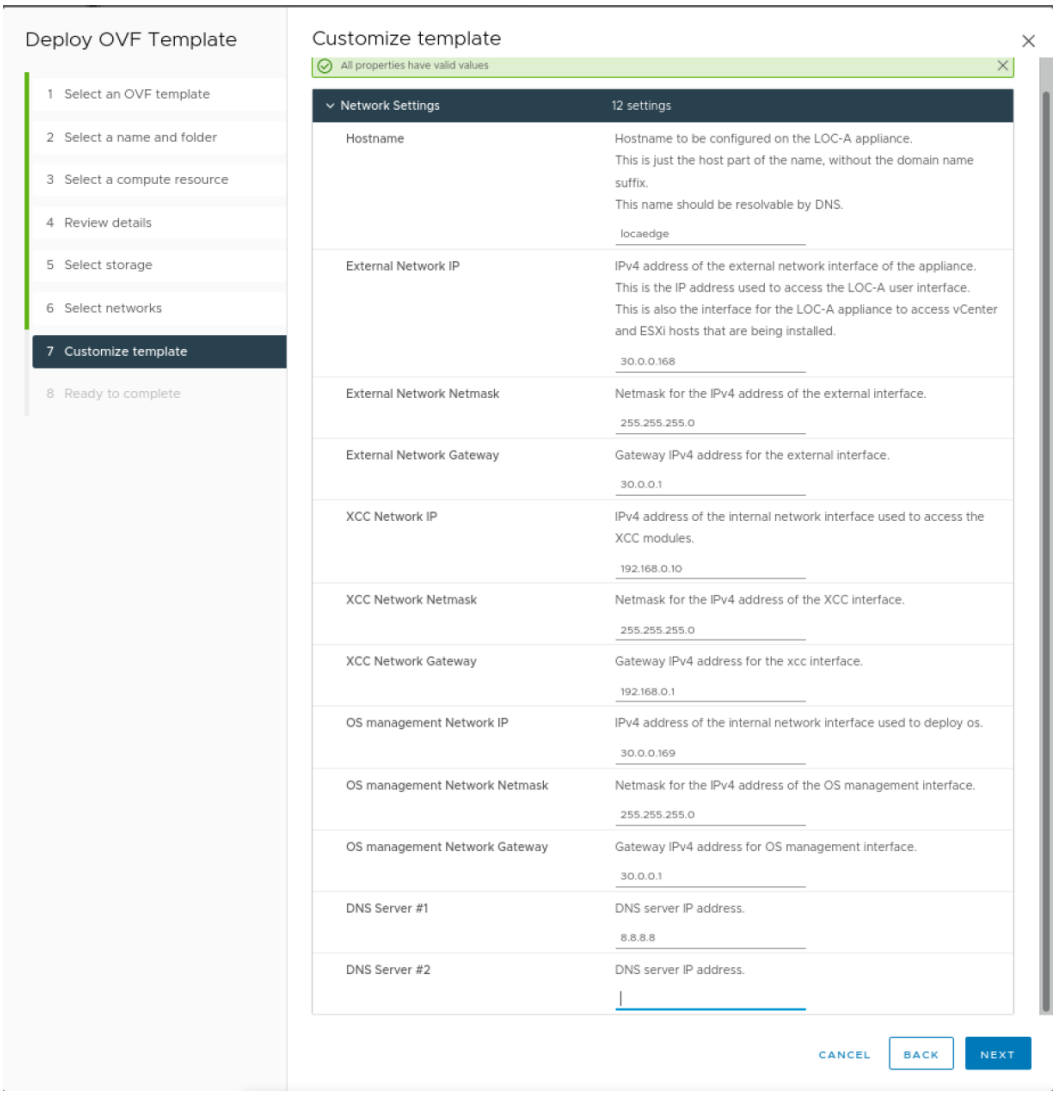


Figure 4: Deployment properties for dedicated XCC network

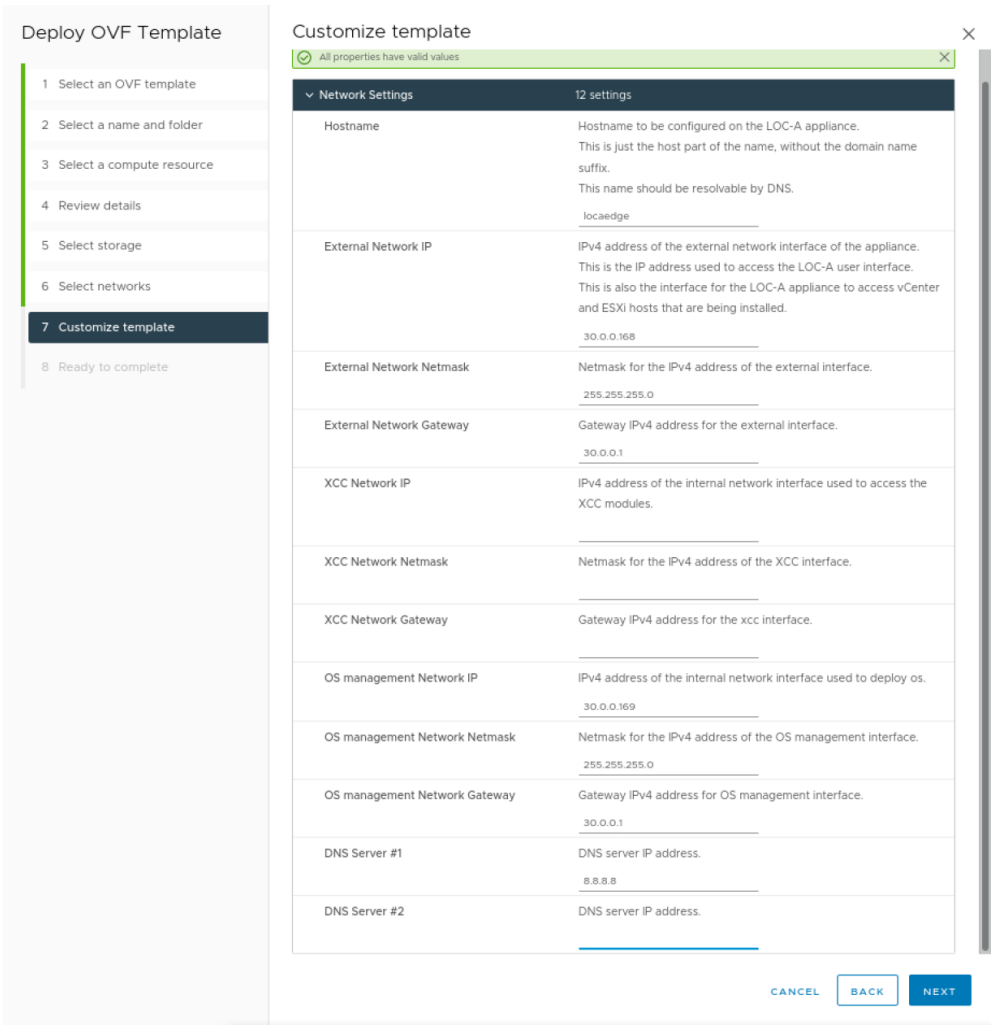


Figure 5: Deployment properties for shared network

i. Click **Next** to complete template customization.
j. Review and accept the OVA installation by clicking **Finish** on the 'Ready to complete' screen. The OVA installation can take quite some time depending on the speed of your network.
k. After the installation of the OVA completes, ensure that the VM starts successfully.

It will take several minutes for LOC-A services to start up after the VM is booted. You will be able to access the LOC-A Core Framework web portal through:

https://[*External Network IP*] .

The default credential is:
username: admin
password: Lenovo@123

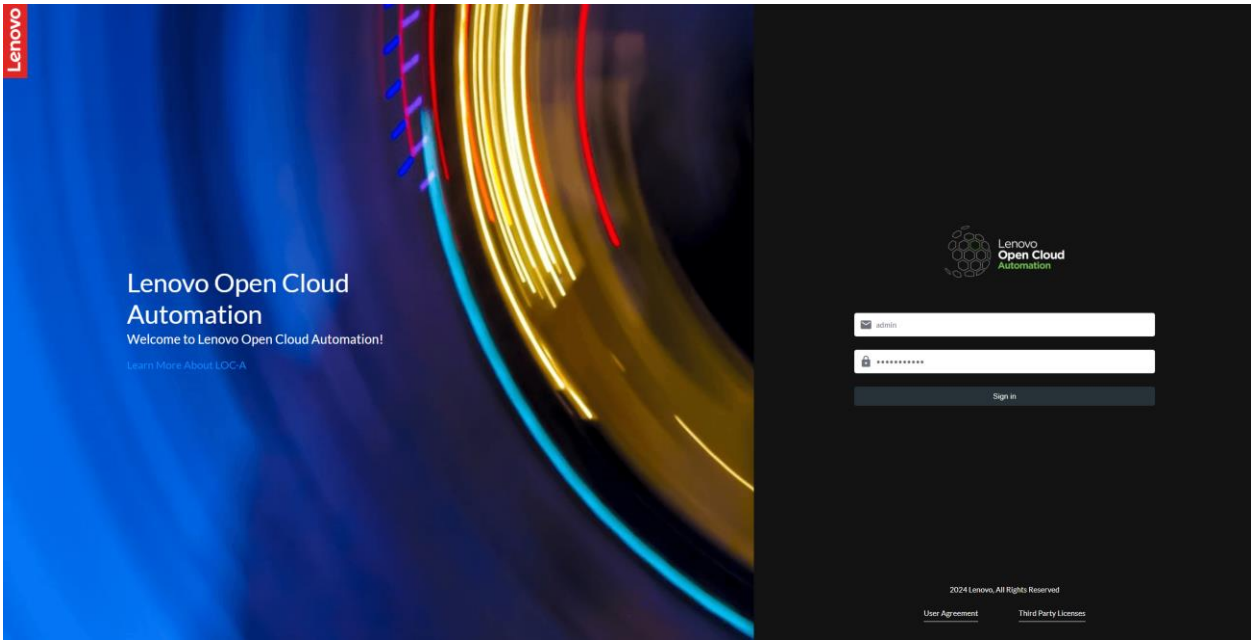


Figure 6: LOC-A Core Framework web portal

Note: After you log in, you are forced to change the initial password for the default admin user. You can also add new users later through **Setup → Users** in section *User management*.

Firewall requirements

The LOC-A VM appliance has two network interface cards. One is the **External-Network**, which is configured with External Network IP and OS management Network IP.

The other one is the **XCC-Network**, which is configured with XCC Network IP. **XCC-Network** is only needed when the customer environment has a separate BMC management network and OS network.

Below are the required infrastructure firewall requirements base on the two network topology options:

- Converged BMC management network and OS network:

Both BMC management network and OS network are converged, LOC-A appliance accesses this network through **External-Network** NIC.

Action	Source	Destination	Service	Port	Appliance NIC
Allow	Customer GUI clients	External Network IP	TCP	443	External-Network
Allow	External Network IP	Appliance DNS server, DNS network services in metadata	TCP/UDP	53	External-Network
Allow	External Network IP	Host Device OS IPs	TCP	Specific to cloud flavors*	External-Network
Allow	External Network IP	Cloud services in metadata	TCP	Specific to cloud services**	External-Network
Allow	XCC Network Devices	XCC network IP	UDP	427, 1900	XCC-Network

Allow	XCC Network Devices	XCC network IP	TCP	13001	XCC-Network
Allow	OS management Network IP	Host Device XCC IPs	TCP	443	External-Network
Allow	Host Device OS IPs	OS management Network IP	TCP	443	External-Network

Table 4: Firewall requirement for converged network

- Separate BMC management network and OS network:

BMC management network and OS network are isolated, LOC-A appliance accesses OS network through **External-Network** NIC, and access BMC network through **XCC-Network** NIC in a dedicated way.

Action	Source	Destination	Service	Port	Appliance NIC
Allow	Customer GUI clients	External Network IP	TCP	443	External-Network
Allow	External Network IP	Appliance DNS server, DNS network services in metadata	TCP/UDP	53	External-Network
Allow	External Network IP	Host Device OS IPs	TCP	Specific to cloud flavors*	External-Network
Allow	External Network IP	Cloud services in metadata	TCP	Specific to cloud services**	External-Network
Allow	XCC Network Devices	XCC network IP	UDP	427, 1900	XCC-Network
Allow	XCC Network Devices	XCC network IP	TCP	13001	XCC-Network
Allow	XCC Network IP	Devices XCC IPs	TCP	443	XCC-Network
Allow	Host Device OS IPs	OS management Network IP	TCP	443	External-Network

Table 5: Firewall requirement for separate network

Note:

*: For ESXi, VMware vSAN Cluster deployment, Host Device OS IPs need to have port 443 accessible. For other cloud/OS flavors, no specific requirements are needed.

**: For VMware vSAN Cluster deployment, vCenter service needs to have port 443 accessibility. For RedHat OpenShift Container Platform deployment, Assisted Installer service needs to have port 8080 accessibility.

For hardware management functionalities, Lenovo LXCA, Lenovo LXCO, Lenovo Management Hub services need to have port 443 accessibility.

Upgrade LOC-A Appliance

LOC-A supports in-place upgrades using a patch since release 3.2. It allows users to upgrade LOC-A from the current version to higher version. LOC-A also provide a CLI for the upgrade from 3.1 to a newer version.

Before you start

You must first check for available upgrade patches and then download the upgrade patch. The upgrade patch contains the LOC-A code changes, including new releases and upgrade patches.

Once you have the new release or upgrade patch, follow these steps to prepare the upgrade:

1. Get the upgrade patch from Lenovo. The patch contains all resources needed for an upgrade.
2. Unpack the upgrade patch. After unpacking the patch, we will get these files:
    a. README.md
    b. changelog
    c. updatePackageSigned.tar
3. Take a snapshot for LOC-A appliance. The snapshot may be used in the case that any issues are encountered during the upgrade. Users can revert the appliance to the previous snapshot.

Upgrade the appliance to a higher version (supported since release 3.2)

Notes:

- Need to make sure there are no running tasks or operations before entering into maintenance mode. The error message will pop up if try to enter maintenance when there are running tasks and operations.
- The patch must be applied under maintenance mode.
- If there are any issues happening during upgrade, you can revert the appliance to previous snapshot taken before upgrade.
- LECP flavor is no longer supported as of 3.2. After upgrading, it is not possible to create new LECP flavor type templates and instances. The historical data will still be there.

Follow these steps to upgrade the LOC-A appliance:

Step 1. Upload upgrade patch.

a) From the LOC-A web interface, click **Maintenance - Patches Upload/Apply**.

b) Click the upload button  .
c) Click **Browse** to find the patch file that you downloaded.
d) Click **Upload** to upload the patch.

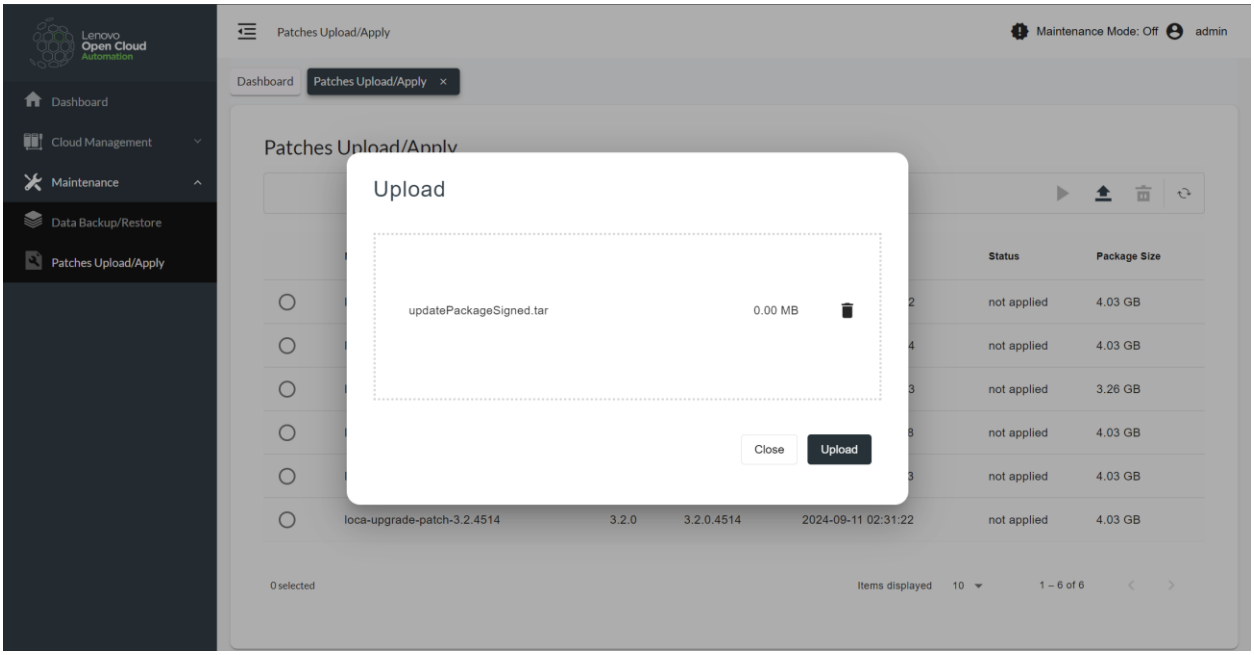


Figure 7: Upload upgrade package

Step 2. Set LOC-A to maintenance mode

a) Click the **Maintenance Mode: Off**.
b) Click the **On** to set maintenance mode.

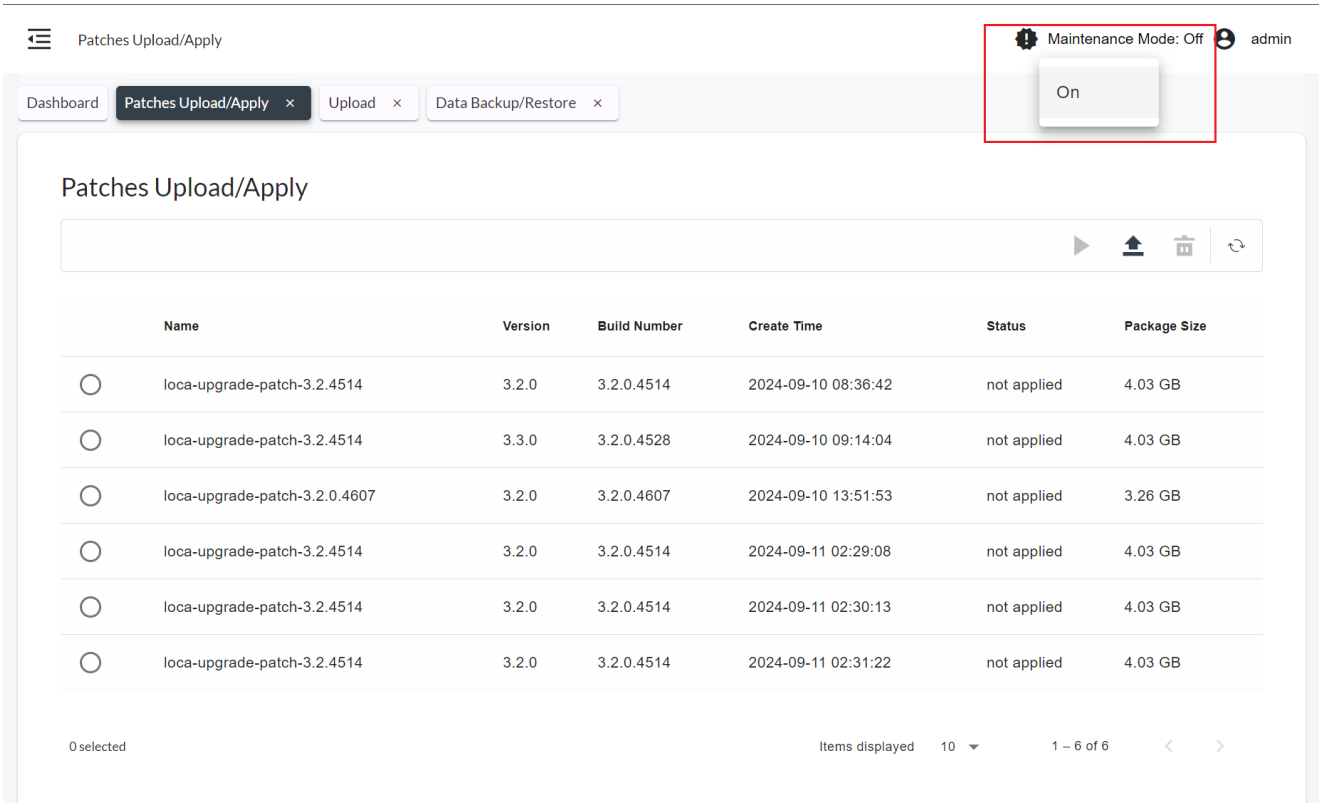


Figure 8: Set maintenance mode

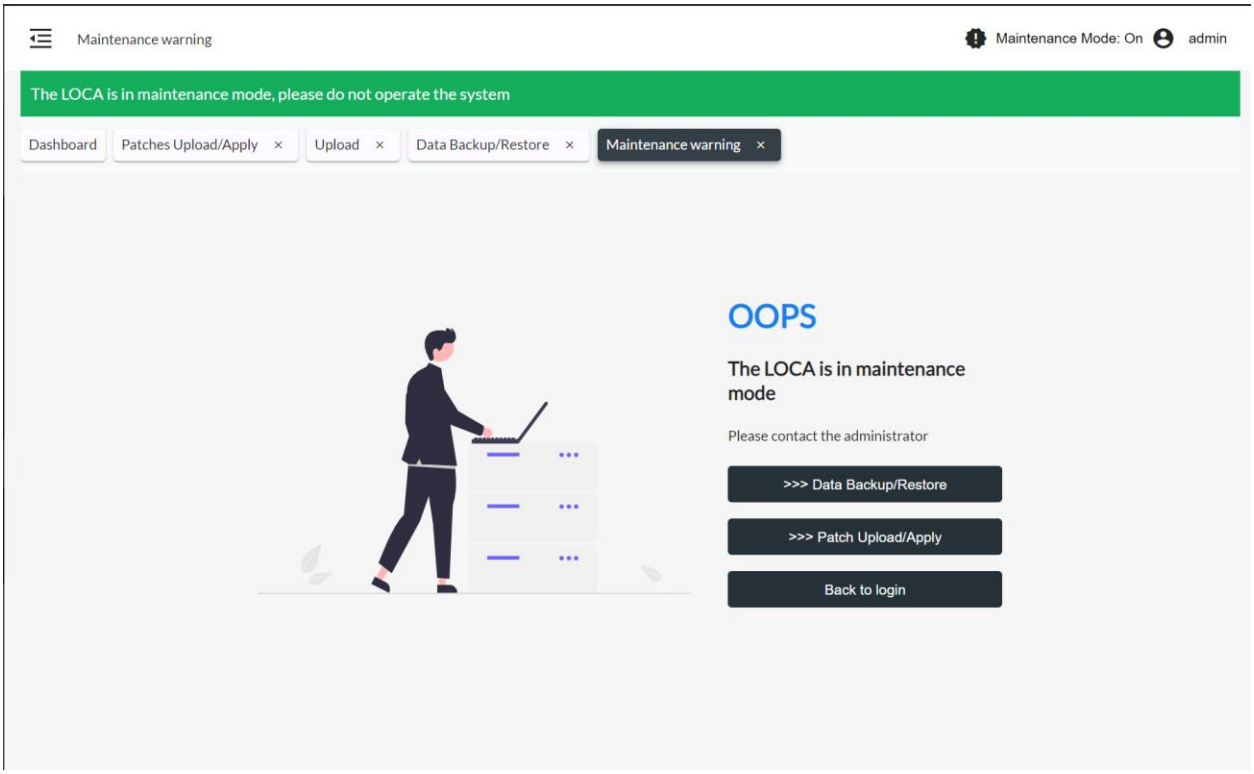


Figure 9: Maintenance mode

Step 3. Apply the patch

a) Click the **>>> Patches Upload/Apply** button.

b) Select a patch and click the Run icon ▶ .

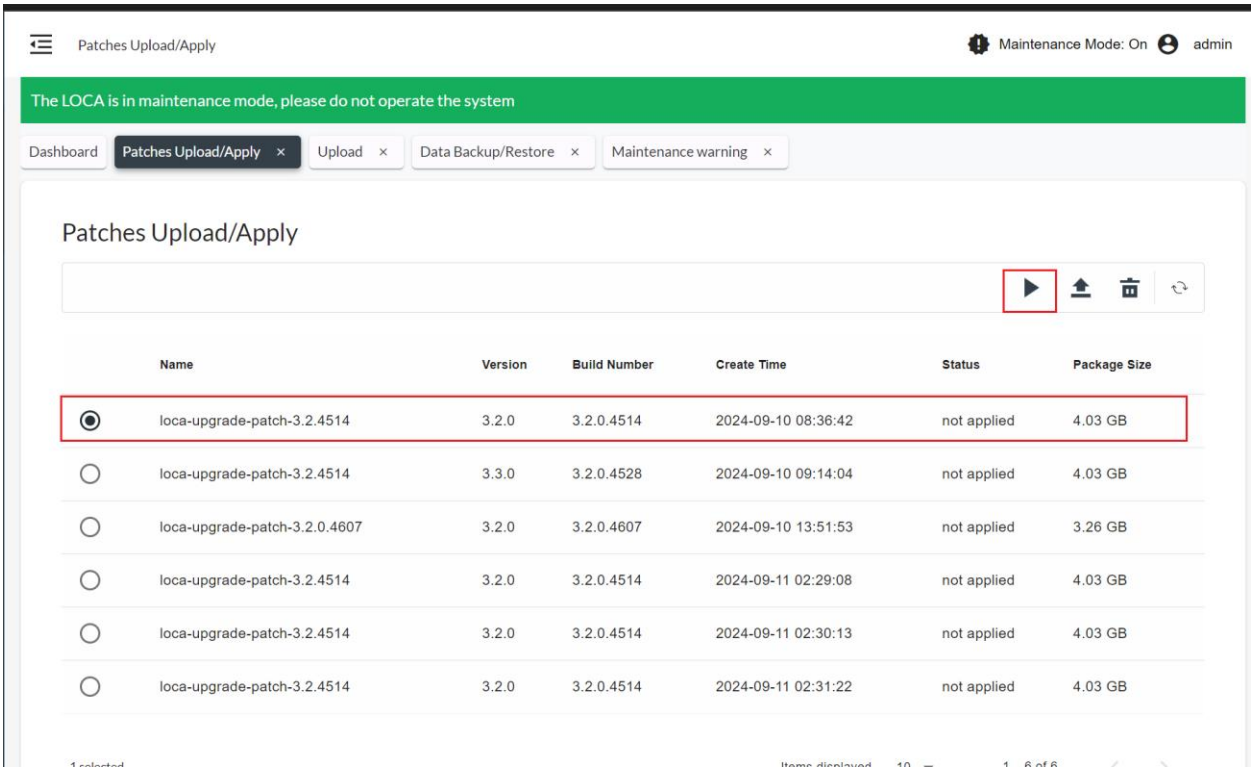


Figure 10: Apply patch

Note:

- Applying the patch will take about 15 minutes. You can click the refresh icon to check the real time status of patch application during the upgrade.
- The patch has possible statuses of **not applied**, **applying**, **failed** and **applied**. The web page needs to be refreshed after restoring data.

Upgrade appliance from 3.1 to higher version

Since there is no web interface implemented for 3.1, you can only use a CLI called “ladm” to do the upgrade from 3.1 to a newer version. Contact the Lenovo support team to get the tool.

Note:

- Debug shell must be enabled before performing a CLI based upgrade.
- LECP flavor is no longer supported as of 3.2. After upgrading, it is not possible to create new LECP flavor type templates and instances. The historical data will still be there.

Following these steps to upgrade the LOC-A appliance:

Step 1. Copy ladm and the upgrade package to the LOC-A appliance of 3.1 through debug shell.

Note: Recommend copying upgrade package to the folder “/tmp” that has enough space available.

Step 2. Login into LOC-A appliance of 3.1 through debug shell

Step 3. Run the following command inside the LOC-A appliance "./ladm upgrade -f <your file path>/updatePackageSigned.tar" to start the upgrade

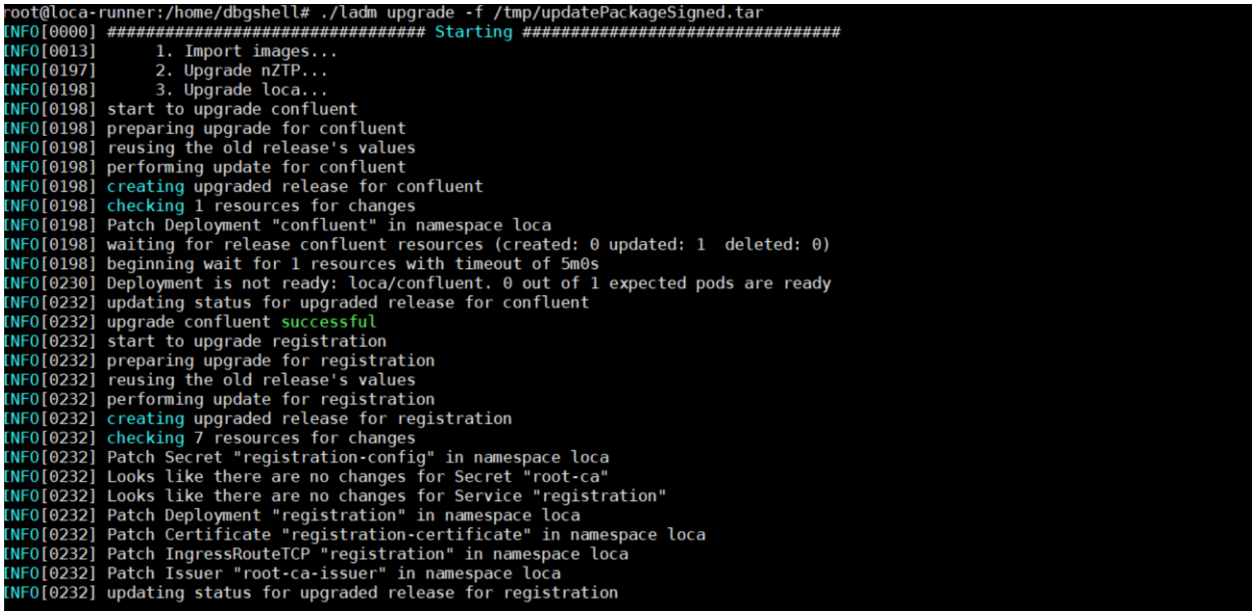


Figure 11: Apply patch for 3.1 appliance

Note:

- Refresh the web page after applying the patch.
- Because the device profile function is optimized, when upgrading from version 3.1 or 3.2 to version 3.3, the previous device profile will be replaced by the new device profile. The new device profile defines different best recipes for different flavors and model combinations. This behavior affects the device profile, template, and instance functions.

Functional user guide

Cloud setup

Cloud Setup is where LOC-A manages all the cloud cluster resources for edge sites. In Cloud Setup, you can make your plans for the edge sites by defining edge sites, IP ranges, network services, and cloud services required for cloud cluster deployment.

Cloud offerings supported by LOC-A are:

Cloud Offering	Supported Versions	Minimum Nodes
VMware ThinkAgile VX cluster (vSAN)	7.0	3
RedHat OpenShift Container Platform (OCP)	4.12 ~ 4.15	3

Table 6: Cloud flavors supported by LOC-A

Furthermore, LOC-A supports bare-metal OS deployment on edge site nodes. LOC-A supports the following OS types:

OS Family	Supported Versions	Minimum Nodes
Ubuntu	18.04.6, 20.04.6, 22.04.6, 22.04.3, 22.04.4, 22.04.5	1
ESXi	7.0.3, 8.0.1	1
CentOS	7.9, 8.3	1

Table 7: OS types supported by LOC-A

LOC-A supports importing your resources in batches via an Excel file.

Follow these steps to prepare planning data:

a) From the LOC-A web interface, click **Setup→Upload**.
b) Click **Download metadata file template** to get the sample Excel file "Cloud_Setup_Standard_Template.xlsx".
c) Follow the embedded instructions to fill in the file with planning data of your sites.
d) Click **Browse** to find the file that you updated.
e) Click **Upload metadata** to upload the template.

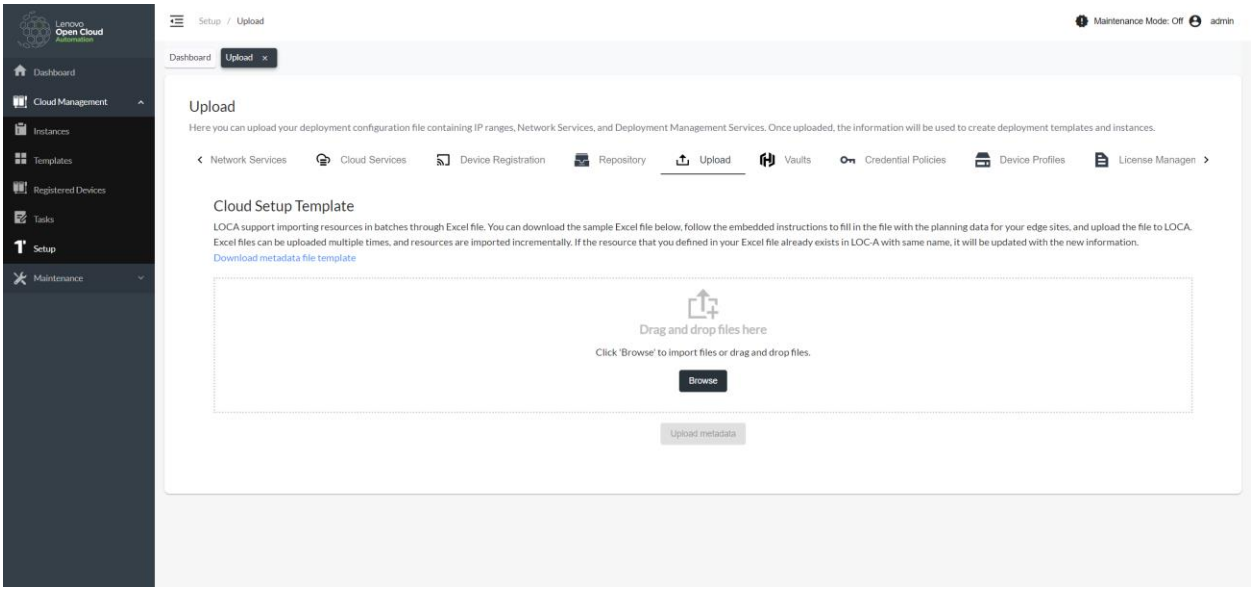


Figure 12: Uploading Excel file to Setup

LOC-A will process the Excel worksheets and create the sites and resources you entered into the LOC-A system. It will take several seconds or minutes for the task to complete, depending on the number of resources you defined. Click **Tasks** to check the progress of the task. When the task is completed, you will see a notification on the page.

Note: Excel files can be uploaded multiple times, and resources are imported incrementally. If the resource (sites, IP ranges, cloud services, network services) that you defined in your Excel file already exists in LOC-A with same name, it will be updated with the new information. If the resource does not exist, it will be created. However, to delete a resource (such as an IP range), you will need to delete it from the LOC-A portal.

After planning metadata is uploaded, you can view the resources details in their corresponding tabs in the **Setup** page.

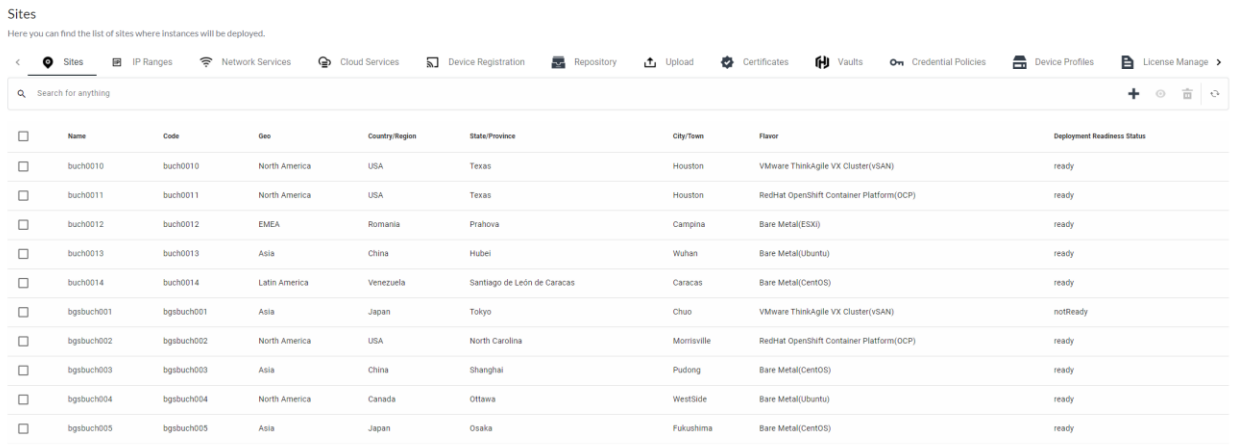
Sites

An edge site is typically several nodes geographically located at a building or a campus. Figure 13 shows an example page that lists all of the edge sites. You can view the site name, site code, and the geographical region it belongs to. The typical hierarchy of edge sites is:

Geo → Country/Region -> State/Province → City/Town →Site →Servers

Site name is the name that identifies a site. In addition, you can specify a site code for the site.

Note: The site name and site code must be unique within the LOC-A system.



Name	Code	Geo	Country/Region	State/Province	City/Town	Flavor	Deployment Readiness Status
buch0010	buch0010	North America	USA	Texas	Houston	VMware ThinkAgile VX Cluster(vSAN)	ready
buch0011	buch0011	North America	USA	Texas	Houston	RedHat OpenShift Container Platform(OCP)	ready
buch0012	buch0012	EMEA	Romania	Prahova	Campina	Bare Metal(ESXi)	ready
buch0013	buch0013	Asia	China	Hubei	Wuhan	Bare Metal(Ubuntu)	ready
buch0014	buch0014	Latin America	Venezuela	Santiago de León de Caracas	Caracas	Bare Metal(CentOS)	ready
bgsbuch001	bgsbuch001	Asia	Japan	Tokyo	Chuo	VMware ThinkAgile VX Cluster(vSAN)	notReady
bgsbuch002	bgsbuch002	North America	USA	North Carolina	Morrisville	RedHat OpenShift Container Platform(OCP)	ready
bgsbuch003	bgsbuch003	Asia	China	Shanghai	Pudong	Bare Metal(CentOS)	ready
bgsbuch004	bgsbuch004	North America	Canada	Ottawa	WestSide	Bare Metal(Ubuntu)	ready
bgsbuch005	bgsbuch005	Asia	Japan	Osaka	Fukushima	Bare Metal(CentOS)	ready

Figure 13: Sites list

Deployment Readiness:

LOC-A performs a deployment readiness check for the site metadata and displays the result in the **Deployment Readiness Status** column. If a site has all metadata validated for cloud deployment, it will be shown as **Ready**. Otherwise, the value is shown as **Not Ready**. Hover your mouse over the field to display a message with a detailed explanation for the issue, such as a mandatory service missing, or the planned IP range is not valid.

Figure 14 shows an example of the detailed explanations that can be shown.

Name	Code	Geo	Country/Region	State/Province	City/Town	Flavor	Deployment Readiness Status
buch0010	buch0010	North America	USA	Texas	Houston	VMware ThinkAgile VX Cluster(vSAN)	notReady
buch0011	buch0011	North America	USA	Texas	Houston	RedHat OpenShift Container Platform(OCP)	network BMC doesn't exist network Management doesn't exist

Figure 15: Deployment Readiness details

When you import the Excel file again with corrected metadata, the deployment readiness status is updated to reflect the latest check result.

View a site's details:

Click a site to view more details, such as IP address ranges, cloud services, network services (NTP and DNS), that are planned for this site.

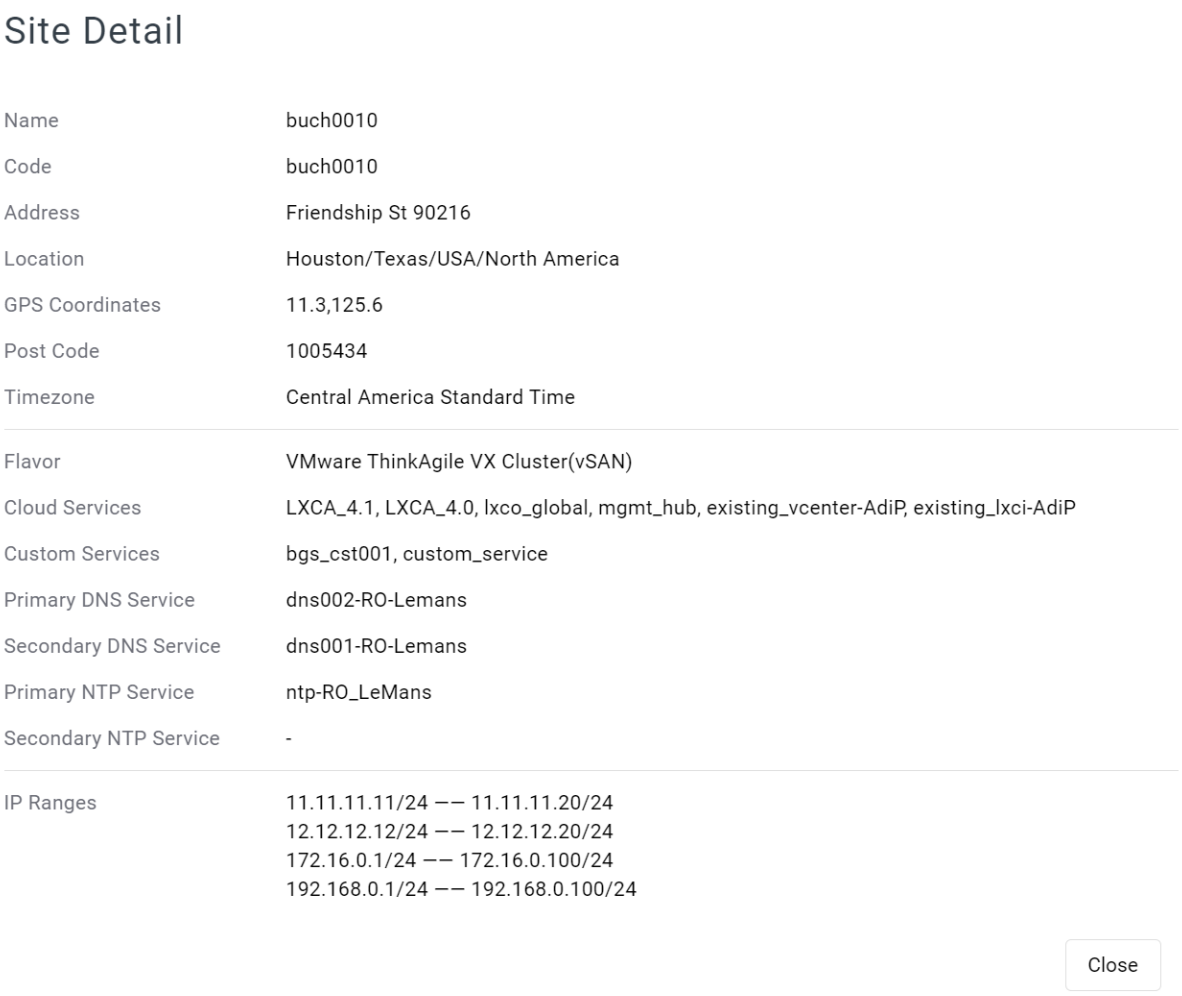


Figure 16: Site details

Create a site:

Starting with LOC-A version 3.3, you can click the **Create** button to create a site, it will pop up a page to guide you through the creation process.

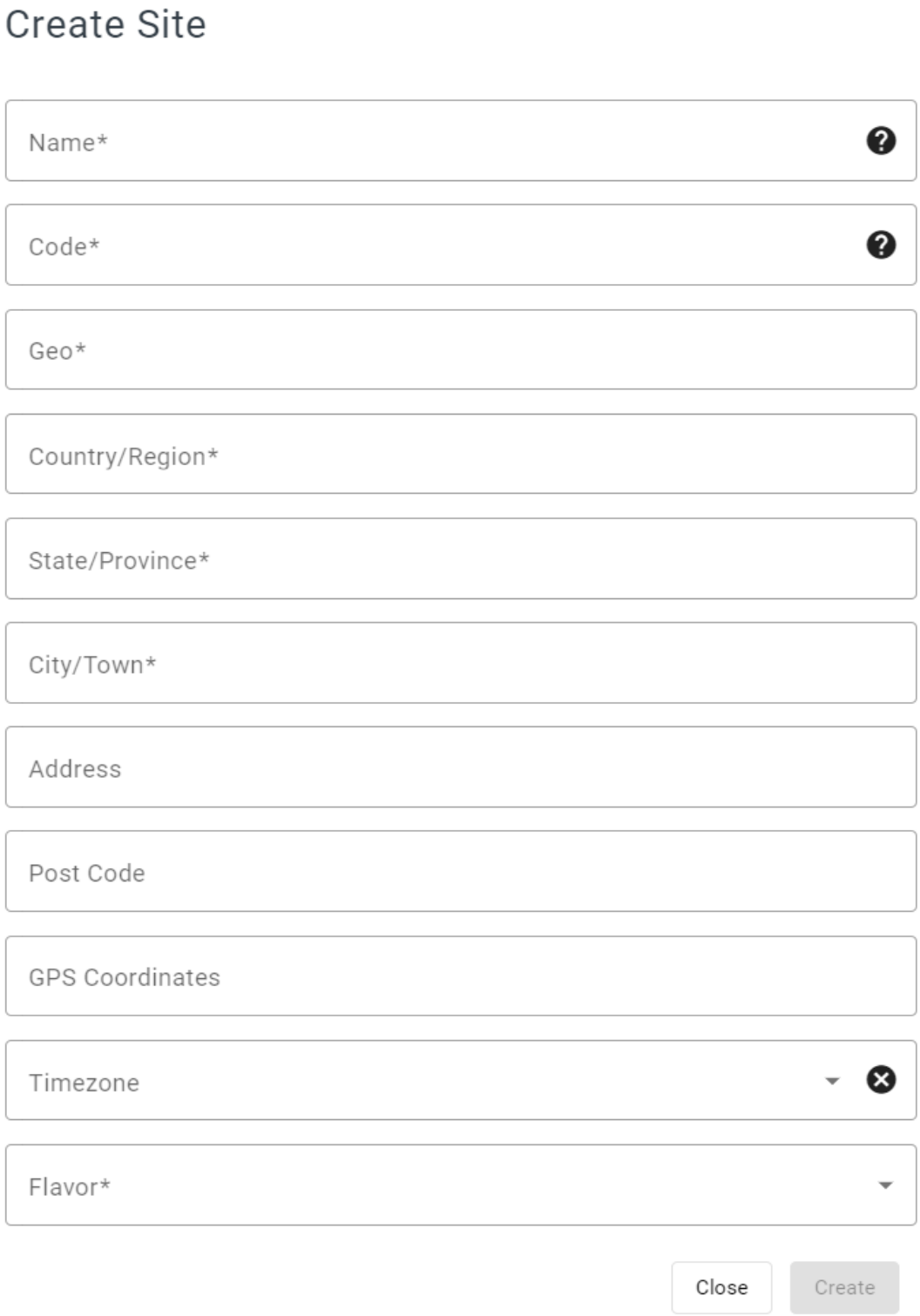


Figure 17: Create a site

Fill in the fields for site creation. These typically include:

- Name*: Enter the name of the site.
- Code*: Enter a unique code for the new site.
- Geo*: Provide the geographical location information.
- Country/Region*: Select the country or region where the site is located.
- State/Province*: Enter the state or province.
- City/Town*: Enter the city or town.
- Address: Provide the detailed address of the site.
- Post Code: Enter the postal code.
- GPS Coordinates: Enter the GPS coordinates if available.
- Timezone: Select the appropriate time zone.
- Flavor*: Choose the flavor to be supported at that site.

The fields marked with an asterisk (*) are mandatory. Fill in any optional fields according to requirements. These might involve extra site-specific details or configurations. Check the entered information to guarantee its correctness. Once the **Create** button is clicked, the system will handle the request and create the new site, bind the IP ranges, and assign services to the site.

Note:

- The Site name must be globally uniquely.
- Ensure that all required fields are filled out before attempting to create the site.
- If there are any validation errors, the site will not be created, and you need to correct the errors before proceeding.
- After the site is successfully created, it may take some time for the system to fully configure and display the new site in relevant lists or dashboards.

Delete a site:

To delete one or more sites, select the sites to be deleted, and click **Delete**. The deletion may take several seconds to clean up site resources. After the deletion is complete the page will be automatically refreshed to show the updated results.

You are not allowed to delete a site that has existing cloud clusters deployed. To delete a site with clusters, you must remove the cluster first.

Note: A site cannot be deleted if there are devices registered to it. You must delete the devices that are registered to the site first. When a site is deleted, all resources (IP ranges, networks services, cloud services) that were planned to the site are also deleted.

IP Ranges

IP ranges are IP resources that can be used by an edge site. The IP range is identified using an IP range name; the IP range name must be unique within LOC-A, and the IP range should not overlap with any other IP ranges.

For each specific cloud flavor, you can define multiple IP ranges for a site to differentiate the purpose or role of the network. An IP range can be dedicated for a site, or it can be common to all sites (labeled as **any** in the Site column), depending on the network role.

IP ranges will be associated to the site in the order of affinity. An IP range dedicated for a site has a higher affinity than an IP range designated for any site. For example:

- range1 of the vSAN-vSAN role is defined for siteA
- range2 of the vSAN-vMotion role is defined as any

In this scenario, siteA will use range1 as its IP pool for the vMotion network.

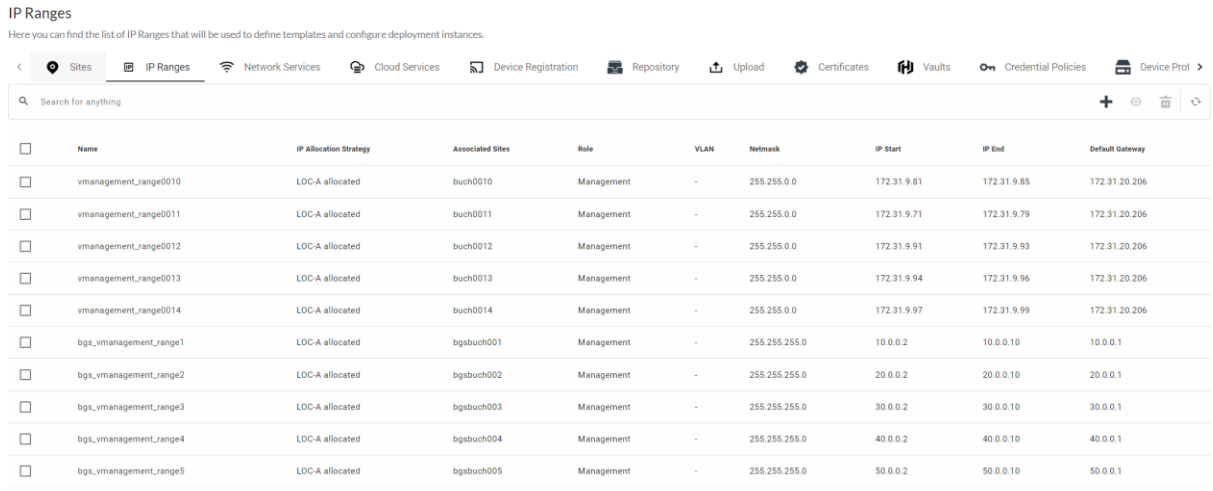


Figure 18: IP ranges list

IP ranges are essential resources to deploy and manage a cloud cluster. Different cloud flavors might have specific roles of IP ranges defined for cloud deployment.

Table 8 shows the IP ranges required for a LOC-A edge site for cloud deployment based on different cloud offerings:

Cloud or Bare Metal OS offering	IP range role	Description	Mandatory	Can be common to all sites	Gateway required
VMware vSAN	Management	Node OS/management network	Yes	No	Yes
	vSAN-vSAN	Node vSAN network	Yes	Yes	No
	vSAN-vMotion	Node vMotion network	Yes	Yes	No
	BMC	XCC (BMC) management network	Yes	No	Yes
RedHat OCP	Management	Node OS/management network	Yes	No	Yes
	BMC	XCC (BMC) management network	Yes	No	Yes
Bare Metal OS (Ubuntu, ESXi, CentOS)	Management	Node OS/management network	Yes	No	Yes
	BMC	XCC (BMC) management network	Yes	No	Yes

Table 8: Cloud cluster IP range requirement

Note:

1. 10.42.0.0/15 is the network CIDR reserved by LOC-A. Make sure that you do not have overlapping IP ranges defined.
   - If this address range is in use within your network and is accessible by the LOC-A Core Framework appliance or the systems being deployed this may also cause an inconsistent OS deployment experience.
2. For RedHat OpenShift Container Platform:

- The last two IP addresses of the Management IP range will be assigned for API VIP and Ingress VIP of the cluster. As a result, you will need to make sure that your Management IP range contains at least N+2 valid IP addresses, N is the number of nodes in the cluster.

For more details about network requirements, please refer to the official documentation of the cloud offering.

View an IP range's details:

You can view an IP range's details by clicking on one IP range.

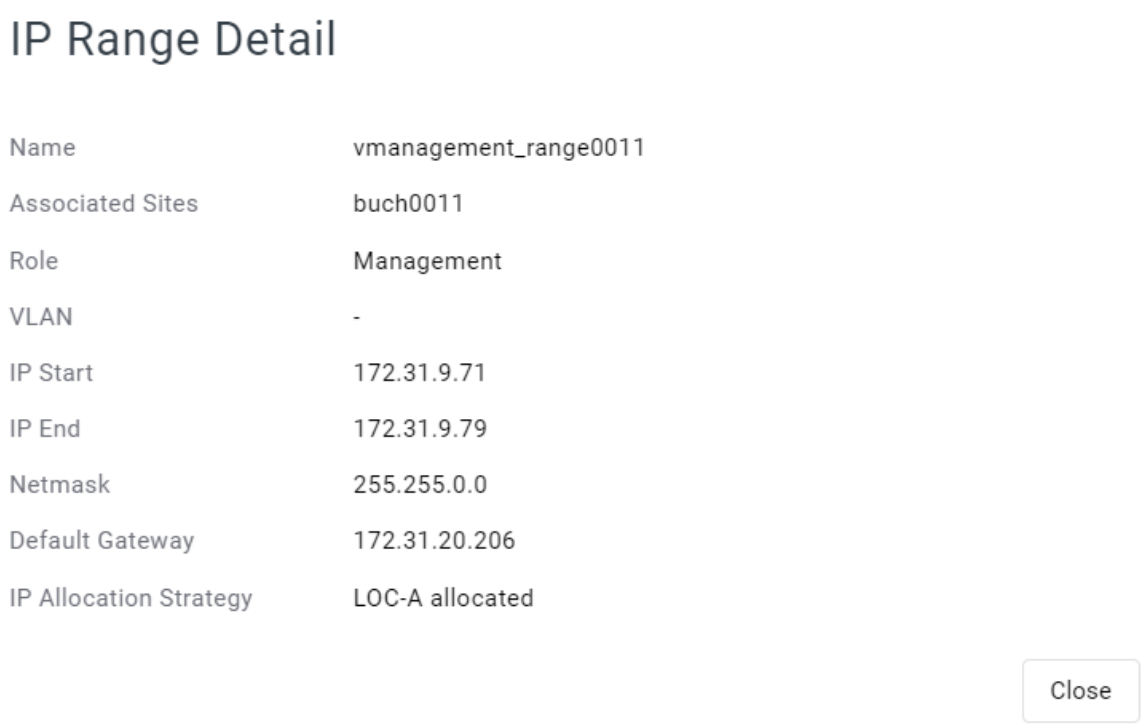


Figure 19: IP range detail

Create an IP range:

Starting with LOC-A version of 3.3, you can click the **Create** button to create an IP range, it will pop up a page to guide the creation process.

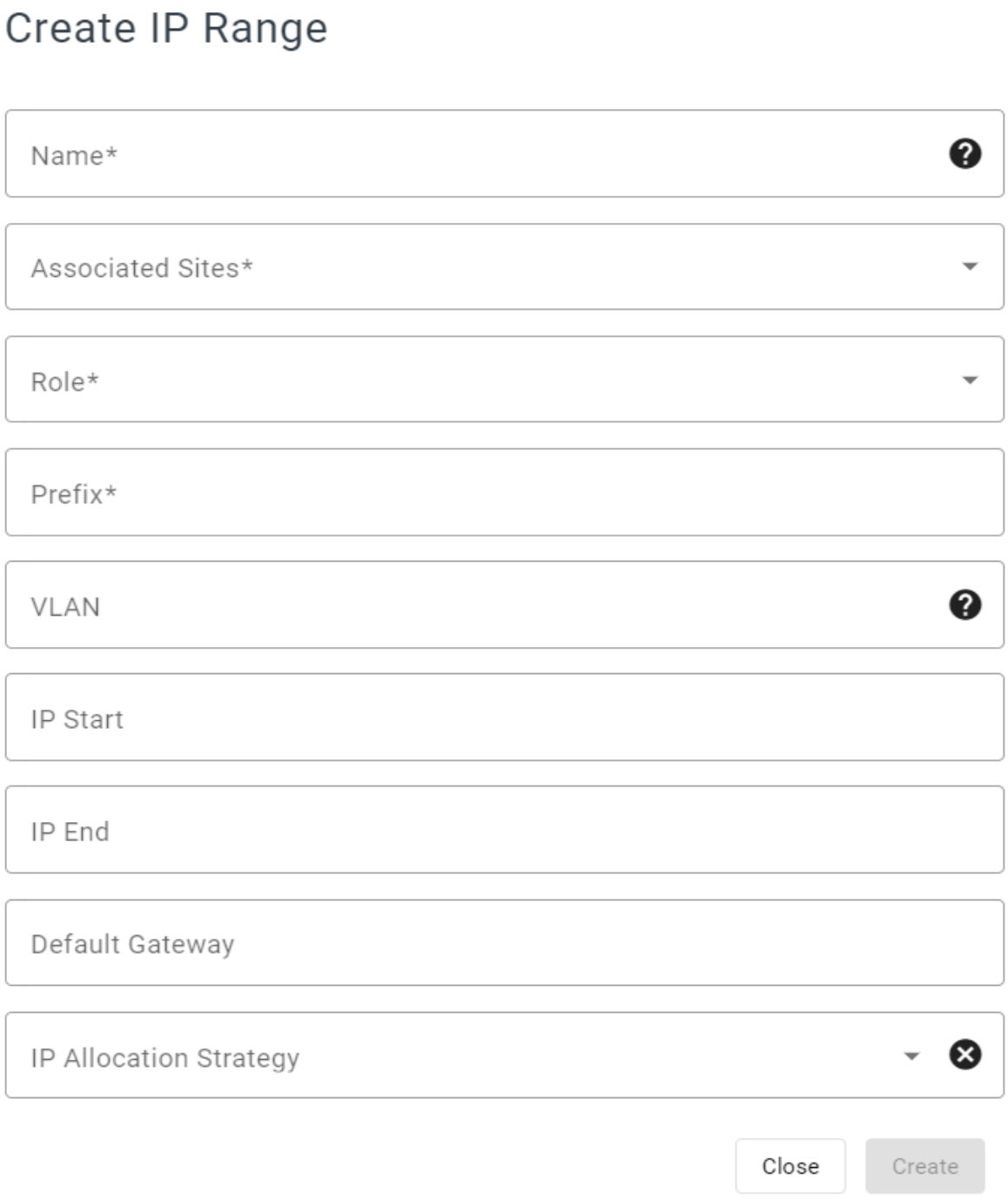


Figure 20: Create an IP range

Fill in the fields for IP range creation. These typically include:

- Name*: Enter the name of the IP range.
- Associated Sites*: Select the associated sites.
- Role*: Select the network role

- Prefix*: Enter the prefix value.
- IP Start: Enter the start IP address.
- IP End: Enter the end IP address.
- Default Gateway: Enter the gateway address.
- IP Allocation Strategy: Select the allocation strategy.

The fields marked with an asterisk (*) are mandatory. Fill in any optional fields according to your requirements. These might involve extra IP range specific details or configurations. Check the entered information to guarantee its correctness. Once the **Create** button is clicked, the system will handle the request and create the new IP range. Meanwhile binding it to associated sites and update the Deployment Readiness Status in the Sites page.

Note:

- If the Start/End IP addresses are not defined, they are automatically assigned based on the prefix.
- If the 'IP Allocation Strategy' option is set to 'User allocated', users should allocate the IP manually. If the 'IP Allocation Strategy' option is set to 'LOC-A allocated', LOC-A will allocate the IPs automatically.
- Ensure that all required fields are filled out before attempting to create the IP range.
- If there are any validation errors, the IP range will not be created, and you need to correct the errors before proceeding.
- After the IP range is successfully created, it may take some time for the system to fully configure and display the new IP range in relevant lists or dashboards.

Delete an IP range:

To delete one or more IP ranges, select the IP range(s) and click **Delete**. The deletion may take several seconds. After the deletion is complete, the page will be automatically refreshed to show the updated results.

Note: If a mandatory IP range is deleted, a site will be not eligible for cloud deployment, and the deployment readiness status will display **notReady**.

Network Services

Network services are the essential external services for cloud deployment, including NTP and DNS servers. You can also define customized network services that may be involved in the cloud deployment and lifecycle management. LOC-A supports an automated connectivity check for network services during the server registration process (Near Zero Touch Provisioning or nZTP). The network service name must be unique within LOC-A.

A network service can be allocated for one or multiple sites. You can specify a site list separated by commas. You can also specify any, which means the network service can be allocated for all sites.

Network services will be associated to the site in the order of affinity. For example,

- dns1 is defined for siteA, siteB
- dns2 is defined for siteA
- dns3 is defined for any

In this scenario, the DNS servers for siteA and siteB are:

- siteA: dns2 (primary), dns1 (secondary)
- siteB: dns1 (primary), dns3 (secondary)

If **Check Connectivity** is checked, this network service will be checked for connectivity during nZTP server registration.

For VMware vSAN cluster deployment, mandatory network services required for each site are:

- Two DNS servers

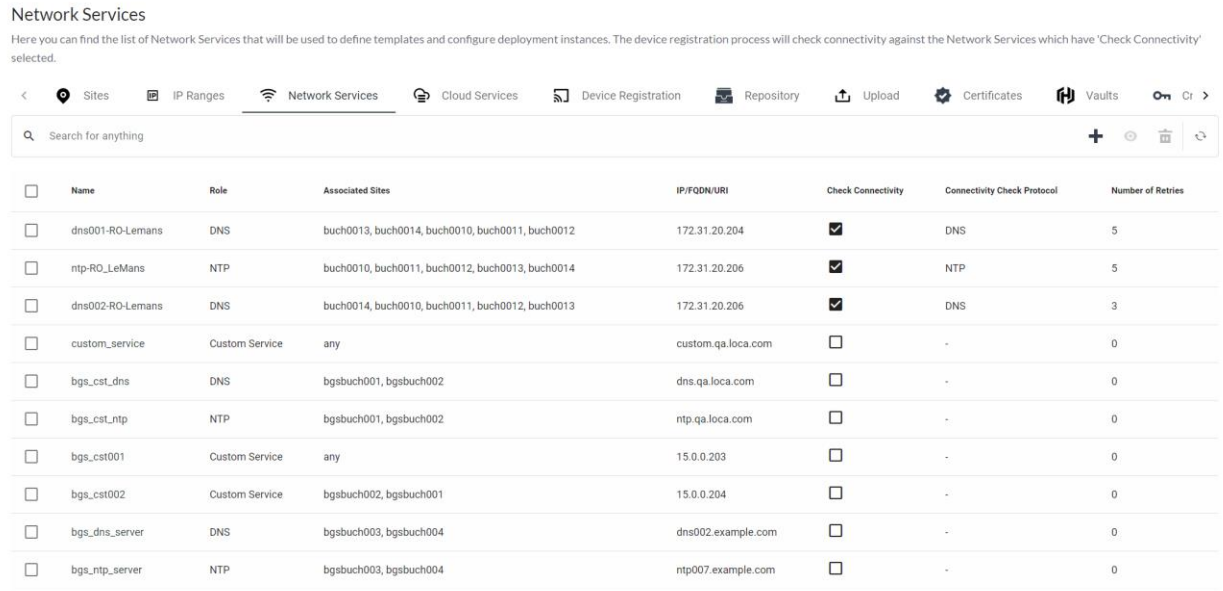
- One NTP server

For RedHat OCP cluster, mandatory network services required for each site are:

- One DNS server
- One NTP server

For Ubuntu bare-metal OS deployment, one DNS server is required. For other bare-metal OS deployment, network services are optional. If DNS or NTP servers are planned for a site, LOC-A automatically configures the deployed OS with the expected network settings when doing bare metal OS deployment.

Figure 21 shows an example page that lists network services:



Name	Role	Associated Sites	IP/FQDN/URI	Check Connectivity	Connectivity Check Protocol	Number of Retries
dns001-RO-Lemans	DNS	buch0013, buch0014, buch0010, buch0011, buch0012	172.31.20.204	☑	DNS	5
ntp-RO_LeMans	NTP	buch0010, buch0011, buch0012, buch0013, buch0014	172.31.20.206	☑	NTP	5
dns002-RO-Lemans	DNS	buch0014, buch0010, buch0011, buch0012, buch0013	172.31.20.206	☑	DNS	3
custom_service	Custom Service	any	custom.qa.loca.com	☐	-	0
bgs_cst_dns	DNS	bgsbuch001, bgsbuch002	dns.qa.loca.com	☐	-	0
bgs_cst_ntp	NTP	bgsbuch001, bgsbuch002	ntp.qa.loca.com	☐	-	0
bgs_cst001	Custom Service	any	15.0.0.203	☐	-	0
bgs_cst002	Custom Service	bgsbuch002, bgsbuch001	15.0.0.204	☐	-	0
bgs_dns_server	DNS	bgsbuch003, bgsbuch004	dns002.example.com	☐	-	0
bgs_ntp_server	NTP	bgsbuch003, bgsbuch004	ntp007.example.com	☐	-	0

Figure 21: Network services list

View a network service's details:

You can view a network service's details by clicking on one network service.

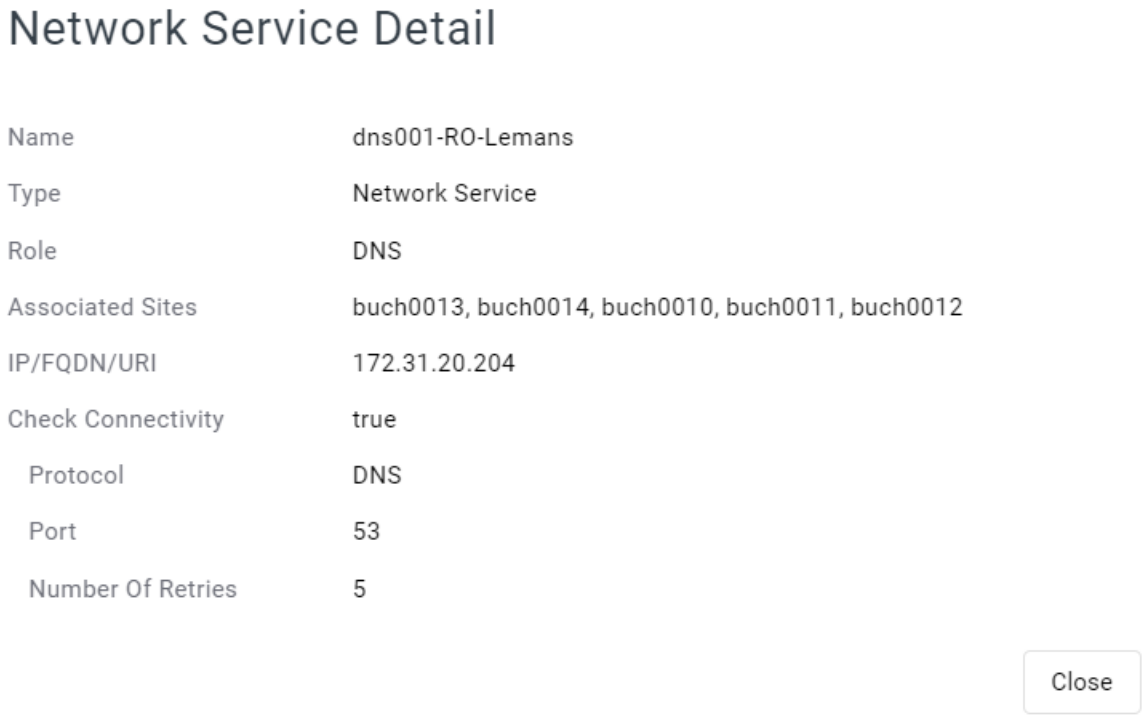


Figure 22: Network services detail

Create a network service:

Starting with LOC-A version of 3.3, you can click the **Create** button to create a network service, it will pop up a page to guide the creation process.

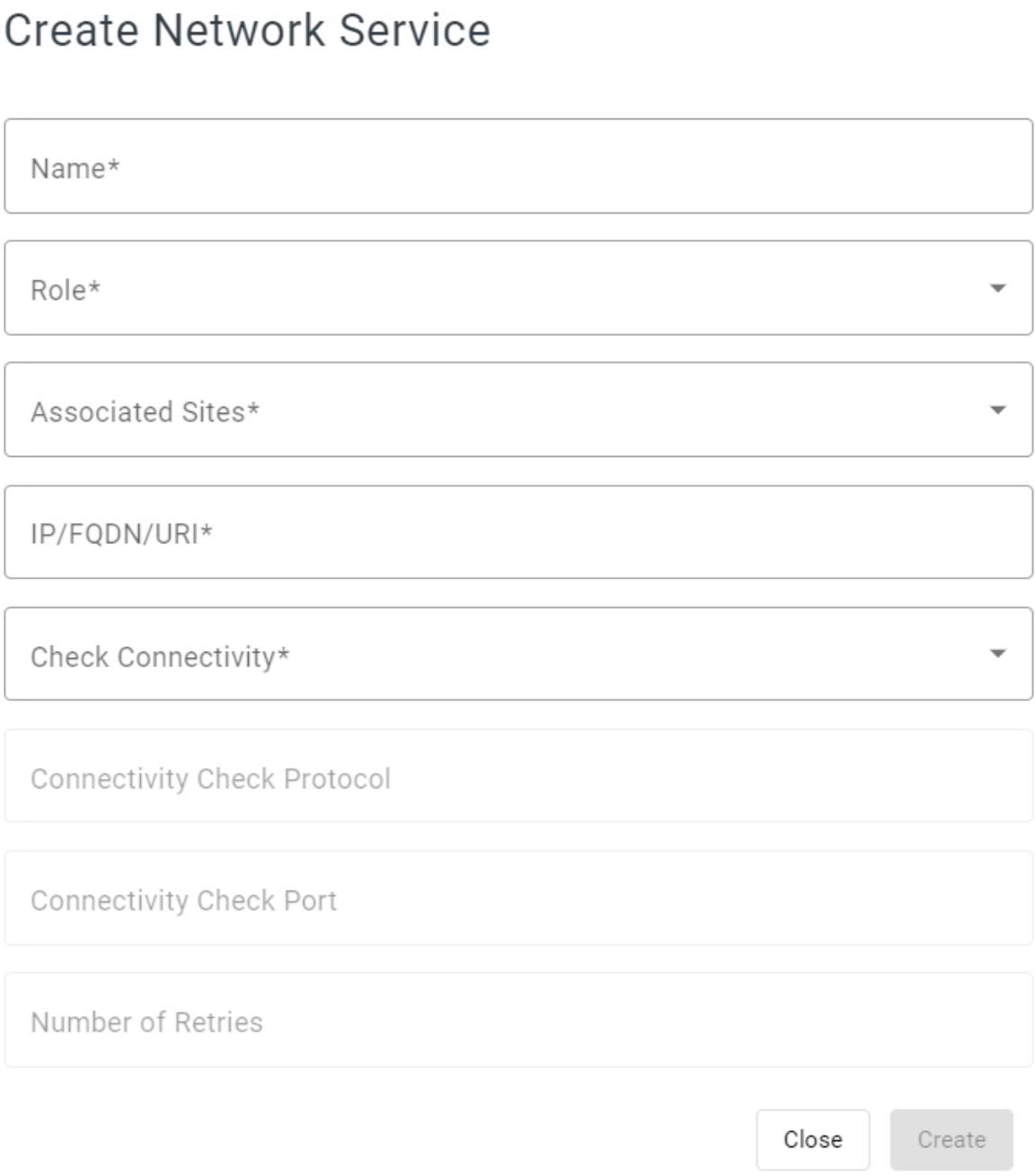


Figure 23: Create a network service

Fill in the fields for network service creation. These typically include:

- Name*: Enter the name of the network service.
- Role*: Select the network service role.
- Associated Sites*: Select the associated sites.
- IP/FQDN/URI*: Specify the service's access address.
- Check Connectivity*: Used for connectivity check.

- Connectivity Check Protocol: Specify the protocol for connectivity checks.
- Connectivity Check Port: Specify the port for the connectivity check.

The fields marked with an asterisk (*) are mandatory. Fill in any optional fields according to your requirements. These might involve extra network service specific details or configurations. Check the entered information to guarantee its correctness. Once the **Create** button is clicked to submit the form, the system will handle the request and create the new network service. Meanwhile binding it to associated sites and updating the Deployment Readiness Status in sites page.

Note:

- If the **Check Connectivity** option is set to **true**, please ensure that the **Connectivity Check Protocol** field is filled with the appropriate supported protocol (TCP, DNS, NTP, HTTP, HTTPS, SSH, PING, SOCKS). If a specific port is required, include the port information (e.g., HTTPS, Port 443), otherwise, the default port for the specified protocol will be used.
- If the **Check Connectivity** option is set to **true**, please ensure that the **Number of Retries** field is populated with a numeric value between 1 and 10, indicating the desired number of retry attempts.
- Ensure that all required fields are filled out before attempting to create the network service.
- If there are any validation errors, the network service will not be created, and you will need to correct the errors before proceeding.
- After the network service is successfully created, it may take some time for the system to fully configure and display the new network service in relevant lists or dashboards.

Delete a network service:

To delete one or more network services, select the network services to be deleted and click **Delete**. The deletion may take several seconds. After the deletion is complete, the page will be automatically refreshed the updated results.

Note: If a mandatory network service is deleted, a site will not be eligible for cloud deployment.

Cloud Services

Cloud services are the essential cloud-specific services for cloud deployment, such as vCenter for a VMware vSAN cluster deployment. You also need to provide credentials of the cloud services for LOC-A to perform automated tasks. LOC-A supports an automated connectivity check for cloud services during server nZTP registration process. The cloud service name needs to be unique within LOC-A.

A cloud service can be allocated for one or more sites. You can specify a site list separated by commas. You can also specify any, which means the cloud service will be allocated for all sites.

Cloud services will be associated to the site in the order of affinity. For example,

- vCenter1 is defined for siteA, siteB,
- vCenter2 is defined for siteA
- vCenter3 is defined for any

In this scenario, the vCenter server planned for siteA and siteB are:

- siteA: vCenter2
- siteB: vCenter1

If **Check Connectivity** is checked, this cloud service is checked for connectivity during nZTP server registration. The number of retries parameter is used to check for cloud service connectivity.

Starting from LOC-A 3.1 release, Site deployment readiness check will also check for sanity of cloud service credentials. Sites with cloud services that don’t have required credential information provided will appear

notReady until you fix the metadata. On the other hand, it's also not valid if you provide wrong credentials to cloud services that don't support.

LOC-A supports the following cloud service types:

Cloud Service Role	Platform Type	Credential Required	Description
Lenovo LXCA	Hardware management	Yes (no readiness check enforced, but you may fail to add/remove devices)	Lenovo xClarity Administrator (LXCA) is Lenovo's system hardware management solution that runs as a virtual appliance. LOC-A supports synchronizing devices to external hardware management tools like LXCA. If you have the LXCA service defined for one or more sites, LOC-A will automatically add the devices that are registered to LOC-A into the LXCA instance. See *Adding devices into external hardware management tools* on page 72 for more information.
Lenovo LXCO	Hardware management	Yes (no readiness check enforced, but you may fail to add/remove devices)	Lenovo xClarity Orchestrator (LXCO) is a Lenovo system hardware management solution that provides centralized monitoring, management, provisioning, and analytics for environments with large numbers of devices. LOC-A supports synchronizing devices to an external LXCO instance. If you have the LXCO service defined for one or more sites, LOC-A will automatically add the devices that are registered to LOC-A into the LXCO instance. Note that at least a Lenovo Management Hub (for ThinkEdge Client devices) or Lenovo LXCA (for Lenovo servers) instance must exist for the LXCO instance as a connected resource manager, so that devices can be added into LXCO. See *Adding devices into external hardware management tools* on page 72 for more information.
Lenovo Management Hub	Hardware management	Yes (no readiness check enforced, but you may fail to add/remove devices)	Lenovo xClarity Management Hub is the LXCO resource manager that manages, monitors, and provisions ThinkEdge Client devices.
Lenovo LXCI	VMware ThinkAgile VX Cluster(vSAN)	Yes, username must be "admin"	Lenovo XClarity Integrator for VMware vCenter provides IT administrators with the ability to integrate the management features of Lenovo XClarity Administrator and ThinkSystem, Flex System, System x and BladeCenter systems with VMware vCenter. Lenovo expands the virtualization management capabilities of VMware vCenter with Lenovo ThinkSystem hardware management functionality, providing affordable foundational, basic management of physical and virtual environments to reduce the time and effort required for routine system administration. It provides the discovery, configuration, monitoring, event management, and power monitoring needed to reduce cost and complexity through server consolidation and simplified management. See *Adding devices into*

			external hardware management tools on page 72 for more information.
vCenter	VMware ThinkAgile VX Cluster(vSAN)	Yes, user must be administrator role, username can be any of string	The VMware vCenter appliance is mandatory for the vSAN cluster. You must provide vCenter management credentials so that LOC-A can add edge nodes into the vCenter instance and create a vSAN cluster. One vCenter instance can be shared for multiple sites. Refer to the VMware documentation on how to setup a vCenter instance, and the maximum number of clusters and nodes that can be managed by one vCenter instance. vCenter selection policy during a new vSAN cluster deployment: 1.User can specify any external vCenter for vSAN cluster deployment. In this case it's the user's responsibility to install the vCenter and upload vCenter info of "active" status with cloud setup metadata before deployment. 2.If user needs LOC-A to deploy a vCenter for a vSAN cluster. The vCenter info should be uploaded in cloud setup metadata with the vCenter status as "inventory". Then the installation will be automatically triggered during the vSAN cluster deployment. LOC-A will deploy the vCenter instance on one of the vSAN clusters that will be managed by this vCenter.
AssistedInstaller	RedHat OpenShift Container Platform (OCP)	No	An instance of RedHat OpenShift Container Platform Assisted Installer (AI) is mandatory for OCP cluster deployment. One AI instance can be used to deploy multiple site clusters. Refer to RedHat documentation on how to setup an AI instance.

Table 9: Cloud Service Types supported by LOC-A

Figure 24 shows the listing of cloud services on the Cloud Services page.

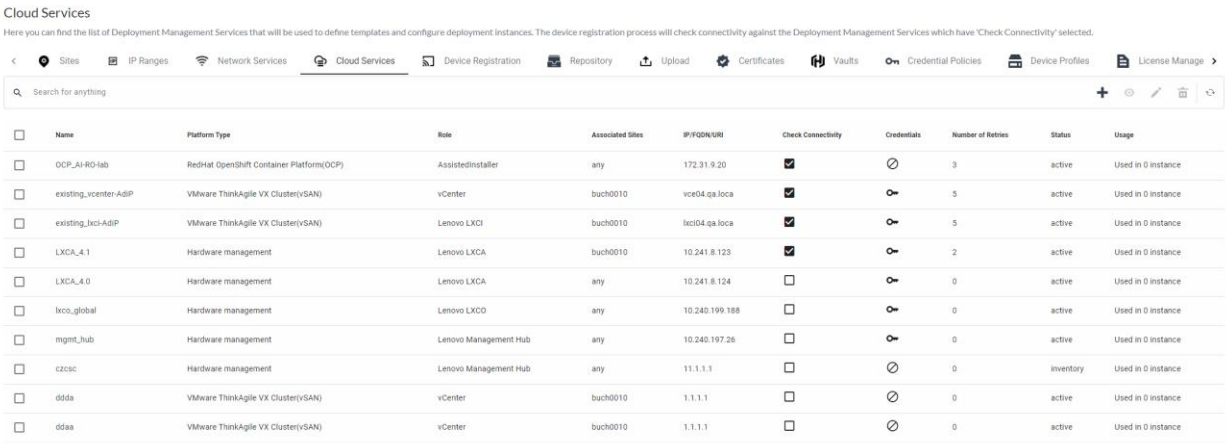


Figure 24: Cloud services list

View a cloud service's details:

You can view a cloud service's details by clicking on one cloud service.

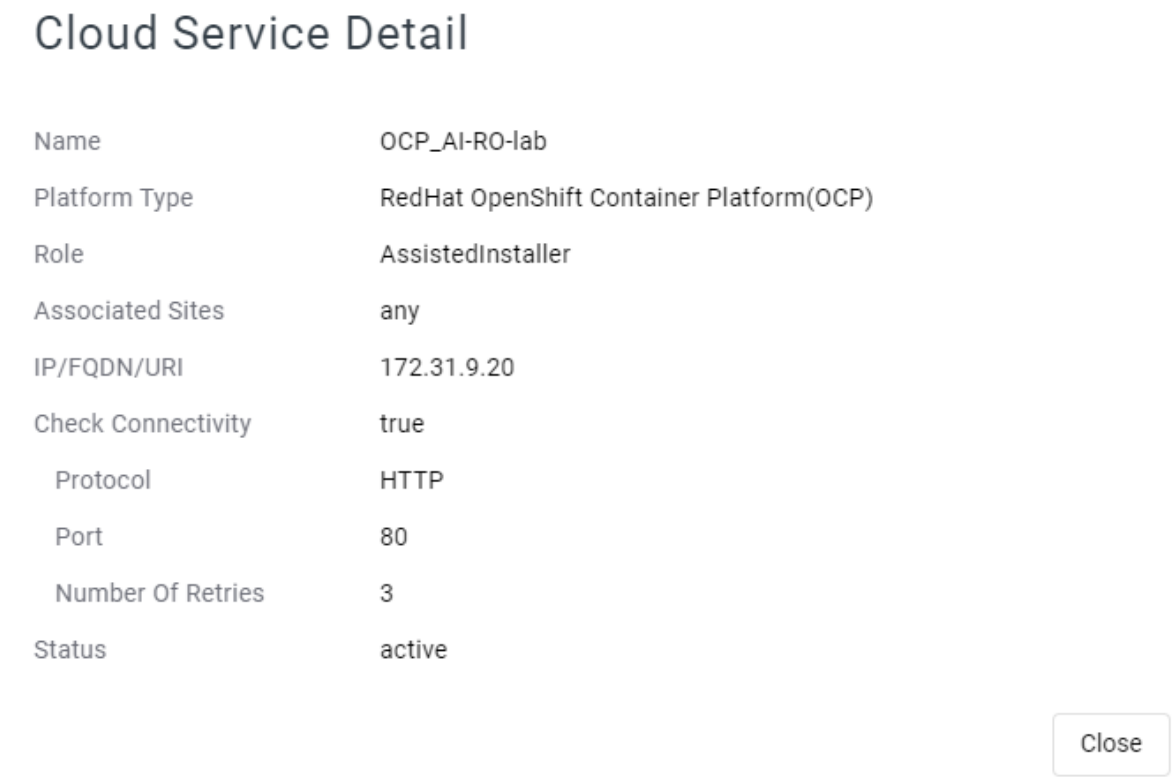


Figure 25: Cloud service detail

Create a cloud service:

Starting with LOC-A version of 3.3, you can click the **Create** button to create a cloud service, it will pop up a page to guide your through the creation process.

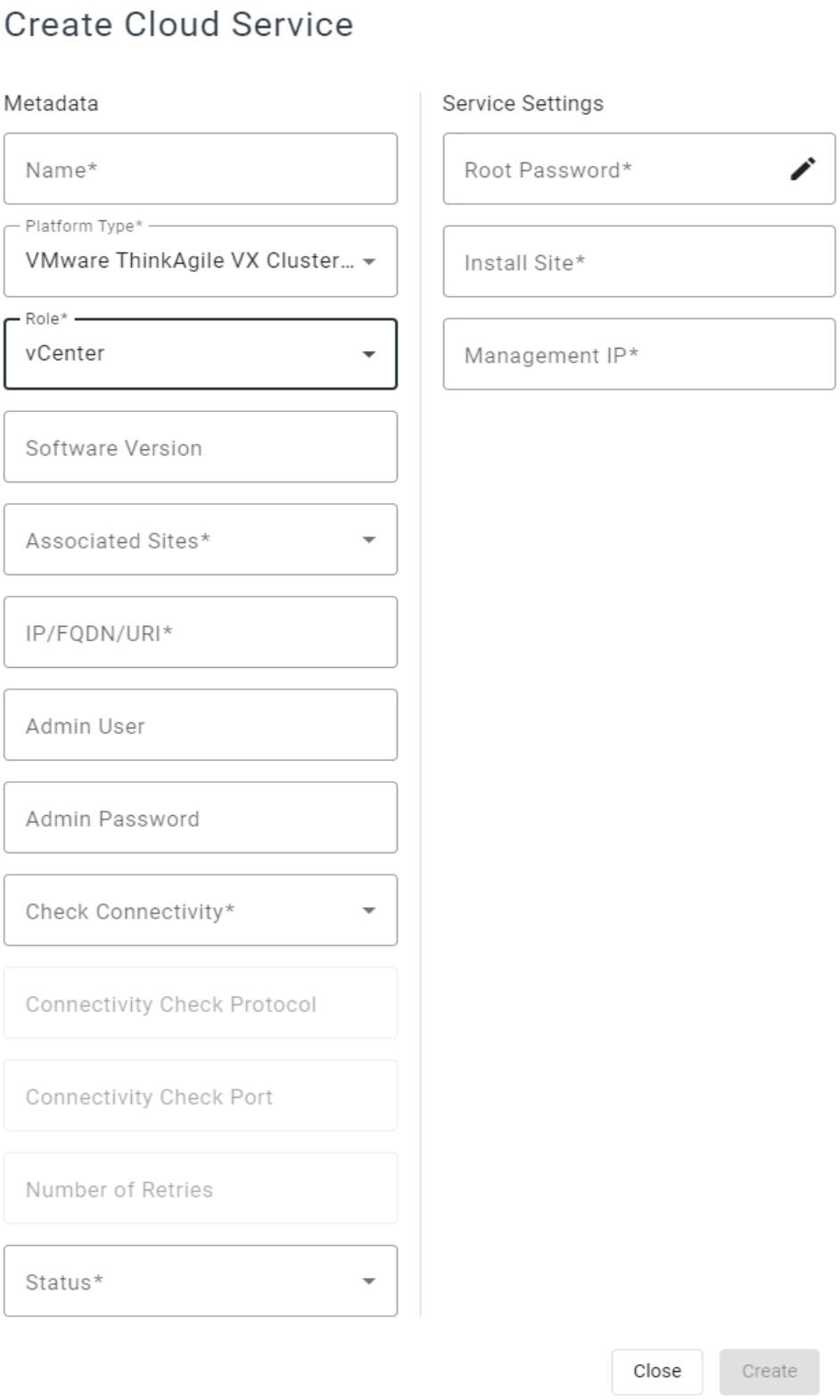


Figure 26: Create a cloud service

If the service role has the configuration requirements for **Service Settings**, this part will be automatically added to the page, as shown in the figure above.

Fill in the required fields. These typically include:

- Name*: Enter the name of the cloud service.
- Platform Type*: Select the platform type.
- Role*: Select the network service role, it must be a role that is defined for the platform type.
- Software Version: Specify the software version of the cloud service.
- Associated Sites*: Select the associated sites.
- IP/FQDN/URI*: Specify the service's access address.
- Admin User: Specify the admin user.
- Admin Password: Specify the admin password.
- Check Connectivity*: Used for connectivity check.
- Connectivity Check Protocol: Specify the protocol for the connectivity check.
- Connectivity Check Port: Specify the port for the connectivity check.
- Number of Retries: Specify the number of retries.
- Status*: Select the status from the list, **inventory** or **active**.

The fields marked with an asterisk (*) are mandatory. Fill in any optional fields according to your requirements. These might involve extra cloud service specific details or configurations. Check the entered information to guarantee its correctness. Once the **Create** button is clicked to submit the form, the system will handle the request and create the new cloud service. Meanwhile binding it to associated sites and update Deployment Readiness Status in the sites page.

Note:

- The cloud services you input may include sensitive data such as admin credentials. Please make sure you protect this document and keep it in a secured location. Once you create the cloud service, LOC-A will extract the data and encrypt the credentials in LOC-A DCIM system at rest.
- If the **Check Connectivity** option is set to **true**, please ensure that the **Connectivity Check Protocol** field is filled with the appropriate supported protocol (TCP, DNS, NTP, HTTP, HTTPS, SSH, PING, SOCKS). If a specific port is required, include the port information (e.g., HTTPS, Port 443), otherwise, the default port for the specified protocol will be used.
- If the **Check Connectivity** option is set to **true**, please ensure that the **Number of Retries** field is populated with a numeric value between 1 and 10, indicating the desired number of retry attempts.
- If the status of vCenter/Lenovo LXCI is set to **active**, the **Service Settings** field must be empty.
- If the status of Lenovo LXCI is set to **inventory**, the **Service Settings** field needs to be input with managementIp, xccIp is optional.
- The vCenter/Lenovo LXCI cannot be updated when the status is staged or active.
- The Lenovo LXCI is a vCenter plugin, so the Lenovo LXCI status cannot be active when the vCenter is not active.
- Ensure that all required fields are filled out before attempting to create the cloud service.
- If there are any validation errors, the form will not submit, and you will need to correct the errors before proceeding.
- After the cloud service is successfully created, it may take some time for the system to fully configure and display the new cloud service in relevant lists or dashboards.

Edit a cloud service:

LOC-A also supports editing an imported cloud service in the GUI. To edit a cloud service, the service needs to meet the conditions documented below. If the condition cannot be met, the corresponding field cannot be edited.

Conditions of cloud service editing:

Cloud Service Status	Is deployed by LOC-A	Used by Instance	Instance status	Editable fields
Inventory	Yes, No	No	Any value	Site List, IP/FQDN/URI, Check Connectivity, Number of Retries, Protocol, Port, Credentials, Service Settings
Active	No	No	Any value	Site List, IP/FQDN/URI, Check Connectivity, Number of Retries, Protocol, Port, Credentials, Service Settings
Active	Yes	Yes	Onboarded, Failed	IP/FQDN/URI, Check Connectivity, Number of Retries, Protocol, Port, Credentials, Service Settings

Table 10: Conditions of cloud service editing

Complete the following steps for editing the imported metadata of a cloud service:

1. Go to **Setup** page then click **Cloud Services.** Select a cloud service and click the **Edit** icon**.**

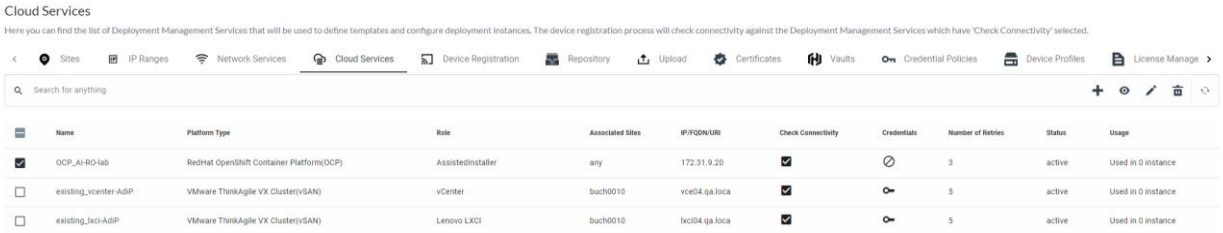


Figure 27: Cloud service edit

Note: **Edit** will be disabled when you select multiple cloud services.

2. After clicking the **Edit** icon, the Cloud Service editing page pops up.

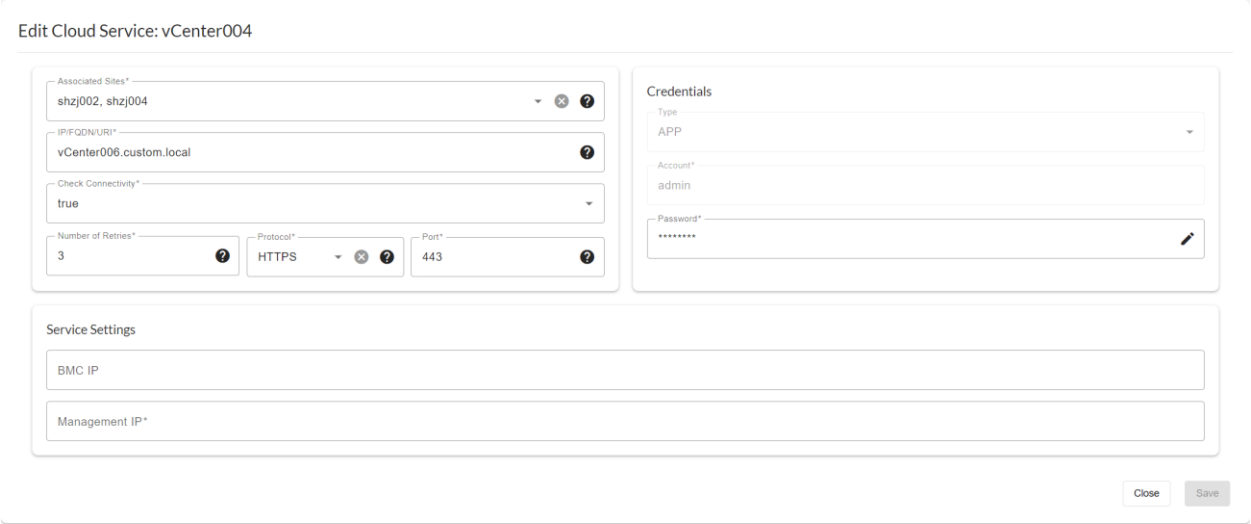


Figure 28: Cloud service editing page

3. Edit **Site List**: click on the **Site List** dropdown menu and select one or more sites.

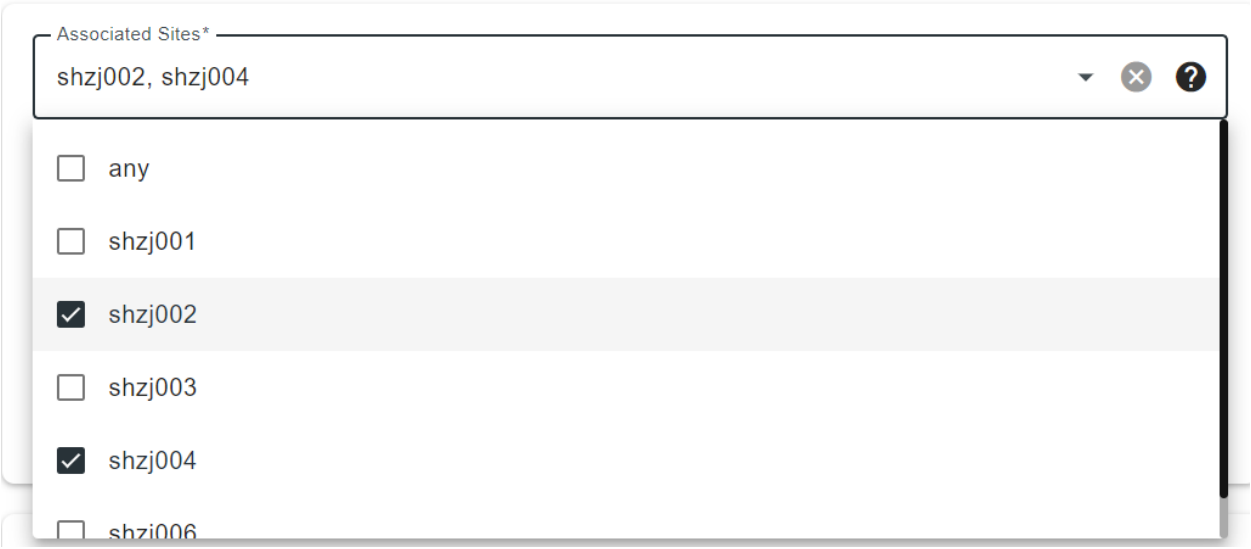


Figure 29: Site list of the cloud service

Note: **Clear Site List** can be clicked to clear selected sites.

4. Edit **IP/FQDN/URI:**

Figure 30: IP/FQDN/URI of the cloud service

Note: IP/FQDN/URI is a mandatory field. IPv4, IPv6, FQDN, or URI formats are allowed.

5. Edit **Check Connectivity**:

Figure 31: Check Connectivity of the cloud service

Note: **Check Connectivity** is a mandatory field. If the **Check Connectivity** is **true**, The **Number of Retries**, **Protocol** and **Port** can be edited.

6. Edit **Number of Retries** for connectivity check**:**

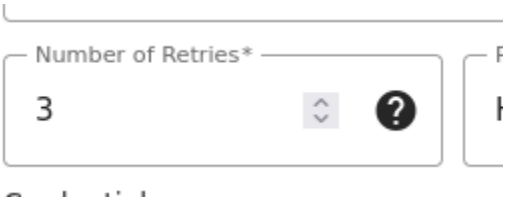


Figure 32: Number of Retries of the cloud service

Note: Number of Retries is a mandatory field if **Check Connectivity** is **true** and the input limit is **1 to 10.**

7. Edit **Protocol** for connectivity check**:**

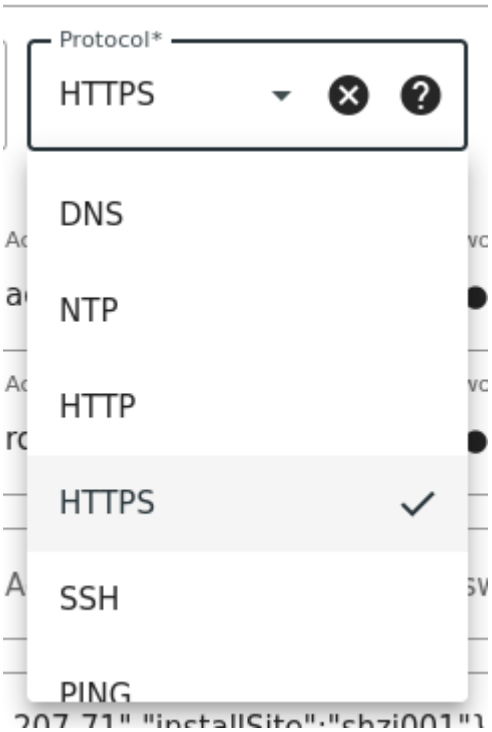


Figure 33: Protocol of the cloud service

Note: **Protocol** is a mandatory field if **Check Connectivity** is **true**. Click the **Clear Protocol** to clear selected protocol.

8. Edit **Port**:

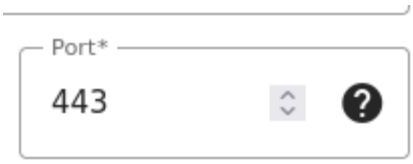


Figure 34: Port of the cloud service

Note: **Port** is a mandatory field if **Check Connectivity** is **true**. The range of ports must be **0** to **65535.**

9. Edit **Credentials**:

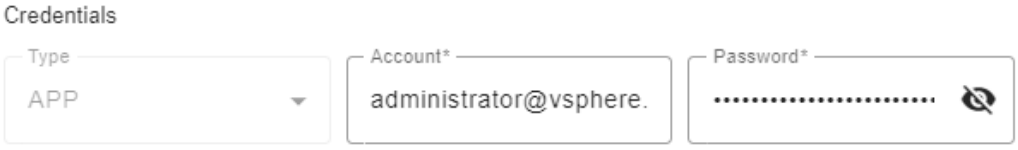


Figure 35: Credentials of the cloud service

a. You will only be allowed to edit credentials for the type supported by this cloud service. The value of **Type** can be only **APP.**
b. Click the input of the **Account** field to edit the **Account** for the specified credential.
c. Click the input of the **Password** field to edit the **Password** for the specified credential. (Note: click the eye button to show and hide the password).

Note:

- For security purposes, you will not be able to view the existing plaintext password value in the Password field. You can modify the current password by inputting the new password value. If the password is specified through an external vault system, you can view the secret path value with format @@@VaultName@@@SecretPath in the Password field. You can modify the secret path value if it's a read-only vault instance. You can also modify it to use a password string instead.
- User cannot remove the username or password for credentials entries from GUI. In order to remove the credential, you will have to upload a new setup template having these fields empty.

10. Edit **Service Settings**:

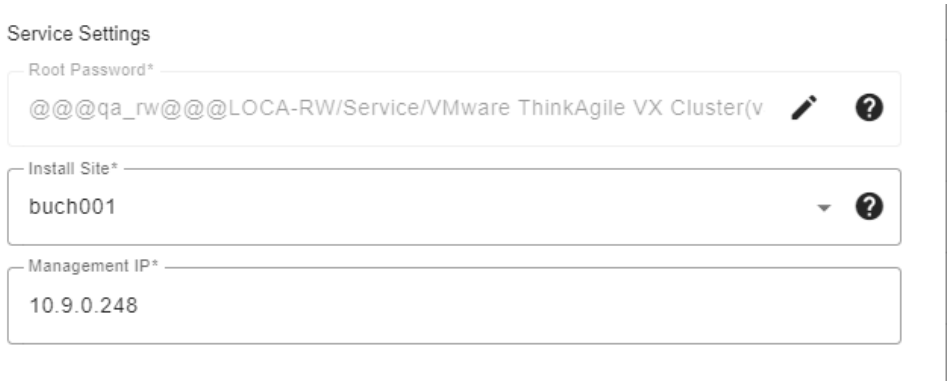


Figure 36: Service Settings of the Cloud Service

Click on each field of the **Service Settings** and edit the data. Service settings fields may vary for different cloud service roles. If there is no service setting available for a cloud service role, this section will not be displayed. Error is shown if the input for a required field is empty.

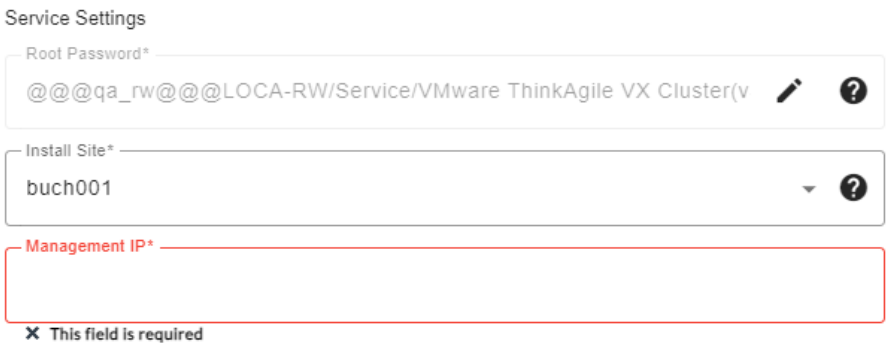


Figure 37: Service Settings check

11. Click **Save** to save the modified **Cloud Service**. The cloud service list page will be automatically refreshed and reloaded.

Note:

- If one supervisor is modifying the metadata of a cloud service, others should not start the Instance Planning and Readiness check workflow simultaneously, otherwise it may result in out-of-date data being used to deploy instances.
- After you have modified cloud services, you may need to re-generate **Registration Packages** to update to the latest metadata for your server registration.

Credential policy

LOC-A provides the credential policy feature to manage the approaches for configuring BMC, UEFI, and OS credentials. The BMC and UEFI approaches include support for static passwords and dynamically generated passwords. For OS, the public key approach is also included along with static passwords and dynamically generated passwords.

Figure below shows an example page that lists credential policies:

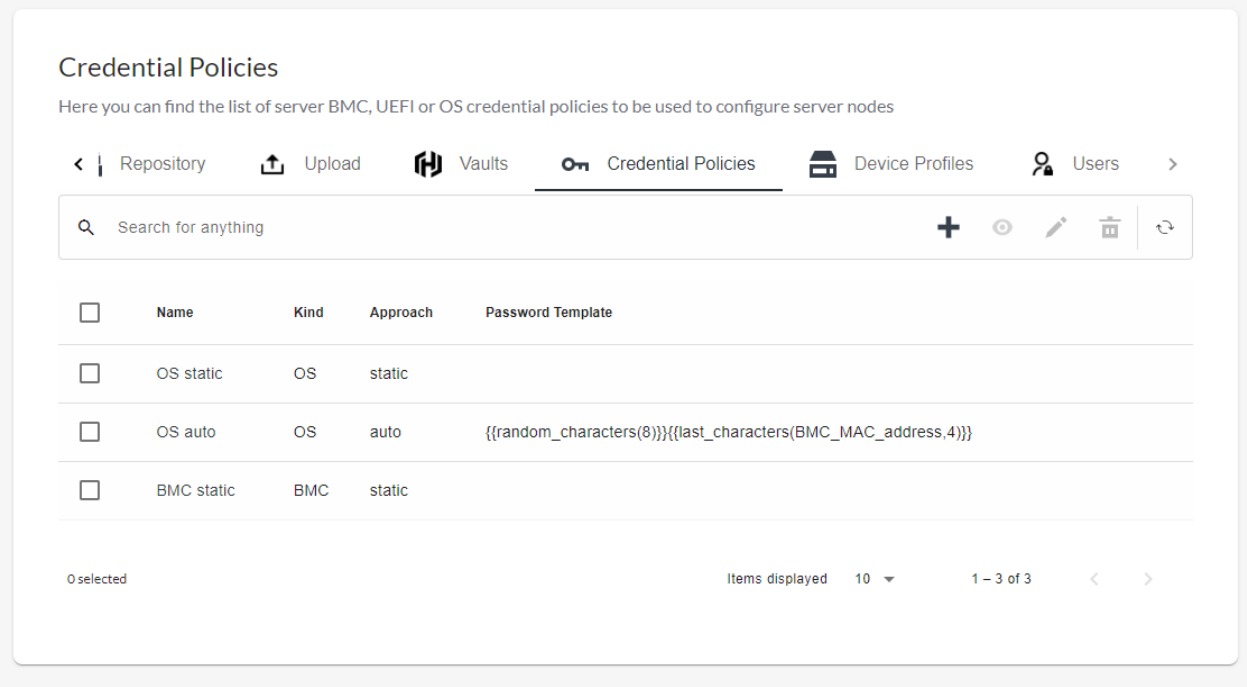


Figure 38: Credential Policy list

Create a credential policy:

Follow these steps to create a credential policy:

1. Click **Setup→ Credential Policies**, click the **Add** icon**.**
2. Input the **Name** of credential policy.

   Note: Name must start with a letter and can only contain letters, numbers, underscores, and hyphens. The length of the name should be between 2 and 50 characters.

3. Select the **Kind** of credential.

   Note: **Kind** is a dropdown list that includes three types, which are **BMC**, **UEFI** and **OS**.

4. Select the **Approach** of credential.

   Note:

   a. **Approach** includes **static**, **auto**, and **publicKey**. **Static** indicates the need for manual password input, **auto** requires the input of password template, and **publicKey** indicates the use of public key.
   b. Starting from LOC-A 3.1, you will not be allowed to create **auto** credential policy if you don't have an external read-write vault registered. Please refer to *Vault secrets management* for more details.

5. Click **Create** button.

   The following is an example of creating a credential policy with the approach of static:

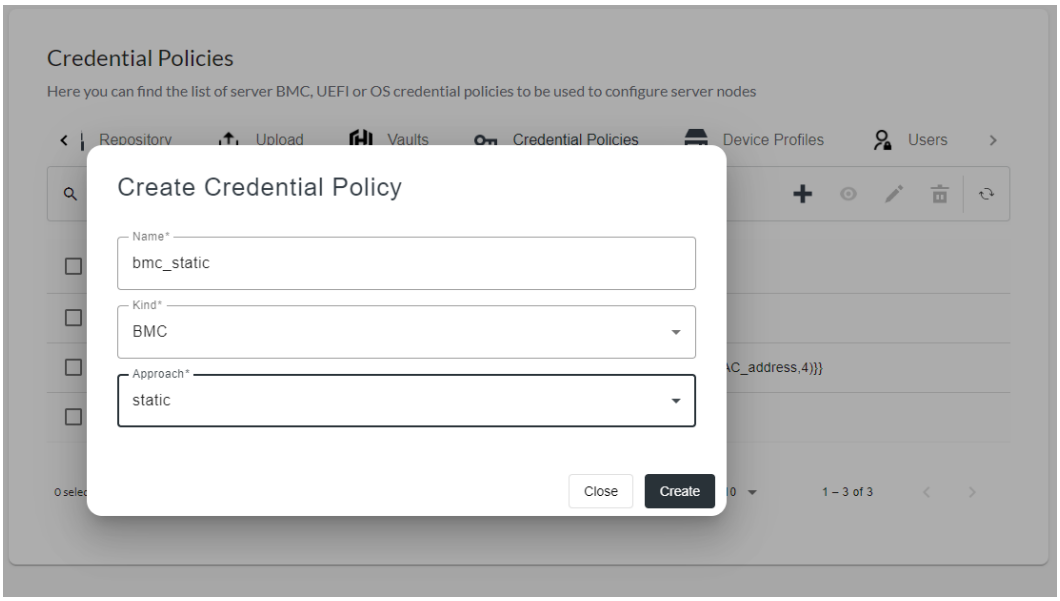


Figure 39: Credential Policy creation with the approach of static

The following is an example of creating a credential policy with the approach of **auto:**

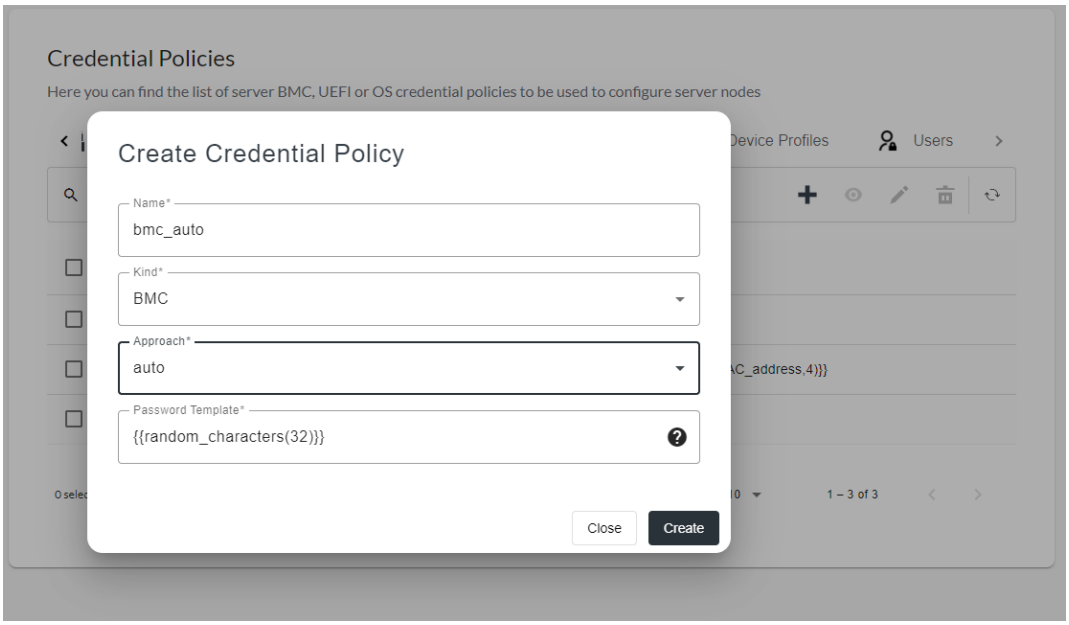


Figure 40: Credential Policy creation with the approach of auto

Modify a credential policy:

Follow these steps to modify a credential policy:

1. Click **Setup→Credential Policies**, select a credential policy, click on the **Edit** icon in the upper right corner.
2. Modify the **Name** of credential policy.
3. Modify **Password Template** of credential.

   Note: This one is editable only when credential approach is auto.

   Password Template:

- Supported built-in template variables that can be used are:
  - *{{random_characters(N)}}*: where N is the length of the random string. For example{{random_characters(32)}} will be a random string of 32 characters.
  - *{{last_characters(BMC_MAC_address,N)}}*: where N is the length of the last characters of the BMC MAC address of the node. N needs to be between 1 and 12. The length of the password should be between 10 and 32 characters.

  For OS type, both *{{random_characters(N)}}* and *{{last_characters(BMC_MAC_address,N)}}* template variables are supported. For BMC and UEFI type, only *{{random_characters(N)}}* is supported.
- The rendered password length should be between 10 and 32 characters for BMC, between 8 and 20 characters for UEFI and between 10-32 characters for OS, in case of the auto approach.

4. Click **Save** button.

   The following is an example of modifying a credential policy with an approach of **auto.**

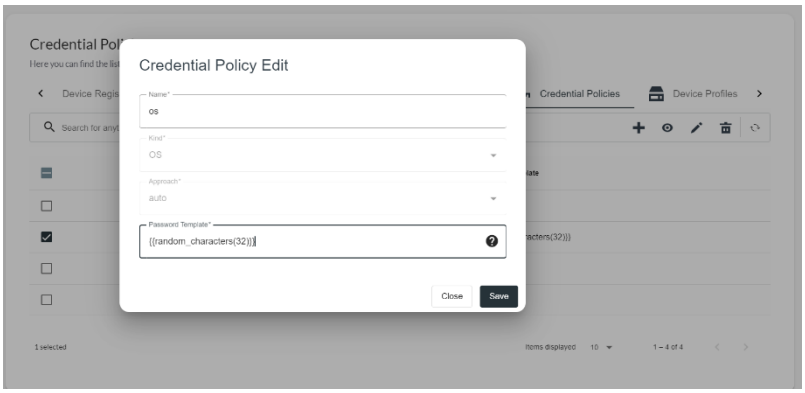


Figure 41: Credential Policy edit with the approach of auto

Note:

- Users are only allowed to modify the name and password template (when approach is auto) of the credential policy.
- After modifying a credential policy, if this credential policy is used by a template, the template will also be updated to use the modified credential policy.

Delete a credential policy:

Follow these steps to delete a credential policy:

1. Click **Setup→Credential Policies**, select a credential policy, click on the **Delete** icon in the upper right corner**.**
2. Click **Delete** button to confirm deletion.

Note: If a credential policy is in use by one or more templates, the credential policy will not be allowed to be deleted.

Device profiles

LOC-A will create default device profiles for each flavor based on the best recipe. The default device profiles are allowed to be modified and deleted. It should be noted that the configuration items belonging to the best recipe in the default device profiles cannot be changed. In addition, users are also allowed to create new device profiles on their own. .

A device profile defines the server BMC and UEFI configurations for the cloud flavor. Device profile is required when creating templates and the BMC/UEFI configurations defined in the device profile will be applied when deploying the cloud/OS instances.

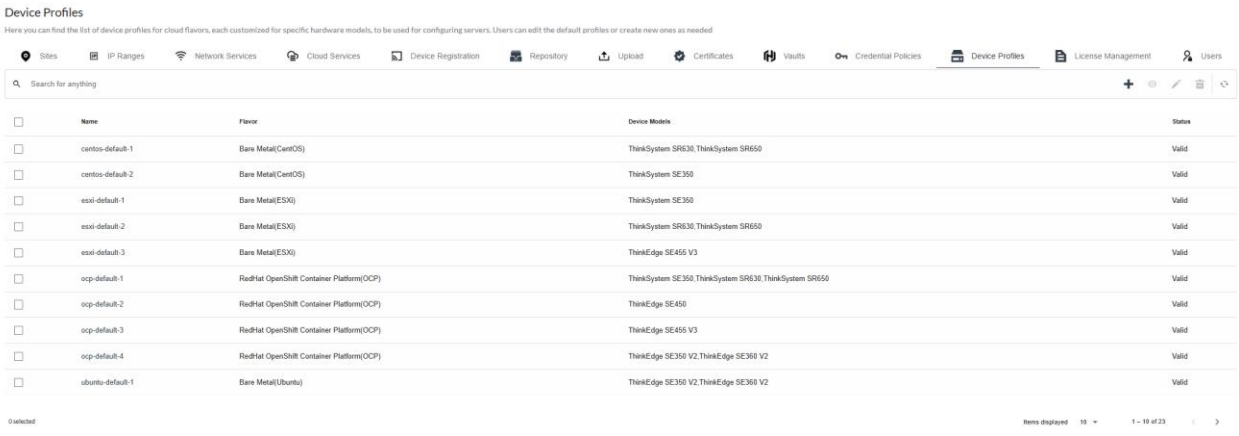


Figure 42: Device Profiles list

View a device profile's details:

You can view a device profile's details by clicking on one device profile.

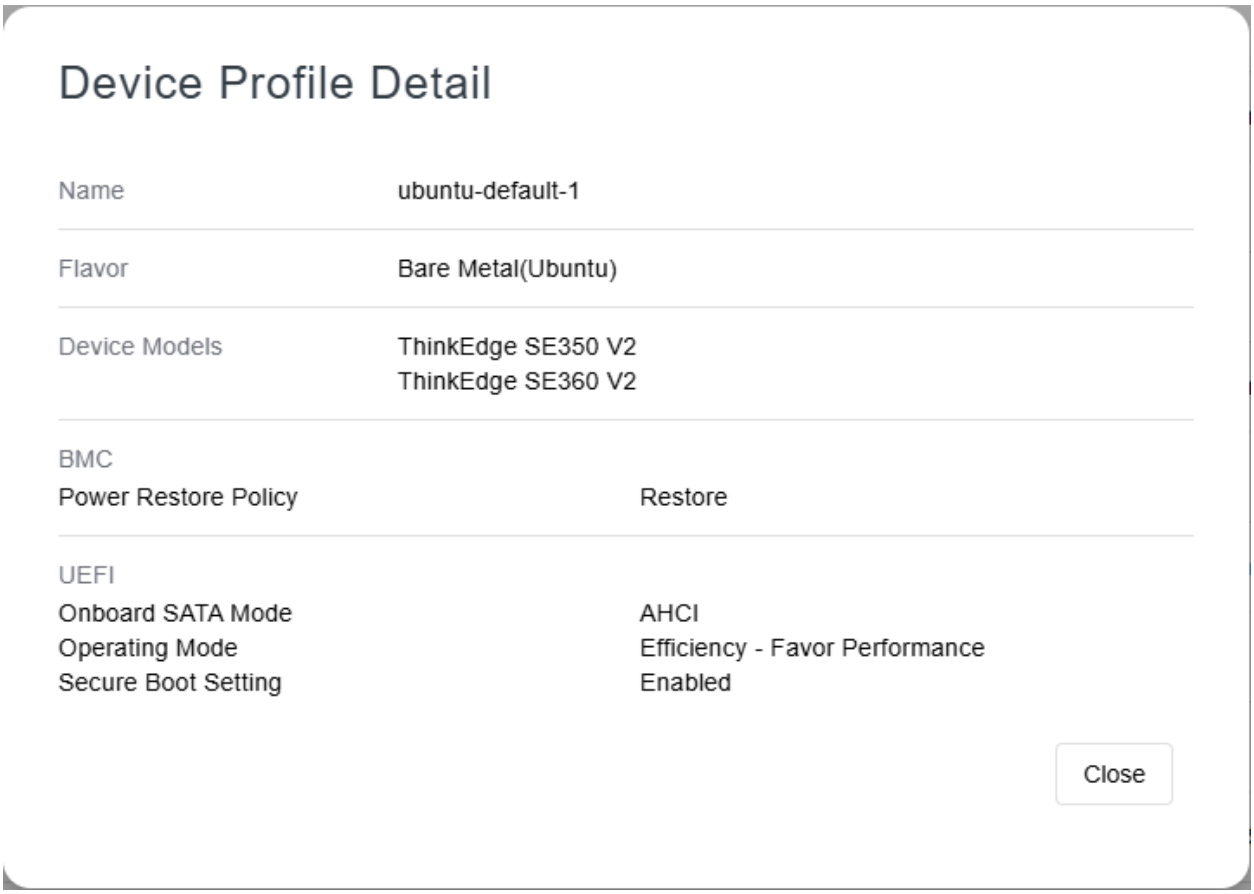


Figure 43: Device Profile Detail

Create a device profile:

Follow these steps to create a device profile:

1. Click **Setup→ Device Profiles**, then click on the **Add** icon in the upper right corner.
2. After flavor and models supported by the flavor are selected, the configuration items that belong to the best recipe of the current model are forcibly added and not allowed to be modified.
3. Enter the name of the newly created device profile.
4. You can click the **Add Field** button to add more configurable BMC and UEFI items.
5. Click the **Save** button in the bottom right corner to save the creation.

Note: When adding a configuration item, if the configuration item has a dependent configuration item, the dependent configuration item is automatically added. Similarly, when you delete a dependency for a configuration item, that configuration item is deleted along with it.

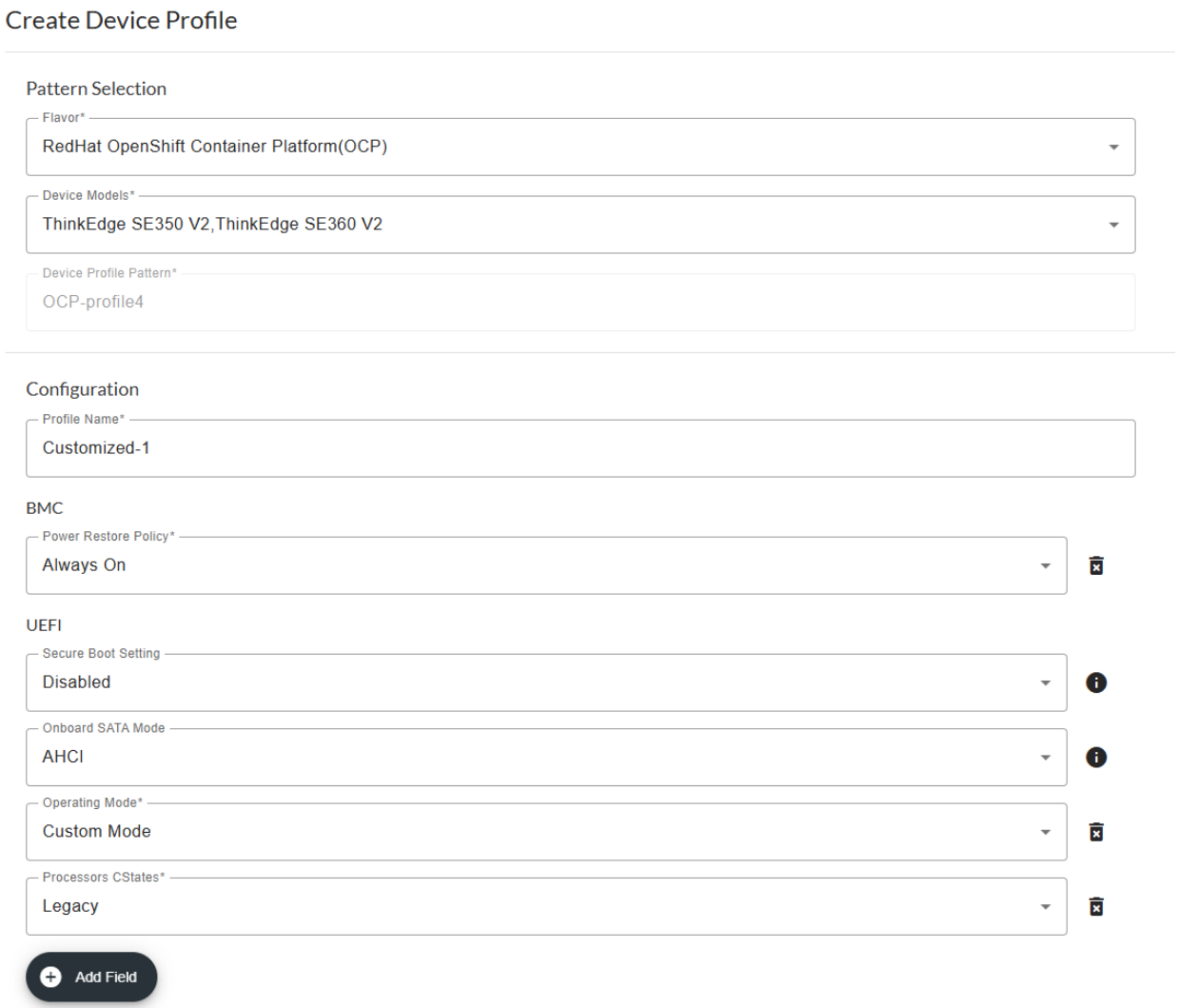


Figure 44: Create Device Profile

Modify a device profile:

Follow these steps to modify a device profile：

1. Click **Setup→ Device Profiles**, select a device profile, then click on the **Edit** icon in the upper right corner.
2. Add, delete, or modify the current BMC, UEFI configuration. Same as creating, the configuration items that belong to the best recipe of the current model are not allowed to be modified.
3. Click the **Save** button in the bottom right corner to save the change.

Note:

- When adding a configuration item, if the configuration item has a dependent configuration item, the dependent configuration item is automatically added. Similarly, when you delete a dependency for a configuration item, that configuration item is deleted along with it.
- The device profiles being used by instances are not allowed to be modified.
- For device profiles that are being used by templates but not by instances, if this device profile is modified, the configuration of the device profile in the template will also change accordingly.

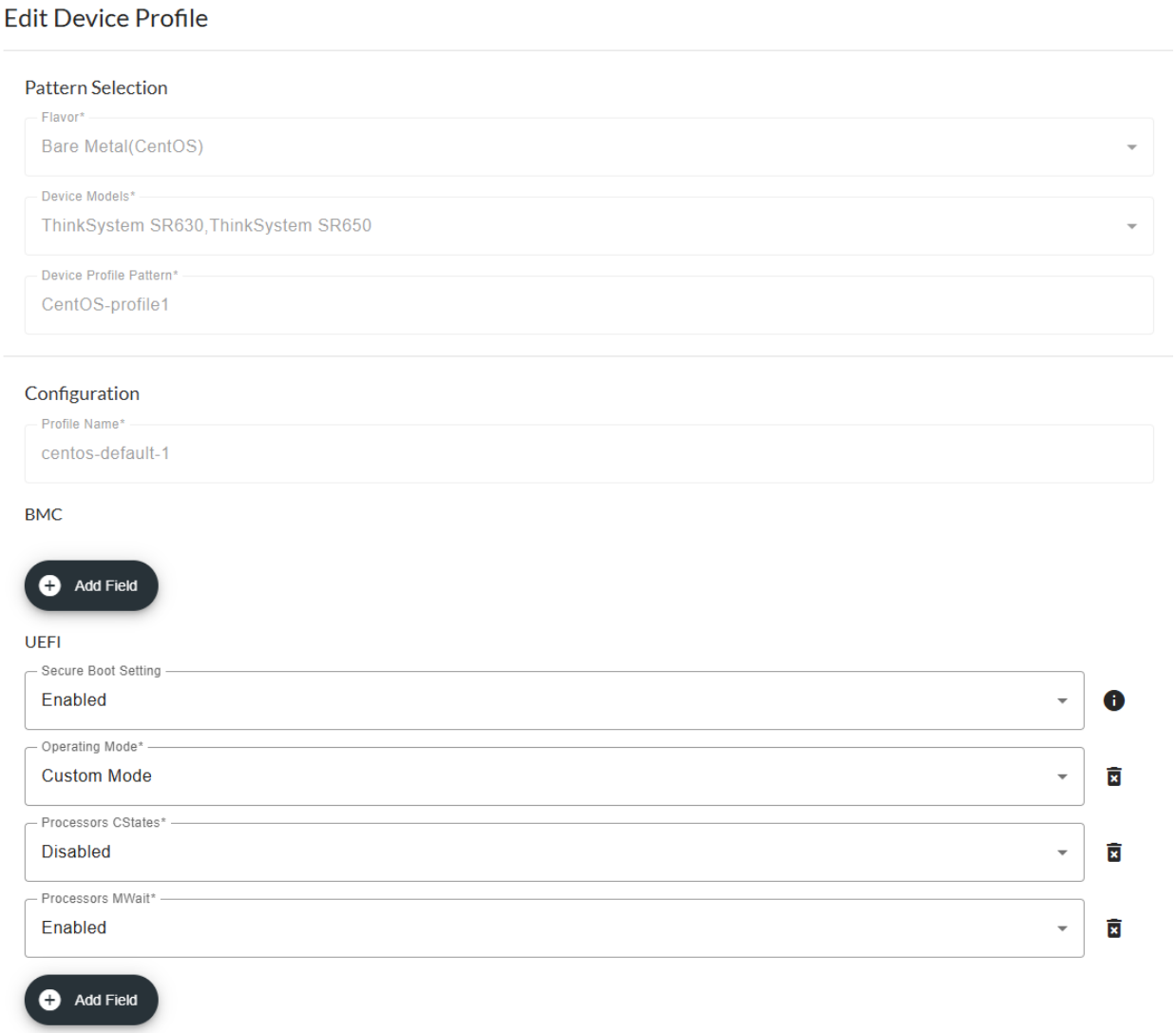


Figure 45: Modify Device Profile

Note:

- Currently, there is no configuration option for vSAN flavor.
- For server model ThinkSystem SE350, ThinkSystem SR630, and ThinkSystem SR650 models, if the user manually disables the UEFI configuration's physical presence policy, when the secure boot is set in the device profile, it may fail because the remote physical presence cannot be configured at this time. The only solution is to assert the Hardware PP jumper on the server mainboard.

Delete device profiles:

Follow these steps to delete a device profile:

1. Click **Setup→ Device Profiles**, select one or more device profiles, click on the **Delete** icon in the upper right corner**.**
2. Click **Delete** button to confirm deletion.

Note: Any device profile currently being used by a template or instance cannot be deleted.

Generate LOC-A registration packages

LOC-A provides various methods to add devices into the inventory. For edge-site server nodes, we recommend you use the nZTP (near zero-touch-provisioning) approach to register the devices with a LOC-A registration package via a USB key or the Lenovo Open Cloud Automation Utility. For other approaches to device registration, see *Register devices* on page 53.

The LOC-A registration package contains site metadata information and other necessary artifacts for nZTP device registration. After importing the edge sites resources metadata, you can generate and then download the LOC-A registration package to facilitate edge-site server node registration.

To create a new registration package, click **Setup→Device Registration→Create**.

LOC-A supports generating an image for a USB key or for Lenovo Open Cloud Automation Utility.

Generate USB type package

USB type registration package is a bootable mini OS image that can be loaded to a USB key for on-site device registration.

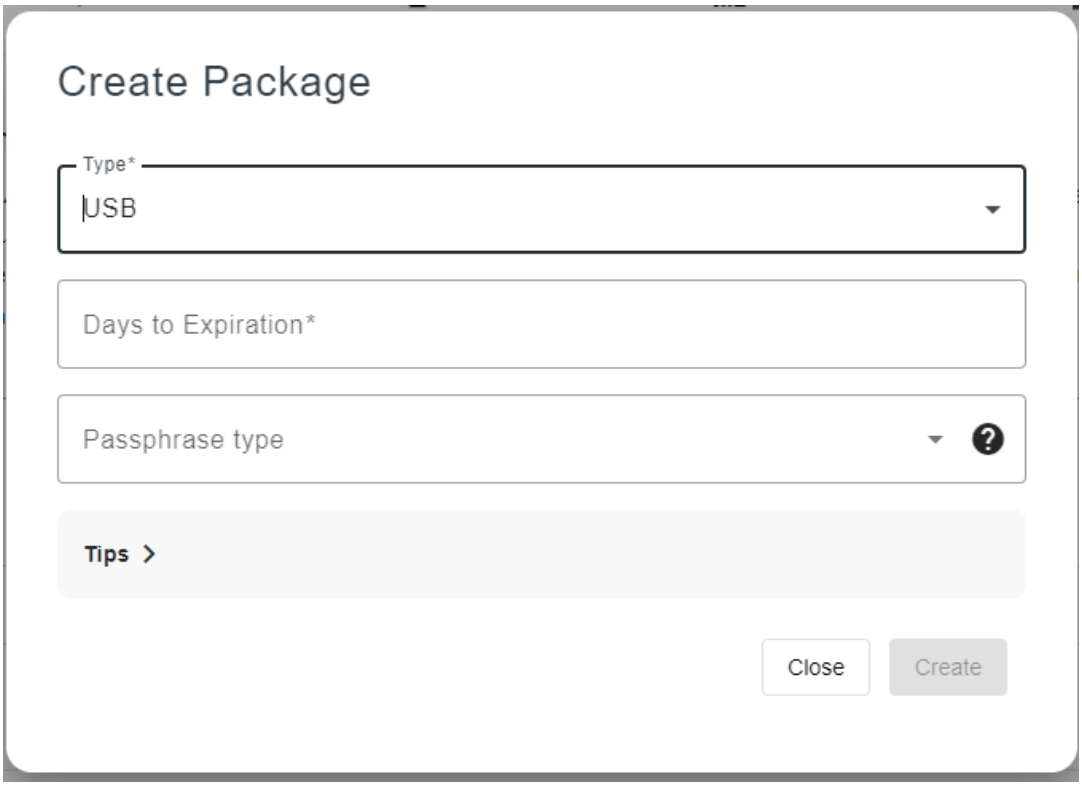


Figure 46: Create USB type registration package

1. Select **USB** and enter the number of days until the image expires.
2. Choose a passphrase type. The registration package for USB key is passphrase protected.
   - Select **Auto-generate passphrase** to let LOC-A generate the passphrase automatically.
   - Select **Use static passphrase** to enter your passphrase.

   The passphrase will be needed later when you perform server registration. See *Register devices* on page 53 for more information.
3. Click **Create** to start generating the package. It usually takes several minutes for the task to complete.

   You can refresh the page or view progress of the task in the Tasks page. Upon completion, an image is shown in the Image List ready for download. The passphrase (automatically generated or user defined) is listed in the **Passphrase** column.

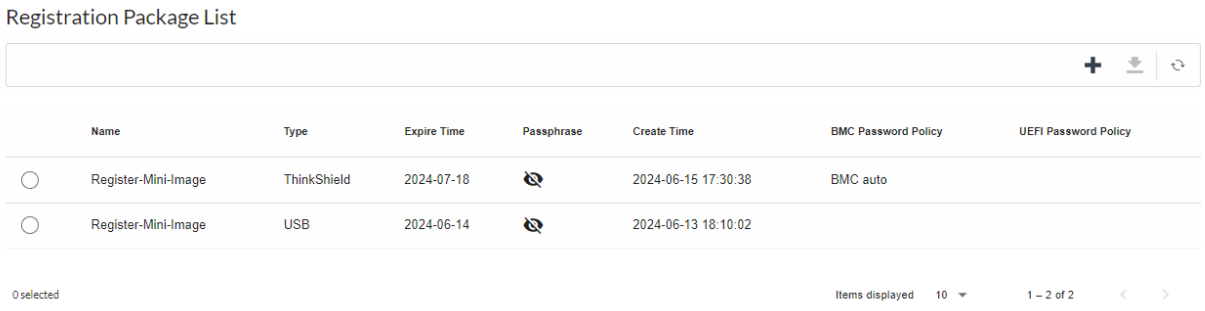


Figure 47: Registration package list

4. Select the image and click **Download** to download the package. The .IMG file is typically around 96 MB.

After downloading the file, you can use tools like ImageWriter or Rufus to flash the bootable image file on a USB key. Ensure that the **enable bootable image** option is used.

Then you can refer to section *Register devices* to register devices via USB key.

Note: If your site resources in Setup are changed (e.g., added new sites, modified IP ranges), you need to re-generate the registration package to include the latest metadata.

Generate ThinkShield type package

ThinkShield type registration package is a .tar file for the Lenovo Open Cloud Automation Utility to use. It includes all the metadata required for registration and is encrypted. After populating the edge sites resources metadata and creating the BMC credential policy, you can generate a LOC-A registration package to facilitate edge-site server node registration.

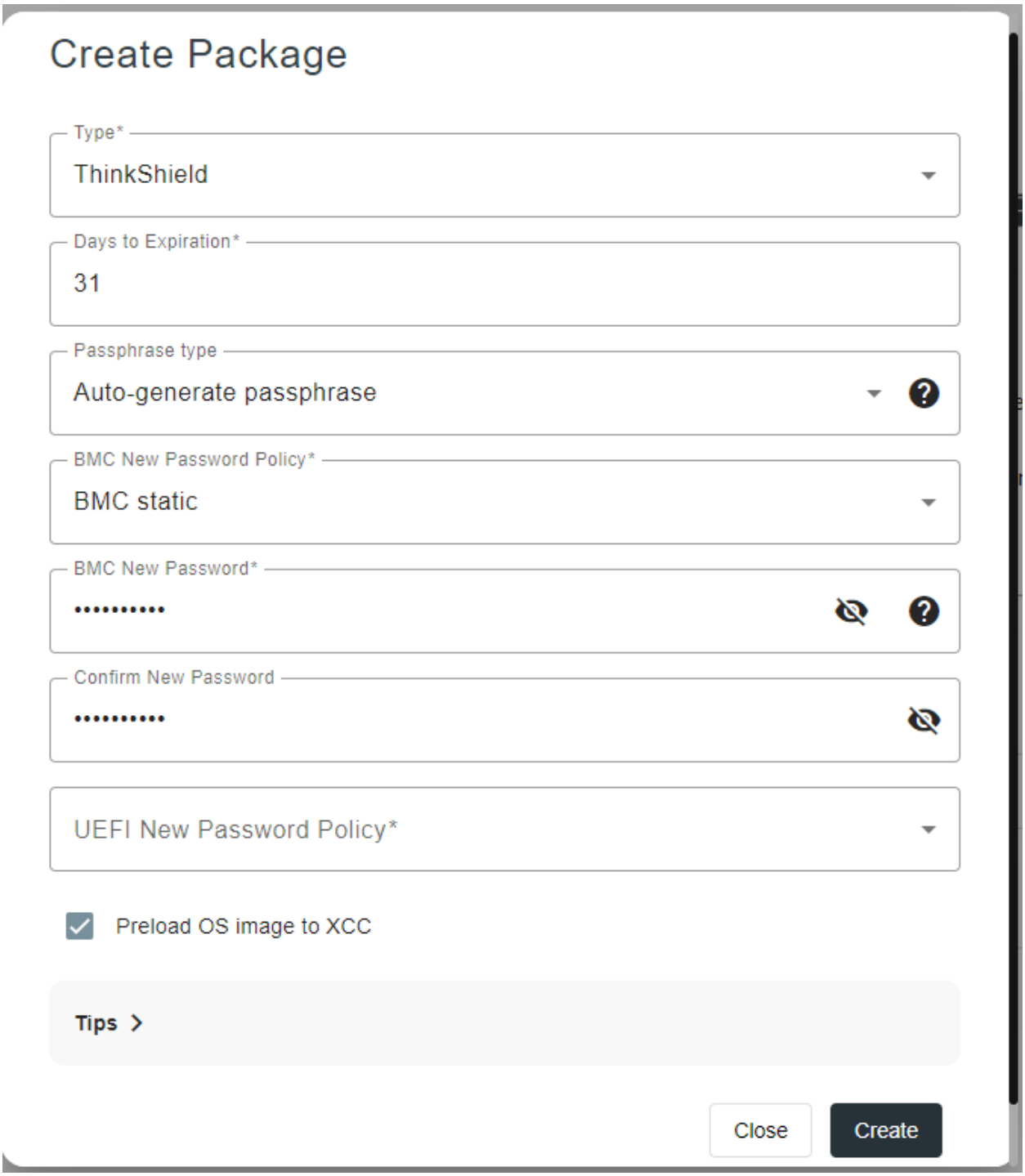


Figure 48: Create ThinkShield type registration package

1. Select **ThinkShield** and enter the number of days until the image expires.
2. Choose a passphrase type. The ThinkShield registration package is passphrase protected.
   - Select **Auto-generate passphrase** to let LOC-A generate the passphrase automatically.
   - Select **Use static passphrase** to enter your passphrase.

   The passphrase will be needed later when you perform server registration through the Lenovo Open Cloud Automation Utility. See *Register devices* on page 53 for more information.

3. Select the expected BMC new password policy. Input BMC new password if the credential policy is of static approach type. During the on-site server registration, LOC-A will follow the password policy to configure BMC's new password.
4. You can optionally select UEFI new password policy as well for expected UEFI admin password.
5. You can optionally enable **Preload OS image to XCC** to sideload OS images on the XCC. Please refer to *OS Image Sideloading* section below for more details.

Click **Create** to start generating the package. It usually takes several minutes for the task to complete.

After downloading the package file, you will need to download the Lenovo Open Cloud Automation utility on your Windows desktop and refer to section *Register devices* to register devices via the Lenovo Open Cloud Automation Utility.

Download Lenovo Open Cloud Automation Utility

Lenovo Open Cloud Automation Utility is a Windows desktop application designed to assist in provisioning and registering edge servers. Each utility software package is specific to a particular LOC-A portal instance. Therefore, you must download the software package corresponding to your LOC-A portal instance.

Click **Download Lenovo Open Cloud Automation - Utility** to download the utility.

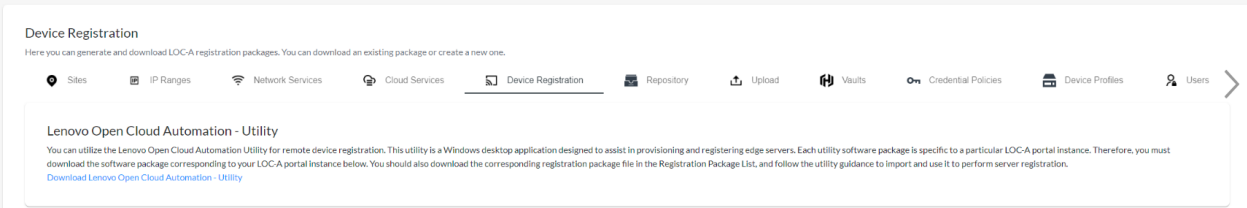


Figure 49: Download Lenovo Open Cloud Automation Utility

Register devices

There are several methods to register servers into LOC-A inventory. For typical edge scenarios, it is recommended that the user register devices using the LOC-A registration package via USB key or through the LOC-A Automation Utility. These two approaches include a connectivity check of related network services and cloud services for the site; the cabling for edge nodes and the network facilities are verified before remote cluster deployment. For datacenter scenarios, you can also register new devices through automatic discovery in the layer 2 network or by manually entering them using **Add device** or by uploading a cloud setup template Excel file.

Register devices via Lenovo Open Cloud Automation Utility

Follow the section Device Registration to generate and download a registration package and download the registration utility.

After downloading the software package Registration-tool.zip:

1. Extract it to your Windows laptop.
2. Goto the directory and you should be able to find LOC-A_Registration_Utility.exe file. This is the executable file for the software.

Cabling

1. Make sure you have unboxed the server and followed the network requirements of your cloud deployment plan to cable the server Ethernet Adapter ports properly.

2. For manufacture default server, connect your laptop Ethernet port with XCC RJ45 Ethernet management port directly. If your laptop does not have an RJ45 Ethernet port, you can use a USB-Ethernet adapter for the connection.

Using the utility

1. Double click **LOC-A Utility.exe** to launch the desktop application. You will need administrator permission to run the application. Click **Next** button to the **Prepare Setup** page.
   Note: Only one application instance is allowed on the same desktop machine.

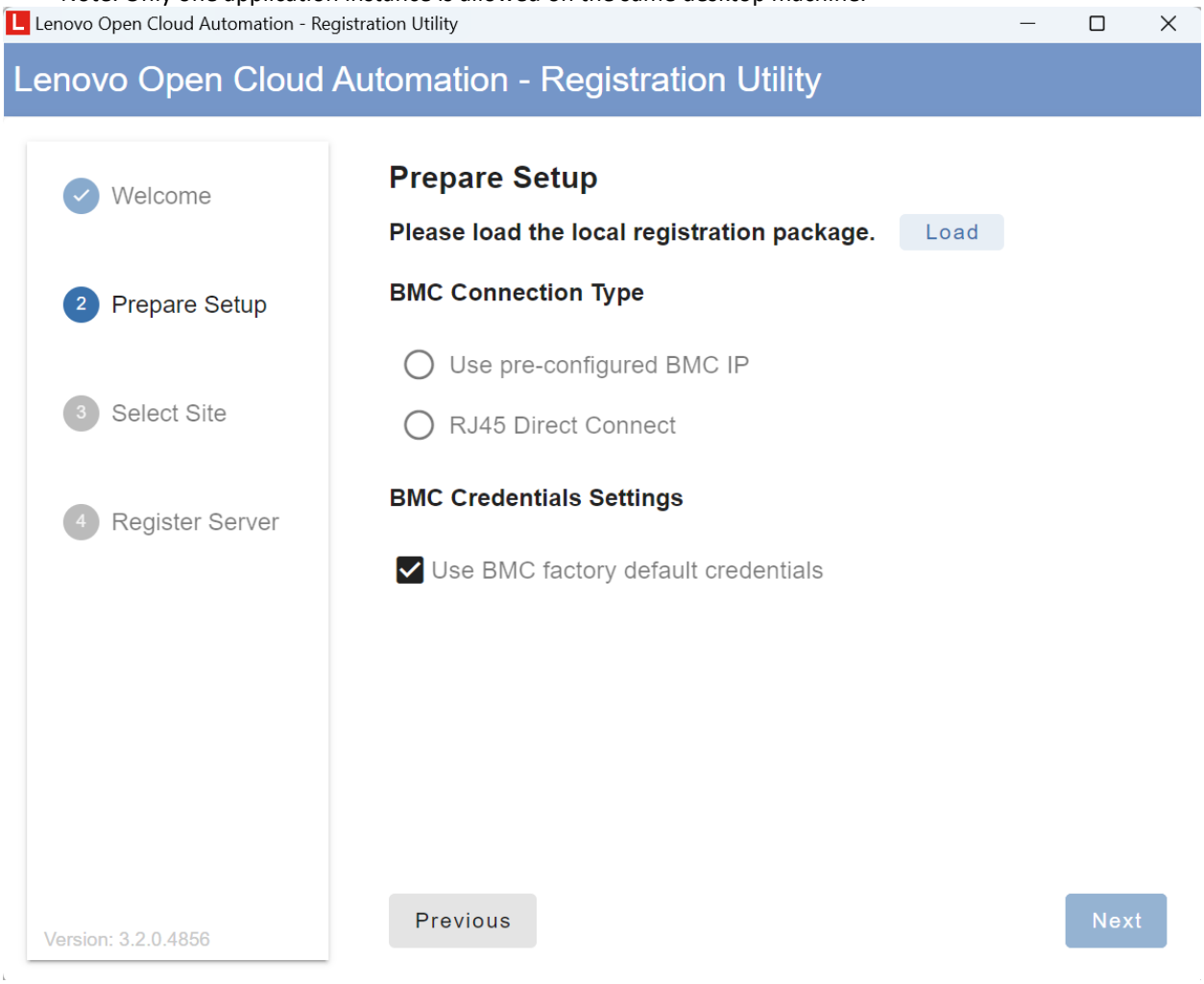


Figure 50: LOC-A Registration Utility - Prepare Setup

2. Click **Load** and load the ThinkShield type registration package that you downloaded from LOC-A portal and then enter the same passphrase used when the package was created.

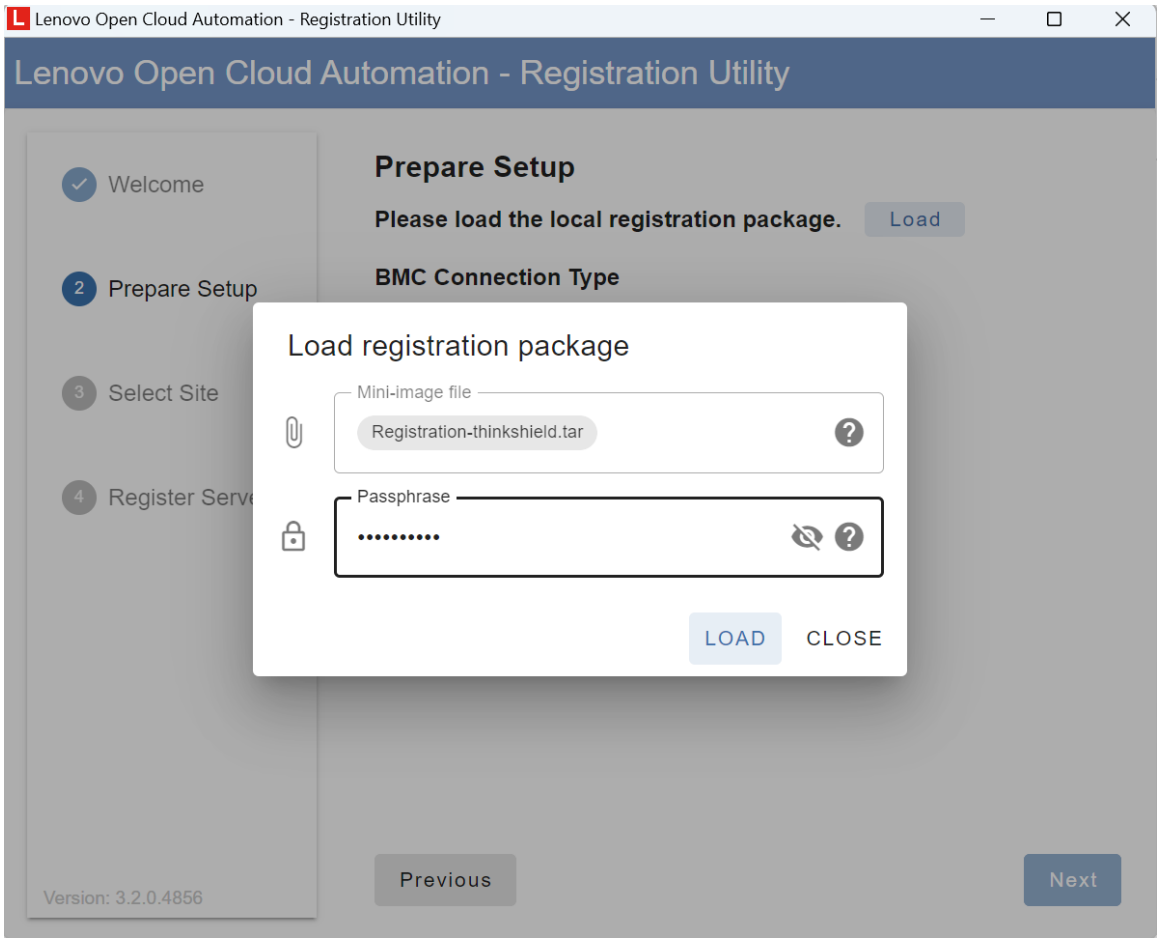


Figure 51: Load registration package

3. Select **BMC(XCC) Connection Type**
   a. **Use pre-configured BMC IP** mode: In this mode, You server BMC(XCC) is already configured with an IP and is connected properly in the planned XCC(BMC) network. LOC-A attempts to connect and provision the server XCC(BMC) through Ethernet IPv4 address. You will need to input existing IP address of XCC(BMC). Please make sure the network is reachable between the device that the registration utility is running upon and the XCC(BMC) Ethernet IP address.
   b. **RJ45 Direct Connect** mode: In this mode, your server is factory default without pre-configuration. LOC-A attempts to connect and provision the server XCC(BMC) management port through direct RJ45 connection. Please ensure you have completed the cabling**.** You will also need to select the local network card on the laptop you are connecting to the server.

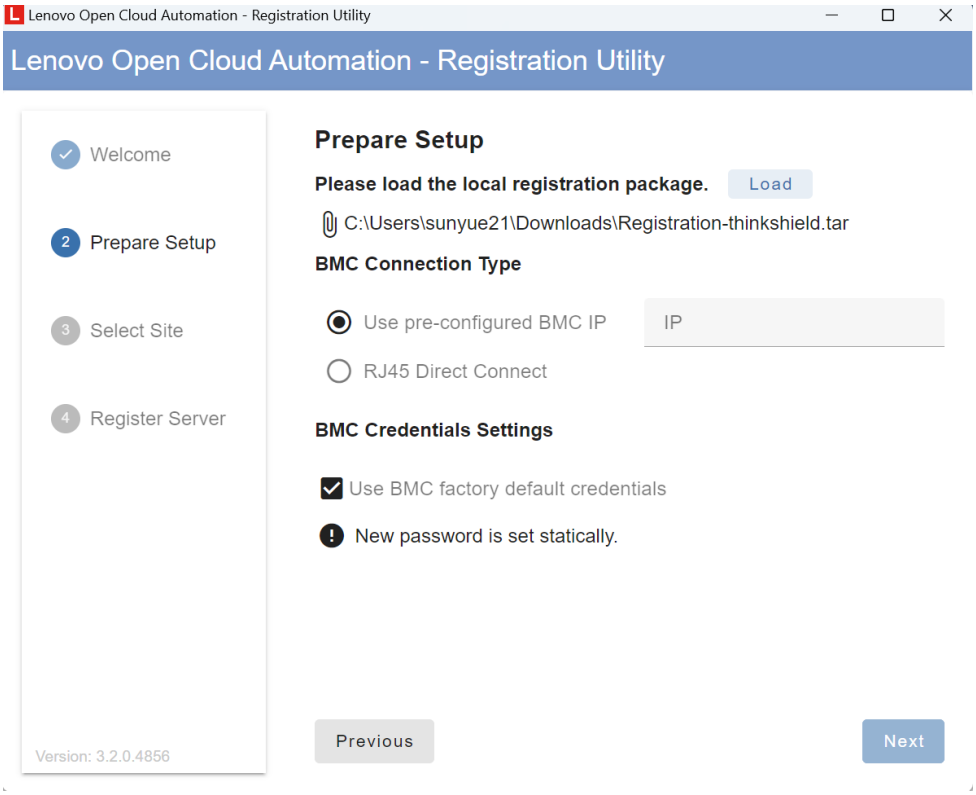


Figure 52: Use pre-configured BMC IP

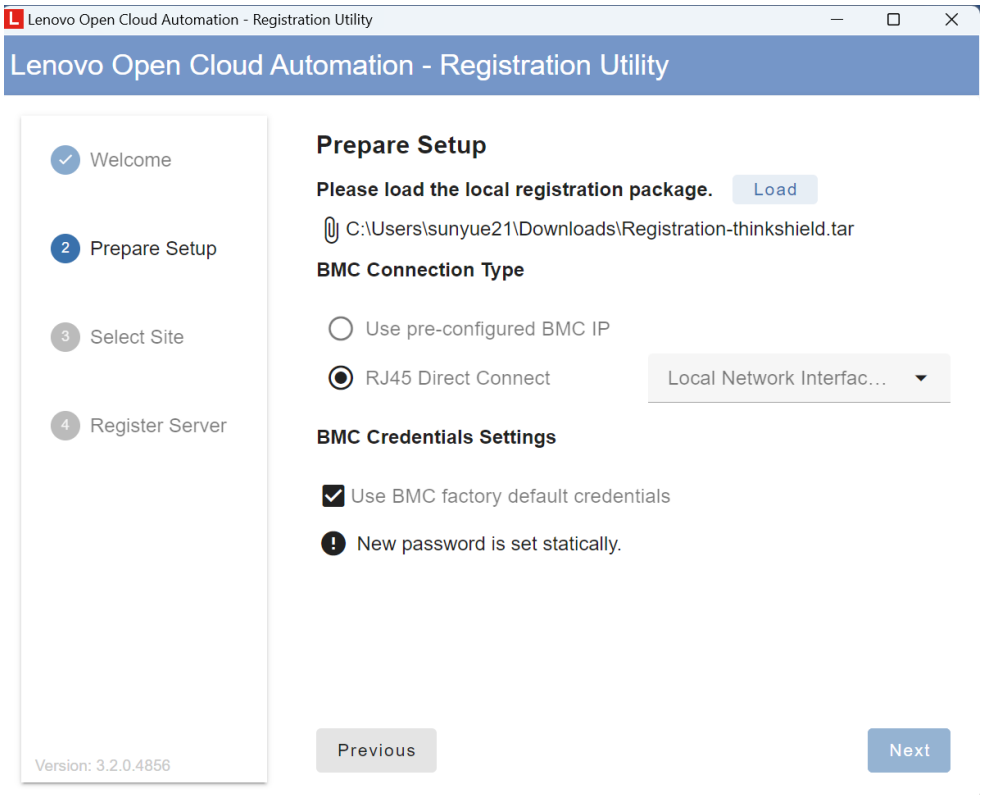


Figure 53: RJ45 Direct Connect

4. Configure **BMC Credentials Settings**

   If the server is factory default, you can choose **Use BMC factory default credentials**, then current username will be USERID and current password should be PASSW0RD (note that the 'O' is a zero).

   If the server's credentials were previously changed, you need to unselect the **Use BMC factory default credentials** checkbox and input the current password manually so the LOC-A Utility can connect to the server properly. Current username needs to be USERID.

   BMC new password is set according to the BMC credential policy you selected when you generated the registration package, so you will not set it in the utility.

   Click **Next** to continue to the next page.

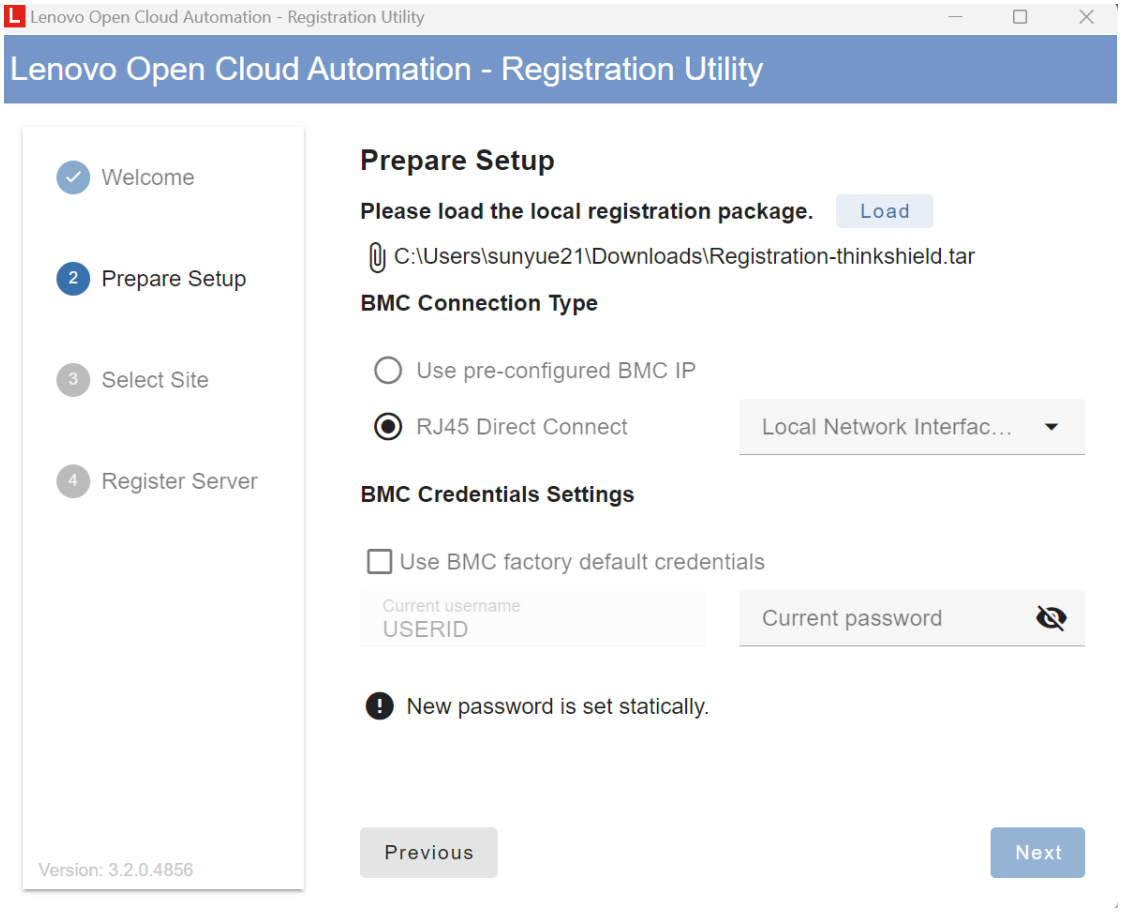


Figure 54: Input current password manually

5. Select Site

   Select the proper site that you want to register your server into. After you have confirmed all the inputs are correct, click **Register**, this will trigger the automatic server registration process.

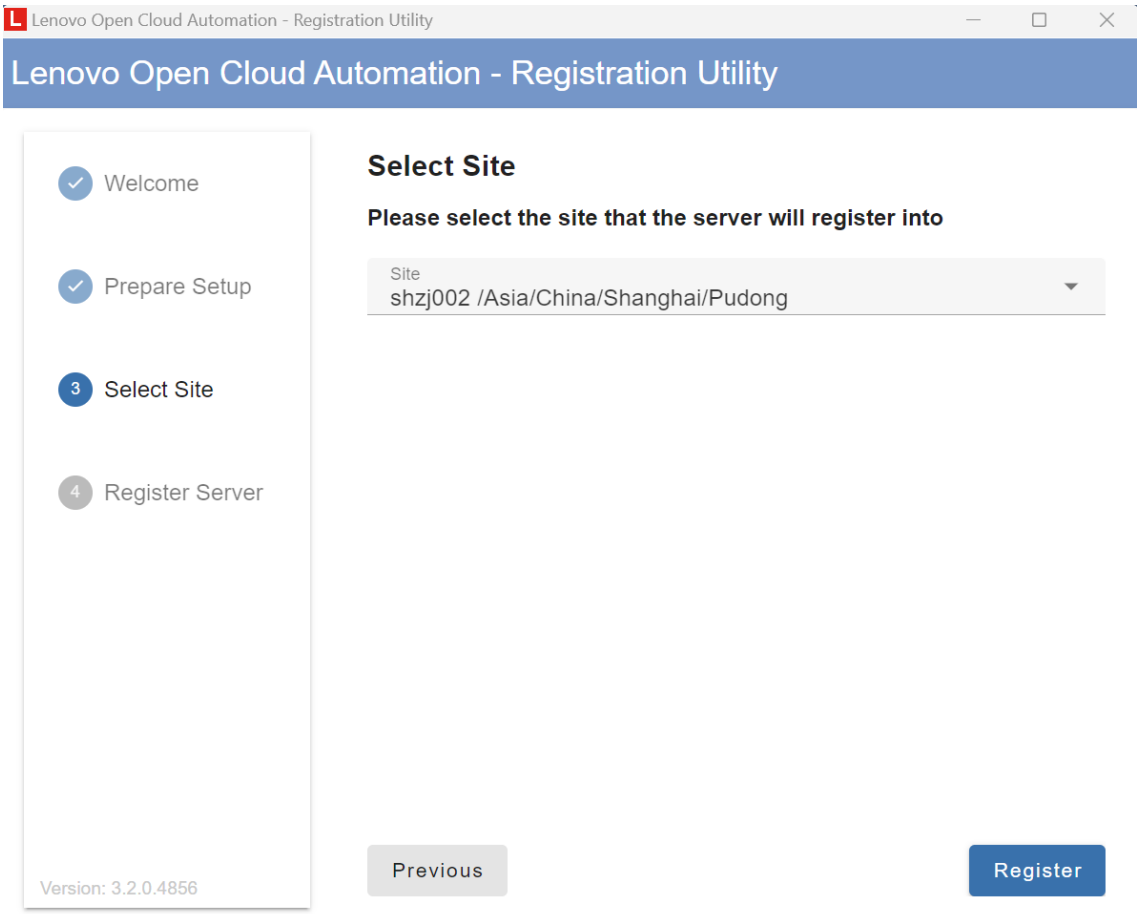


Figure 55: Select Site

6. Server Registration

A workflow will launch automatically which includes the following content:

- Change BMC password: change XCC(BMC) password.
- Set up BMC configuration: configure XCC(BMC) network settings and configure port forwarding.
- Mount image and change boot order: mount the LOC-A mini-OS image.
- System startup and start registration agent: boot system into the mini-OS image where LOC-A registration client will run.
- Configure BMC IP: set the BMC IP according to the planned site metadata. LOC-A will automatically find an available BMC IP for this site.
- Server connectivity check: perform connectivity check according to the planned site metadata. Network and cloud services for this site will be checked to make sure the server is properly cabled.
- Sideload image: optionally sideload the OS image to the server
- Register server: LOC-A registration client will collect server inventory and register the server to the LOC-A portal.

You can click the **Retry** button if any steps of the workflow fail. When the server completes the registration, it will be shown in the Registered Devices list on the LOC-A portal.

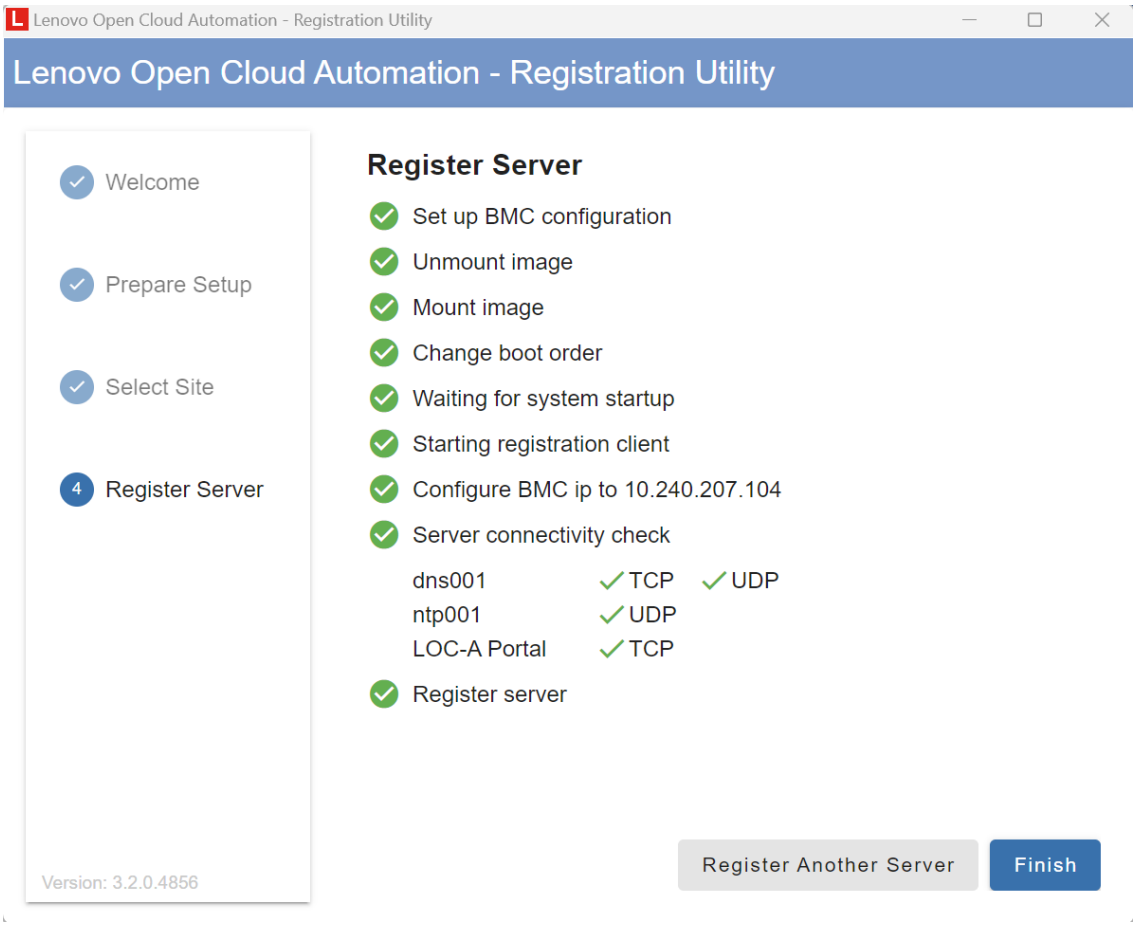


Figure 56: Register server through LOC-A Registration Utility

Error Recovery

In the LOC-A automatic registration process, passwords for BMC will be changed. However, when certain steps in the process fail, resulting in incomplete registration, users may attempt to reopen the utility and execute the automation process again. In this situation, the LOC-A Utility records the server registration failing point and provides recovery. The next time the utility starts, if there are servers that failed to register before, the utility will prompt the user whether to continue registering the server. If you want to continue registering, you need to select the corresponding Serial Number and click **OK**. If you are attempting to register another server, click **CANCEL** and all processes will proceed normally.

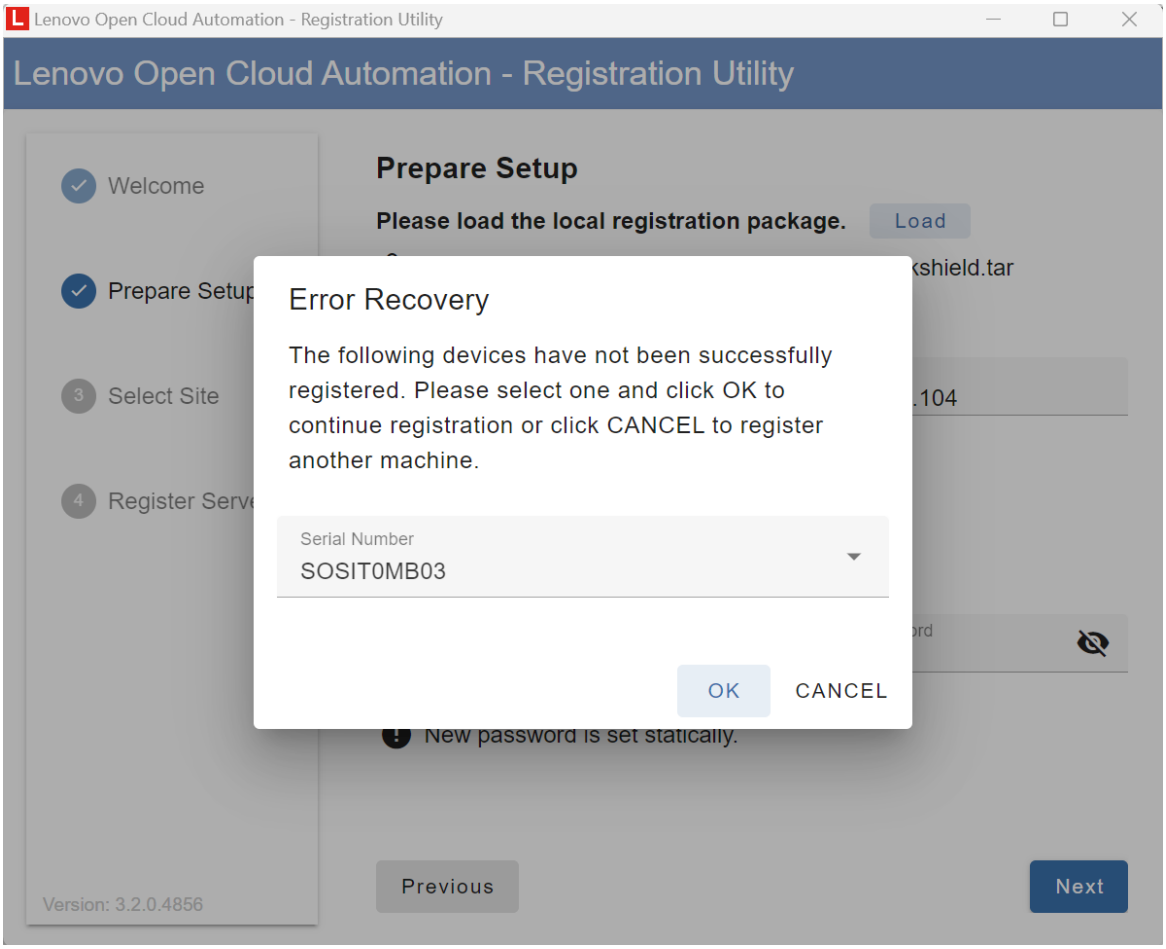


Figure 57: Error recovery

Log

The logs for the LOC-A Utility are located at: *C:\Users\%USERPROFILE%\Documents\LOCA_Utility_logs\xxx.log.* In case you need Lenovo Support, please send the log fille to the Lenovo support team. Max size of the log file is 1M, when the max size is reached, it will be backed up to *xxx.old.log*. Only 1 backup log file is reserved.

Register devices via USB key

You can use the USB key to register edge site server nodes to the LOC-A Core Framework appliance.

Prerequisite

Make sure you have **Ethernet Over USB enabled** with BMC IP address set to 169.254.95.118 (default). This can usually be configured through the BMC interface to the server. Figure 58: Ethernet Over USB shows an example configuration through the XCC user interface.

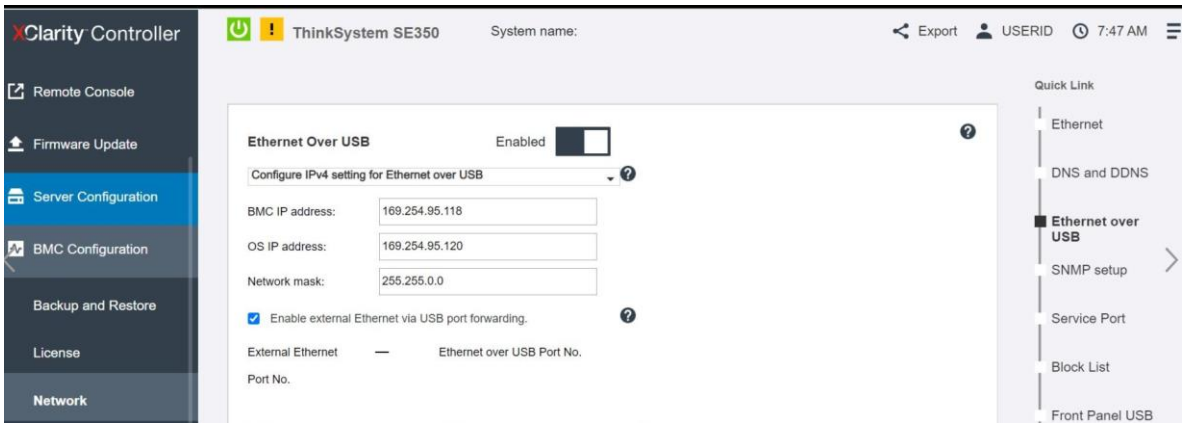


Figure 58: Ethernet Over USB

Complete the following steps to register devices using a USB key:

1. Boot from USB key.
    a. Attach a Keyboard/Video/Mouse (KVM) to the server or open a Remote Media Console from server XCC user interface.
    b. Insert the bootable USB key that you created in one of the USB ports of the system.
    c. Boot the server into the bootable image by pressing F12 during the boot process and selecting the USB device.

    Note: If you are using XCC Remote Media console, you can also mount the .IMG file through the XCC Remote Media Console and choose to reboot the server from the image.

2. Register the server.
    a. After the server is booted, enter the encryption password you receive or defined during registration package creation.

Figure 59: Input encrypt password

    b. Change XCC password.
    To change the XCC password in this step. You will need to enter the original XCC password and then the new credential.

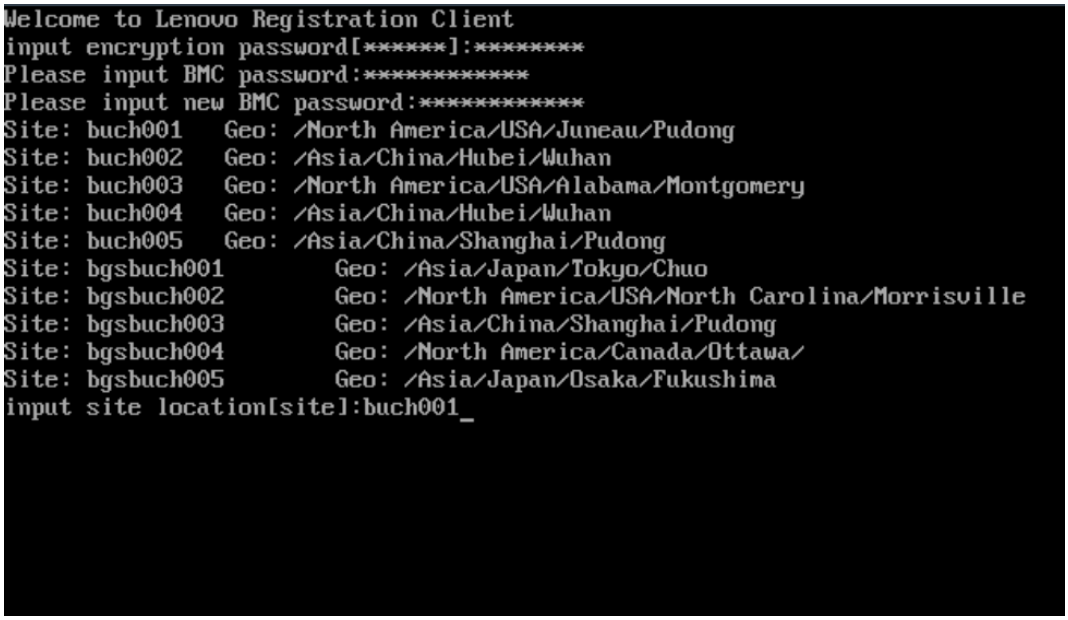


Figure 60: Change XCC password

c. Configure the server.
Select the expected site to which your device will be registered, and enter the correct IP address. The XCC IP needs to align with the one specified during the Ethernet over USB configuration (the default is 169.254.95.118).

Figure 61: Config the server

Note: The output appears only when choosing **Option 1.**

d. Register the server.
After the server is configured, an action menu is displayed. Choose action 3 to register the server directly. If the connectivity check was not performed earlier, LOC-A will attempt the connectivity

check first. If the check is successful, this server is registered. If the check fails, check the cabling and use action 2 (connectivity check) to re-check the connectivity until the check is successful.

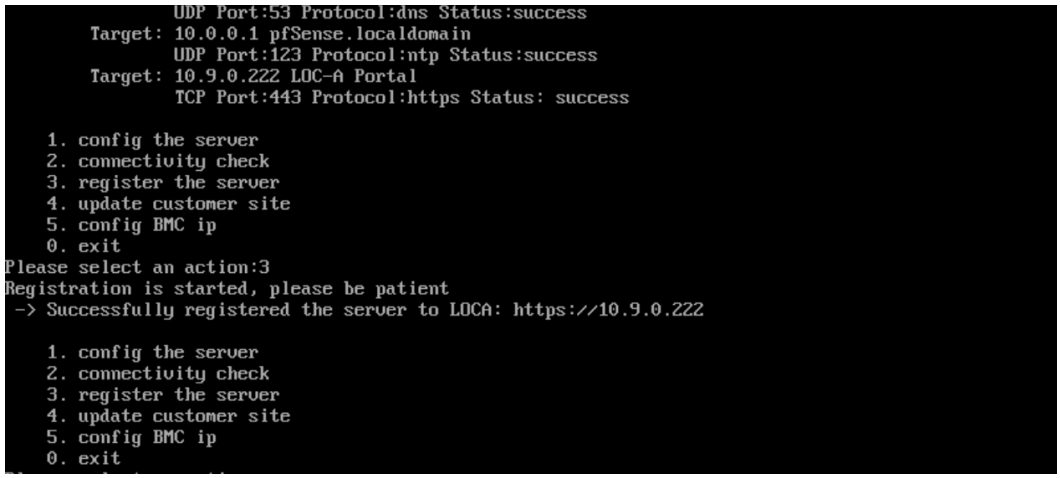


Figure 62: Register the server

e. Configure the XCC IP address (optional).
Use action 5 to assign an IP from the XCC IP address range for the site to the XCC automatically.

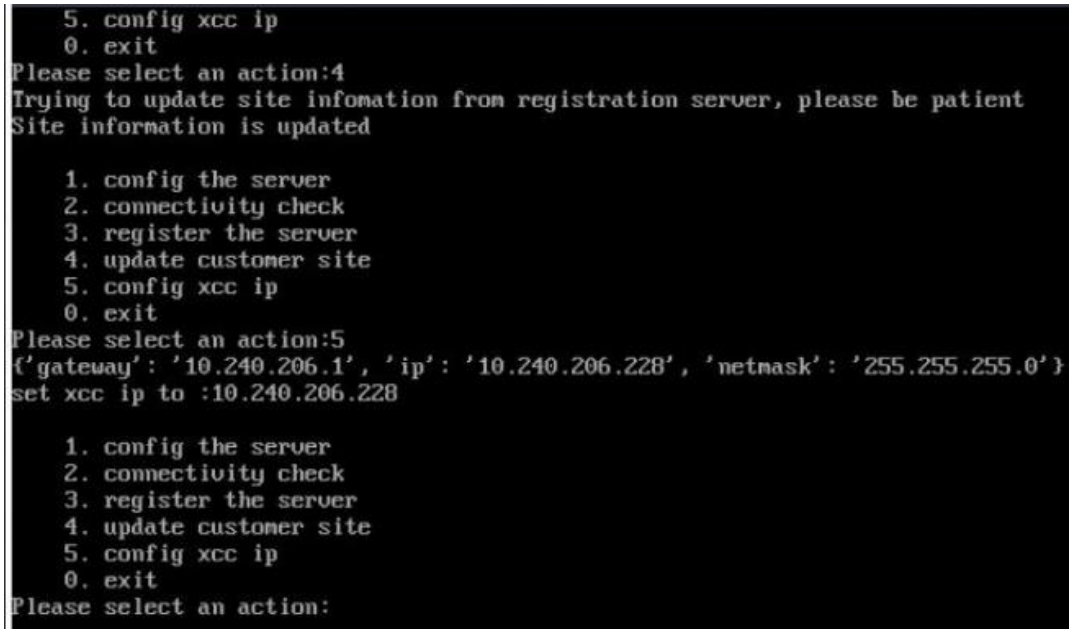


Figure 63: Config the server

f. Reconfigure the server (optional).
If the server registration failed because of an incorrect configuration, such as selecting the wrong site or entering the wrong credentials, use action 1 (config the server) to reconfigure the server.

g. Update customer site (optional)
If the site information inside the image is not up to date, use action 4 (update customer site) to update the site information from the LOC-A Core Framework appliance.

After you have completed server registration, unplug the USB key from your server. Repeat the same steps to register other server nodes in the edge sites. In the LOC-A portal GUI, you can find all registered devices listed on the Registered Devices page.

Add devices by Discovery

You can use LOC-A to discover server nodes within the same layer 2 network or accessible layer 3 network and add them into LOC-A inventory.

Complete the following steps to register devices through automatic discovery within the same layer 2 network:

1. Click **Registered Devices→Add Device→Add Device by Discovery**.

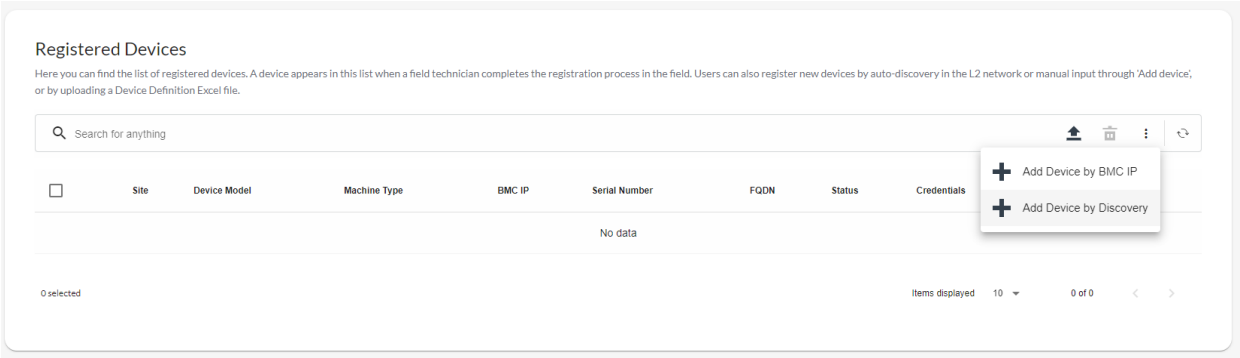


Figure 64: Add devices by discovery

2. Make sure the site from which you want to register devices has a BMC network pre-planned in the Setup so that LOC-A can assign BMC IP addresses for those devices based on the BMC IP range you defined.

   Note: If the value shown in the BMC Network column is not **'ready'**, it indicates that the BMC(XCC) network was not properly planned, and you will not be able to select that site.

   Select the site that you want to add devices into and click **Next**.

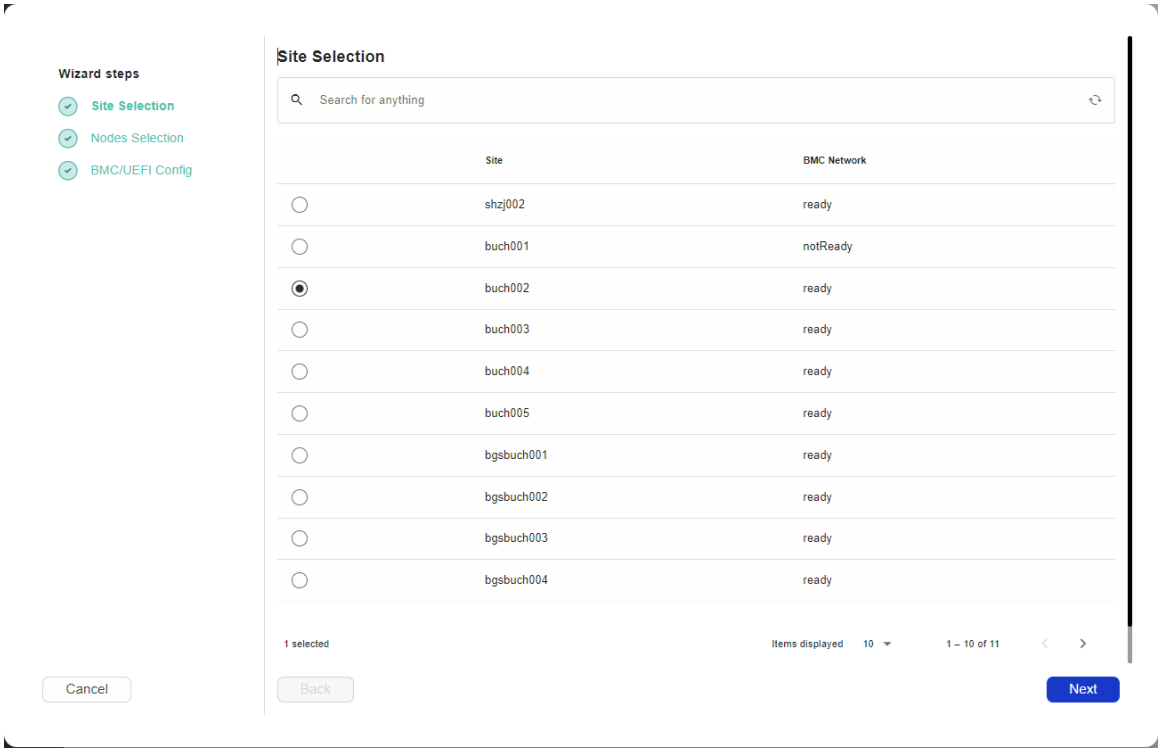


Figure 65: Add devices by discovery - site selection

3. A list of discovered nodes is displayed. Click **Rediscover** to rescan the layer 2 network. Select the devices you want to register and click **Next**.

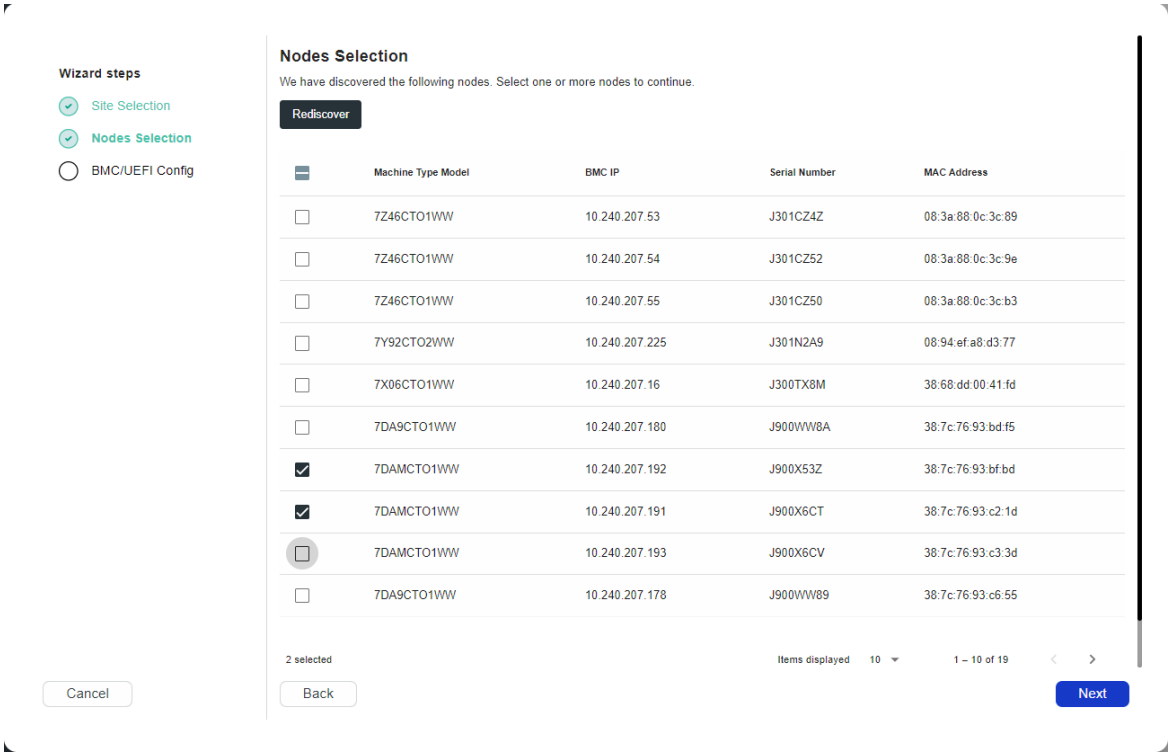


Figure 66: Add devices by discovery - nodes selection from discovered list

4. On the BMC/UEFI configuration page, specify BMC and UEFI new password policy and reconfigure BMC IP addresses. As each site has a BMC IP range defined, the new BMC IP address for each node can be selected from the dropdown list of available IP addresses in the BMC IP range. Specify existing BMC and UEFI passwords as well in the case that the server is not using a factory default configuration.

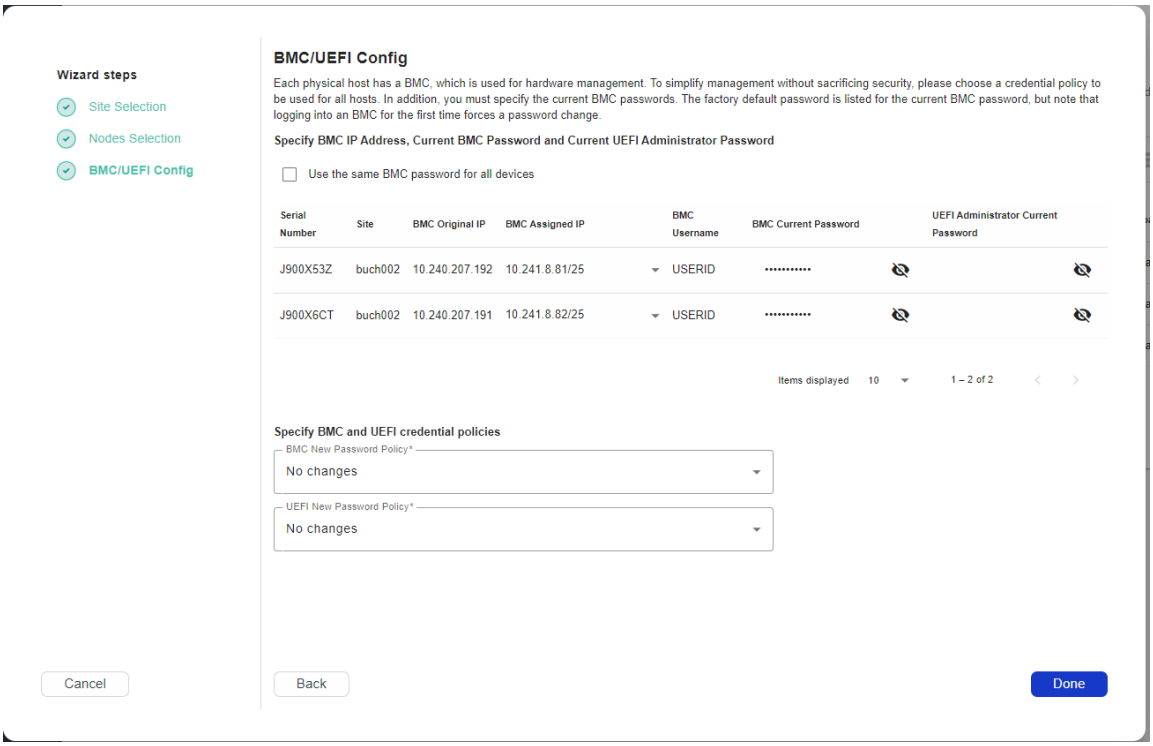


Figure 67: Add devices by discovery - BMC/UEFI config

5. After completing the form, click **Done** to start the registration process. You can view the progress of the registration process from the Tasks page.

After the task has completed, you can see the server in the list of registered devices.

Complete the following steps to register devices through automatic discovery via accessible layer 3 network:

1. User needs to configure, in advance, the IP addresses of the XCC devices (by static allocation or through DHCP)
2. In the Cloud Setup Template document, the user would need to configure as **User allocated** the **IP Allocation Strategy** column for an IP range of **BMC** role as in the following example:

- If the 'Allocation Strategy' option is set to 'User allocated', users should allocate the IP by themselves.

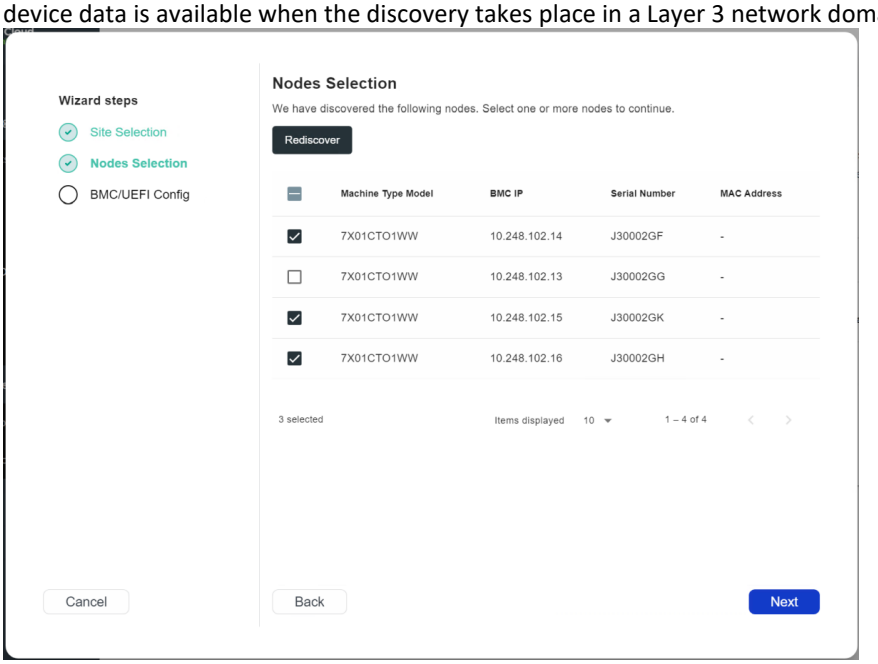
IP ranges

Name *	Associated Sites*	Role*	Prefix*	Vlan	IP Start	IP End	Default Gateway	IP Allocation Strategy
vmanagement_range0010	buch0010	Management	172.31.0.0/16		172.31.9.81	172.31.9.85	172.31.20.206	LOC-A allocated
vmanagement_range0011	buch0011	Management	172.31.0.0/16		172.31.9.71	172.31.9.79	172.31.20.206	LOC-A allocated
vmanagement_range0012	buch0012	Management	172.31.0.0/16		172.31.9.91	172.31.9.93	172.31.20.206	LOC-A allocated
vmanagement_range0013	buch0013	Management	172.31.0.0/16		172.31.9.94	172.31.9.96	172.31.20.206	LOC-A allocated
vmanagement_range0014	buch0014	Management	172.31.0.0/16		172.31.9.97	172.31.9.99	172.31.20.206	LOC-A allocated
bgs_vmanagement_range1	bgsbuch001	Management	10.0.0.0/24		10.0.0.2	10.0.0.10	10.0.0.1	LOC-A allocated
bgs_vmanagement_range2	bgsbuch002	Management	20.0.0.0/24		20.0.0.2	20.0.0.10	20.0.0.1	LOC-A allocated
bgs_vmanagement_range3	bgsbuch003	Management	30.0.0.0/24		30.0.0.2	30.0.0.10	30.0.0.1	LOC-A allocated
bgs_vmanagement_range4	bgsbuch004	Management	40.0.0.0/24		40.0.0.2	40.0.0.10	40.0.0.1	LOC-A allocated
bgs_vmanagement_range5	bgsbuch005	Management	50.0.0.0/24		50.0.0.2	50.0.0.10	50.0.0.1	LOC-A allocated
vsan_range0010	buch0010	vSAN-vSAN	11.11.11.0/24		11.11.11.11	11.11.11.20		LOC-A allocated
vmotion_range0010	buch0010	vSAN-vMotion	12.12.12.0/24		12.12.12.12	12.12.12.20		LOC-A allocated
vsan_global_range	any	vSAN-vSAN	172.16.0.0/24		172.16.0.1	172.16.0.100		LOC-A allocated
vmotion_global_range	any	vSAN-vMotion	192.168.0.0/24		192.168.0.1	192.168.0.100		LOC-A allocated
xcc_range0010	buch0010	BMC	10.241.8.0/25		10.241.8.85	10.241.8.88	10.241.8.1	User allocated
xcc_range0011	buch0011	BMC	10.248.0.0/16		10.248.102.13	10.248.102.16	10.248.102.110	User allocated
xcc_range0012	buch0012	BMC	10.241.8.0/25		10.241.8.113	10.241.8.114	10.241.8.1	User allocated

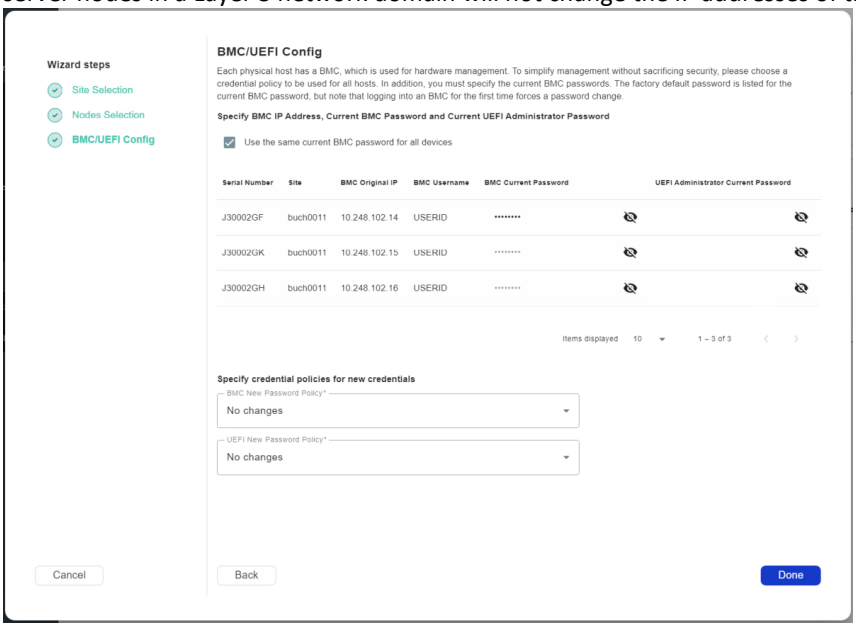
Sites | IP Ranges | Network Services | Cloud Services

Ready | Accessibility: Investigate | Display Settings

3. In the **Node selection** dialog, the *MAC address* column will be empty since, at this stage, not all the XCC device data is available when the discovery takes place in a Layer 3 network domain.



4. In the **BMC/UEFI Config** dialog, the *BMC Assigned IP* column is no longer present, since the registration of server nodes in a Layer 3 network domain will not change the IP addresses of the selected nodes.



5. After completing the form, click **Done** to start the registration process. You can view the progress of the registration process from the Tasks page.

After the task has completed, you can see the server in the list of registered devices.

Note:

- The XCC IP of the target server must not conflict with the XCC IP configured on LOC-A appliance
- Mutiple sites should not use the same XCC IP address range

Add device by BMC IP

You can add a single device into LOC-A inventory by manually entering the BMC information. Complete the following steps to add a device using the BMC IP address:

1. Click **Registered Devices→Add Device→Add Device by BMC IP**.
2. Select the site to which the BMC will be added and click **Next**.
3. In BMC configuration page, enter the BMC IP address, the BMC user ID, the existing BMC passwords.
4. Select BMC New Password Policy or keep it as **No changes** which means do not change BMC password.
5. Select UEFI New Password Policy or keep it as **No changes** which means do not change UEFI password.
6. After completing the form, click **Done** to begin the registration process. You can view the progress on the Tasks page.

   Note: The BMC IP address you enter must be a valid IP address in the BMC(XCC) IP address range that you defined for your selected site.

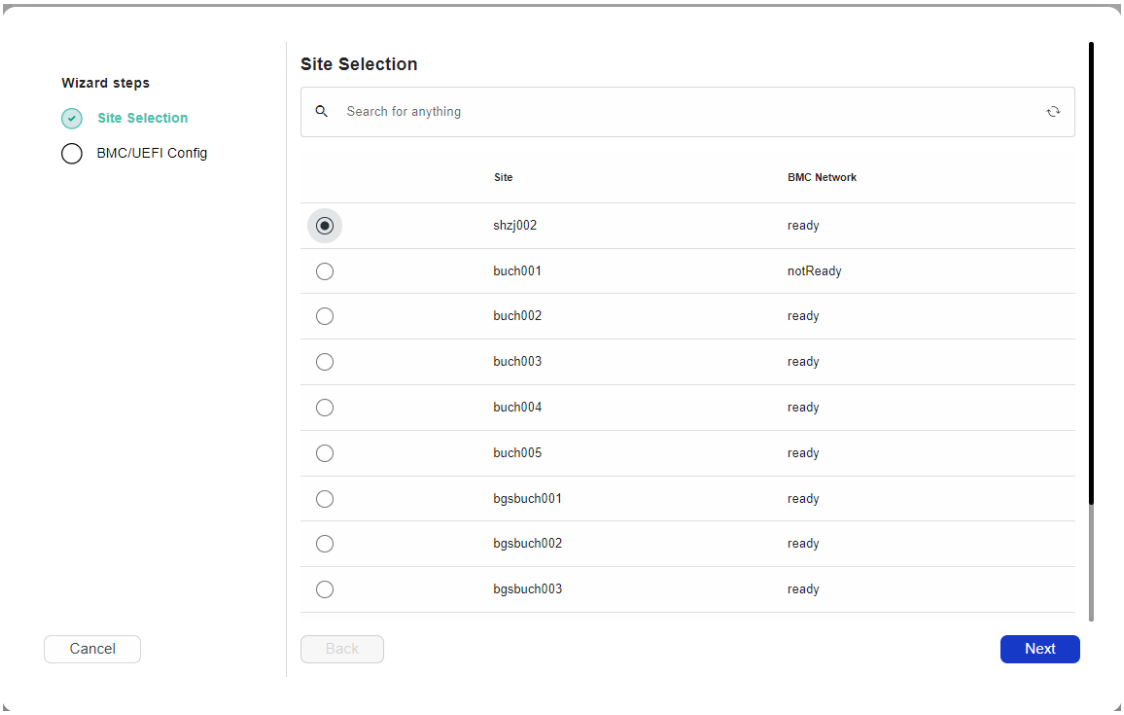


Figure 68: Add device by BMC IP – select site

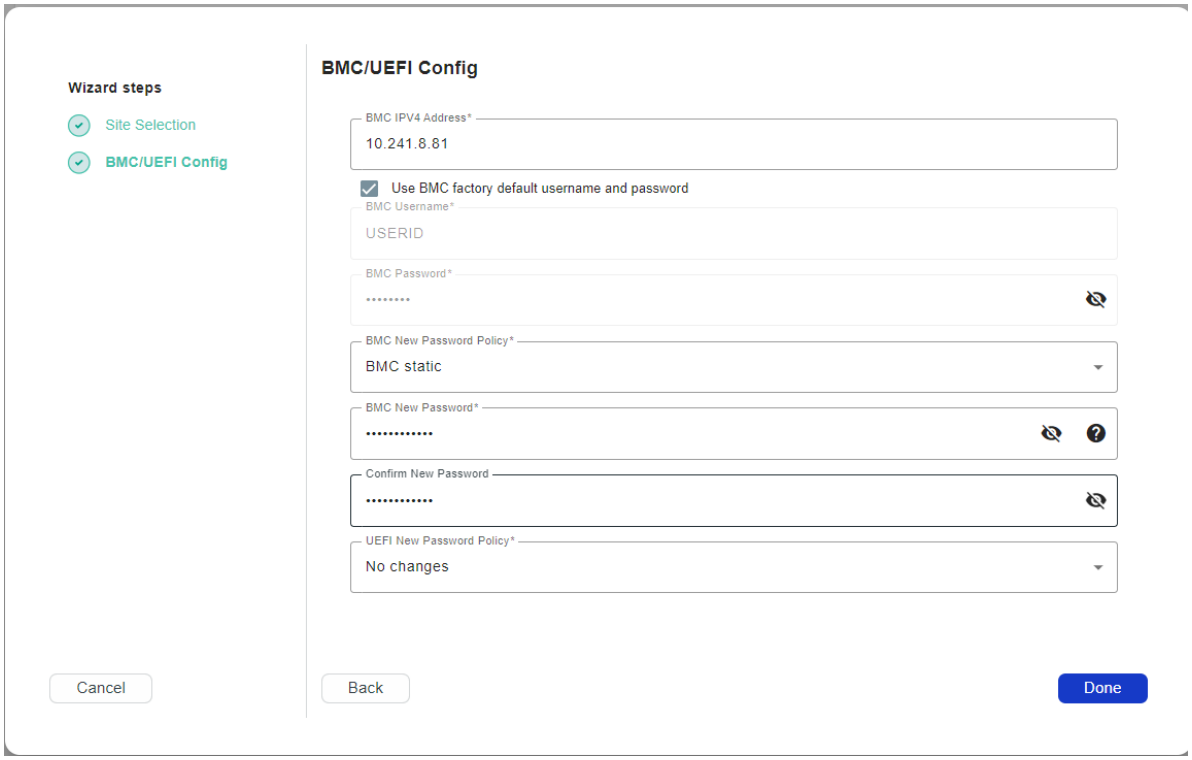


Figure 69: Add device by IP – BMC/UEFI Config

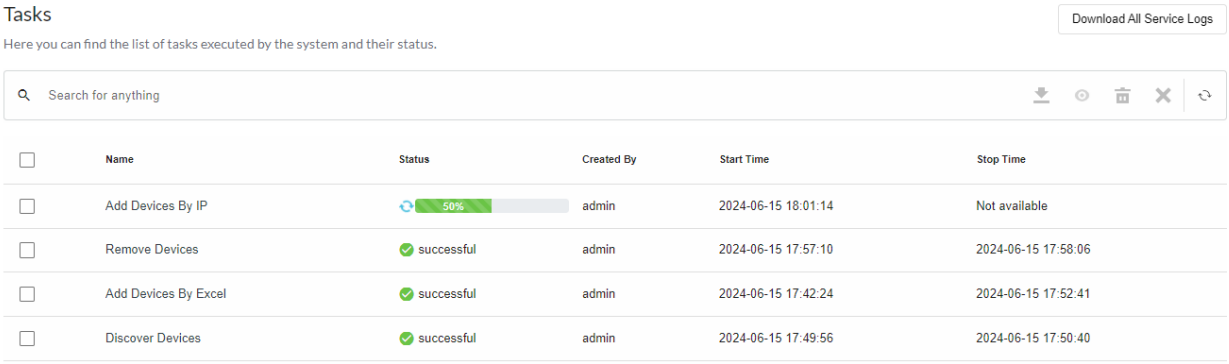


Figure 70: Task of add devices

7. Once the device is processed, you will be able to view it in the Registered Devices list.

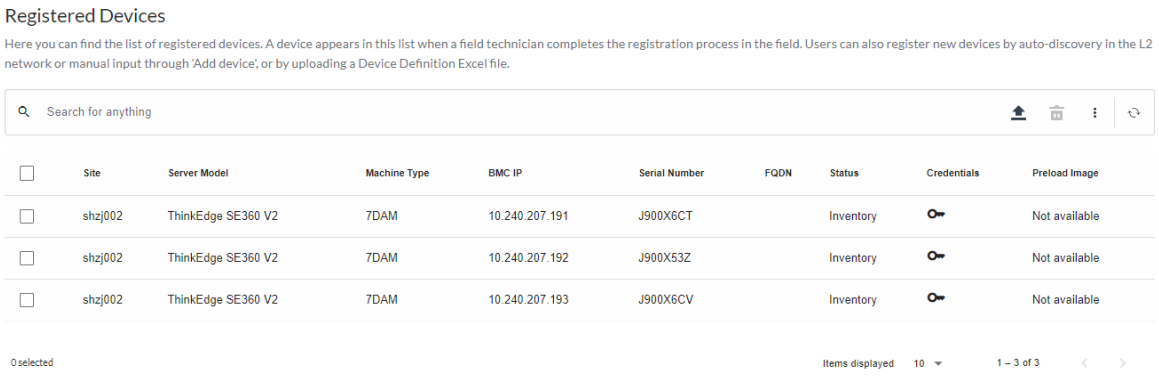


Figure 71: Registered device list

Upload device Excel file

LOC-A also supports importing your devices in batches through an Excel file. Complete the following steps to import devices through an Excel file.

Prerequisite

1. From the LOC-A web interface click **Registered Devices** -> **Download Device Definition file template** to get the sample Excel file "Device_Definition_Standard_Template.xlsx", and follow the embedded instructions to fill in the file with the planning data for your devices.
2. Click **Upload** icon.
3. Click **Browse** to find the file that you created.
4. Select BMC New Password Policy or keep it as **No changes** which means do not change BMC password.
5. Select UEFI New Password Policy or keep it as **No changes** which means do not change UEFI password. In addition these two options, you can also select **Clear Password** which means clear the UEFI password.
6. Click **Upload** to upload the file.

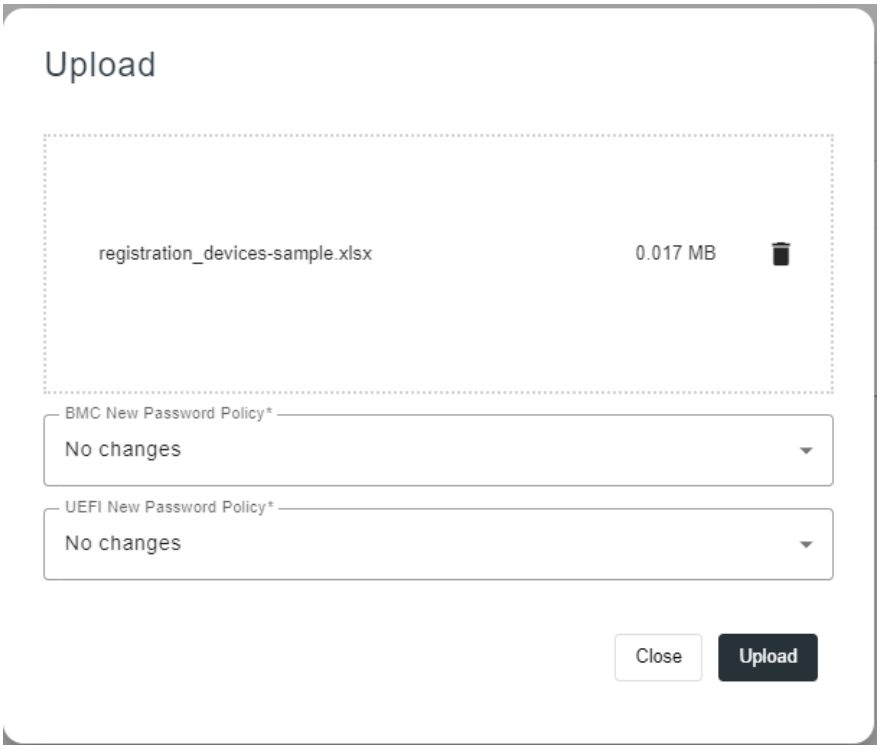


Figure 72: Upload device Excel file

7. After the devices have been processed, you can view them in the Registered Devices list.

Adding devices into external hardware management tools

LOC-A provides integration with external device management tools like Lenovo xClarity Administrator (LXCA) or Lenovo xClarity Orchestrator (LXCO). If you have an external LXCA or LXCO instance defined for your sites, when new devices are registered into LOC-A, they will also be added automatically to LXCA for continued lifecycle management.

To enable this function, you need to define a cloud service with type Hardware management in your metadata Excel file. For example:

Name *	Platform Type*	Type*	Site List*	IP/FQDN*	Admin user	Admin password	Used for connectivity check*	Connectivity check protocol	Num of retries in connectivity check
lxca	Lenovo LXCA	Hardware management	any	lxca.global.custom.local	xxx	xxxxx	Yes	HTTPS, Port 443	3

Figure 73: LXCA cloud service of Hardware management type

The LXCA or LXCO instance can either be an IP address or an FQDN that is resolvable by the DNS configured for the LOC-A Core Framework appliance. If you specify a site list, all nodes from those sites will be added to this LXCA instance.

A server node can only be managed by one LXCA instance. Therefore, the sites are associated with LXCA services in the order of affinity. For example, assume that you have two LXCA instances defined:

- LXCA1 is dedicated for siteA
- LXCA2 has a site list of any.

In this scenario, new servers from siteA will be added to the LXCA1 instance.

Note: Make sure that you provide the correct administrative credentials for the LXCA instance so that the nodes may be added to LXCA automatically when new servers are added to LOC-A.

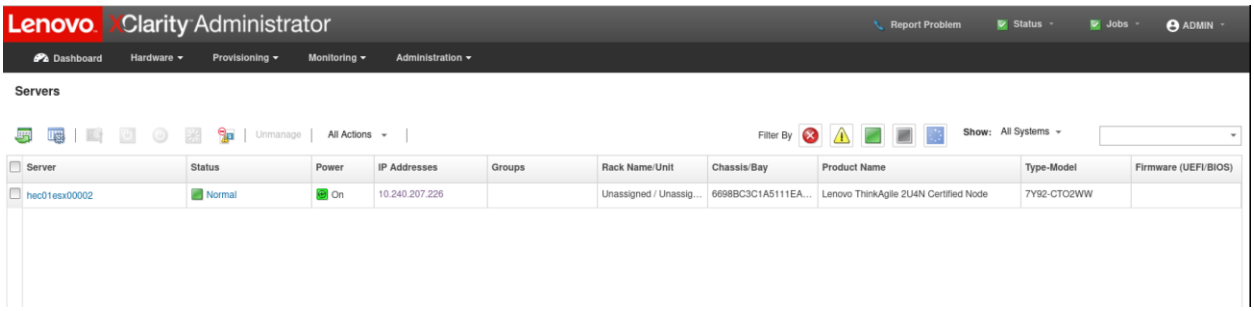


Figure 74: Devices added into LXCA instance

Repository management

LOC-A provides an internal repository where you can upload your ISO files for bare metal or cloud deployments, upload firmware packages for your operations, or the OVA files for LXCI service deployment.

From the LOC-A web interface, click **Setup→Repository** to view the list of files in the repository.

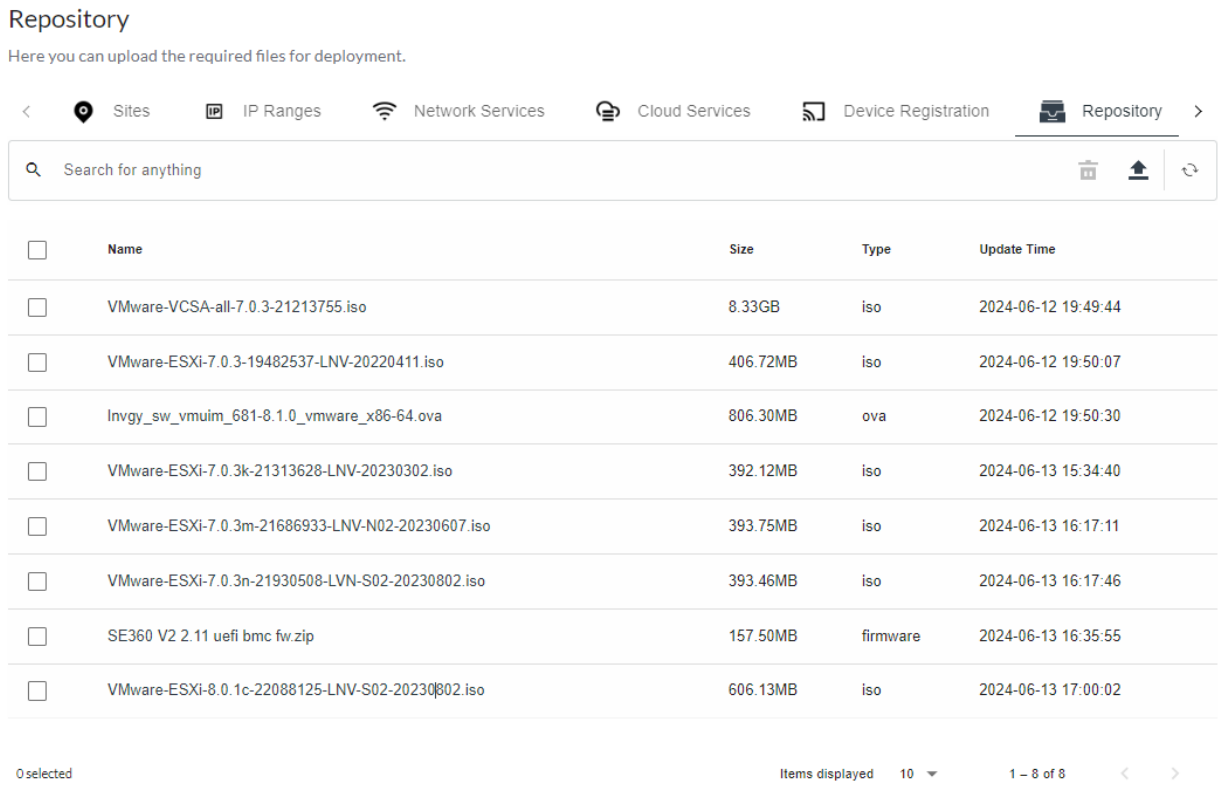


Figure 75: LOC-A repository page

View image details:

You can view image details by clicking on one file from the Repository page. For ISO files, the MD5 checksum value is displayed. If the ISO file is supported by LOC-A for OS deployment, it is shown as Deployment Supported. Figure 76 shows an example of the ISO image details.

Figure 76: ISO image detail

For firmware package files, the firmware type (XCC or UEFI), release date, version/build information, and all supported device types of this firmware package are listed in detail.

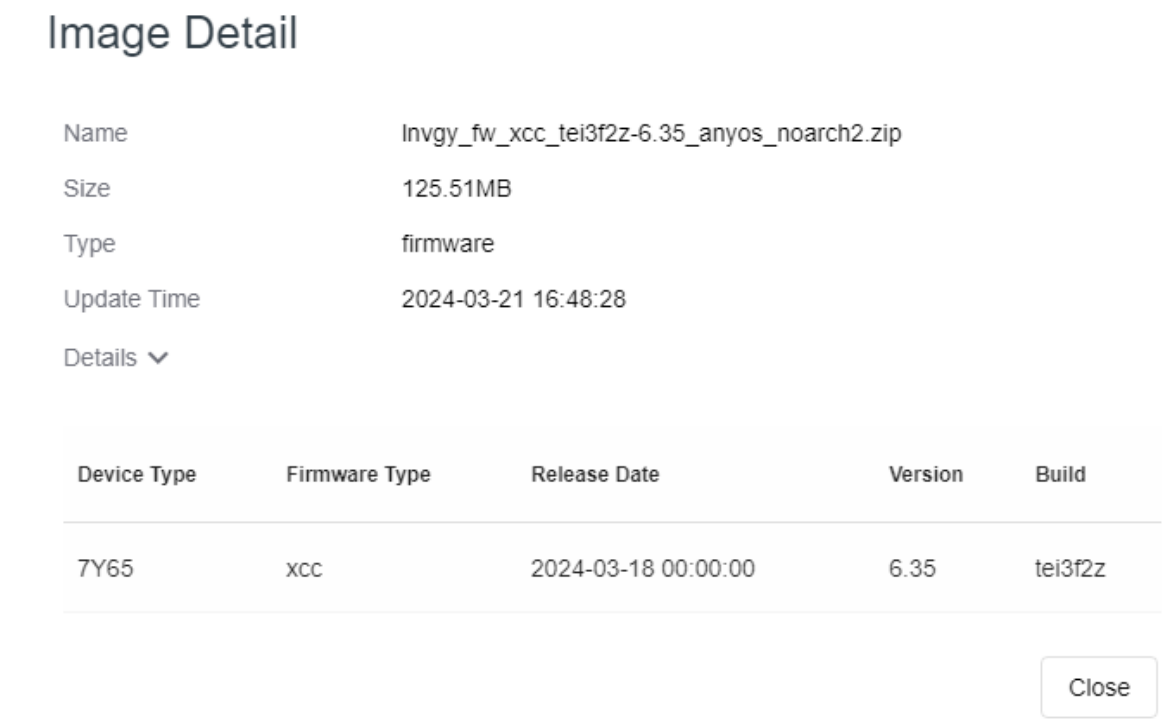


Figure 77: Firmware package detail

Upload a file to the LOC-A repository:

Complete the following steps to upload a file to the LOC-A repository:

1. Click (**Upload)** from the Repository page.
2. Choose the file type of the file to be uploaded and click **Browse** to find the file.

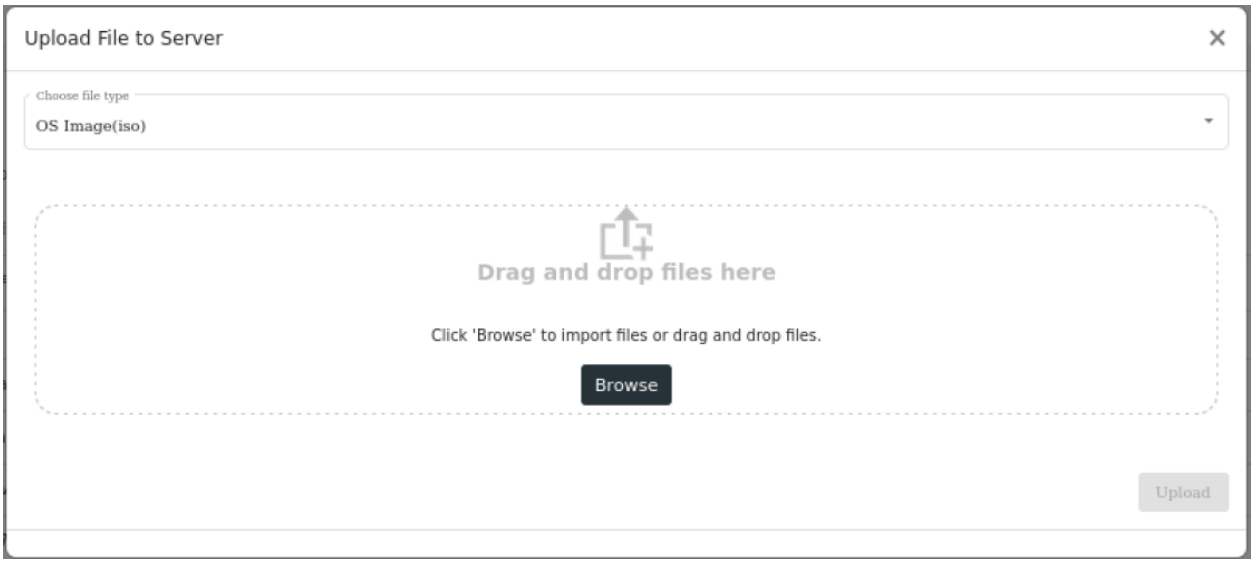


Figure 78: LOC-A Repository – Upload File to Server

3. Click **Upload**.
    - For an ISO file, the verification is done during upload. If the image is not supported, the upload operation to the repository will fail.
    - For a firmware file, for firmware of servers that are not ThinkEdge SE455v3, make sure that the file you upload is a zip file that contains one or more Lenovo firmware bundles. Each firmware bundle needs to contain a .uxz firmware payload file, and an .xml file for manifests with the same filename prefix. The zip file supports only one directory level, please do not put .uxz or .xml files into a subdirectory in the zip archive, otherwise the firmware can't be detected properly. For ThinkEdge SE455v3 server, the firmware payload file you get from Lenovo support site is a .zip file without an .xml file, please use this .zip file for upload directly and do not package this payload file again with other firmware bundles. You can visit https://datacentersupport.lenovo.com/ to get the expected firmware files for your servers.
    - For an Open Virtualization Appliance (OVA) file, you can upload a supported VMware VCSA OVA file bundle. LOC-A only supports to use the OVA file for vCenter cloud service deployment.

Note: Repository files are important artifacts for your cloud and bare metal OS deployments. Make sure that you have the necessary files uploaded into the repository before you attempt to create a cloud or OS template and perform a deployment.

Vault secrets management

Starting with 3.1 the LOC-A VM will use an internal Hashicorp Vault server for storing the user credentials, instead of using mongodb as in previous versions. Since Hashicorp Vault is a professional secret management solution this will be a step forward for a more secure environment.

The user's secrets, stored into the LOC-A internal vault server, will be used only to fulfill the LOC-A specific tasks/jobs and will not be accessible outside the LOC-A appliance through GUI or rest-api calls.

Both GUI and rest-apis that also return credentials into their outputs will hide those credentials under the "********" string, if there is no external read-write vault instance registered by the user, or will return "a pointer" to the credential stored into the external read-write vault instance if the user already registered such an instance in LOC-A. The format of the "pointer" will be @@@vaultname@@full_secret_path. The vault_name will stand for the name of the registered external read-write vault, while the full_secret_path will contain the full secret path for that credential in the external read-write vault instance, including the root secret path used during external read-write vault instance registration.

Another new behavior in 3.1, is that the auto credential policy cannot be created if there is no external read-write vault registered by the user into the LOC-A appliance. Since LOC-A will not display any of the user's secrets into its GUI (or rest-apis) anymore, a LOC-A auto generated secret can only be seen by the user in the external read-write vault instance. That instance points to a user controlled Hashicorp Vault server, which belongs to the LOC-A user and not to LOC-A itself.

Also if the user wants to unregister the last read-write vault instance from LOC-A, and there are auto credentials policies defined in LOC-A, the unregister process will fail.

Any of the vault instances registered by the user in LOC-A – read-only or read-write – are using vault tokens for the registration purpose. Those vault tokens have a limited existence in time, the validity period of the token being controlled by the Hashicorp Vault Server manager (by default 32 days). Until 3.1 if the token used expires, the user is expected to unregister the vault instance for that token and register it back with the new token. In 3.1 a vault instance can be updated with a new token value, without the need of removing the instance and adding it back. So in the case that the user already has auto credential policies defined in LOC-A and an external read-write vault instance with an expired token, the user can just update the token and will not need to delete the auto credential policy, unregister the vault instance, re-register the vault instance with the new token and re-create the auto credential policies.

Since LOC-A will no longer display the user's secrets, the GUI pages related to vault registered instances will also change, so the credentials that are stored into a read-only or read-write vault instance will no longer be displayed or exported as an encrypted file.

Hashicorp Vault instance can be used as a user owned backup solution for the LOC-A user's secrets, or as a user owned secrets source for LOC-A's user's secrets. This feature integrates LOC-A with the HashiCorp Vault application. Users can opt to centralize all secrets in a HashiCorp Vault server. This application offers identity-based security, automatically authenticating and authorizing access to confidential and sensitive information for organizations and can be integrated with other cloud management applications.

Information about Hashicorp Vault can be found under these tutorials –
https://developer.hashicorp.com/vault/tutorials

Here are the steps to use vault management in LOC-A. A user needs to setup an external vault server before starting to use the vault management feature in LOC-A. More users with different rights over different secret paths can be created by the user in the vault server. One or more key/values secrets engine may be enabled. After that, in LOC-A a user may register two types of Vault Instances or Vault Clients. The read-write Vault Instance in which LOC-A will automatically save all user's secrets (including the auto generated secrets), and one or more read-only Vault Instances, that will be pre-populated by the user (LOC-A will not update any secret in a read-only Vault Instance) and used by LOC-A to load user's secrets from those instances during service xls onboarding, device registration, OS and cloud deploy template creation or OS/Cloud instance creation

1. Registration of a read-write/ready-only Vault Instance in LOC-A

   Navigate to **Setup →Vaults** and click the **Add** icon:

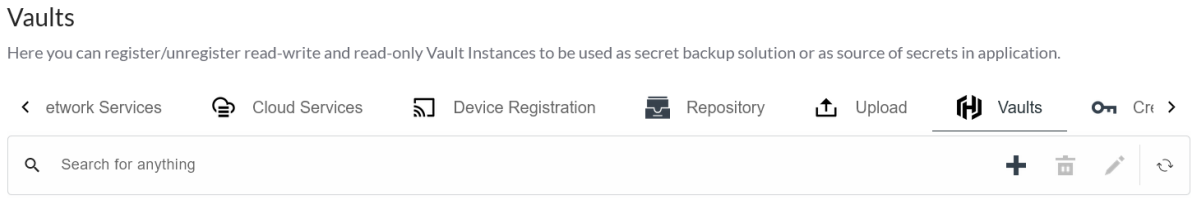


Figure 79: Vaults list

After clicking the **+** icon, you will get the prompt dialog for you to input the vault instance information:

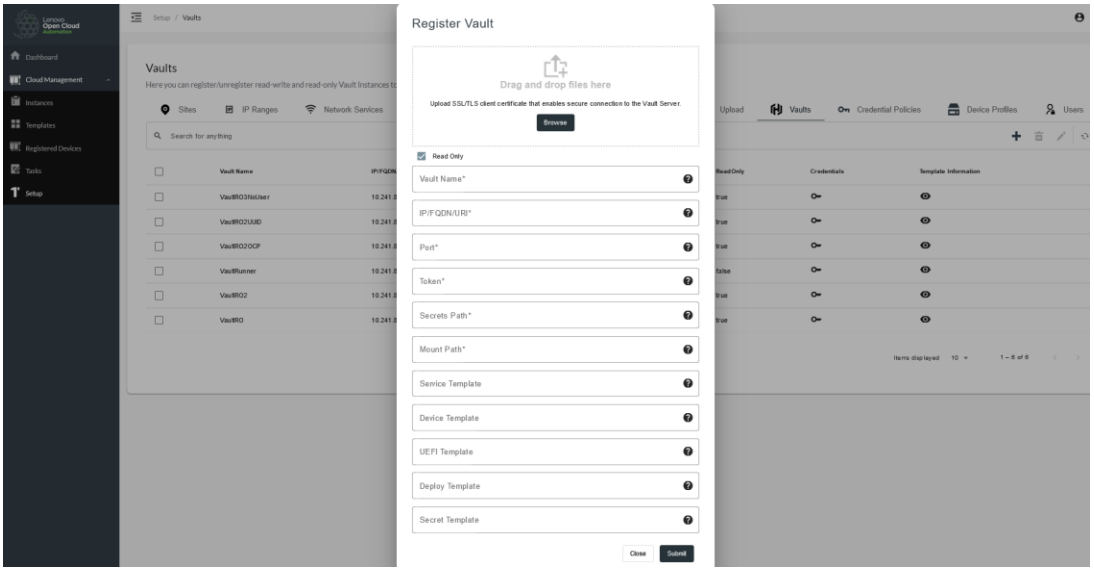


Figure 80: Register a vault

- “File Path” field is the SSL certificate used by the Hashicorp Vault server to initialize its SSL communication (as described above). The Hashicorp Vault user should be able to provide this certificate.
- "Vault Name" field is the Hashicorp Vault instance name registered into LOC-A. It is just a name for a Cloud Service like resource into LOC-A, so the LOC-A administrator use can use whatever name they want for it. Should be unique in the LOC-A system.
- "FQDN or IP" field is the FQDN/IP of the Vault service
- "Port" field is the tcp port on which the Vault service was started, same as the port used to start the vault server.
- "Token" field: This is a token associated with one of the Hashicorp users. This user should be created in Vault with read-write rights over the "secretsPath": "LOCA/" inside the secret engine identified by "mountPath": "kv-v1/"
- "SecretsPath" field– All secrets that will be written by LOC-A into the “VaultRunner” instance will be written under this root path. The full root path will be in fact a concatenation between secret engine mount path and this one -> kv-v1/LOCA/ in our example.
- "mountPath": – the mount point for the secret-path from Hashicorp Vault service (for example kv-v1/)
- "readOnly" checkbox: unchecked – will mean a read-write Vault Instance, an instance that will give LOC-A the right to save secrets under its registered secret Path -> kv-v1/LOCA/ (in our example). This parameter will make the distinction between a read-only Vault Instance, used only as a secret source for LOC-A, and the read-write instance used for saving LOC-A secrets.

The following templates will be used only with read-only Vaults and will enable the user to define some rules for the secrets path computation in the Vault server. The vault-server will be pre-populated accordingly, the path to the secrets in the server using the same rules. These templates are not mandatory, but if specified during registration, when the user will push later a secret into LOC-A, it will be enough to specify the Vault Instance Name only, while the secret path will be computed based on these templates/rules.

- "Service Template" - Secret path template used for computing the secret path during Cloud_Setup_sample xls onboarding for Cloud Services credentials

Supported built-in template variables that can be used are:
{{service_name}}: the name of the Cloud Service
{{platform_key}}: Cloud Service Platform Type taken from onboarding xls
{{role}}: Cloud Service Role taken from onboarding xls
{{ip_fqdn}}: Cloud Service IP/(FQDN)/URI taken from onboarding xls
Example: **Service/{{service_name}}**

- "Device Template" - Secret path template used for computing the BMC new secret path during device registration

  Supported built-in template variables that can be used are:
  {{site_name}}: string, the site name where the device will be registered
  {{mgmt_ip}}: string of the BMC IP
  {{serial_number}}: string, the device serial number
  {{uuid}}: string, the UUID of the device
  Example: **Dev/{{serial_number}}/BMC**
- "UEFI Template" - Secret path template used for computing the UEFI new secret path during device registration

  Supported built-in template variables that can be used are:
  {{site_name}}: string, the site name where the device will be registered to
  {{mgmt_ip}}: string of the BMC IP
  {{serial_number}}: string, the device serial number
  {{uuid}}: string, the UUID of the device
  Example: **Device/{{serial_number}}/UEFI**

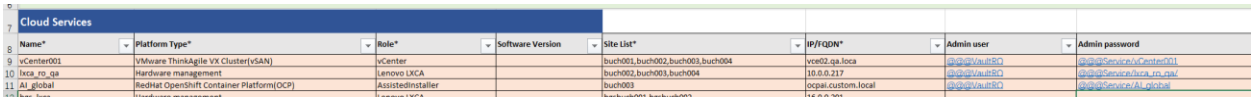
- "Deploy Template" - Secret path template used for computing the OS root/ssh key secret path during OS/Cloud template creation or instance deployment.

  Supported built-in template variables that can be used are:
  {{site_name}}: string, the site name where the instance will be deployed
  {{flavor_name}}: string, deployment flavor name
  {{geo}}: geo string of the site
  {{country}}: country string of the site
  {{province}}: province string of the site
  {{city}}: city sting of the site
  {{hostname}}: string, resulting Host FQDN of the device from the OS and Cloud deploy template wizard
  {{ip_fqdn}}: string, IP associated with above hostname
  {{serial_number}}: serial number of the device
  Example: **Dev/{{serial_number}}/OS**

- "Secret Template" - Secret format template. A vault secret is a dictionary containing different keys and values. LOC-A is interested in the format of only two keys: the username and password keys.

  Examples:
  "user@@@U, Pwd@@@P" - username key will be “user” and password key will be “Pwd”
  "password@@@P" – the vault secret will contain only the password, the username may be part of the secret path
  If not specified, the expected default keywords in vault server secret will be UserName and Password. Same as the default for secrets written by LOC-A in read-write Vault Instance.

2. Use vault instance in LOC-A:
   2.1 use vault management in excel file during setup files upload

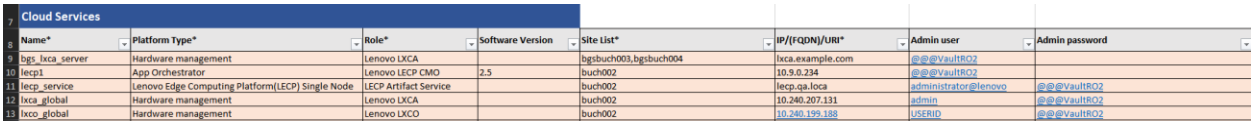


Cloud Services							
Name*	Platform Type*	Role*	Software Version	Site List*	IP/FQDN*	Admin user	Admin password
vCenter001	VMware ThinkAgile VX Cluster(vSAN)	vCenter		buch001,buch002,buch003,buch004	vce02.qa.loca	@@@VaultRO	@@@Service/vCenter001
lxca_ro_qa	Hardware management	Lenovo LXCA		buch002,buch003,buch004	10.0.0.217	@@@VaultRO	@@@Service/lxca_ro_qa/
AI_global	RedHat OpenShift Container Platform(OCP)	AssistedInstaller		buch003	ocpai.custom.local	@@@VaultRO	@@@Service/AI_global

Figure 81: Vault in excel file

@@@VaultRO in above table under Admin user column will identify the read-only Vault Instance Name registered under LOC-A from where the credentials will be read. While @@@Service/vCenter001 will identify the relative secret path for that credential under VaultRO instance. The full secret path will be constructed by LOC-A by appending the LOC-A Vault registration Mount Path and Secret Path to the relative path introduced here by the user.

In this case the VaultRo may have been registered without secret path template support, so secrets need to be given in their full format with @@@VaultName and @@@SecretPath. Below is an extract from another xls for a Vault Instance registered with secret path templates and here is enough to specify only the Vault Name, since the secret path will be computed based on pre-registered secret path templates:



Cloud Services							
Name*	Platform Type*	Role*	Software Version	Site List*	IP/(FQDN)/URI*	Admin user	Admin password
bgs_lxca_server	Hardware management	Lenovo LXCA		bgsbuch003,bgsbuch004	lxca.example.com	@@@VaultRO2	
lecp1	App Orchestrator	Lenovo LECP CMO	2.5	buch002	10.9.0.234	@@@VaultRO2	
lecp_service	Lenovo Edge Computing Platform(LECP) Single Node	LECP Artifact Service		buch002	lecp.qa.loca	administrator@lenovo	@@@VaultRO2
lxca_global	Hardware management	Lenovo LXCA		buch002	10.240.207.131	admin	@@@VaultRO2
lxco_global	Hardware management	Lenovo LXCO		buch002	10.240.199.188	USERID	@@@VaultRO2

Figure 82: Vault in excel file with pre-registered secret path templates

2.2 Vault can be used from the GUI for device upload, device profile set or cloud template creation, etc. For example:

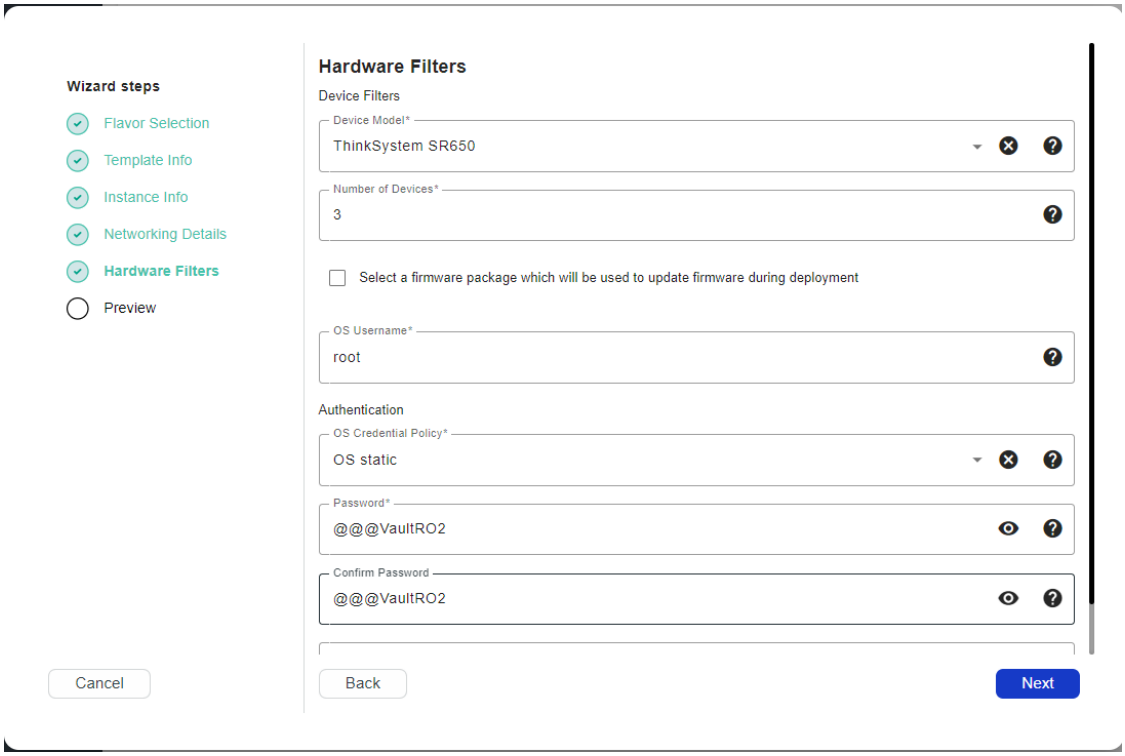


Figure 83: Configure to use Vault with secret path template

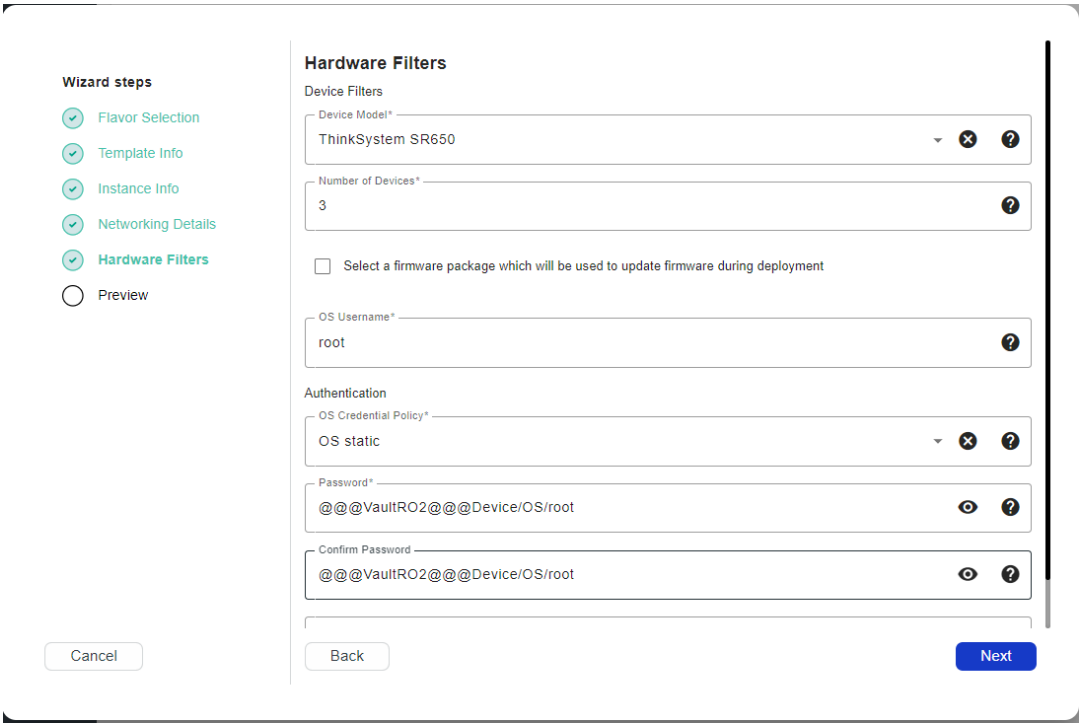


Figure 84: Configure to use Vault without secret path template

In the first example I have used VaultRO2 Vault Instance with template support while in the second example a read-only vault without secrets templates has been used, so the secret should be fully described with its vault instance name and secret path.

3. How to delete(unregister) a vault instance from the GUI:

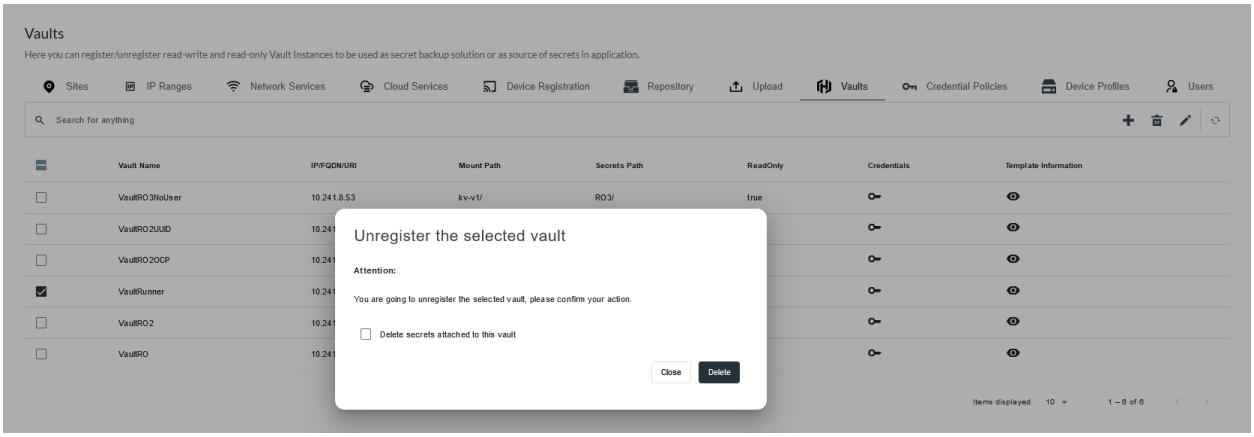


Figure 85: Delete vault instance

Select the vault Instance that you want to delete and click on the delete icon. If the selected vault instance is a read-write instance, the user will be asked if he wants to also delete all the secrets in the vault associated with that vault instance. If the instance is a read-only instance the secrets will remain unchanged in the Vault system.

A vault instance can be registered at any time during LOC-A usage, so if the user has chosen by mistake to delete the secrets pushed by LOC-A in a read-write vault, the user can re-register the vault and the secrets will be pushed back by LOC-A.

Create a cloud template

A cloud deployment template is a way to pre-define how one or more edge-site deployment instances should be configured. You can define the expected cloud flavor, hardware definition, parameters, naming conventions, and password policies in the cloud deployment template.

Complete the following steps to create a cloud template:

1. Go to the Templates page and click **Add** to add a cloud template.

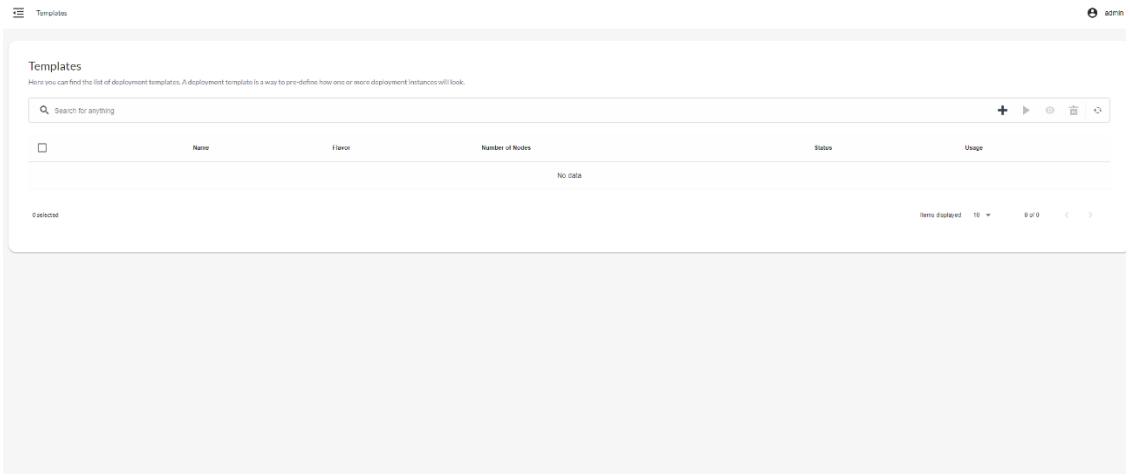


Figure 86: Templates page

2. Select a cloud flavor for the template.

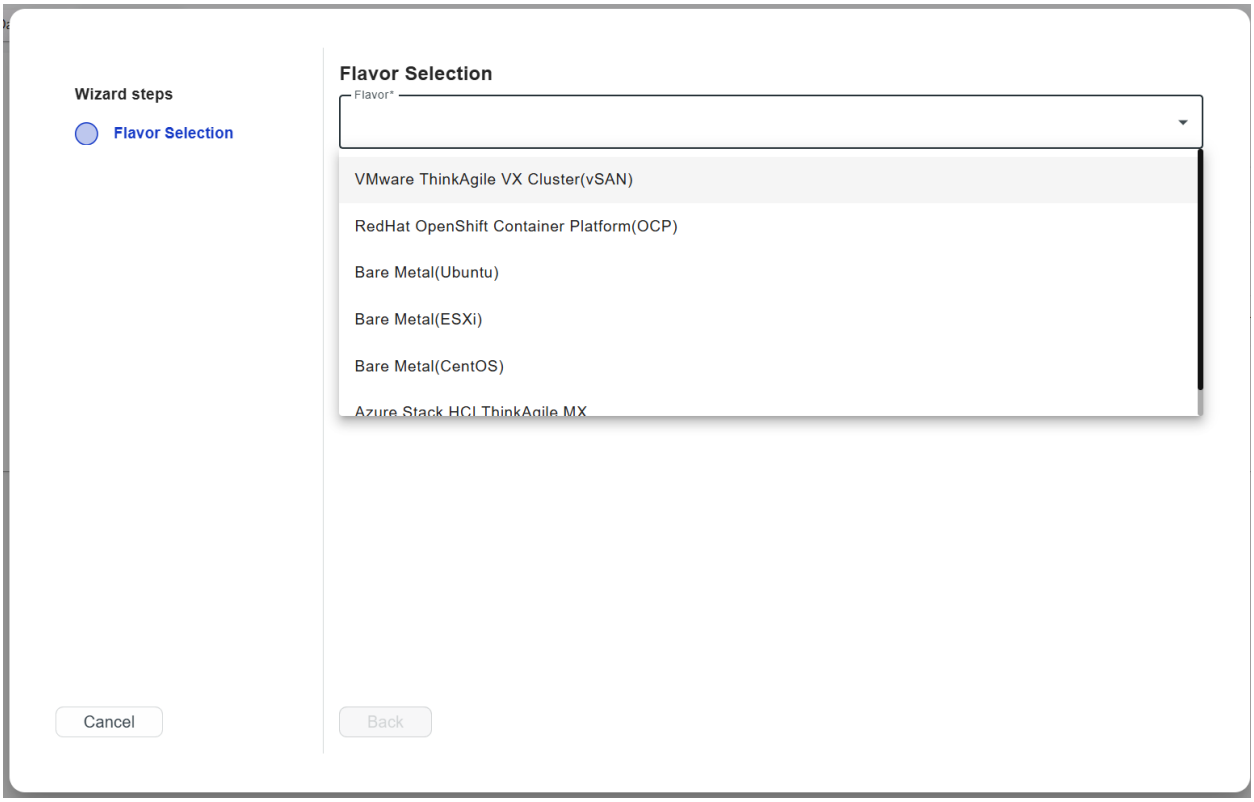


Figure 87: Flavor selection

3. Specify a unique template name. Template name length needs to be 5 to20 characters.

Figure 88: Cloud template wizard

4. Click **Next** to enter the **Instance Info**.
5. On the Instance Info page, select the target cluster type from the dropdown list. Then, define additional cloud-specific parameters for your cluster.

   For example, when you select cluster type “VMware ThinkAgile VX cluster(vSAN)”, you have to configure Instance Name, Flavor Version, OS version and Datacenter Name. LOC-A supports vSAN version 7.0. The version of ESXi supported by LOC-A is ESXi 7.0U3 Build 1948253 please make sure you have downloaded the ISO file from https://vmware.lenovo.com and uploaded it into the LOC-A repository.

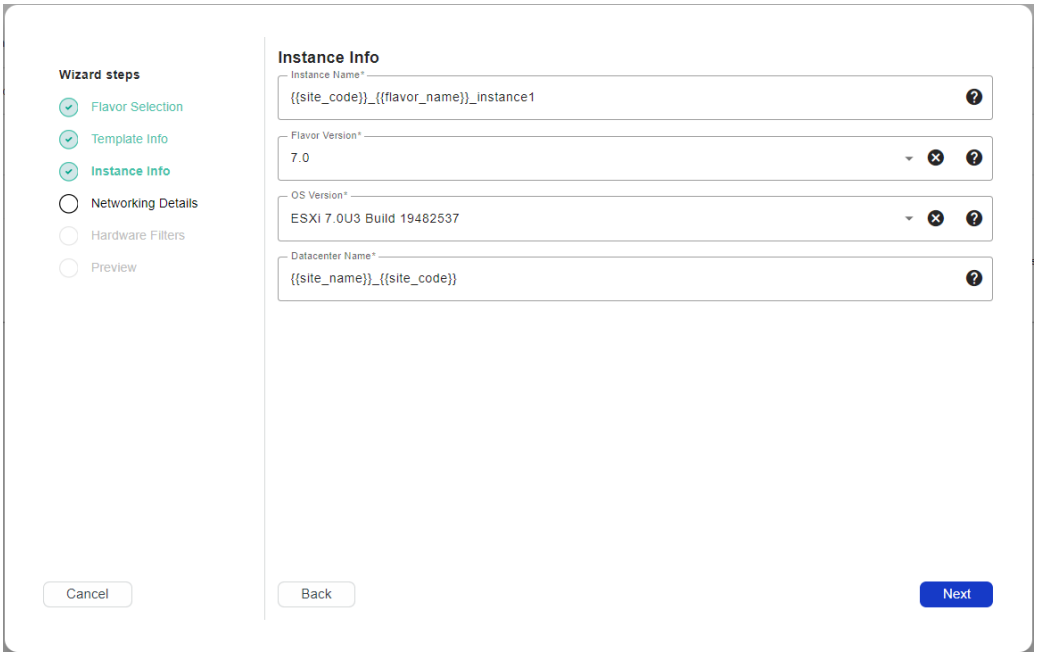


Figure 89: Cloud template – Instance Info

If your cloud template is for a RedHat OCP cluster deployment, you will need to provide the cluster name, cluster network, service network, RedHat OCP version, and the OpenShift Pull Secret for your deployment.

Below is an example of OpenShift Pull Secret:

```
{
    "auths": {
        "cloud.openshift.com": {
            "auth": "xxxxxxxxxxxxxxx",
            "email": "example@abc.com"
        },
        "quay.io": {
            "auth": "xxxxxxxxxxxxxxx",
            "email": " example@abc.com"
        },
        "registry.connect.redhat.com": {
            "auth": "xxxxxxxxxxxxxxx",
            "email": "example@abc.com"
        },
        "registry.redhat.io": {
            "auth": "xxxxxxxxxxxxxxx",
            "email": "example@abc.com"
        }
    }
}
```

Note: LOC-A supports the use of built-in template variables to enable naming flexibility so that the cloud deployment template can apply to multiple sites. As an example, for cluster name, supported built-in template variables that can be used are:

- {{*site_code*}} : site code string of the site
- {{*flavor_name*}}: flavor name string of the site.
- {{*site_name*}}: site name string of the site
- {{*geo*}}: Geo string of the site.
- {{*country*}}: Country string of the site.
- {{*province*}}: Province string of the site.
- {{*city*}}: City string of the site

For example, if the templated cluster name is {{*site_name*}}_{{*flavor_name*}}_cluster1, the cluster name for site ABC will be created as **ABC_vmware-thinkagile-vx-clustervsan_cluster1**. You can refer to the hint of each input field to get the supported built-in template variables list.

6. Click **Next** to display networking details. In this page you can define DNS namespace for your site cluster, and the node hostname FQDNs.

Ensure that the DNS namespace and hostname FQDNs you specify here align with the existing DNS entries you configured in the DNS servers associated with the site (defined as network services). See *Cloud setup*, on page 19 for more information.

For example, if templated Node hostname FQDN is esxi{{#}}.{{site_code}}.{{province}}.{{country}}.customer.com

The node FQDN for a 3-node vSAN cluster site in site1 in Shanghai will be 'esxi001.site1.shanghai.customer.com', etc. If the vSAN-vManagement IP range of site1 is 10.0.0.21/24 - 10.0.0.30/24, you will need to configure DNS entries as follows:

address=/esxi001.site1.shanghai.china.customer.com/10.0.0.21

ptr-record=21.0.0.10.in-addr.arpa.,esxi001.site1.shanghai.china.customer.com

address=/esxi002.site1.shanghai.china.customer.com/10.0.0.22

ptr-record=22.0.0.10.in-addr.arpa.,esxi002.site1.shanghai.china.customer.com

address=/esxi003.site1.shanghai.china.customer.com/10.0.0.23

ptr-record=23.0.0.10.in-addr.arpa.,esxi003.site1.shanghai.china.customer.com

LOC-A will perform an environment pre-check for DNS entries in the cloud deployment task, if you don't have proper entries configured, the cloud deployment task will fail.

Note:
For vSAN cluster deployment, two DNS servers are mandatory, so you will need to configure proper entries for both DNS servers.

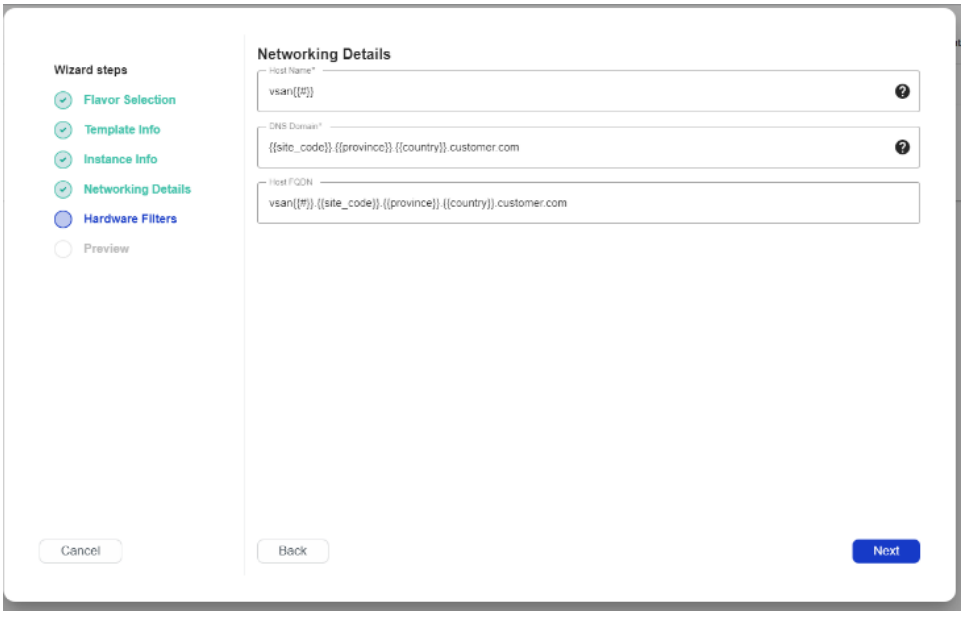


Figure 90: Cloud template - networking details

7. Click **Next** to view the Hardware Filters page where you can specify the expected device type and number of nodes for your cloud cluster deployment.

The minimum number of devices varies based on the cloud cluster type you selected. For VMware vSAN and RedHat OpenShift Container Platform, the minimum number of nodes is 3.

Check the option **Select a firmware package**, and you can choose a specific firmware package. The dropdown lists all supported firmware packages in your repository based on the device model you select.

In the **Device Profile** section, you can choose the available device profile that corresponds to the current flavor. This item is optional.

In the **OS Credential Policy** section, you can select credential policy for root credentials of your cluster nodes. LOC-A supports three authentication types based on the cloud cluster type you selected.

- **Use a public key (approach of the credential policy is publicKey)**.
  Provide a public key as the authorized key, and you can SSH to your cluster nodes via the corresponding private key. All cluster nodes deployed with this cloud template will use the same authorized key.

- **Use a statically defined password (approach of the credential policy is static).**
  Provide a static string as the root password. All cluster nodes deployed with this cloud template will use the same root password. This is usually not recommended because it is not secure.

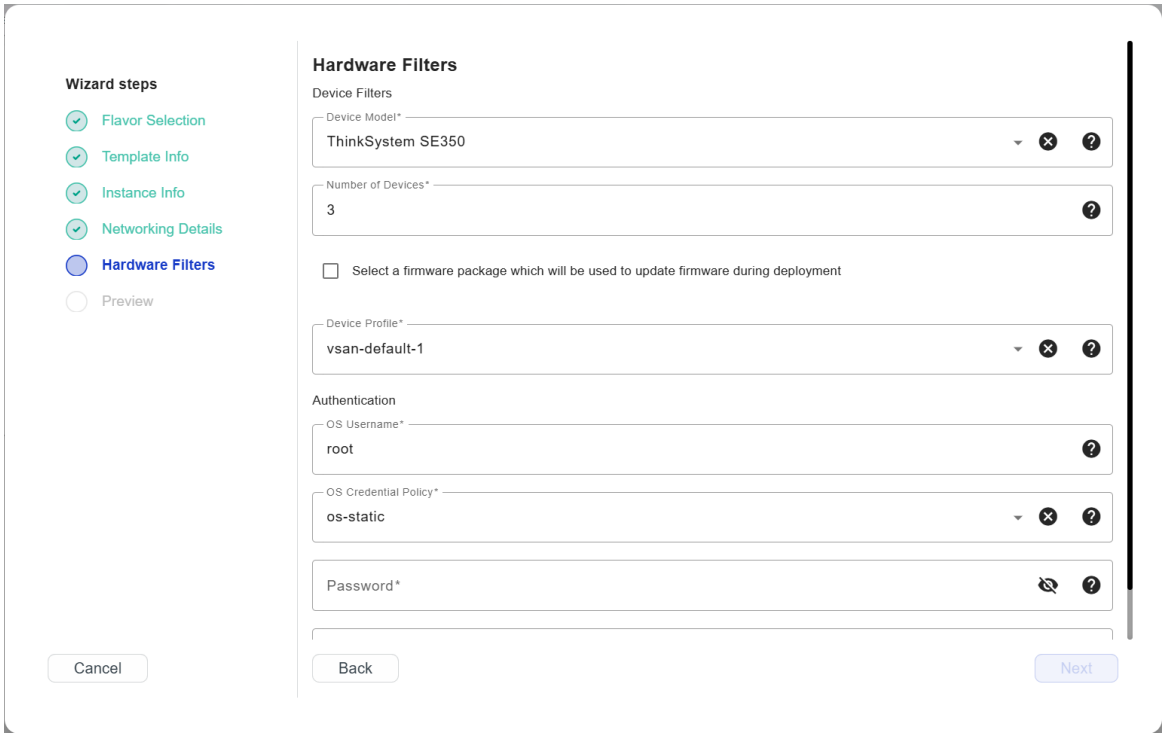


Figure 91: Cloud template - define hardware filter and static root password policy

- **Use a template to generate unique passwords (approach of the credential policy is auto).**
  You will use the template string defined in the credential policy to generate random passwords. Eg. template {{random_characters(12)}} makes a 12 character, random string for each of your nodes' operating system.

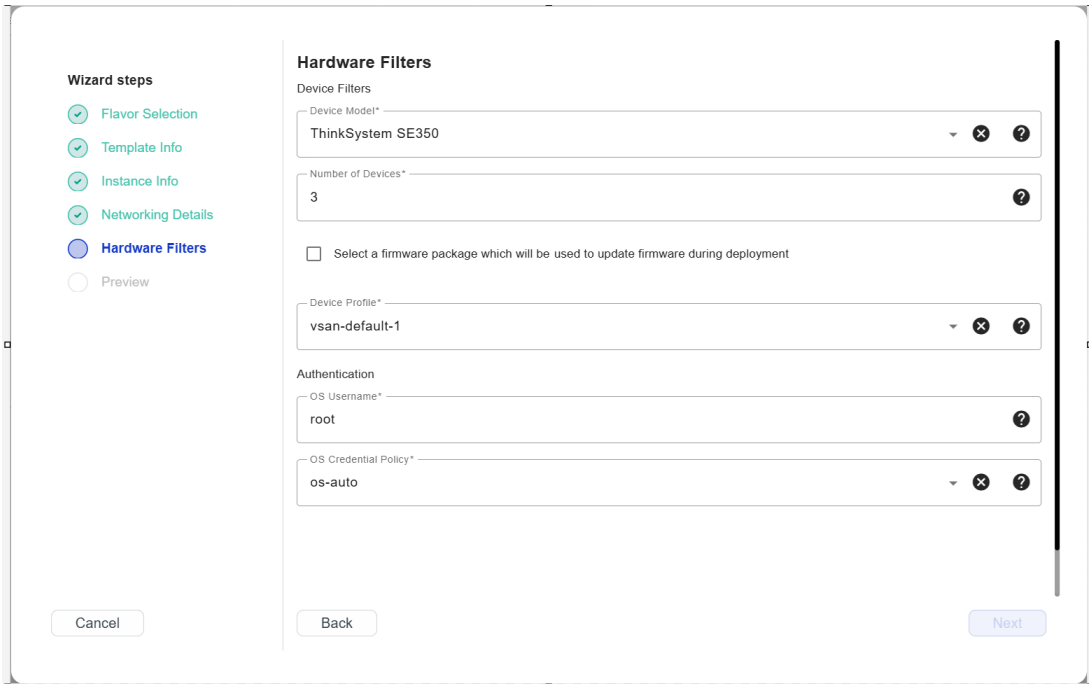


Figure 92: Cloud template - define hardware filter and auto root password policy

Available authentication options vary based on the cloud cluster type you selected. Below is the matrix for the options supported by each cloud flavor.

Cloud or Bare metal OS offering	Authentication Type Support
RedHat OCP	• public key
VMware vSAN	• static password • password template string
Bare metal OS	• static password • password template string

Table 11: Nodes Authentication Types supported by LOC-A

After filling in all the information for the template, click **Save** to save the cloud template. Alternatively, click **Proceed to deployment** to save your cloud template and display the cloud deployment wizard page with this template selected.

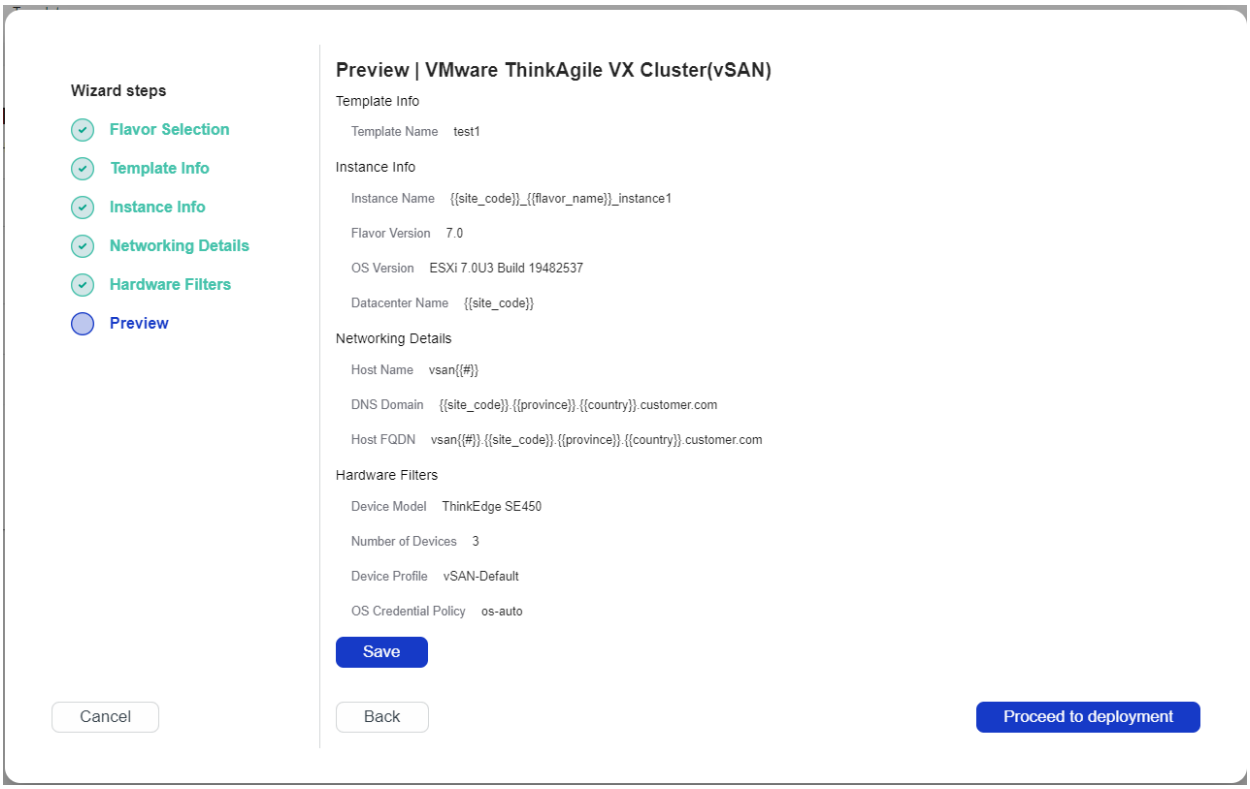


Figure 93: Cloud template summary

8. It takes several seconds to save the cloud template. After that, you should be able to see your template listed in the page. You can view template details or delete a cloud template from this page.

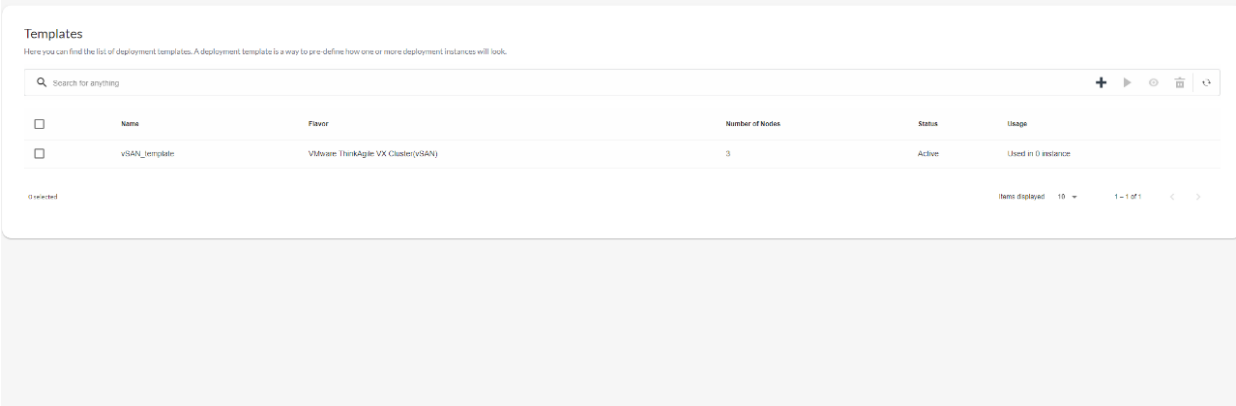


Figure 94: Cloud templates list

View cloud template details:

To view cloud template details, click on a template from the Templates page.

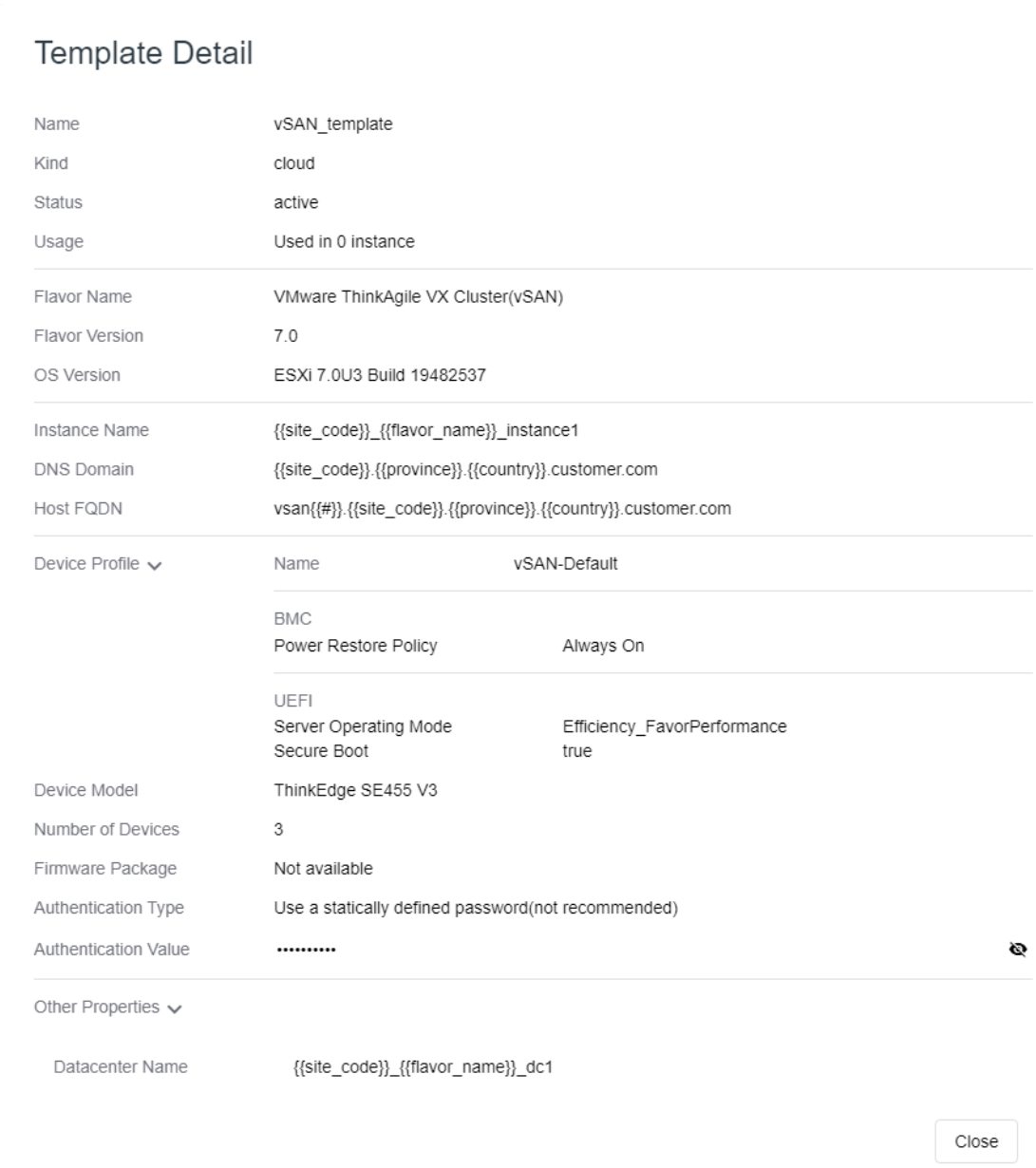


Figure 95: Cloud template detail

Update a cloud template

Starting with LOC-A version 3.3, you can click **Edit** button to update a cloud template. The modification wizard is the same as that for template creation. However, the Flavor cannot be modified. If a new Flavor is needed, it is recommended to create a new template.

Note:

- If the template is being used by an instance, modification will not be supported. Meanwhile, the associated device profile and credential policy will also not be available for modification.

- All sensitive data will be shown as eight asterisks on the initial editing page. If no modification is required, just leave the eight asterisks as they are.

Cloud deployment

After you have created your cloud template and uploaded the metadata for your edge sites, you have completed the planning phase for your edge sites.

Complete the following steps to instantiate the edge cluster:

1. From the LOC-A portal, click **Instances**. Then click **Add** to start the process.
2. Select the target cloud template to apply in the dropdown. All sites ready for deployment will be dynamically displayed in the list.

   LOC-A Core Framework will calculate the site readiness through the following rules:

   - **Deployment Readiness Status** needs to be **Ready**, indicating mandatory IP ranges, network services and cloud services with valid information are imported for the site. This is also dependent upon the cloud flavor of your selected cloud template. For example, for VMware vSAN cloud flavor, if you plan to use LOC-A to install vCenter and LXCI services during vSAN cloud deployment, LOC-A will also check whether the specific VCSA and LXCI images are present in the repository and mark the **Deployment Readiness Status** as **notReady** if the requirement is not met. Please refer to Section Cloud setup if you don't have your resources imported.
   - Devices with the expected device type are registered to the sites, the number of devices and available cluster IP resources meet the minimal requirement of "Number of devices" defined in your cloud template. Please refer to the Section Register devices if you don't have proper servers registered into LOC-A.

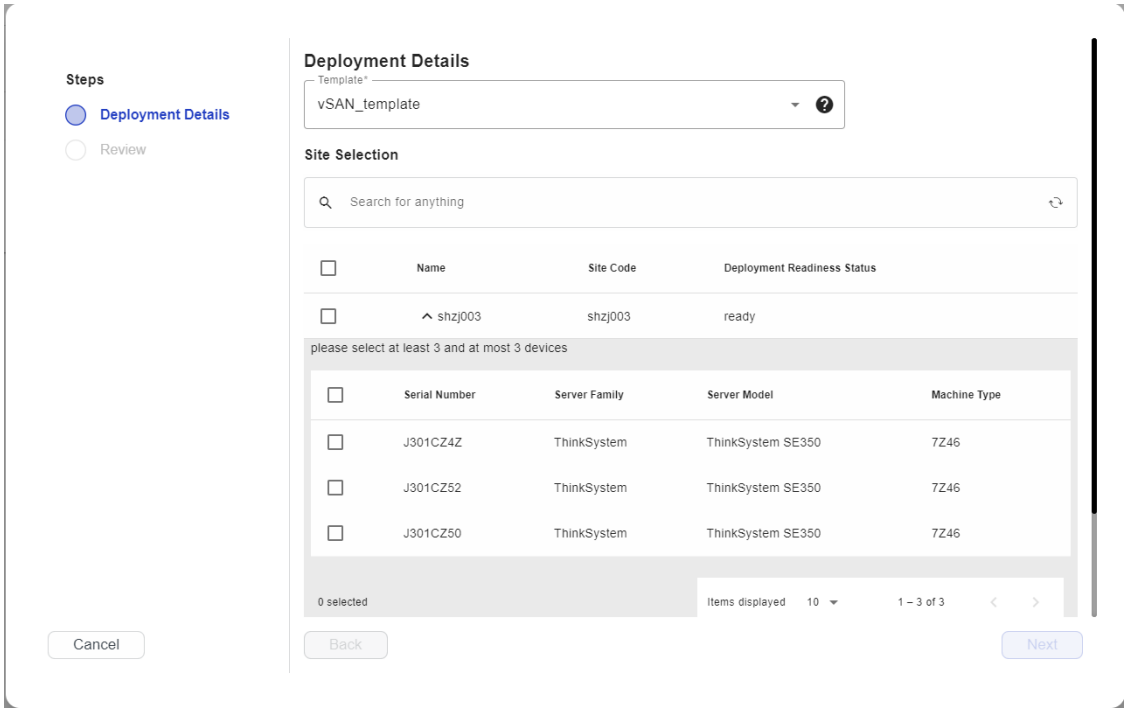


Figure 96: Create new cloud instance via template

3. Select one or more sites to be deployed. By default, the selected device count for each site is the number of devices defined in your cloud template. You can add more devices in the dropdown list of the site. If the count of selected devices exceeds the available IP addresses, you will not be able to select more devices.
4. Click **Next** to review deployment details. You can expand each cluster to view detailed deployment parameters. Click **Previous** to go back to the site selection if there are changes you want to make.
5. After confirming cluster details, click **Deploy** to start the deployment. LOC-A supports performing the deployment to edge sites in parallel. Deployment tasks will be started, and you can view the progress of the tasks on the Tasks page.
6. Alternatively, you can click **Save** to save the plan, but the deployment will not be started immediately. The cluster instance will be displayed on the **Instances** page with status of plan. You can select the site and click **Run** on the toolbar menu to kick off the deployment task.

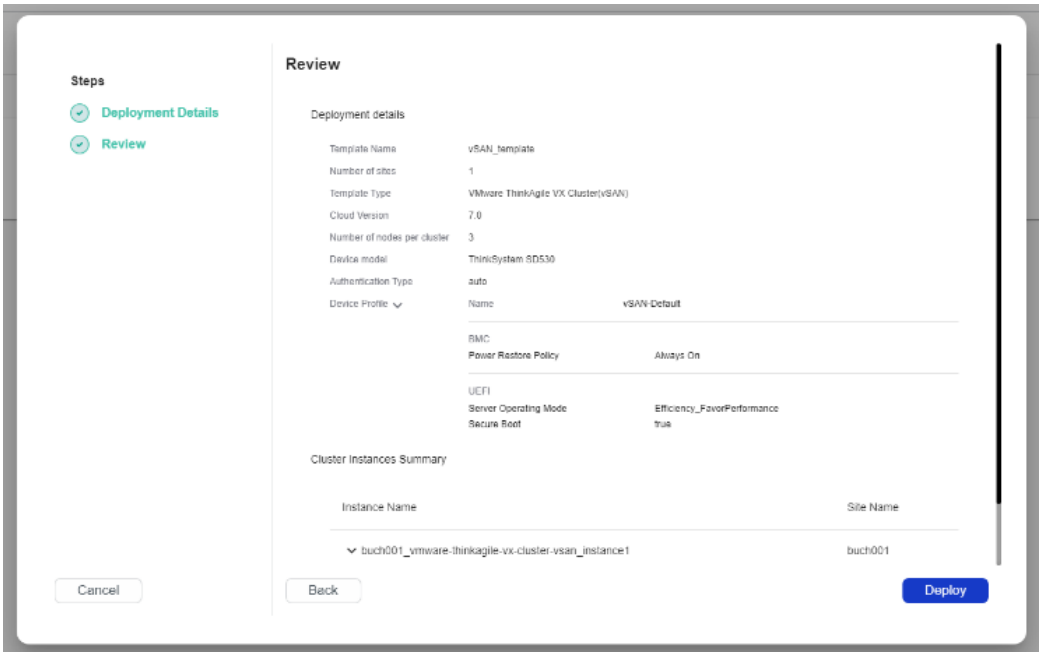


Figure 97: Review cloud deployment

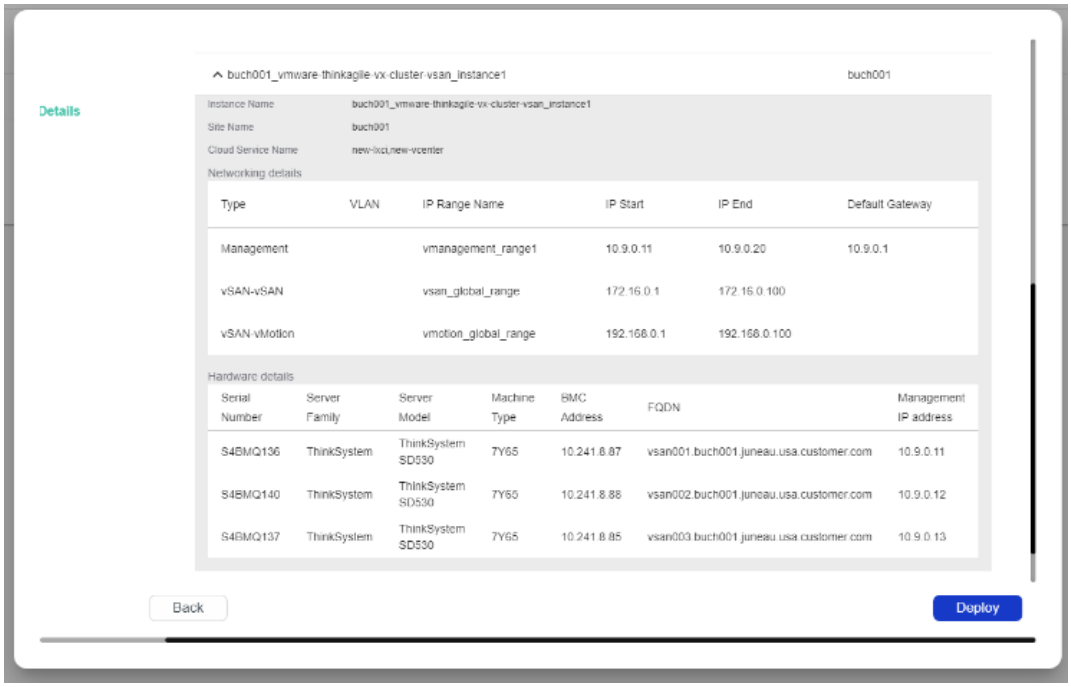


Figure 98: Expand to view cluster details

Cloud expansion

You can select a deployed cluster instance and perform cloud expansion to add server nodes into the cluster. LOC-A supports cloud expansion of VMware vSAN clusters.

Complete the following steps to add new nodes into a VMware vSAN cluster:

2. Select the vSAN cluster which has finished deployment successfully, click **View** to view cluster instance detail.

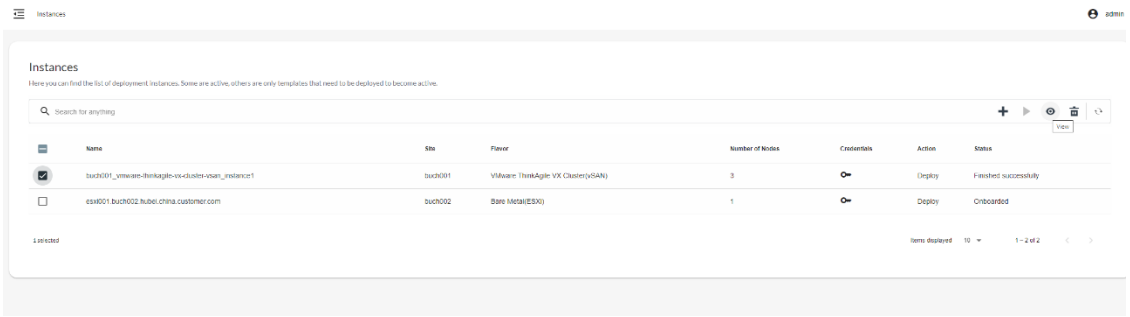


Figure 99: Select installed cluster to expand

3. In the instance detail, you can see general cluster information and device information for the cluster. Click **Add Hosts** to initiate the cloud expansion wizard.

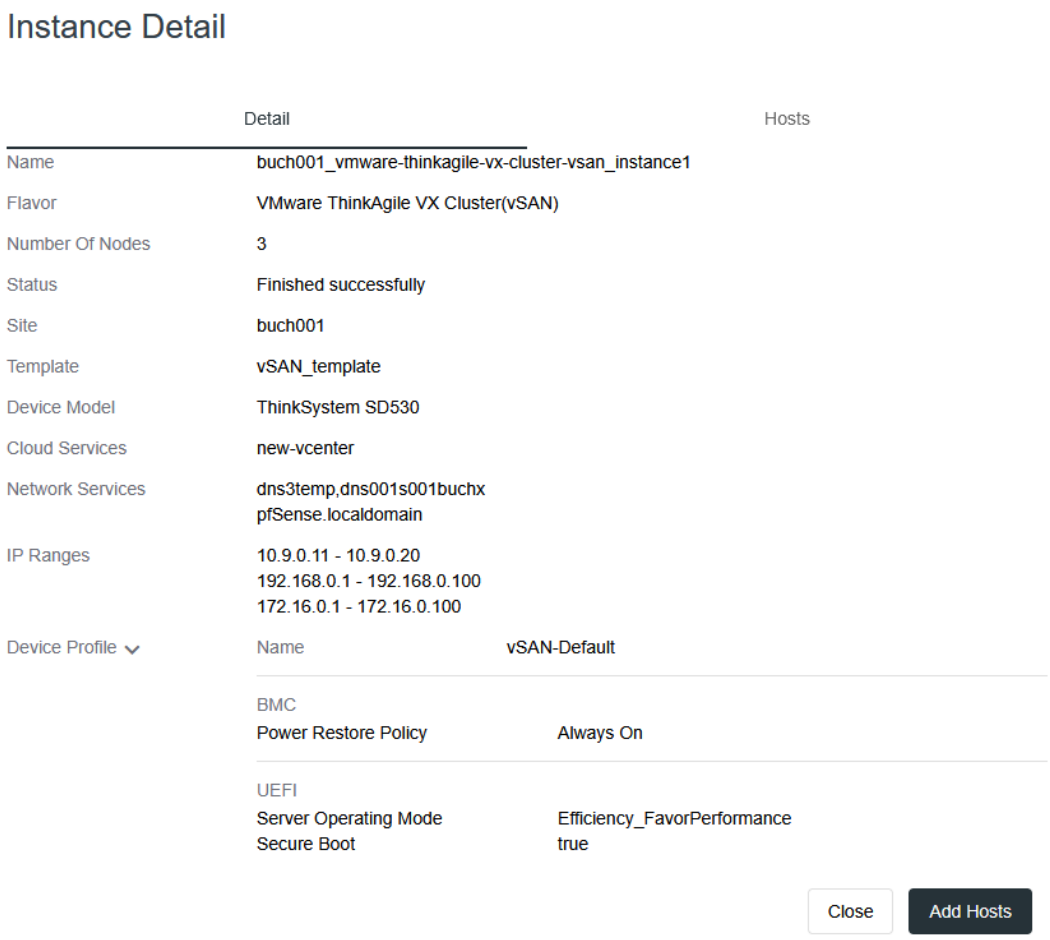


Figure 100: View cluster details

4. The cloud expansion operation will apply the original cloud template settings that were used for cloud deployment. All free devices in this site that meet the device filtering requirement will be listed. You can select the devices that you want to add into the cluster, then click **Next**.

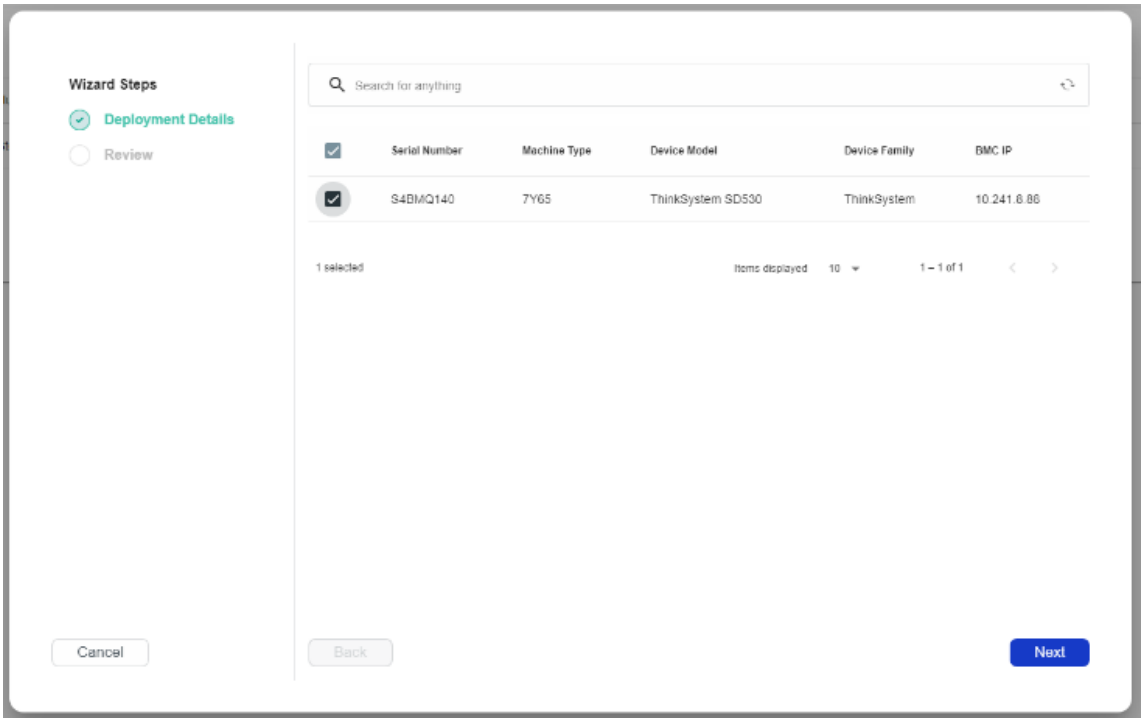
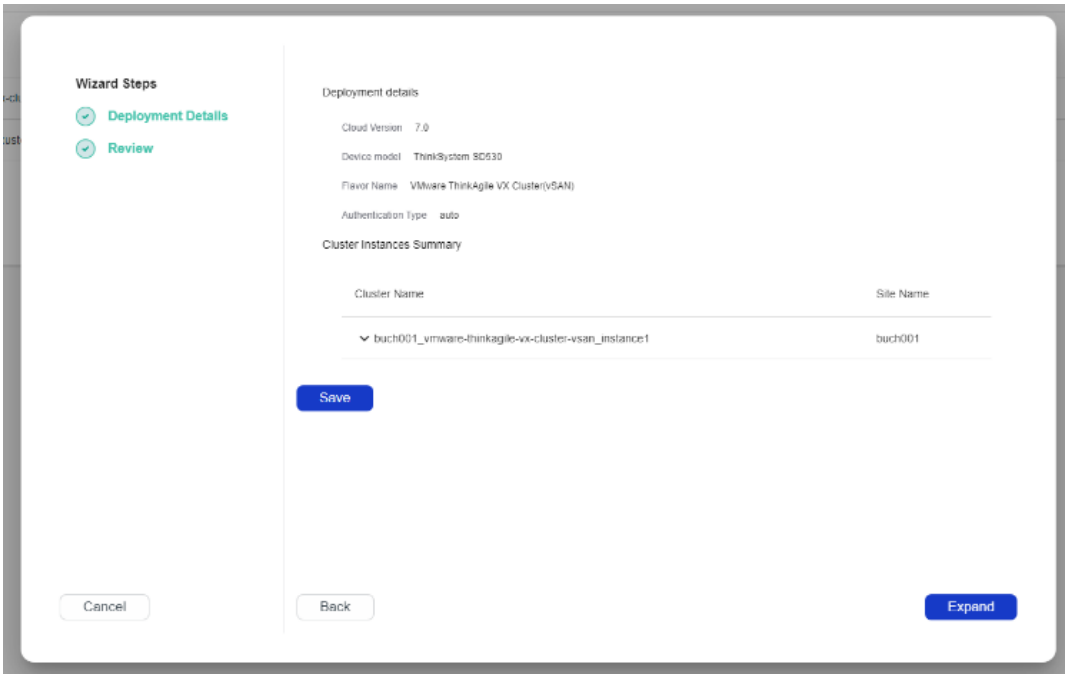


Figure 101: Cloud expansion wizard

5. Review the expansion details. You can expand the cluster to view detailed parameters. Click **Previous** to go back to the device selection screen if there are changes you want to make.



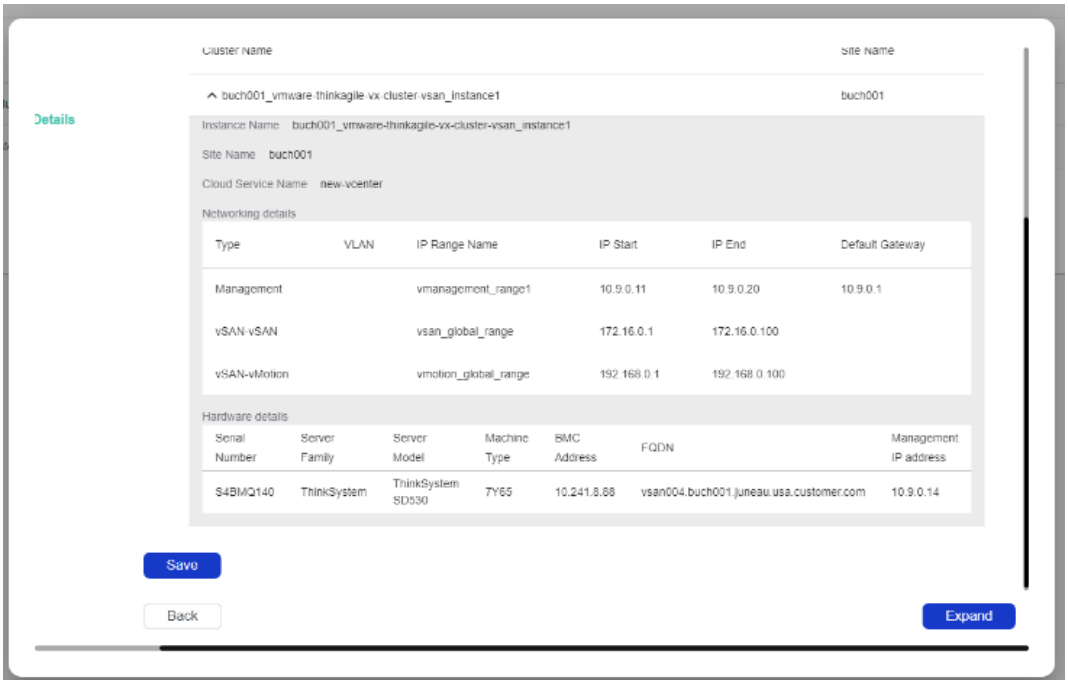


Figure 102: View cloud expansion details

6. After confirming cluster details, click **Expand** to start the cloud expansion. A task will be started, and you can view the progress on the Tasks page. The cluster instance will be displayed on the Instances page with the action of **Expand** and **Status** will be **In Progress**.

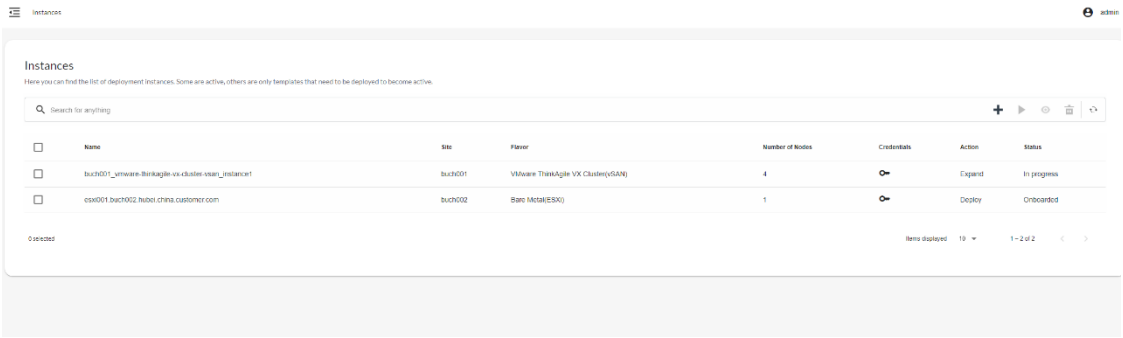


Figure 103: Instance during expansion

Alternatively, you can click **Save** to save the plan, but the cloud expansion will not be started immediately. The cluster instance will be displayed on the **Instances** page with status of **Onboarded** and action of **Expand**. You can select the site and click **All Actions→Run** to kick off the cloud expansion task.

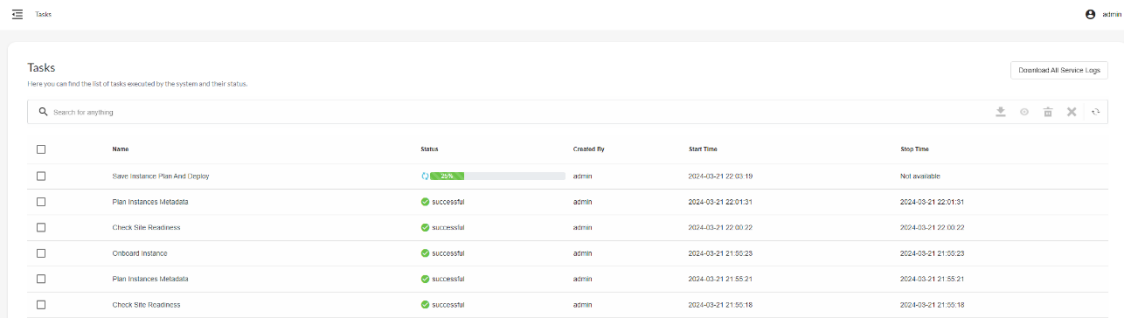


Figure 104: Cloud expansion task

Instance deletion

An instance can be deleted when its status is not **In progress**. When you delete an instance, LOC-A will free metadata resources of this instance, but LOC-A will not try to tear down the real cluster/OS for now.

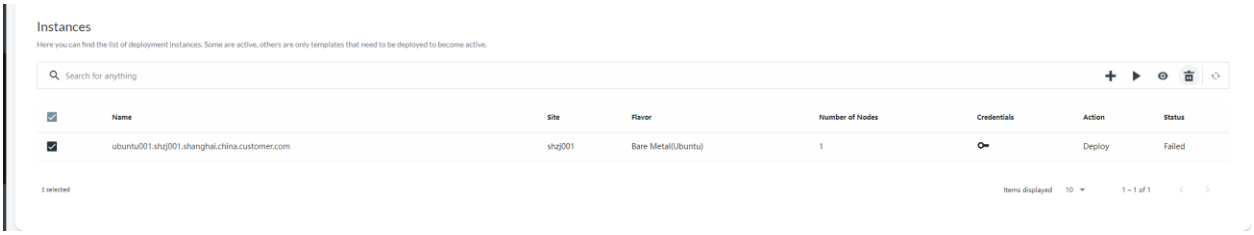


Figure 105: Instance deletion

Create an OS template

Creating an OS template is like creating a cloud template; it facilitates bare metal OS deployment for multiple devices in batches. Check OS type supported list for the OSes verified and supported by LOC-A.

Note: In this release, LOC-A supports Ubuntu OS deployment only in a layer 2 network topology.

Complete the following steps to create an OS template:

1. From the LOC-A portal, click **Templates**. Then click **+ (Add)** to start the template creation process.
2. Select the OS flavor from the dropdown list of Flavor Selection page and click **Next**.
3. On Template Info page, fill in the desired template name.
4. On the Instance Info page, choose the OS version from the dropdown Flavor Version list.

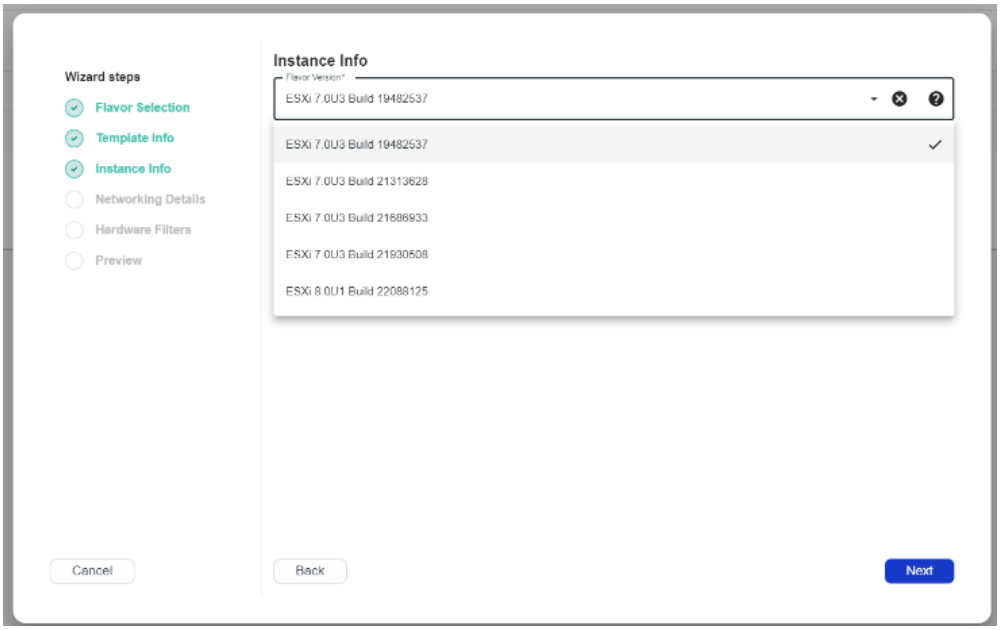


Figure 106: Select OS version for OS template

Note: The OS image file must be available in the LOC-A Repository. If it's missing, an error message will be displayed.

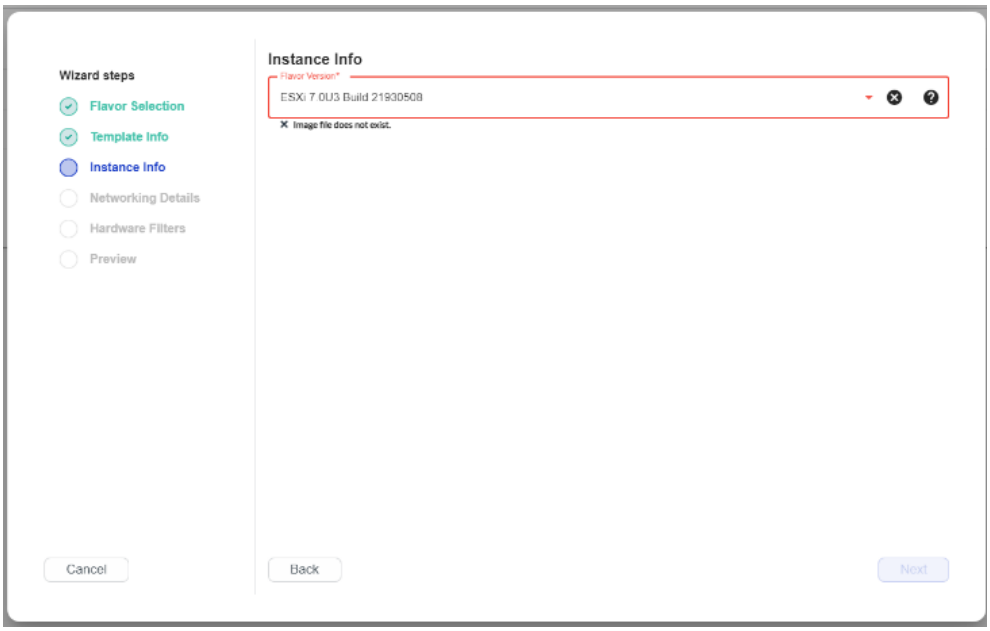


Figure 107: Missing image file in LOC-A repository

Below is the list of official download URLs for LOC-A supported OS image files:

Flavor	Version	Download Link
BareMetal (Ubuntu)	18.04.6	http://www.cdimage.ubuntu.com/ubuntu/releases/18.04/release/ubuntu-18.04.6-server-amd64.iso
	20.04.6	https://ftp.ulak.net.tr/ubuntu-releases/20.04.6/ubuntu-20.04.6-live-server-amd64.iso
	22.04.3	https://old-releases.ubuntu.com/releases/22.04.3/ubuntu-22.04.3-live-server-amd64.iso
	22.04.4	https://old-releases.ubuntu.com/releases/22.04.3/ubuntu-22.04.4-live-server-amd64.iso
	22.04.5	https://releases.ubuntu.com/22.04.5/ubuntu-22.04.5-live-server-amd64.iso
BareMetal (ESXi)	ESXi 7.0U3 Build 19482537	https://vmware.lenovo.com/content/2022_05/Lenovo_Custom_ISO/7.0u3/VMware-ESXi-7.0.3-19482537-LNV-20220411.iso
	ESXi 7.0U3 Build 21930508	https://vmware.lenovo.com/content/2023_08/Lenovo_Custom_ISO/7.0u3/s/VMware-ESXi-7.0.3n-21930508-LVN-S02-20230802.iso
	ESXi 7.0U3 Build 21686933	https://vmware.lenovo.com/content/2023_08/Lenovo_Custom_ISO/7.0u3/n/VMware-ESXi-7.0.3m-21686933-LNV-N02-20230607.iso
	ESXi 7.0U3 Build 21313628	https://vmware.lenovo.com/content/2023_03/Lenovo_Custom_ISO/7.0u3/VMware-ESXi-7.0.3k-21313628-LNV-20230302.iso

Table 12: LOC-A supported OS images

Note: You can also enter a shell post-processing script to run when OS deployment is completed. Be aware, however, for ESXi deployments, this feature is not supported.

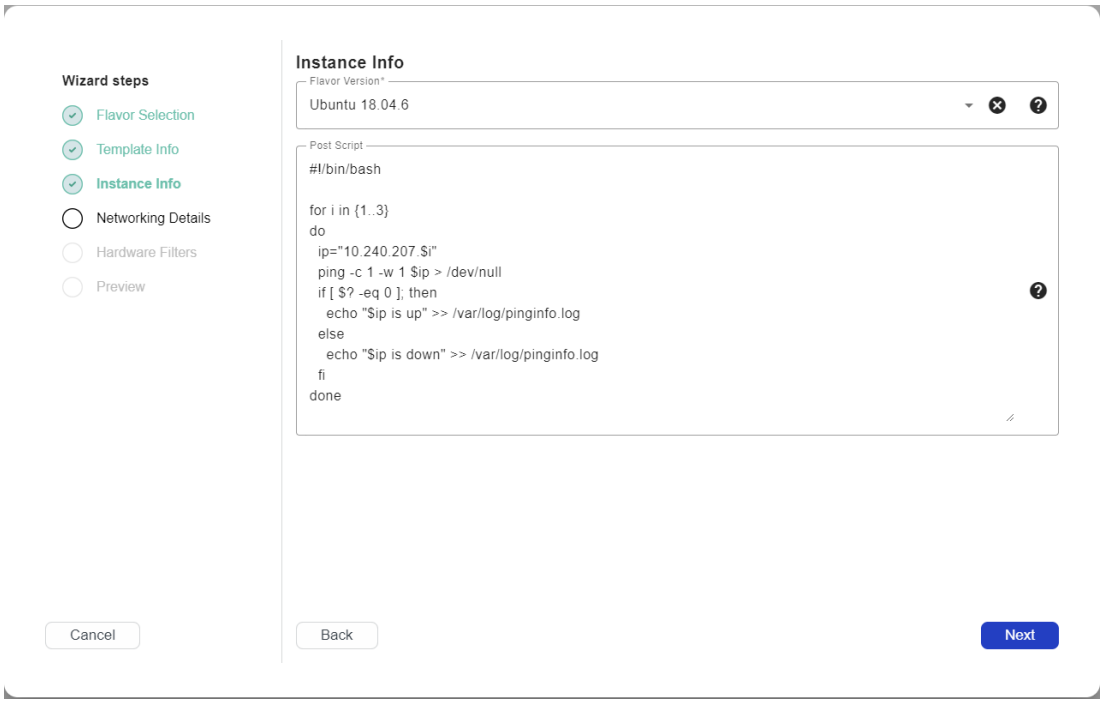


Figure 108: OS template – Instance info

For example, the following post-processing script checks if an IP address is accessible via ping, and saves the result into /var/log/pinginfo.log.

```
#!/bin/bash

for i in {1..3}
do
  ip="10.240.207.$i"
  ping -c 1 -w 1 $ip > /dev/null
  if [ $? -eq 0 ]; then
    echo "$ip is up" >> /var/log/pinginfo.log
  else
    echo "$ip is down" >> /var/log/pinginfo.log
  fi
done
```

The configuration of the networking details and hardware filters are the same as the configuration used for creating a cloud template. The settings will be applied to every bare metal server node to be deployed. See *Create a* cloud template on page 82 for more information.

5. Review the template details. Click **Save** to save the template or click **Proceed to deployment** to save the template and move to the Instance page where you can start the deployment.

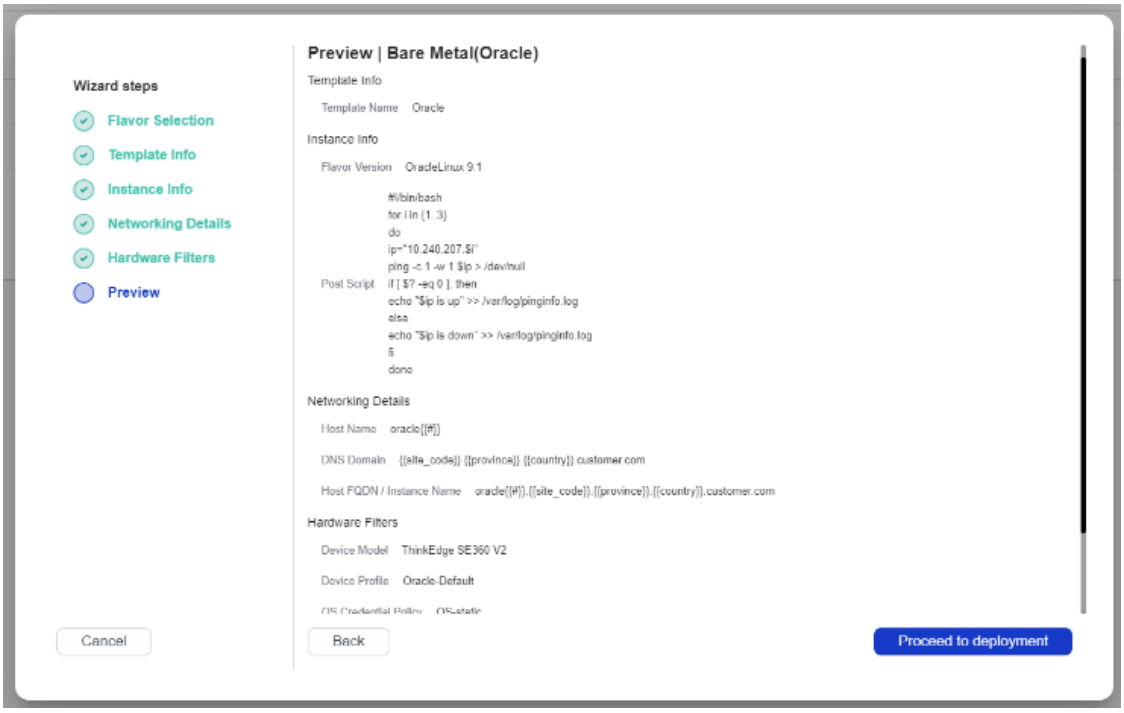


Figure 109: Review OS template

In the particular case of **Bare Metal (Ubuntu)** flavor, full disk encryption can be enabled by completing the following steps:

1. Ensure that **TPM2.0** is enabled on the server.
2. Ensure that TPM TCM policy is set to TPM Only on the server. You can check or set the TPM TCM policy through UEFI F1 Setup or Lenovo OneCli tool.
3. Ensure that Internet access is available from the server. This is required by the OS deployment. When full disk encryption is enabled, the package((libtss2-rc0) needs to be installed on the system from Ubuntu APT repository.
4. From the LOC-A portal, click **Templates**. Then click **+ (Add)** to start the template creation process.
5. Select the **Bare Metal (Ubuntu)** OS flavor from the dropdown list of Flavor Selection page and click **Next**.
6. On **Template Info** page, fill in the desired template name.
7. On the **Instance Info** page, choose any of the Ubuntu OS versions, starting with **22.04** from the dropdown Flavor Version list.

8. Check the **Encrypt boot disk** checkbox and click **Next**

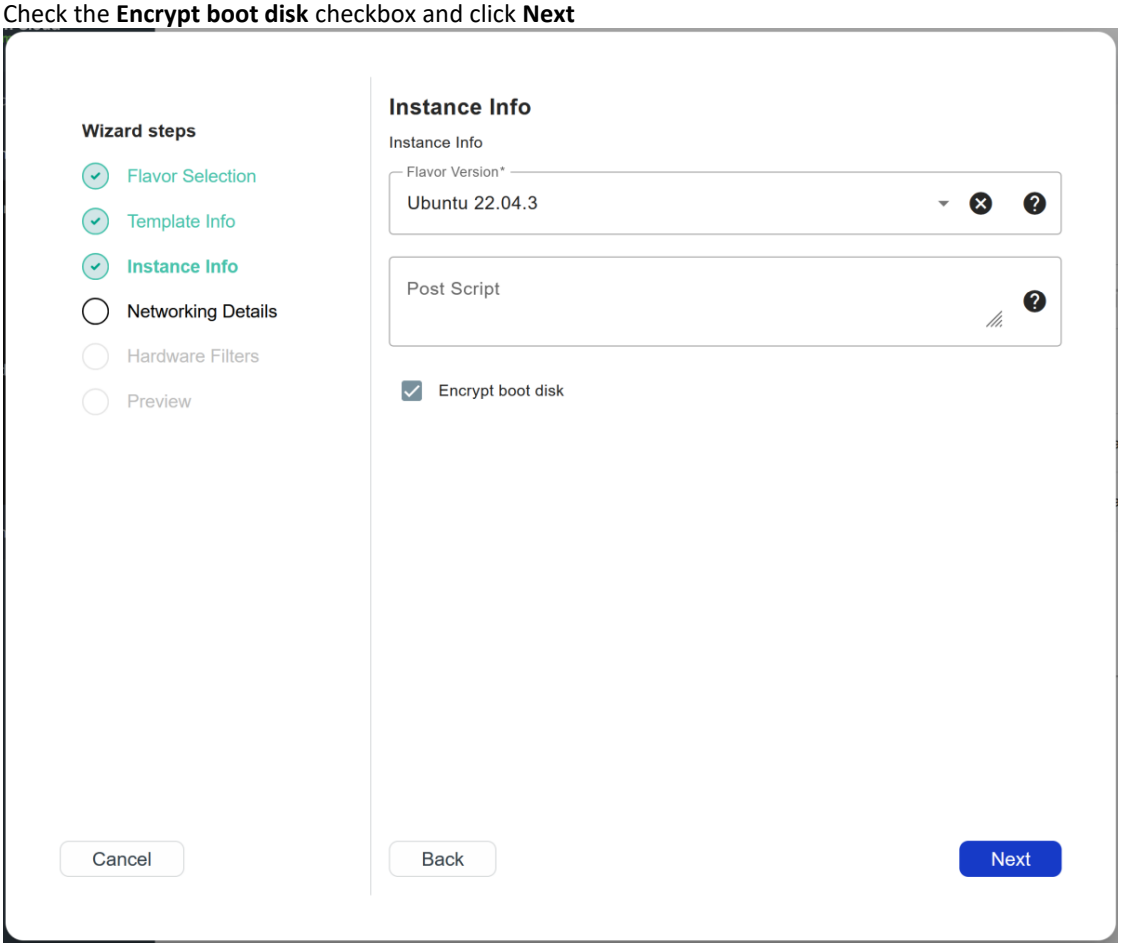


Figure 110: Encrypt boot disk option

9. Complete the rest of the steps just as was before.

Update an OS template

Starting with LOC-A version 3.3, you can click the **Edit** button to update an OS template. The modification wizard is the same as that for template creation. However, the Flavor cannot be modified. If a different Flavor is needed, it is recommended to create a new template.

Note:

- If the template is being used by an instance, modification will not be supported. Meanwhile, the associated device profile and credential policy will also not be available for modification.
- All sensitive data will be shown as eight asterisks on the initial editing page. If no modification is required, just leave the eight asterisks as they are.

Bare metal OS deployment

You can perform a bare-metal OS deployment to multiple servers for multiple sites. The instantiation of bare metal instances is similar to cloud deployments. See *Cloud deployment* on page 91 for more information.

Complete the following steps to perform a bare-metal deployment:

1. From the LOC-A portal, click **Instances** to display the instances page.

2. Click **+ (Add)** and select the OS template that you created.
   All sites that are ready for deployment will be listed in the Instances list. You can then select the sites and devices to which you want to apply the OS template. Then click **Next**.

   The Review page displays deployment details of your attempted operations.

3. Click **Deploy** to start the deployment task or click **Save** to save it as a plan.

Note:

LOC-A will generate OS instances with the same value of instance FQDN for ease of management.

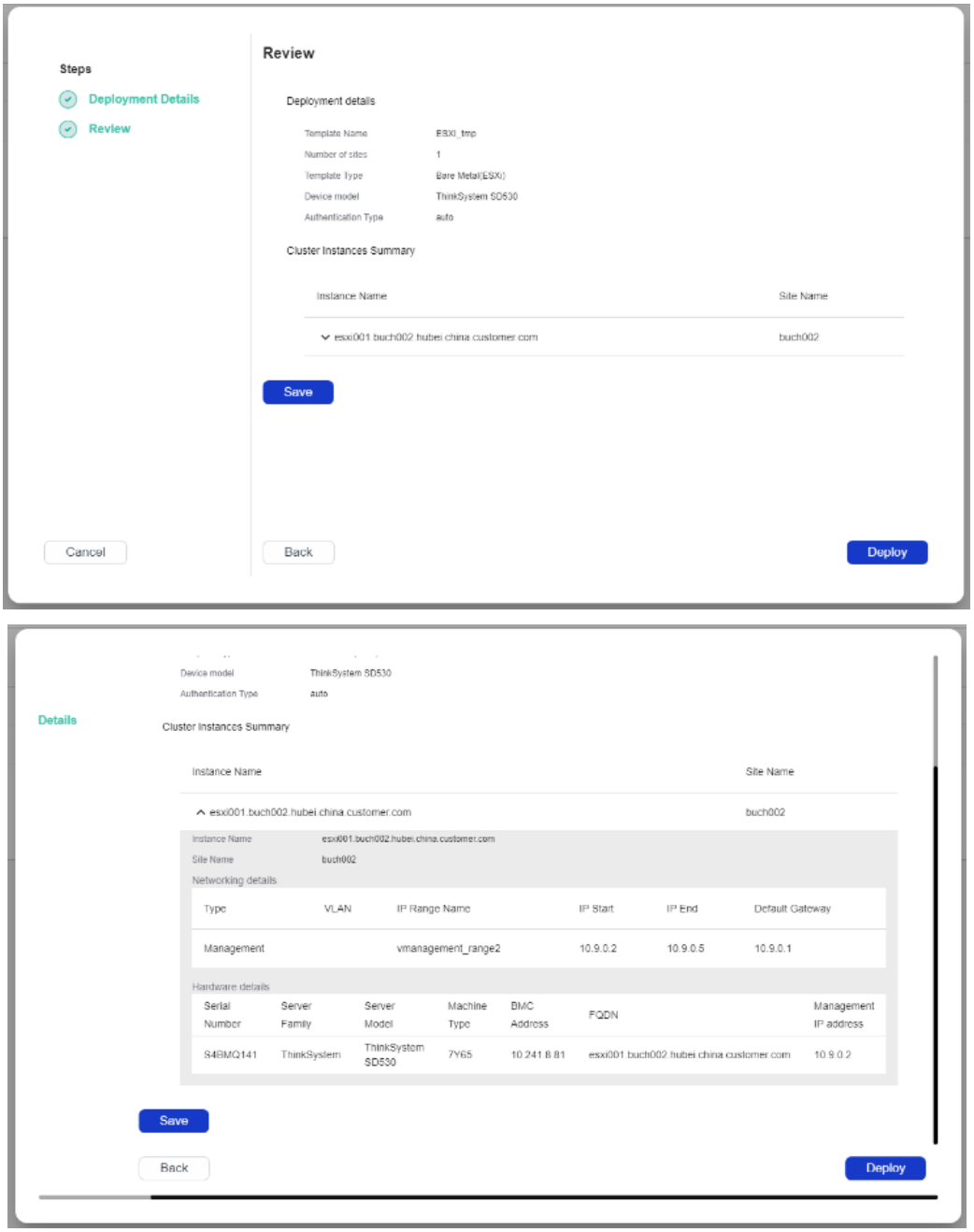


Figure 111: Review bare metal OS deployment details

Automatic instance creation

LOC-A provides automatic instance creation capability that enables users to create deployment plans. When all conditions defined in the deployment plans are met, LOC-A will trigger the automatic creation and deployment of cloud/OS instances.

There is a default deployment when the LOC-A appliance is started. If not specified explicitly, all sites and cloud templates will be associated with the default deployment plan.

Note:

- It is not allowed to associate with two or more cloud/OS templates of the same flavor in a Deployment plan. For default deployment plans, only the first cloud/OS template for a flavor will be automatically associated.
- The default deployment plan cannot be deleted.

When all the conditions for the specific site and templates are met, the cloud/OS instance creation will be triggered:

1. Site and cloud template have been associated with a Deployment plan which enables **Auto Deploy**.
2. Metadata for the site in LOC-A is correct.
3. Metadata for the cloud/OS templates in LOC-A are correct.
4. The correct HW models and the appropriate number of devices have been registered.

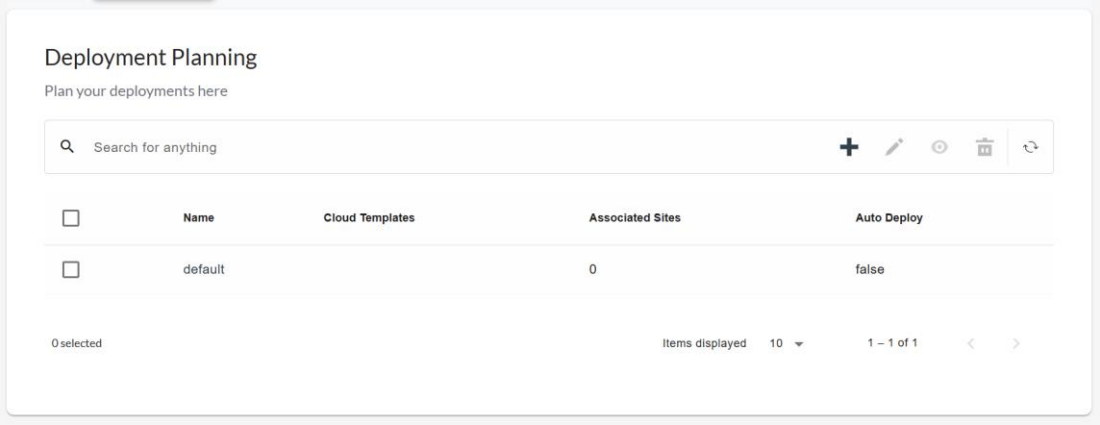


Figure 112:Deployment Planning page

Complete the following steps to create a new deployment plan:

1. From the LOC-A portal, click **Deployments** to display the deployments page.
2. Click **+ (Add)** button to start the creation.

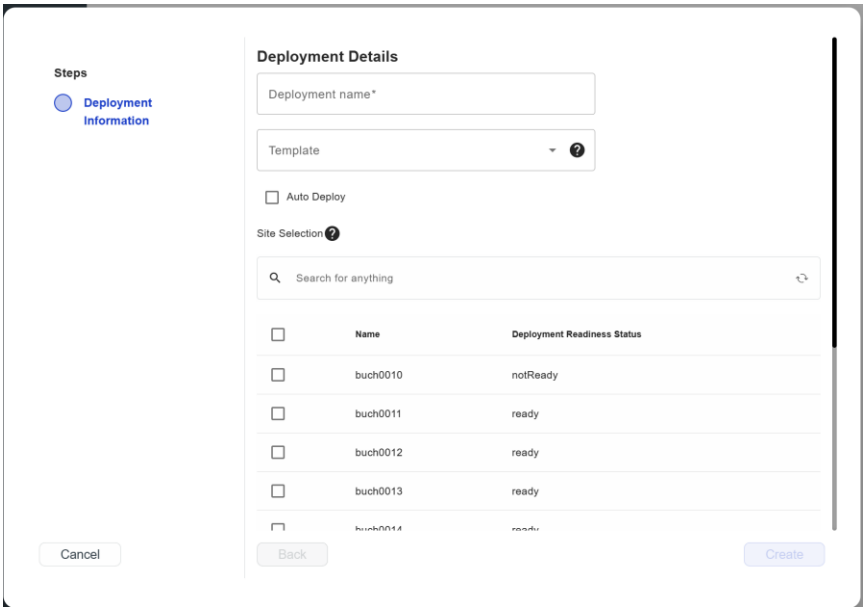


Figure 113: Deployment creation wizard

3. Specify a unique deployment name. The name is required.
4. Select the target templates that need to be applied. The templates in the dropdown list do not belong to any deployment. A deployment can contain multiple cloud/OS templates but must be with different cloud/OS flavors. For each cloud/OS flavor, only one template can be bound to the deployment. Users can skip the templates selection.
5. Select the sites. A site can be assigned to a new deployment, or it belongs to the default deployment. The sites in the table do not belong to any deployment. Users can skip the sites selection.
   Note: the deployment readiness status refers to the metadata sanity checks

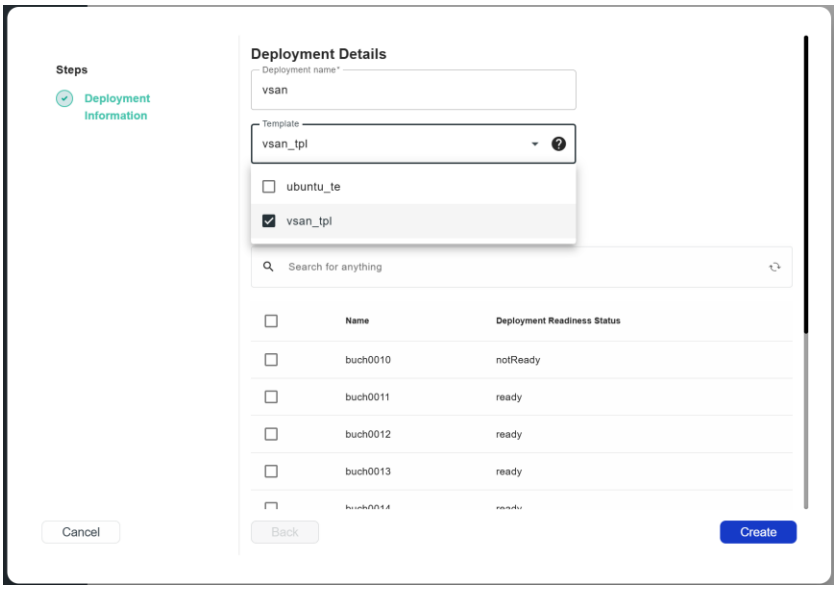


Figure 114: Deployment creation wizard, configurable fields

6. Configure the **Auto Deploy** setting to control whether automatic execution of cloud deployment will be triggered when sites under this deployment get ready. Users can skip this configuration.

7. Click **Create** to save it as a deployment.

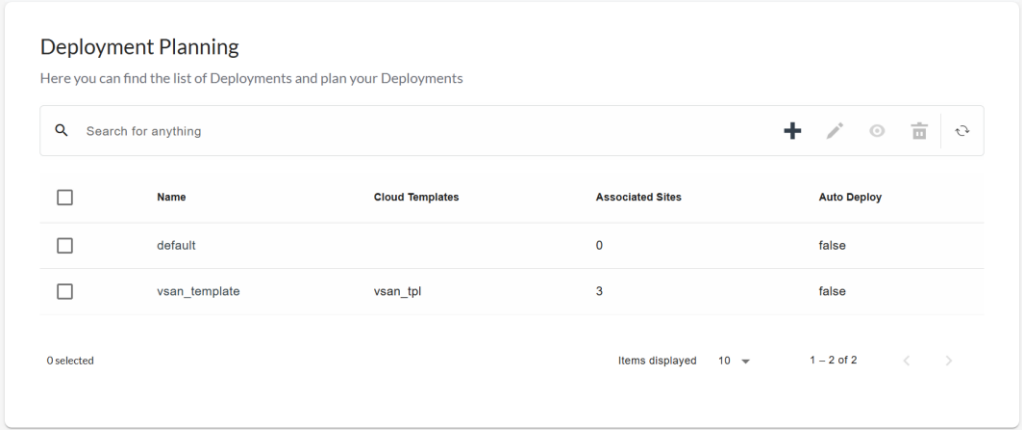


Figure 115: A new deployment after creation

8. If you check the **Auto Deploy**, LOC-A will start to create instance when conditions are met.

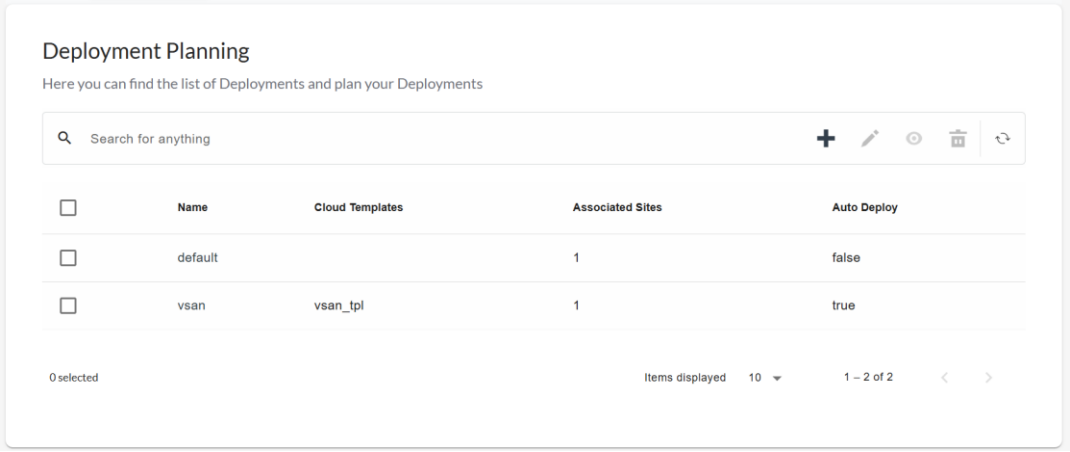


Figure 116: Set deployment's Auto Deploy to true

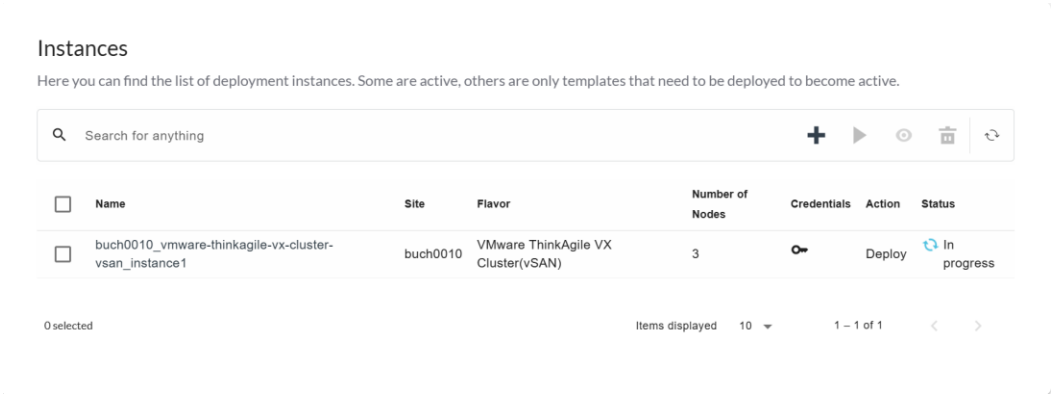


Figure 117: A new instance is created when all conditions are met

Update Deployment plan:

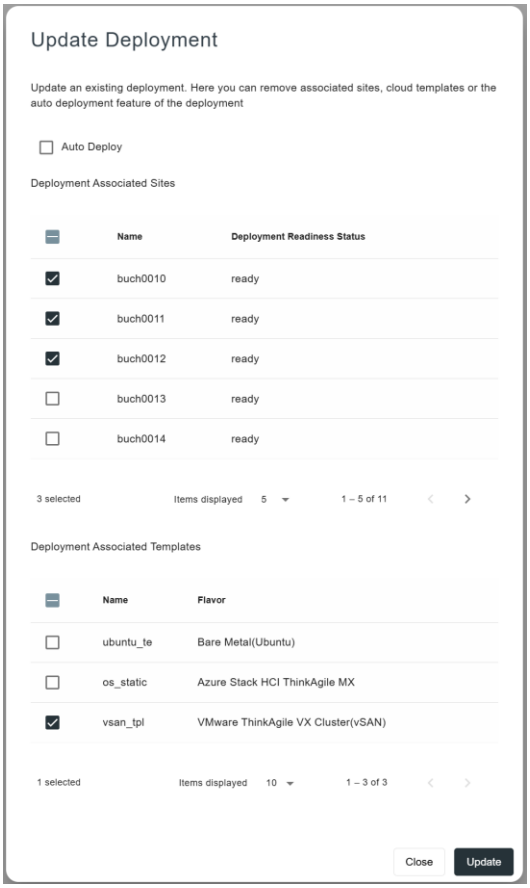


Figure 118: Update Deployment modal

LOC-A supports editing deployment. Select a deployment and click the **Edit** button to edit the deployment. Users can configure the **Auto Deploy** setting, remove or add templates and sites in modal.

Only templates that belong to current deployment and unassigned templates will be shown in the list.

Only Sites that belong to current deployment and unassigned sites will be shown in the list.

Note: A template in a deployment cannot be removed if a site in the deployment is in the middle of onboarding process.

Delete Deployment plan:

Follow these steps to delete a deployment:

1. Select a deployment and click the **Delete** button in the upper right corner.
2. Click **Delete** button to confirm deletion

View Deployment planning details:

Select a deployment and click eye icon(**view**) to see the deployment details. The detail displays all templates and related sites. Click **View All Sites** will navigate to **Sites** page with filter parameters.

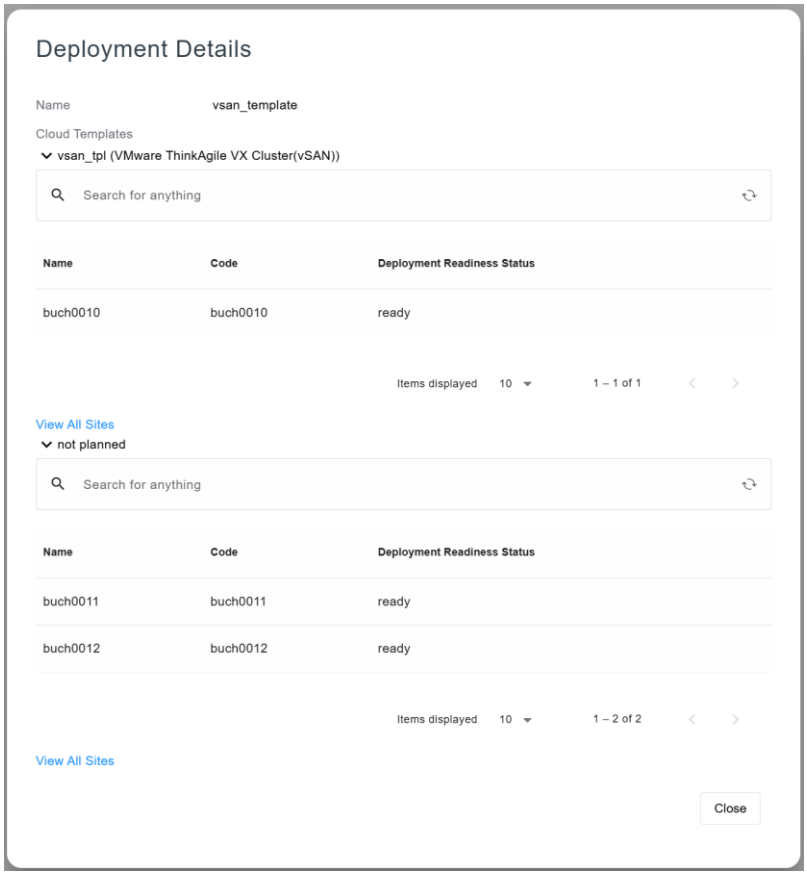


Figure 119: Deployment Details modal

OS Image sideloading

The Lenovo Open Cloud Automation Utility supports OS image sideloading on the XCC SD card during server registration to accelerate OS deployment during OS/cloud deployment.

Prerequisite:

Optional Micro SD card needs to be installed in the server. This will extend RDOC storage space to 4 GB. Please refer to the Lenovo server's user guide for more information.

Figure 120: Optional server SD card slot example

Supported server list:

- ThinkEdge SE350 V2
- ThinkEdge SE360 V2

Supported OS image list:

- ESXi 7.0U3 Build 21930508
- ESXi 7.0U3 Build 21686933
- ESXi 7.0U3 Build 21313628
- ESXi 8.0U1 Build 22088125

To use OS image sideloading feature, you need to make sure you have a supported OS image uploaded in the repository. The image should remain there during the installation even if it was transferred to server RDOC storage during registration.

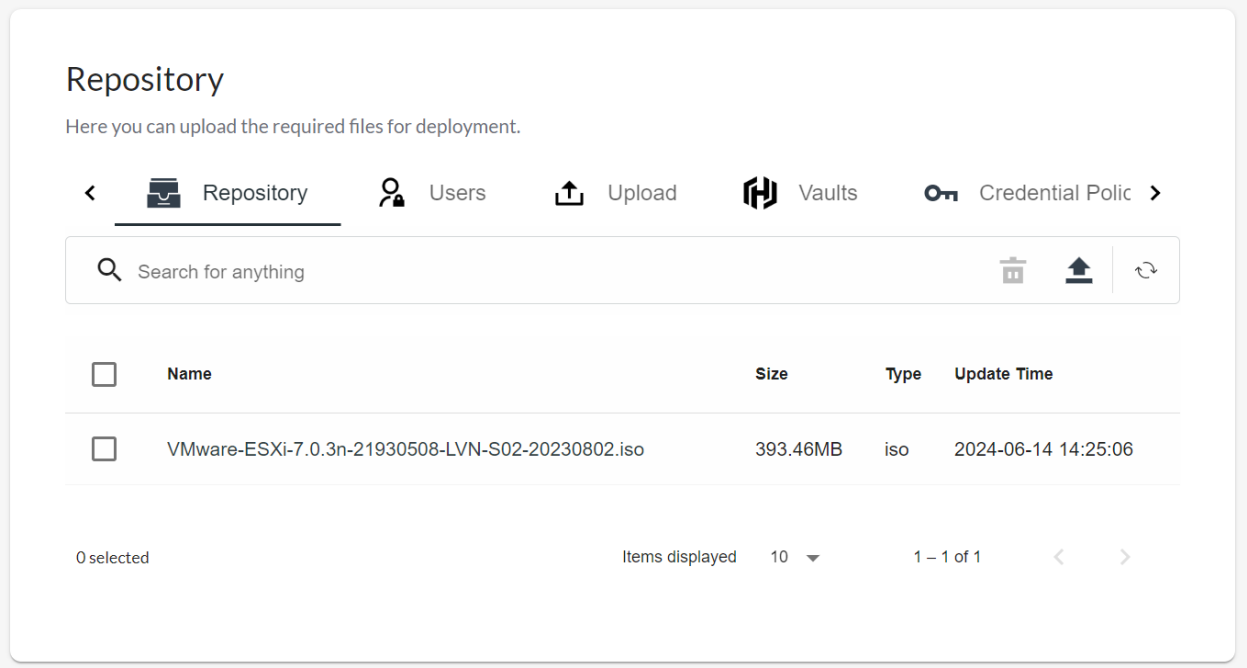


Figure 121: Upload supported OS image

When you create a ThinkShield type registration package, enable the **Preload OS image to XCC** option, this will include the target OS image(s) in the registration package so that it can be sideloaded during edge server nZTP. If there are multiple versions of the OS image file for the same OS flavor in the Repository, LOC-A will automatically preload the latest version of the OS image.

When a technician uses the Lenovo Open Cloud Automation Utility to register the edge server, the utility will automatically preload the target OS image onto the MicroSD card for the XCC based on the planned OS/Cloud flavor type of the site. For example, assuming ESXi 7.0U3 Build 21930508 image is included in the registration package, then if siteA is planned for Baremetal (ESXi), the image file will be preloaded, if siteB is planned for Baremetal (Ubuntu), the image will not be preloaded. You will see a step “Sideload OS image” during server registration if image is preloaded.

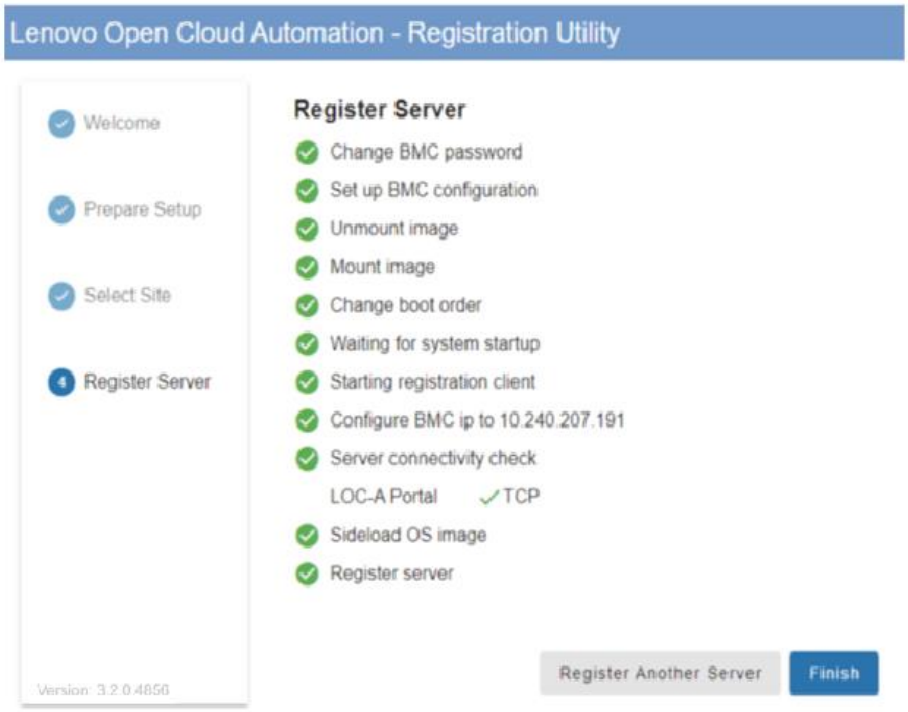


Figure 122: Sideload OS image during server registration

When the device is registered into the LOC-A portal, you will be able to view the Preload Image details.

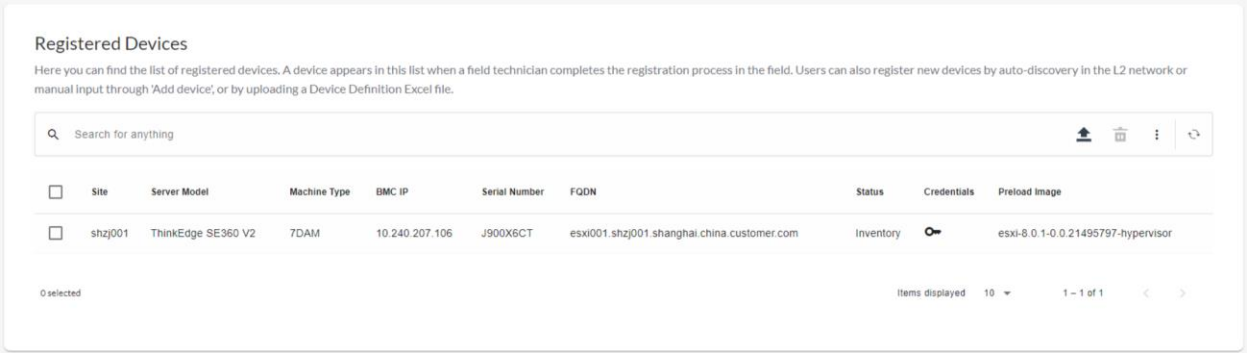


Figure 123: Registered device with preload image

When you attempt to create a new OS/Cloud instance upon registered devices, if the OS image version defined in the OS/Cloud template doesn't match with the preloaded OS image on the device, a warning will be shown for the user to confirm to proceed with the deployment. This will deploy the server with the OS version defined in OS/Cloud template, and the OS deployment will not benefit from image sideloading acceleration.

Figure 124: Warning during instance creation when image version mismatches

View tasks

The Tasks page allows you to view the progress of running tasks and the status of completed tasks.

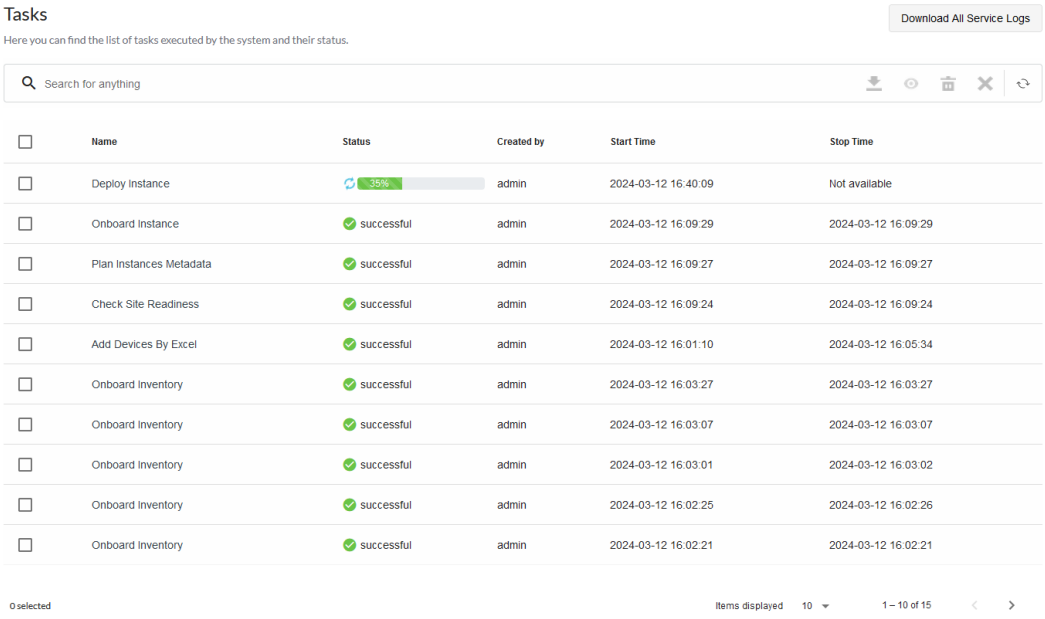


Figure 125: Tasks list

View task details:

Click on a task to view details for the task. All subtasks will also be listed with elapsed time and progress.

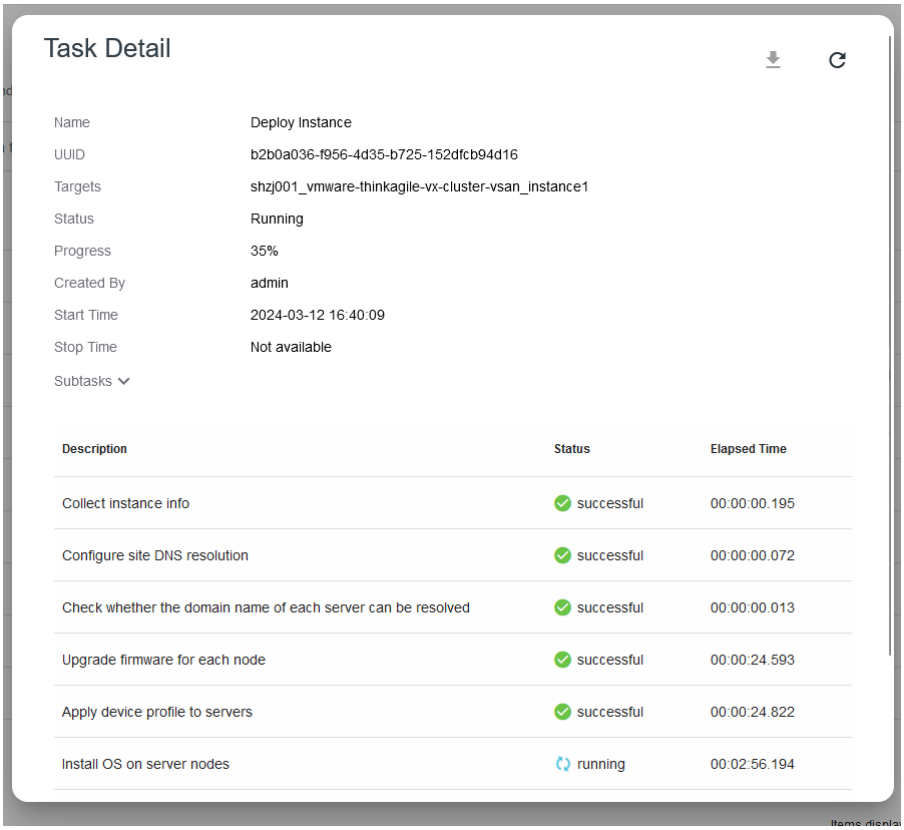


Figure 126: Task detail with subtasks

License management

Starting from release 3.2, license control is enforced in LOC-A. Once an admin user logs in to LOC-A for the first time after installing the LOC-A appliance, a 90-day free trial license is activated. After the 90-day free trial expires, you must purchase and install LOC-A licenses to continue using LOC-A's features.

Before you begin

Review the following license considerations.

- A LOC-A FoD license is tied to a specific cloud flavor. You need to apply for the specific license for the cloud flavor type you expect to support. For example, in order to perform device registration and OS deployment of flavor "Bare Metal(CentOS)", you must purchase the license for "Lenovo Open Cloud Automation - Cent OS Bare-metal OS Deployment for 1-socket ThinkEdge server".
- A LOC-A license can have constraints on expiration time and number of nodes. When the license expires, or the nodes of this flavor exceeds the number of node constraint in the license, you will not be able to further register new devices for this flavor, or perform flavor operations. Existing cloud templates, registered devices, or deployed instances will remain in the system. The flavor operation tasks in progress will not be impacted until they complete or fail.
- The activation period for the license starts when the license is purchased, and the authorization code is created.
- During the 90-days free trial, there is no limit on LOC-A functions.
- You must have Supervisor privileges to install licenses.
- For LOC-A 3.2 and later, if licenses are already installed, new licenses are not required when upgrading to a new release of LOC-A. For LOC-A 3.1, which doesn't have the license management feature, when you upgrade it to the 3.2 version, a trial license is created and activated. Please refer

to Upgrade the appliance to a higher version (supported since release 3.2) for more details. For LOC-A versions before 3.1, you need to re-install the instance to 3.2 version.

LOC-A supports the following licenses:

- Lenovo Open Cloud Automation - nZTP with Device Management platform onboarding for 1-socket ThinkEdge server
- Lenovo Open Cloud Automation - VMware ESXi Bare-metal OS Deployment for 1-socket ThinkEdge server
- Lenovo Open Cloud Automation - Cent OS Bare-metal OS Deployment for 1-socket ThinkEdge server
- Lenovo Open Cloud Automation - Ubuntu Bare-metal OS Deployment for 1-socket ThinkEdge server
- Lenovo Open Cloud Automation - Oracle Linux Bare-metal OS Deployment for 1-socket ThinkEdge server
- Lenovo Open Cloud Automation RedHat 1-socket ThinkEdge server
- Lenovo Open Cloud Automation VMware 1-socket ThinkEdge server

View licenses

To manage and view licenses from the LOC-A web portal, click **Setup→License Management**. The page lists all licenses installed in the system, with details of license status, number of Nodes constraints, start time, and expire time. The license status can be:

- Valid: License is active and healthy.
- Expired: License is expired. You will need to purchase a new license.
- Limit of entitlements reached: The number of nodes for the flavor reached the number of nodes constraint of the license. You will need to purchase a new license to expand the count of entitlement.

Trial license is also listed in the page with No Limit for number of license nodes. You can check the expire time for the trial.

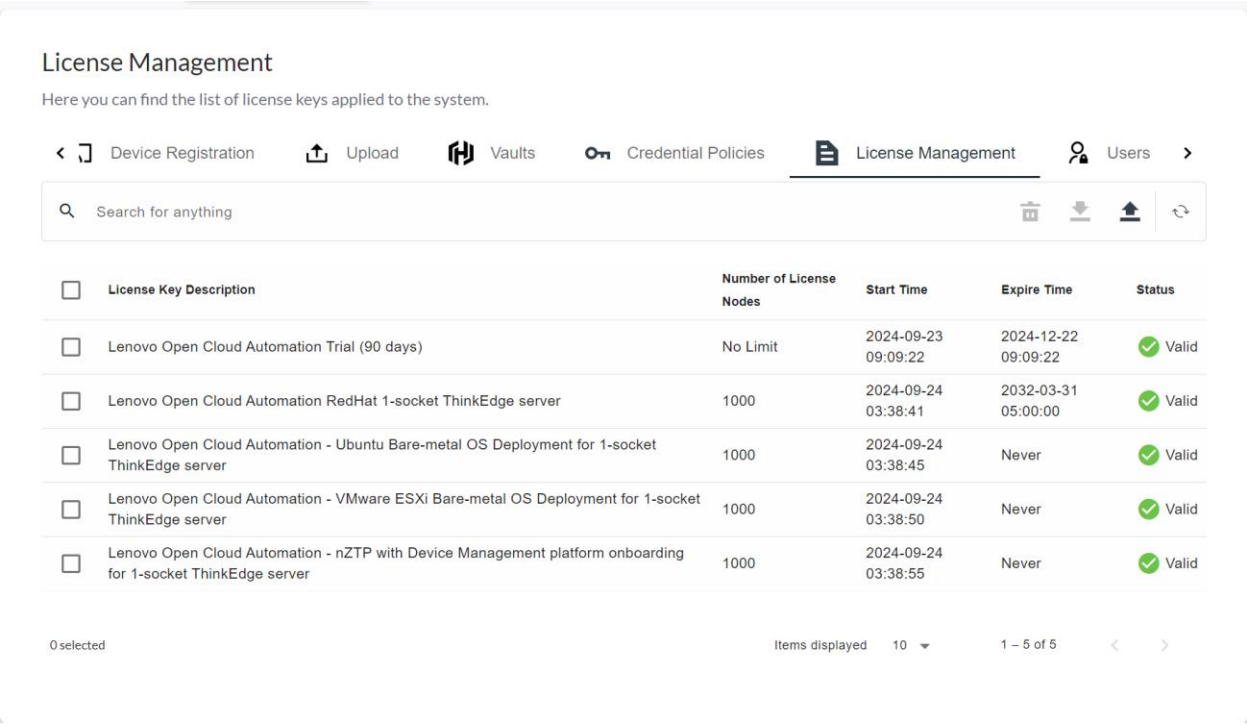


Figure 127: License list

A notification message will pop up when you login to LOC-A portal if any license will expire within 30 days.

Install licenses using the Features on Demand web portal

To install LOC-A licenses in the management server, complete the following steps:

1. Purchase the expected LOC-A license for your OS/cloud flavor.
   Contact your Lenovo representative or authorized Business Partner to purchase LOC-A licenses based on the flavor type that you want to enable and the number of devices that you want to register/deploy. After purchasing licenses, an authorization code is sent to you in an *electronic proof of entitlement* email. The authorization code is a 22-character alphanumeric string, which you need to redeem and install the licenses. If you do not receive the email and you purchased licenses through a Business Partner, contact your Business Partner to request the authorization code.
   You can also retrieve your authorization codes from the Features on Demand web portal by clicking **Retrieve authorization code**.
2. Redeem all or a subset of licenses using the authorization code. When licenses are redeemed, a license-activation key file is generated.
   a. Open the Features on Demand web portal from a web browser, and log in to the portal using your email address as your user ID.
   b. Click **Request activation key**.
   c. Select Input a Single Authorization Code.
   d. Enter the 22-character authorization code and click **Continue**.
   e. Enter your Lenovo customer number in the Lenovo Customer Number field.
   f. Enter the number of licenses that you want to redeem in the Redeem Quantity field, and then click **Continue**.
      To redeem all the available licenses in this authorization code, match the number in Available licenses field.
      If you redeem a subset of available licenses, you can redeem the remaining licenses in another license-activation key using the same authorization code.
   g. Follow the prompts to enter product details and contact information and click **Continue** to generate the license-activation key.
   h. Optionally specify additional recipients to receive the license-activation keys.
   i. Click **Submit** to send the license-activation keys.
      The person assigned to the purchase order and the additional recipients will receive an email with the license-activation key. The key is a file in .KEY format.
3. Import and install the licenses in LOC-A
   a. From the LOC-A portal, click **Setup→License Management** to display the License Management page.
   b. Click the **Upload** icon to install the licenses.
   c. Click **Browse** to select the license-activation key file for the licenses that you want to install.
   d. Click **Import** to import and apply the licenses. When the installation is complete, the license-activation key is listed in the table with the number of installed licenses and the activation period (start and expiration dates).

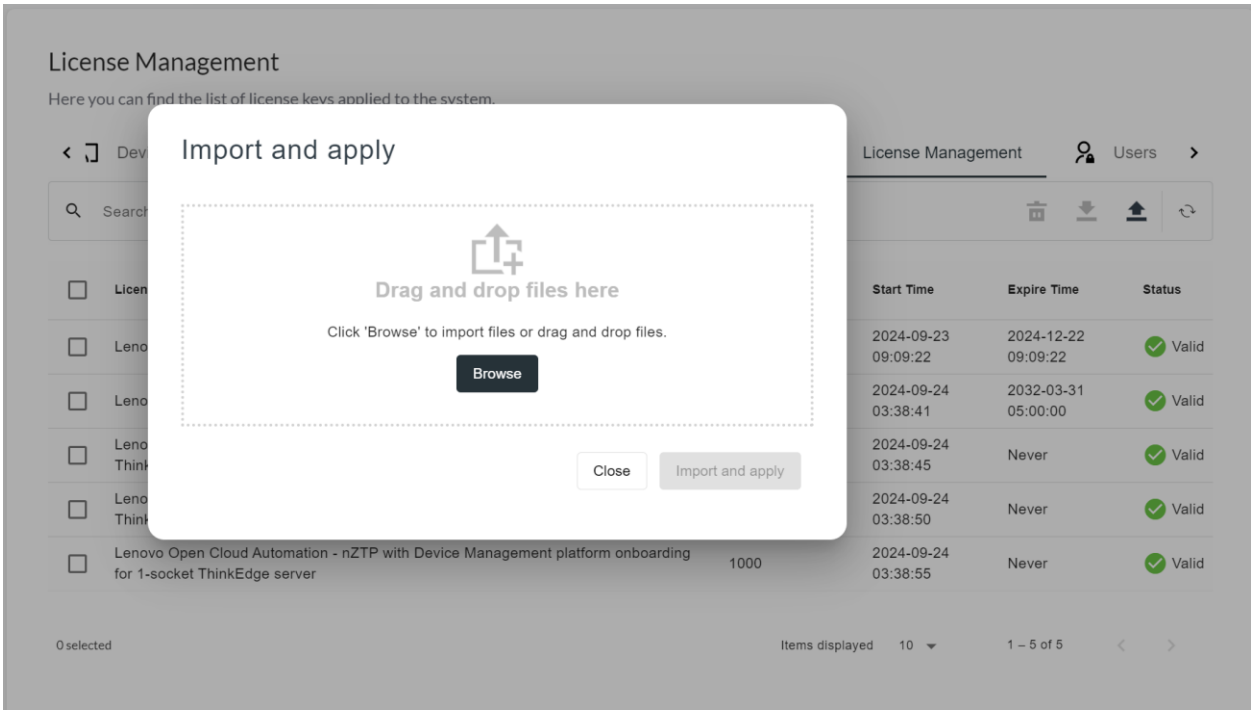


Figure 128: Import and install a license

Delete licenses

Follow the following steps to delete a license:

1. Click **Setup→ License**, select a license, click on the **Delete** icon in the upper right corner**.**
2. Click Delete button to confirm deletion.

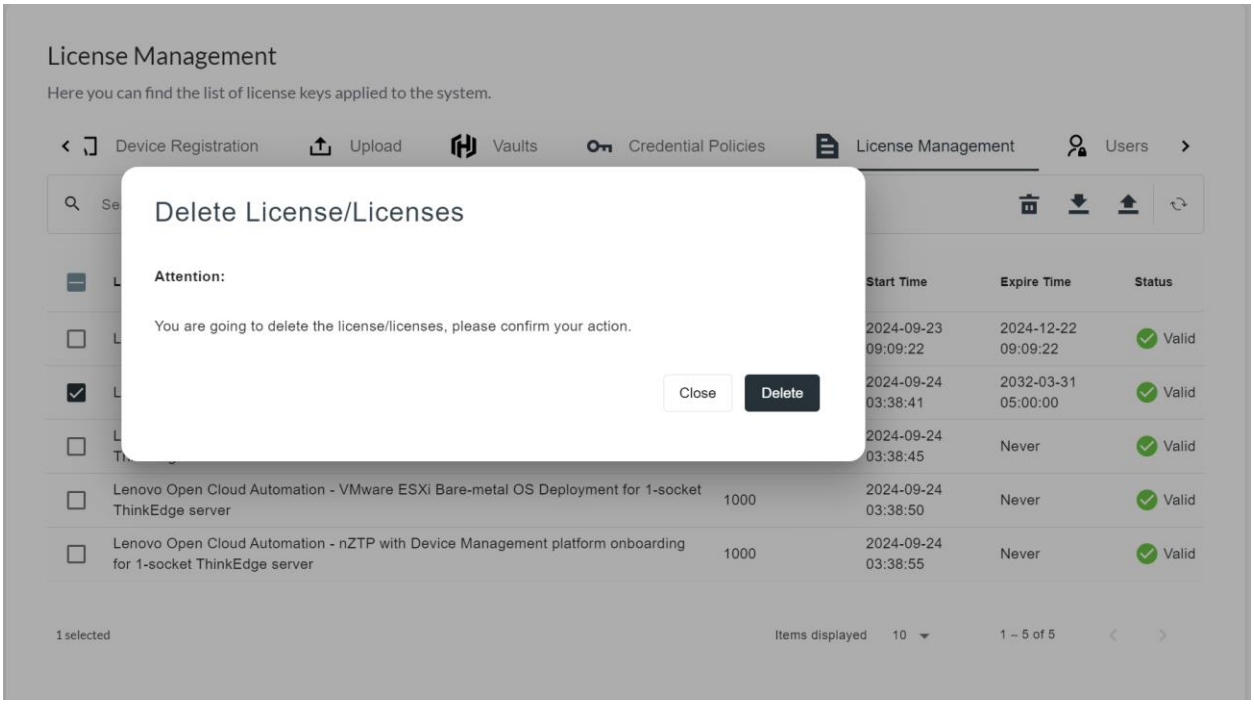


Figure 129: Delete a license

Note: Trial license can be deleted but cannot be retrieved or re-activated. Please use care when working with the trial license.

Export licenses

You can export a license to a key file for backup purposes. Follow the following steps to export a license:

1. Click **Setup→ License**, select a license, click on the **Export** icon in the upper right corner**.**
2. The license key file will be automatically downloaded to your system.

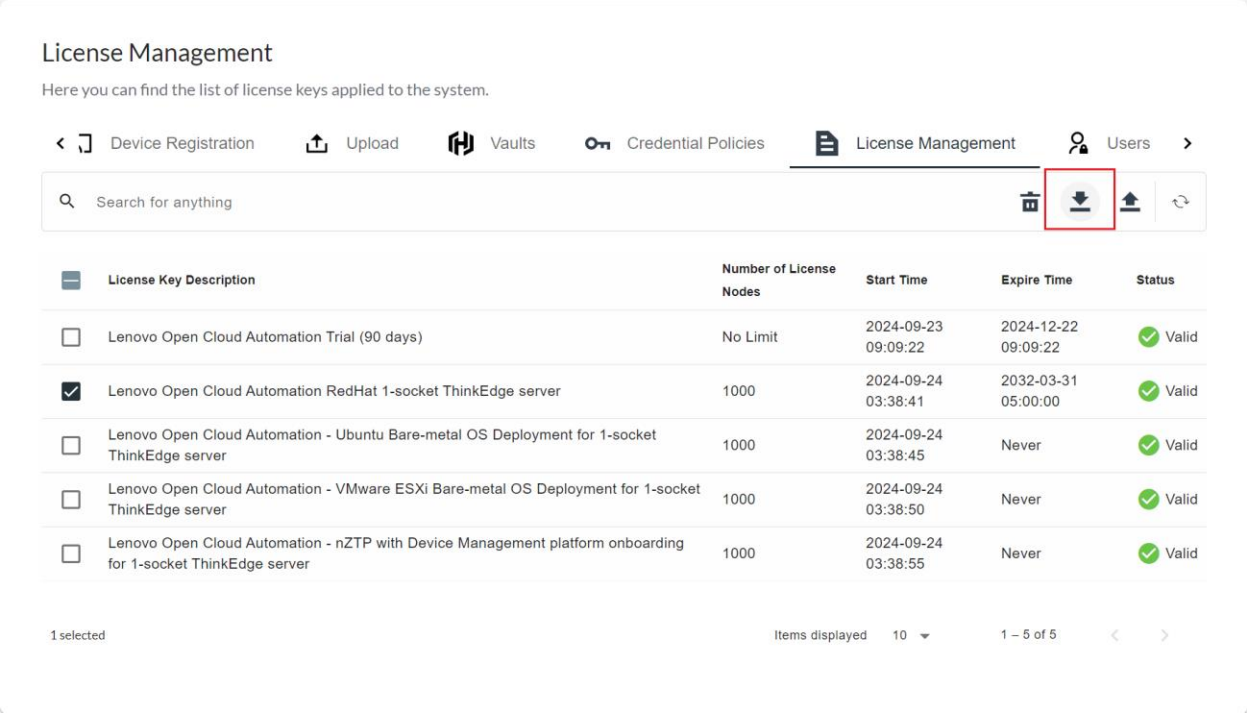


Figure 130: Export a license

Note: Trial license cannot be exported.

Get help

- If you have issues and you used a Business Partner, contact your Business Partner to verify the transaction and entitlement.
- If you did not receive your electronic proof of entitlement, authorization codes, or activation keys, or if they were sent to wrong person, contact one of the regional representatives, based on your geography.
  - ESDNA@lenovo.com (North American countries)
  - ESDAP@lenovo.com (Asia Pacific countries)
  - ESDEMEA@lenovo.com (European, Middle Eastern, and Asian countries)
  - ESDLA@lenovo.com (Latin American countries)
  - ESDChina@Lenovo.com (China)
- If information about my entitlement is not correct, contact Lenovo Support at SW_override@lenovo.com and include the following information:

- Order number
- Your contact information, including email address.
- Your physical address
- Changes that you want made

- If you have issues or questions about downloading the license, contact Lenovo Support at -eSupport_-_Ops@lenovo.com.

Administration

User management

To manage users and authentication, from the LOC-A web portal, click **Setup→Users**.

Note: The built-in user admin has a default password of Lenovo@123 and a role of Supervisor. You are forced to change the default password immediately after you login.

User passwords must meet the following rules:

- The minimum length of 8 characters.
- The maximum length of 256 characters.
- Must contain at least one uppercase letter, one lowercase letter, one special character (!@#~$%^&*()+|_), and one number.

You can click the login name on the upper right page of the portal to change the password of the current user. You must specify the existing password and the new password.

Role-based Access Control (RBAC)

The Users page shows all users currently defined for the system and the role that is assigned to each user.

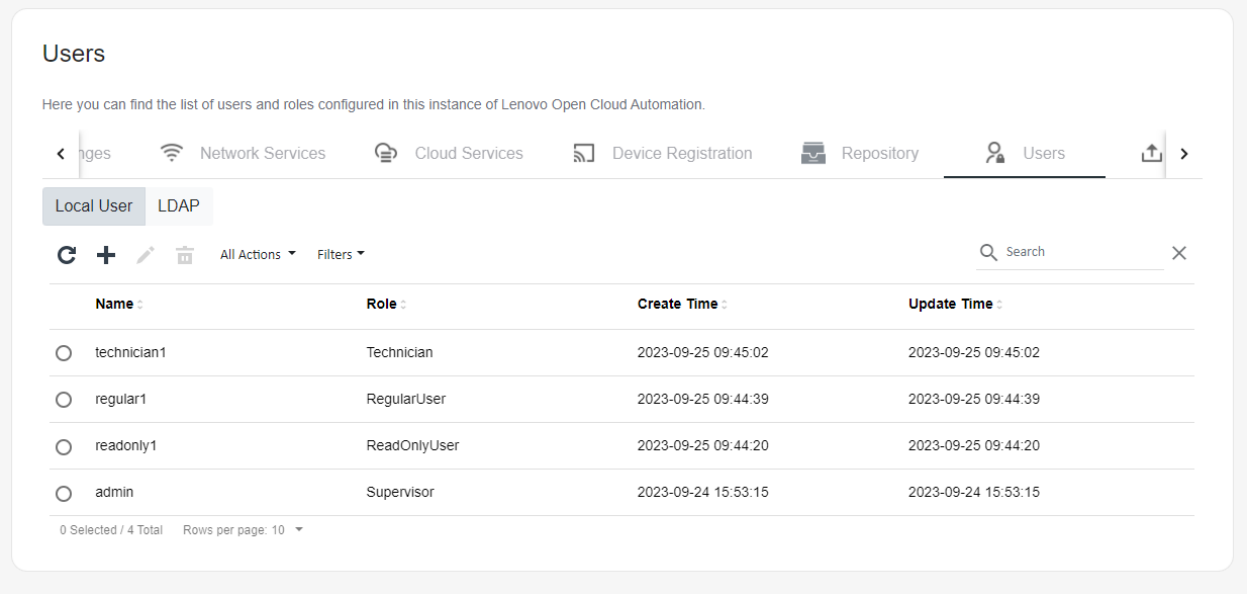


Figure 131: Users

LOC-A supports four roles with access control:

- **Supervisor**
  The Supervisor user is usually an edge infrastructure architect or administrator. The Supervisor has full access to all LOC-A functions. A Supervisor can also assign roles to other users.

  Note: You cannot delete the default admin user.

- **RegularUser**
  A regular user is usually an edge system engineer. The Regular User has no permission to upload metadata from sites in batches, but the Regular User can create, modify, or delete a single resource from the LOC-A web portal. The Regular User can also create cloud templates and deploy new clusters.

- **ReadOnlyUser**
  A Read-Only user is usually an edge project manager. The Read Only user can view infrastructure metadata, cloud templates, and tasks, but the Read Only user cannot make any changes.

- **Technician**
  A Technician is usually the field engineer that performs edge site onboarding and provisioning. The Engineer cannot configure any planned metadata. The Technician can view the infrastructure metadata, and tasks, but has no access to cloud templates and instances.

  The Technician can generate and download LOC-A registration packages and utility, and then register the devices through nZTP methods.

Enable LDAP authentication

LOC-A supports users logging in via LDAP authentication. LDAP protocol version 3 is supported.

You must configure an LDAP server for LDAP authentication. To configure the LDAP server, navigate to the LDAP tab on the Users page.

- Click **Allow Logins from** to choose how user login attempts are authenticated. You can select one of the following authentication methods:
  - **Local only**: Users are authenticated by a search of the local user accounts in LOC-A. If there is no match of the user ID and password, access is denied.

  - **LDAP only:** LOC-A attempts to authenticate the user with credentials kept on the LDAP server you configured.

  - **Local first then LDAP:** Local authentication is attempted first. If local authentication fails; then, LDAP authentication is attempted.

  - **LDAP first then Local:** LDAP authentication is attempted first. If LDAP authentication fails; then, local authentication is attempted.
- Fill in the information on the LDAP tab. You can specify the following parameters:
  - **LDAP IP**: A valid IP address for the LDAP server.
  - **LDAP Port Number:** The port number of your LDAP server.
  - **Enable TLS:** There are three options to enable TLS:
    - **Enable TLS = True, Skip Verify = False**: This option enables secured LDAP. A valid SSL certificate must be uploaded into LOC-A as the trusted certificate to the LDAP server.

      Note: The LDAP server must support TLS.

- **Enable TLS = True, Skip Verify = True**: With this option, LOC-A will connect to the LDAP server with TLS, but it does not verify the certificate of the server.
- **Enable TLS = False**: LOC-A will access LDAP server over an insecure connection.

- **LDAP Username**: The bind username of the LDAP server.

- **LDAP Password**: The bind password of the LDAP server.

- **LDAP Root DN**: The distinguished name (DN) of the root entry of the directory tree on the LDAP server (for example, dn=mycompany,dc=com). This DN is used as the base object for all search requests.

- **User Search:** LOC-A sends a bind request to the LDAP server followed by a search request that retrieves specific information about the user, including the user's DN and group membership. This field defines the user search filter. For example the user search filter can be **(objectClass=inetOrgPerson)** or **(&(objectClass=inetOrgPerson)(employeeType=Owner))**.

- **User Search Attribute**: The user search request must specify the attribute name that represents the user IDs on that server. This attribute name is configured in this field. For example, for OpenLDAP, the attribute name is usually **uid** or **cn**.

  For example,
  User Search: (objectClass=inetOrgPerson)
  User Search Attribute: uid
  login name: hermes
  Then, the actually query filter will be: (&(objectClass=inetOrgPerson)(uid=hermes))

  Note:

  1. If the User Search is (& (objectClass=inetOrgPerson)), the actual query filter to the LDAP server will be: (&(&(objectClass=inetOrgPerson))(uid=hermes)), which returns same result in this case as above.
  2. If the User Search is configured as (&(objectClass=inetOrgPerson)(%(USER_ATTRIBUTE)=%(USERNAME))) in above example, the actual query filter to LDAP server will also be: (&(objectClass=inetOrgPerson)(uid=hermes))

- **Group Search**: Group search is used for group authentication. Group authentication is attempted after the user query is successful and matches one unique user. If group authentication fails, the user's attempt to log on is denied. This field defines the group search filter.

- **Group Search Attribute**: This field defines the attribute name that is used to identify the groups to which a user belongs. For example,

  Group Search: (&(objectClass=Group)(cn=admin_staff))
  Group Search Attribute: uniqueMember

  Assume that user query matches a user with DN=cn=Hermes Conrad,ou=people,dc=planetexpress,dc=com

  The actual group query for this case is:
  (&(&(objectClass=Group)(cn=admin_staff))(uniqueMember=cn=Hermes Conrad,ou=people,dc=planetexpress,dc=com))

- **Select User Role**:

All of the LDAP entries that match group search filter and user search filter will be authenticated and mapped to the selected user role. The permission control of this role is defined by LOC-A in the same way as local users.

Figure 132 shows an example LDAP configuration page.

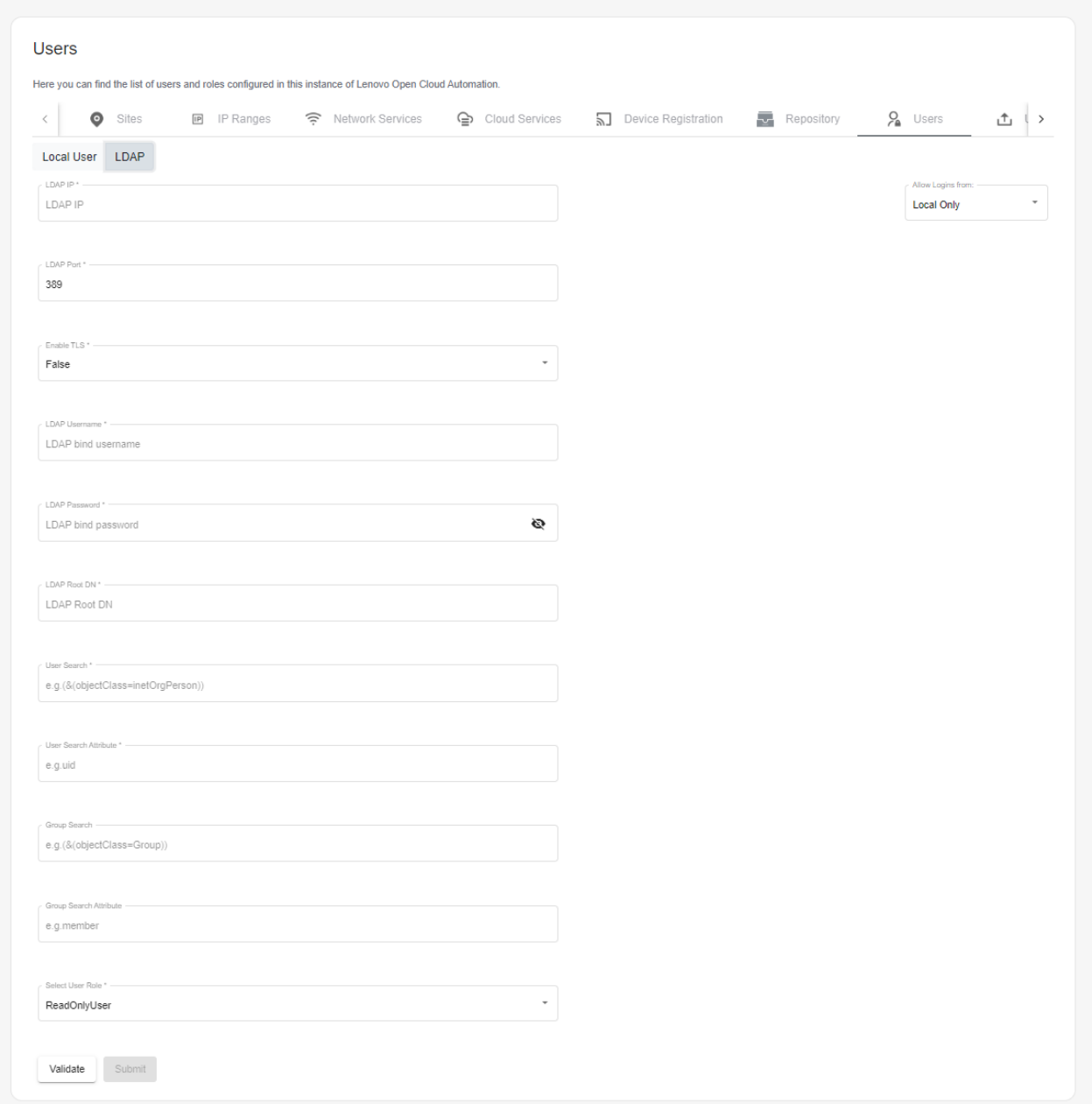


Figure 132: LDAP authentication configuration

- You can validate your LDAP server configuration by clicking the **Validate** button at the bottom of the page.

Certificate management

The LOC-A portal provides certificate management capabilities, allowing users to import and apply certificates signed by their own CA certificate. By default, the LOC-A appliance uses a self-signed certificate that is automatically generated during LOC-A appliance installation.

Note: Only users with the supervisor role can manage certificates on the LOC-A appliance.

Follow the steps below to import and apply a new signed certificate:

1. Generate a new Certificate Signing Request (CSR) and save it locally.
   a) Navigate to **Certificate** from **Settings** page, go to **Generate Certificate Signing Request (CSR)** sub-tab and fill mandatory fields such as Country/Region, State and Organization. Optionally, enable the SAN checkbox to add extra fields like IP addresses or DNS names. Then click **Generate and Download CSR**

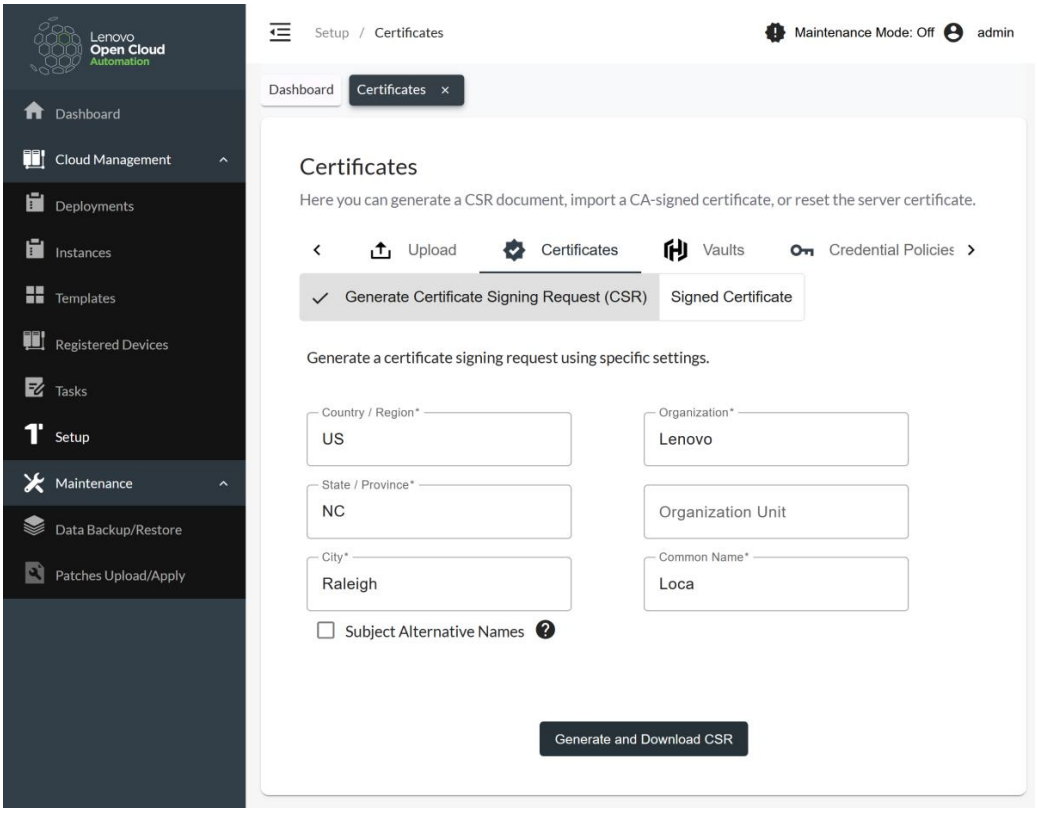


Figure 133: Generate CSR

   b) The CSR will be presented in PEM-encoded format and can be downloaded or copied from the text box.

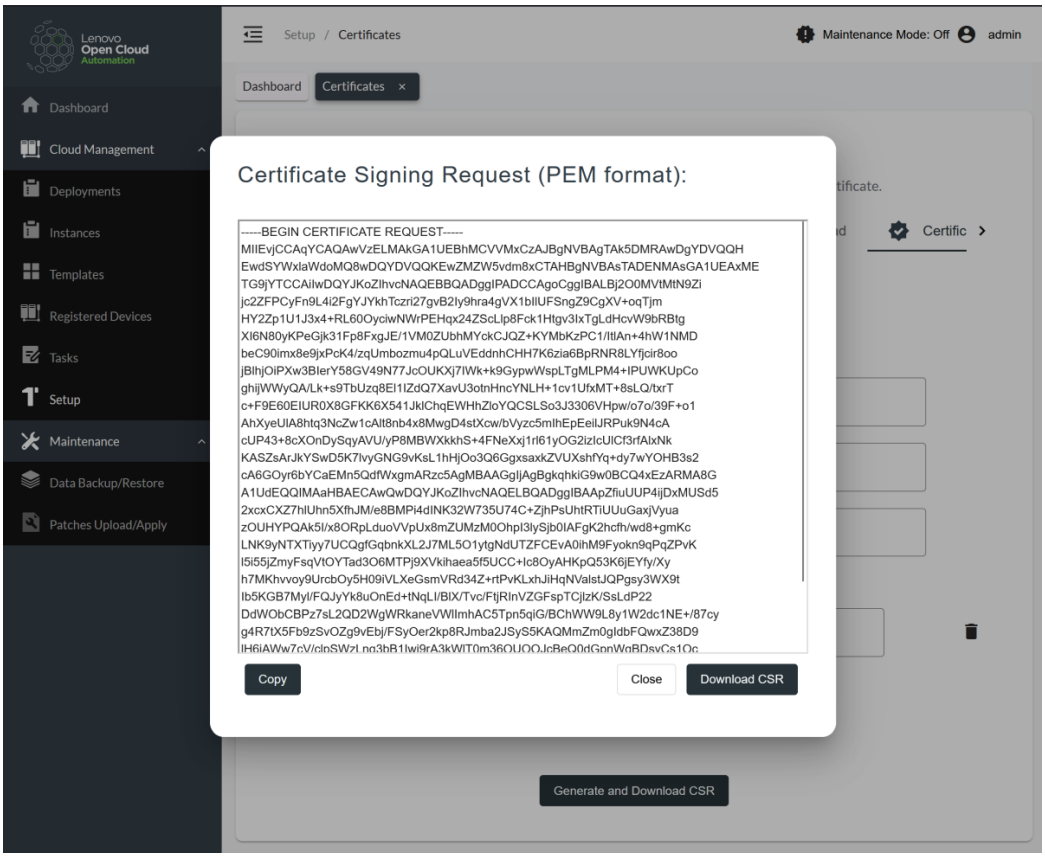


Figure 134: Download CSR

Note:

- With every CSR generation, a new private key is being stored on the LOC-A appliance.
- The generated CSR can be downloaded only once. If the user generates a new CSR, the old private key will be replaced with a new one.
- When using registration packages, the CSR should include at least a SAN of type '*IP address*' with value set to the IP address of the LOC-A appliance (otherwise, the device registration will fail when running the mini-OS image included in the registration package).

2. Obtain a signed certificate by signing the CSR with the user's CA certificate. The generated CSR must be signed by a CA certificate. The resulting signed certificate should be saved in PEM-encoded format, including the full certificate chain.
3. Import the new signed certificate into the LOC-A portal.
   a) The newly signed certificate can be imported in the Signed Certificate sub-tab

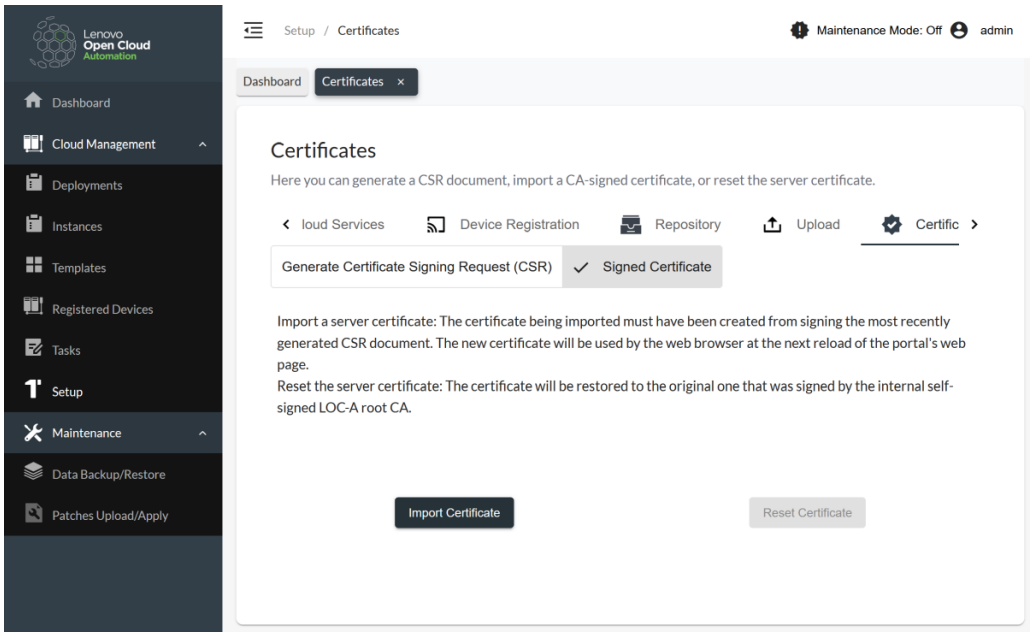


Figure 135: Signed certificate

b) By pressing the **Import Certificate** button, a new dialog is presented where the certificate can be uploaded as a single file or pasted in a text box.

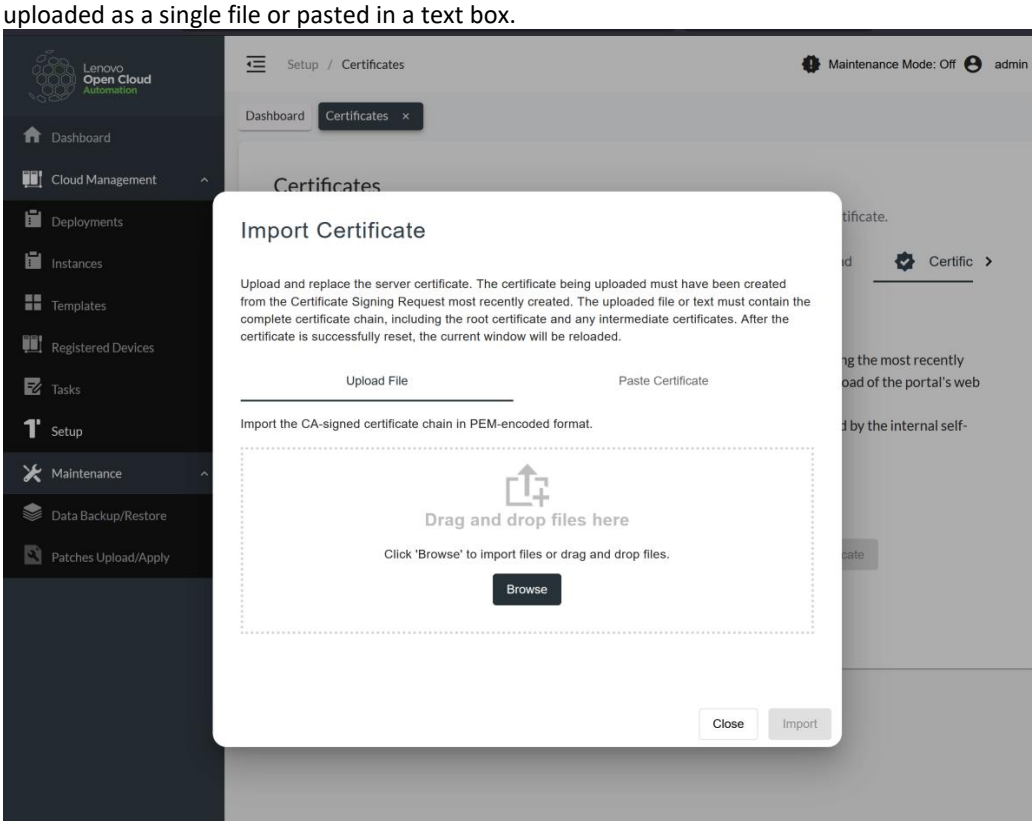


Figure 136: Upload signed certificate

Note: The PEM-encoded file would need to include the full certificate chain. The first PEM block in the file would be the leaf certificate (known as server certificate), followed by any intermediate CAs and ending with the root CA. So, a certificate chain with at least two PEM-blocks would need to be imported (leaf certificate + root CA)

c) After pressing **Import** and if the certificate has been successfully validated, the following message will be presented by letting the user know that the services are being restarted.

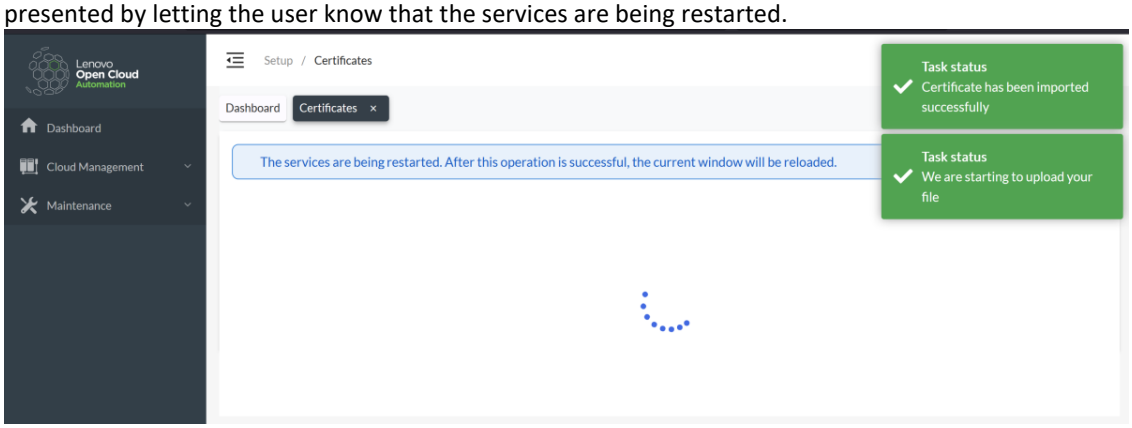


Figure 137: Applying certificate

d) After a delay of around 10 seconds, the LOC-A portal web page will be automatically reloaded.

Notes:

- After reloading the current window, a new warning could appear in case the issuer of the new certificate is not present in the browser's trust store.
- To see if the new certificate has been imported, click the icon next to the left of the URL box which should provide information about the site's security.
- In the case at the time of the certificate import there are any valid registration packages generated, the existing packages will be **invalidated** only when the new imported certificate chain will include a different root CA (or different intermediate CAs) than the currently installed certificate chain. And you need to regenerate the registration package in that case.

Reset the certificate

The currently installed certificate can also be reset to factory default where the original self-signed certificate from LOC-A will replace the existing one.

For this, in the **Signed Certificate** sub-tab, the **Reset Certificate** button can be pressed which will be followed by a warning.

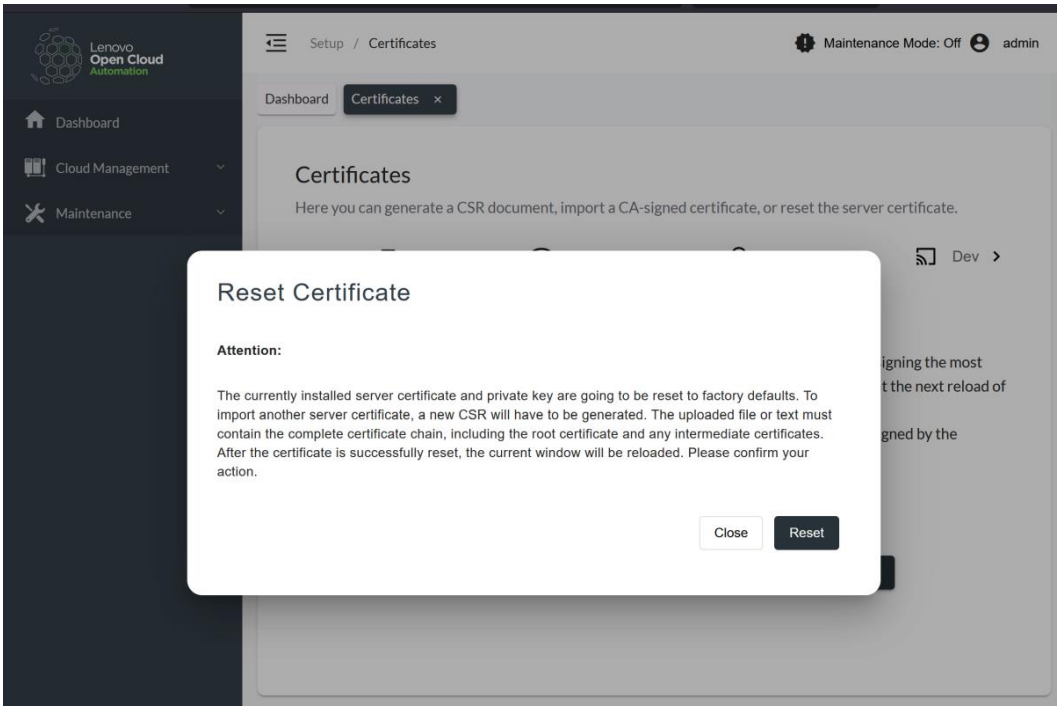


Figure 138: Reset certificate

Note: After the certificate has been reset, the **Import Certificate** and **Reset Certificate** buttons will be disabled until a new CSR is generated

Backup and Restore

LOC-A supports a backup and restore feature to allow users to backup their data and restore in another LOC-A appliance.

Notes:

- The backup data can only be restored in same version or higher version of theLOC-A appliance.
- LOC-A web interface supports backup and restore since version 3.2.
- The CLI called ladm can only be used to backup the data for 3.1 and it will not provide restore support for 3.1. That means you can only to backup 3.1 data and restore the data in a higher version appliance through web interface. You can contact Lenovo team to get the ladm CLI.
- LECP flavor is no longer supported as of 3.2. After upgrading, it is not possible to create new LECP flavor type templates and instances. The historical data will still be there.

Follow these steps to create a backup package for an appliance through the web interface:

Step 1. Login into the LOC-A web interface. Turn on the maintenance mode. Navigate to **Maintenance** -> **Backup/Restore** and click the **+** icon to create backup package. Passphrase is needed and the data will be encrypted with the passphrase. Then click **Create**.

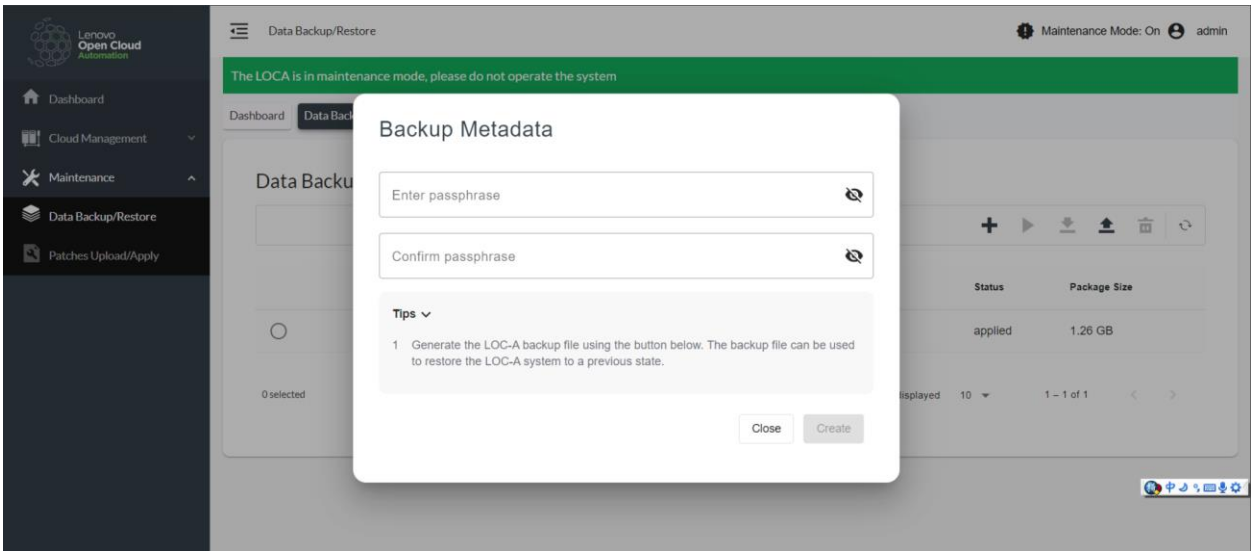


Figure 139: Create backup package through web interface

Step 2. Select the package created before and download it.

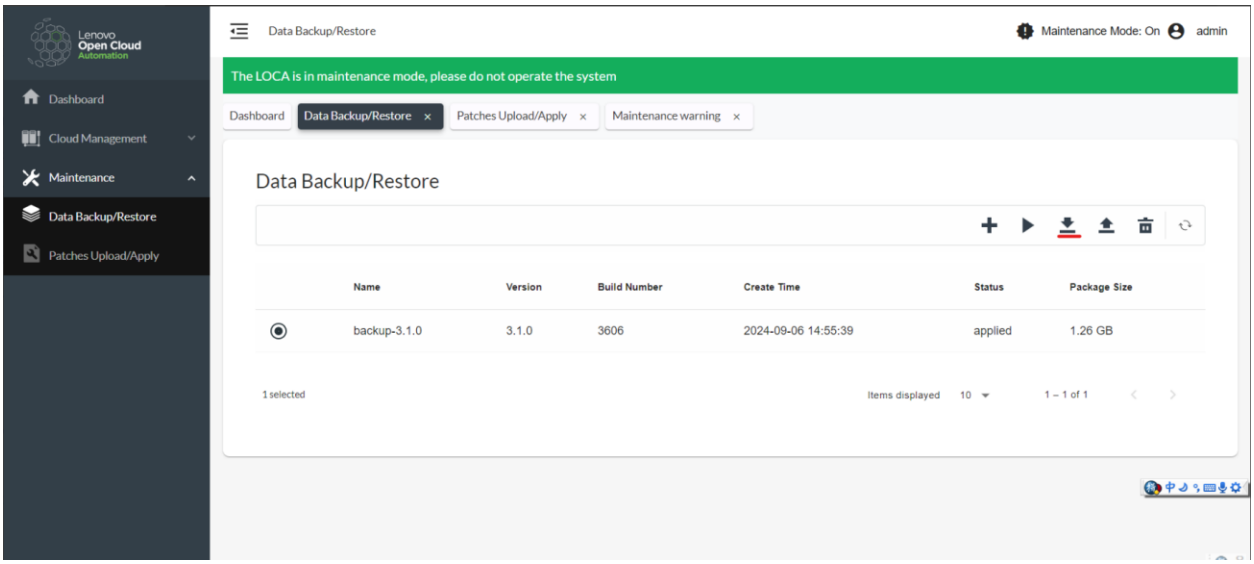


Figure 140: Download backup package

Follow these steps to create a backup package for an appliance through ladm CLI:

Step 1. Enable debug shell and copy the CLI to the LOC-A appliance

Step 2. Run "./ladm backup" and input passphrase to backup metadata of 3.1.0

Step 3. Copy the backup package in the command output to your local environment

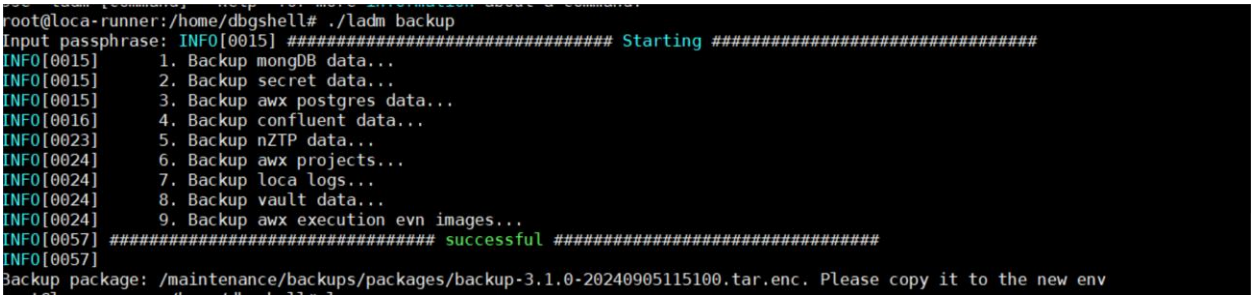


Figure 141: Create backup package through ladm CLI

Follow these steps to restore the data from a backup package:

Step 1. Login to the web interface of the new appliance that you will restore data upon. Navigate to **Maintenance** -> **Data Backup/Restore** and click upload icon to upload the backup package. The passphrase which you used for creating backup package is needed.

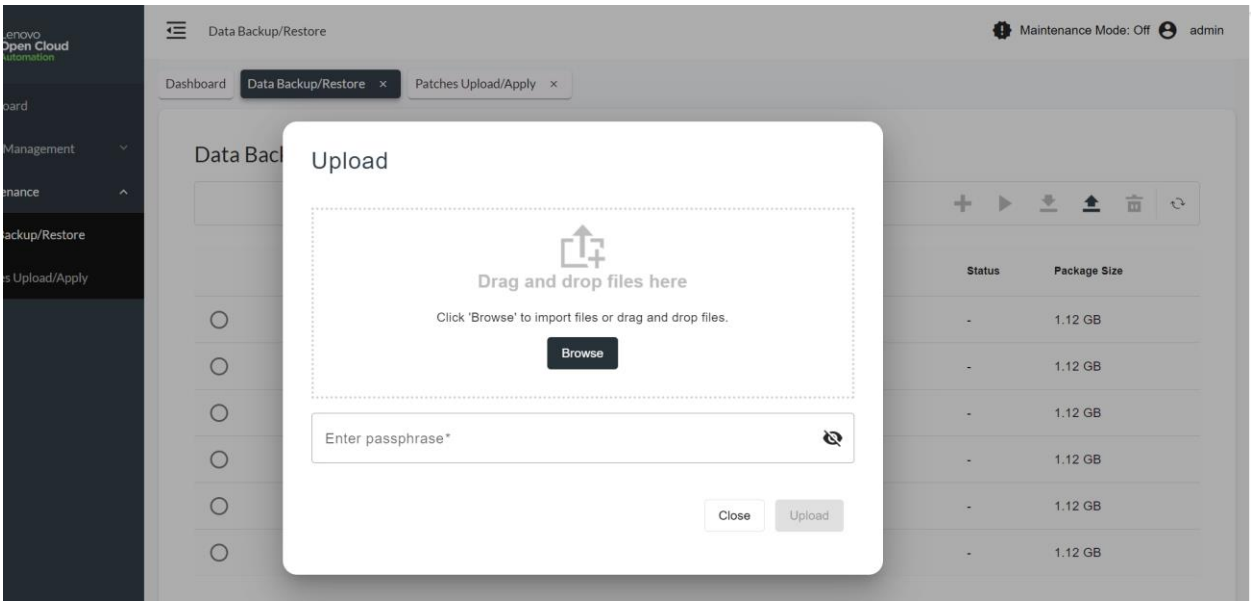


Figure 142: Upload backup metadata

Step 2. Select the uploaded package then click restore icon to restore data in that appliance

Note:

- The package can have statuses of not applied, progressing, failed and applied.
- The web page needs to be refreshed after restoring data.

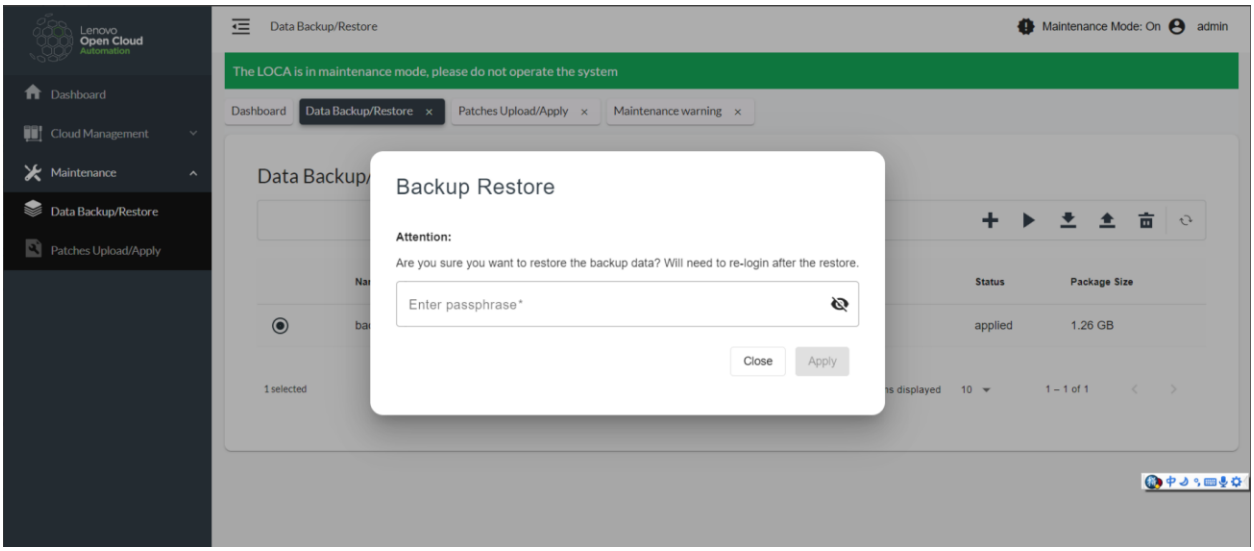


Figure 143: Restore data

Troubleshooting

Log collection

You can download detailed task logs from the LOC-A web portal. Click **Download All Service Logs** on the Tasks page or select the task checkbox that you want to download, you will be prompted with a download window to save the .tgz log file.

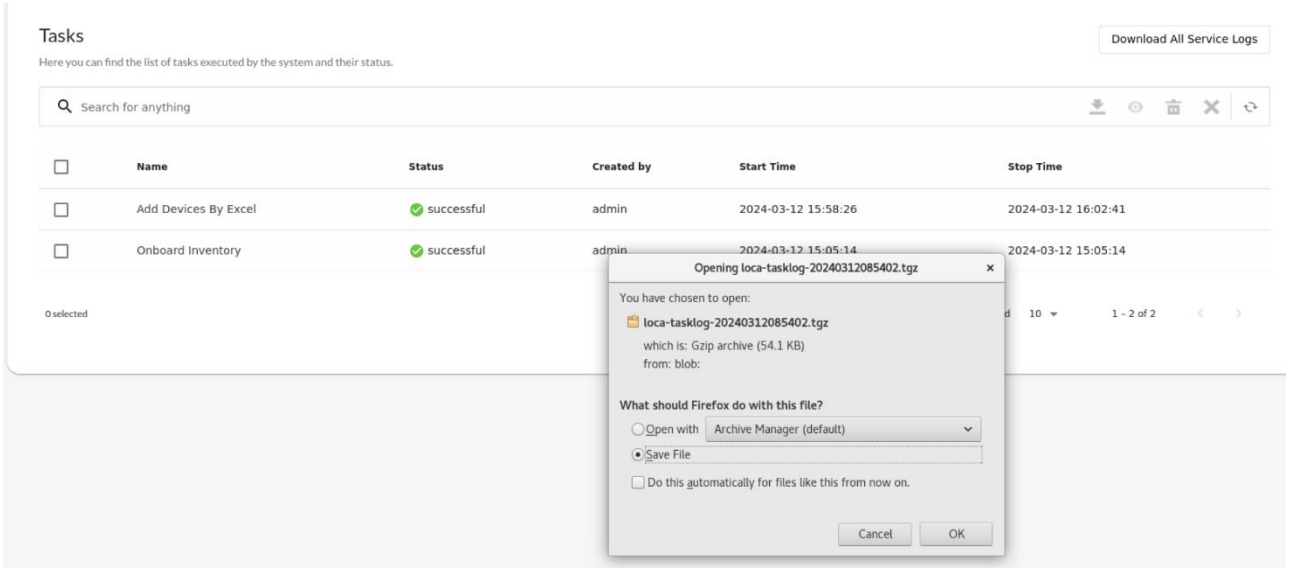


Figure 144: Collect and download logs

Debug shell enablement

In the situation that the Lenovo Support Team needs to troubleshoot the LOC-A appliance by enabling SSH debug shell (port 22) with the assistance of the customer, please follow the following procedure:

1. Login to the normal SSH interface (port 22 – clish) using a default username and password. default username is admin, default password is Lenovo@123. You can also do this from LOC-A console, e.g. access your LOC-A VM from VMware vCenter Remote Console.
   Note:
   - Changing the password on first login and relogin is required.
   - The console will be disconnected with “Too many authentication failures” after 4 consecutive failed login attempt and will be locked for 60 minutes before you can try login again.
2. At the prompt, you will enter the command ‘dbgshloca’.
3. Copy the lines of challenge text into your computer’s clipboard (control-c), then send to the Lenovo support team to generate the response string.

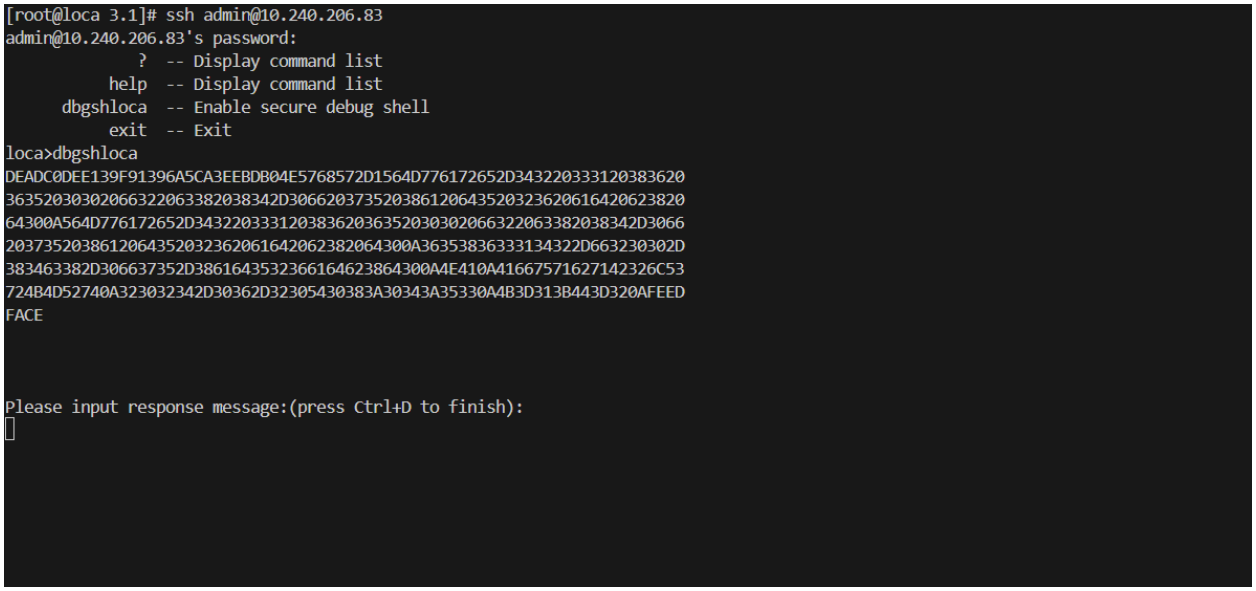


Figure 145: Generate challenge text

4. Copy the response that you get from the Lenovo support team into your computer’s clipboard (control-c) and paste it into the LOC-A clish that provided you the original challenge text.

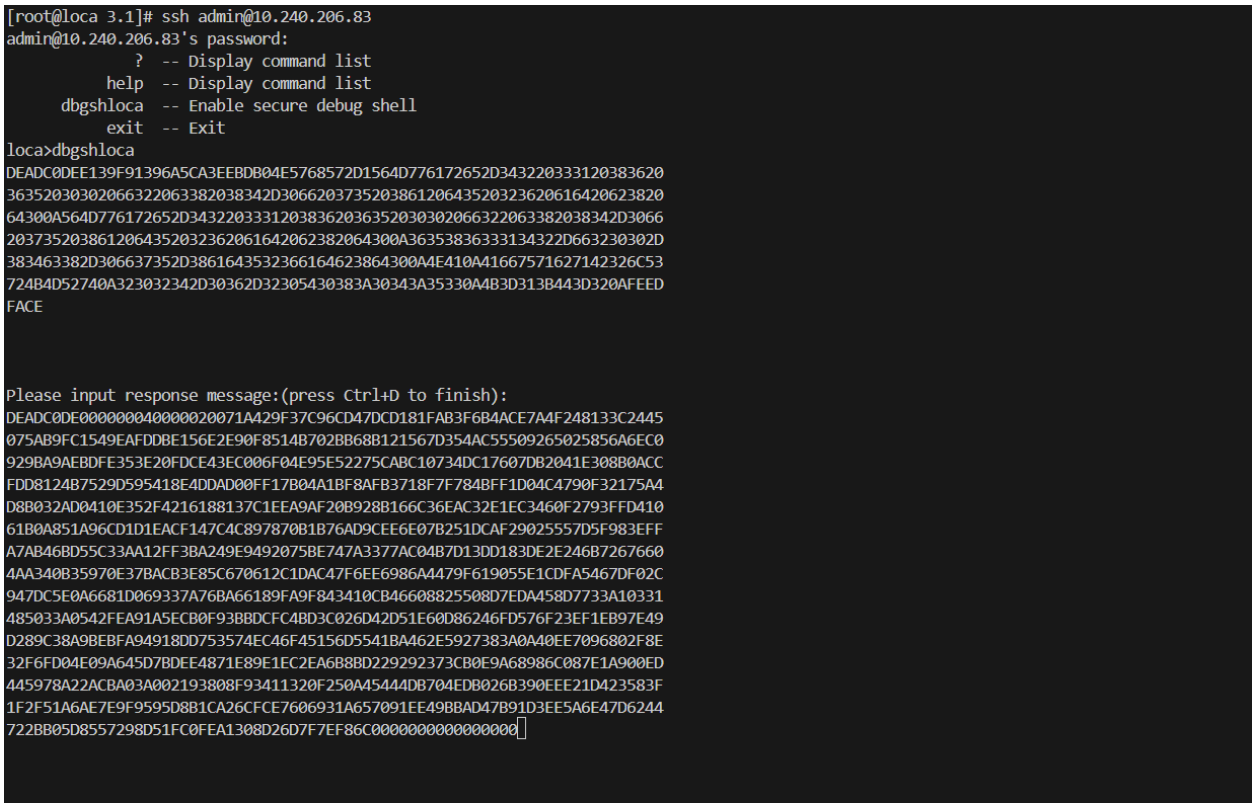


Figure 146: Input response text

5. Press control-d twice. If the response was valid, you will see a message about the unlocked interface. It will ask you to enter a temporary password.

```
[root@loca 3.1]# ssh admin@10.240.206.83
admin@10.240.206.83's password:
             ?  -- Display command list
          help  -- Display command list
     dbgshloca  -- Enable secure debug shell
          exit  -- Exit
loca>dbgshloca
DEADC0DEE139F91396A5CA3EEBDB04E5768572D1564D776172652D343220333120383620
3635203030206632206338203834 2D3066203735203861206435203236206164206238
64300A564D776172652D343220333120383620363520303020663220638203834 2D3066
203735203861206435203236206164206238 2064300A3635383633313432 2D663230302D
383463382D306637352D386164353236616462386430 0A4E410A416675716271423 26C53
724B4D52740A323032342D30362D32305430383A30343A35330A4B3D313B443D320AFEED
FACE



Please input response message:(press Ctrl+D to finish):
DEADC0DE000000040000020071A429F37C96CD47DCD181FAB3F6B4ACE7A4F248133C2445
075AB9FC1549EAFDDBE156E2E90F8514B702BB68B121567D354AC55509265025856A6EC0
929BA9AEBDFE353E20FDCE43EC006F04E95E52275CABC10734DC17607DB2041E308B0ACC
FDD8124B7529D595418E4DDAD00FF17B04A1BF8AFB3718F7F784BFF1D04C4790F32175A4
D8B032AD0410E352F4216188137C1EEA9AF20B928B166C36EAC32E1EC3460F2793FFD410
61B0A851A96CD1D1EACF147C4C897870B1B76AD9CEE6E07B251DCAF29025557D5F983EFF
A7AB46BD55C33AA12FF3BA249E9492075BE747A3377AC04B7D13DD183DE2E246B7267660
4AA340B35970E37BACB3E85C670612C1DAC47F6EE6986A4479F619055E1CDFA5467DF02C
947DC5E0A6681D069337A76BA66189FA9F843410CB46608825508D7EDA458D7733A10331
485033A0542FEA91A5ECB0F93BBDCFC4BD3C026D42D51E60D86246FD576F23EF1EB97E49
D289C38A9BEBFA94918DD753574EC46F45156D5541BA462E5927383A0A40EE7096802F8E
32F6FD04E09A645D7BDEE4871E89E1EC2EA6B8BD229292373CB0E9A68986C087E1A900ED
445978A22ACBA03A002193808F93411320F250A45444DB704EDB026B390EEE21D423583F
1F2F51A6AE7E9F9595D8B1CA26CFCE7606931A657091EE49BBAD47B91D3EE5A6E47D6244
722BB05D8557298D51FC0FEA1308D26D7F7EF86C0000000000000000---



A password is required to access debug shell.
Please input password:
Please confirm  your password:
Password changed successfully.


Use 'ssh -p 122 dbgshell@IPADDR' to access debug shell.
Secure debug port will be available for 24 hours.
loca>
```

Figure 147: Enable SSH debug shell

6. You can now SSH into port 122 using the username ‘dbgshell’ and the temporary password created in the last step. The debug port will be available for 24 hours.

```
A password is required to access debug shell.
Please input password:
Please confirm  your password:
Password changed successfully.


Use 'ssh -p 122 dbgshell@IPADDR' to access debug shell.
Secure debug port will be available for 24 hours.
loca>exit
Connection to 10.240.206.83 closed.
[root@loca 3.1]# ssh -p 122 dbgshell@10.240.206.83
dbgshell@10.240.206.83's password:
ssrbreview:~$
```

Figure 148: SSH into debug shell

7. To check the status of the unlocked SSH (port 122 – bash), log back into SSH (port 22 – clish) and run the ‘dbgshloca status’ command.

```
[root@loca 3.1]# ssh admin@10.240.206.83
admin@10.240.206.83's password:
             ?  -- Display command list
          help  -- Display command list
     dbgshloca  -- Enable secure debug shell
          exit  -- Exit
loca>dbgshloca status
Secure debug port is open: 23.00 hours 56.00 minutes remaining
loca>
```

Figure 149: Check debug shell status

8. To relock the SSH (port 122 – bash), use run the ‘dbgshloca disable’ command.

```
[root@loca 3.1]# ssh admin@10.240.206.83
admin@10.240.206.83's password:
             ?  -- Display command list
          help  -- Display command list
     dbgshloca  -- Enable secure debug shell
          exit  -- Exit
loca>dbgshloca status
Secure debug port is open: 23.00 hours 56.00 minutes remaining
loca>dbgshloca disable
debugshell is disabled
loca>
```

Figure 150: Disable debug shell

Known issues and limitations

This release has the following issues and limitations:

- A failed task in the LOC-A web portal cannot be retried; instead, you must perform the operation again.
- Only one cloud cluster can be onboarded and deployed for a site that is planned with cloud flavor. But a site that is planned with bare metal OS flavor can have multiple nodes deployed.
- A site cannot be deleted if there is an existing cluster associated with that site.
- You should not configure an OVA XCC IP address, netmask, and gateway if your edge XCC(BMC) network is routable to the OS/Cloud Management network. Otherwise, the Cloud OS deployment may fail.
- When an instance is in Failed status, you can select and click **Run** to kick off the deployment again, but for VMware vSAN and RedHat OCP cloud flavors, the deployment may still fail in some situations if the previous failure happens during cloud deployment stage after OSes are installed, because when rerunning the deployment, LOC-A will skip the OS deployment, thus all failure conditions may not be corrected.

- Changing connected LDAP user password is not allowed from LOC-A. If a user attempts to change it from the GUI, an error will pop up.
- RedHat OCP deployment may fail on some server types with some types of Intel onboard Ethernet adapters that don't support to report MAC address information to BMC(XCC). For example, in case this happens, you can't get physical port burn-in address from the BMC(XCC) server inventory page. Thus, RedHat OCP deployment will fail due to missing MAC to Interface name mapping.

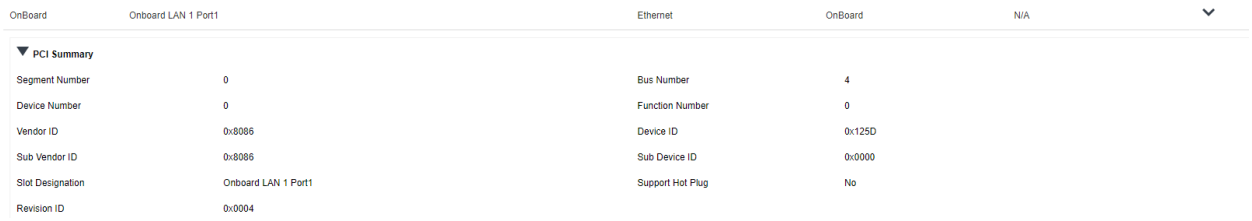


Figure 151: Unsupported onboard LAN ports in server inventory

- Uploading large backup packages or patches can be resource-intensive, causing significant system slowdowns and delays in task execution.
- Lenovo Management Hub relies on Lenovo LXCO to add new devices. So if a Management Hub doesn't have the associated LXCO service in metadata, e.g., the user deletes an LXCO service, but doesn't delete the Management Hub associated with it, then the task to add devices will fail with task error message "name: is not found". In case this happens, please ensure the Management Hub is also deleted.

Appendix

A. End User License Agreement (EULA)

Lenovo License Agreement

L505-0009-06-R2

This Lenovo License Agreement (the "Agreement") applies to each Lenovo Software Product that You acquire, whether it is preinstalled on or included with a Lenovo hardware product, acquired separately, or downloaded by You from a Lenovo Web site or a third-party Web site approved by Lenovo. It also applies to any updates or patches to these Software Products. This license agreement does not apply to non-Lenovo software that's either preloaded on or downloaded to your product. This Lenovo License Agreement is available in other languages at https://support.lenovo.com/us/en/solutions/ht100141.

Lenovo will license the Software Product to You only if You accept this Agreement. You agree to the terms of this Agreement by clicking to accept it or by installing, downloading, or using the Software Product.

If You do not agree to these terms, do not install, download, or use the Software Product(s).

- If You acquired the Software Product(s) and paid a license fee, return the Software Product to the party from whom You acquired it to obtain a refund or a credit of the amount You paid.

- If You acquired the Software Product(s) preinstalled on or provided with a Lenovo hardware product, You may continue to use the hardware product, but not the Software Product(s) covered under this Agreement.

"Open Source software" means any computer program, including any modification, improvement, derivative work, release, correction, governed by the terms and conditions of an Open Source license.

"Open Source License" means a license that gives you legal permission to freely use, modify, and share the Open Source software and is

(i) approved by the Open Source Initiative (here after OSI) principles defined in the following website: https://opensource.org/osd and/or
(ii) certified by the OSI (cf. list of such licenses in https://opensource.org/licenses/category) and/or
(iii) compliant with the free software foundation criteria and/or
(iv) that requires the human readable source code of software to be made available to the general public.

"Software Product" includes Lenovo computer software programs (whether preinstalled or provided separately) and related licensed materials such as documentation.

"You" and "Your" refer either to an individual person or to a single legal entity.

1. Entitlement

You must maintain Your original dated sales transaction document, such as a receipt, invoice or similar document, as Your proof of Your right to use the Software Product. The transaction document specifies the usage level acquired. If no usage level is specified, You may install and use a single copy of the Software Product on a single hardware product. Your transaction document also provides evidence of Your eligibility for future upgrades, if any. For Software Products preinstalled on, included with, or distributed at no charge for use on a Lenovo hardware product, Your hardware product sales transaction document is also the proof of Your right to use the Software Product.

2. License

The Software Product is owned by Lenovo or a Lenovo supplier, and is copyrighted and licensed, not sold. Lenovo grants You a nonexclusive license to use the Software Product when You lawfully acquire it.

You may a) use the Software Product up to the level of use specified in Your transaction document and b) make and install copies, including a backup copy, to support such use. The terms of this Agreement apply to each copy You make. You may not remove or alter any copyright notices or legends of ownership.

If You acquire the Software Product as a program upgrade, after You install the upgrade You may not use the Software Product from which You upgraded or transfer it to another party.

You will ensure that anyone who uses the Software Product (accessed either locally or remotely) does so only for Your authorized use and complies with the terms of this Agreement.

You may not a) use, copy, modify, or distribute the Software Product except as provided in this Agreement or in any way that violates any applicable laws including but not limited to copyright laws; b) reverse assemble, reverse compile, or otherwise translate the Software Product except as specifically permitted by law without the possibility of contractual waiver; or c) sublicense, rent, or lease the Software Product.

Lenovo may terminate Your license if You fail to comply with the terms of this Agreement. If Lenovo does so, You must destroy all copies of the Software Product.

Lenovo uses the System Update program to update Software Products on Your computer. By default, critical updates are downloaded and installed automatically. Updates are classified as critical when they

are needed for the computer to function properly. Failure to install critical updates could result in data corruption or loss, a major system malfunction, or a hardware failure. For example, critical updates could include an update to the harddisk-drive firmware, a BIOS upgrade, a device-driver fix, or a fix for the operating system or other preinstalled software. You can disable this automatic feature by changing the settings of the System Update program at any time.

3. Transferability

   You may not transfer or assign the Software Product to any other party, except as permitted in this section.

   Preinstalled Software Products are licensed for use only on the Lenovo hardware product on which they are preinstalled or included with and may be transferred only with that Lenovo hardware product. They may not be transferred independent of the Lenovo hardware product.

4. Open Source and Other Third Party Software Components and Products

   Portion(s) of the Software Products and future updates and patches provided hereunder may include Open Source software licensed under a particular Open Source License. To the extent that the terms of this Agreement conflict with the terms of such Open Source License, then the terms of such Open Source License shall control for such applicable Open Source software. For the sake of clarity, for any portion(s) of the Software Products, which is not governed by such Open Source License, this Agreement shall control.

   Some Lenovo Software Products and future updates and patches may contain third party components, which may include Microsoft Windows Preinstallation Environment. These third party components are provided to You under separate terms and conditions different from this Agreement, typically found in a separate license agreement or in a README (or similarly titled) file. The third party's license terms and use restrictions will solely govern the use of such components.

   Third Party Software Products provided by Lenovo may be governed by the terms of this Agreement but are usually licensed by the Third Party under its own terms and conditions. Third Party Software Products that are not licensed by Lenovo are subject solely to the terms of their accompanying license agreements.

5. Software Product Specifications

   The Software Product specifications and specified operating environment information may be found in documentation accompanying the Software Product, if available, such as a README or similarly titled file, or otherwise published by Lenovo.

6. Privacy

   Please review the Lenovo privacy policy statement (http://www.lenovo.com/privacy/software/) that's associated with Your product. Depending on Your particular Lenovo device or software product, the Lenovo privacy statement is located at the point of activation and set-up and/or via "Settings".

7. Charges

   Charges for the Software Product are based on the level of use acquired.

   If You wish to increase the level of use, contact Lenovo or the party from whom You acquired the Software Product. Additional charges may apply.

   If any authority imposes a duty, tax, levy or fee, excluding those based on Lenovo's net income, upon the Software Product, then You agree to pay the amount specified or supply exemption documentation. You are responsible for any personal property taxes for the Software Product from the date that You acquire it.

8. No Warranty

   The Software Product(s) is provided to You “AS IS.” SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, LENOVO MAKES NO WARRANTIES OR CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE

   IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE SOFTWARE PRODUCT OR TECHNICAL SUPPORT, IF ANY.

   The exclusion also applies to any of Lenovo’s developers and suppliers.

   Suppliers or publishers of non-Lenovo Software Products may provide their own warranties. Lenovo does not provide technical support, unless Lenovo specifies otherwise in writing.

9. Limitation of Liability

   Circumstances may arise where, because of a default on Lenovo's part or other liability, You may be entitled to recover damages from Lenovo. In each such instance, regardless of the basis on which You
   are entitled to claim damages from Lenovo (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), except and to the extent that liability cannot be waived or limited by applicable laws, Lenovo is liable for no more than the amount of actual direct damages suffered by You, up to the amount You paid for the Software Product. This limit does not apply to damages for bodily injury (including death) and damage to real property and tangible personal property for which Lenovo is required by law to be liable.

   This limit also applies to Lenovo's suppliers and resellers. It is the maximum for which Lenovo, its suppliers and resellers are collectively responsible.

   UNDER NO CIRCUMSTANCES IS LENOVO, ITS SUPPLIERS OR RESELLERS LIABLE FOR ANY OF THE FOLLOWING EVEN IF INFORMED OF THEIR POSSIBILITY: 1) THIRD PARTY CLAIMS AGAINST YOU FOR DAMAGES; 2) LOSS OF, OR DAMAGE TO, YOUR DATA; OR 3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, BUSINESS

   REVENUE, GOODWILL, OR ANTICIPATED SAVINGS. SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

10. Consumer Rights

    Nothing in this Agreement affects any statutory rights of consumers that cannot be waived or limited by contract. You may have additional consumer rights under applicable local laws, which this Agreement cannot change.

11. General

    a) In the event that any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions of this Agreement remain in full force and effect.

    b) You agree to comply with all applicable export and import laws and regulations.

    c) Neither You nor Lenovo will bring a legal action under this Agreement more than two (2) years after the cause of action arose unless otherwise provided by local law without the possibility of contractual waiver or limitation.

12. Dispute Resolution

If You acquired the Software Product in Cambodia, Indonesia, Philippines, Vietnam or Sri Lanka, disputes arising out of or in connection with this Software Product shall be finally settled by arbitration held in Singapore and this Agreement shall be governed, construed and enforced in accordance with the laws of Singapore, without regard to conflict of laws. If You acquired the Software Product in India, disputes arising out of or in connection with this Software Product shall be finally settled by arbitration held in Bangalore, India. Arbitration in Singapore shall be held in accordance with the Arbitration Rules of Singapore International Arbitration Center ("SIAC Rules") then in effect. Arbitration in India shall be held in accordance with the laws of India then in effect. The arbitration award shall be final and binding for the parties without appeal and shall be in writing and set forth the findings of fact and the conclusions of law. All arbitration proceedings shall be conducted, including all documents presented in such proceedings, in the English language, and the English language version of this Agreement prevails over any other language version in such proceedings.