



# LOC-A Core Framework User Guide (Version 3.1)



**Date:** 2024-06-28

---

**© Copyright Lenovo 2023.**

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS- 35F-05925.

# Table of Contents

Summary of Statement.....	1
LOC-A Core Framework Overview .....	1
Getting started .....	2
Deployment environment requirements.....	2
Sample network configuration .....	4
Step-by-step LOC-A Core Framework appliance installation.....	4
Functional user guide .....	11
Cloud setup.....	11
Sites .....	12
IP Ranges.....	15
Network Services .....	17
Cloud Services.....	19
Credential policy.....	28
Device profiles .....	31
Generate LOC-A registration packages.....	33
Generate USB type package .....	34
Generate ThinkShield type package .....	35
Download Lenovo Open Cloud Automation Utility .....	37
Register devices .....	37
Register devices via Lenovo Open Cloud Automation Utility .....	37
Register devices via USB key.....	44
Add devices by Discovery .....	48
Add device by BMC IP .....	50
Upload device Excel file .....	52
Adding devices into external hardware management tools.....	53
Repository management .....	54
Vault secrets management.....	57
Create a cloud template .....	63
Cloud deployment .....	71
Cloud expansion .....	73
Instance deletion .....	77
Create an OS template.....	77
Bare metal OS deployment.....	81
OS Image sideloading .....	82
View tasks.....	85
User management .....	86

Role-based Access Control (RBAC).....	86
Enable LDAP authentication .....	87
Log collection.....	90
Debug shell enablement.....	91
Known issues and limitations .....	94
Appendix.....	96
A. End User License Agreement (EULA) .....	96





## 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

## Getting started

### Deployment 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.**  
An Out-of-band management network for the BMC(XCC) of each server in the cluster, and optionally switch discovery and management
  - **Cloud Networks.**  
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. Cloud networks consist of vManagement, vMotion and vSAN networks.  
  
**Note:** The vManagement 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 (RHOC)
  - Lenovo Edge Computing Platform (LECP) Single Node



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

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

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	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	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	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	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	N/A	7.0.3k,7.0.3m, 7.0.3n, 8.0.1c
ThinkEdge SE350 V2 (MT: 7DA9)	22.04.3	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	N/A	7.0.3d, 7.0.3k, 7.0.3m, 7.0.3n, 8.0.1c

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.

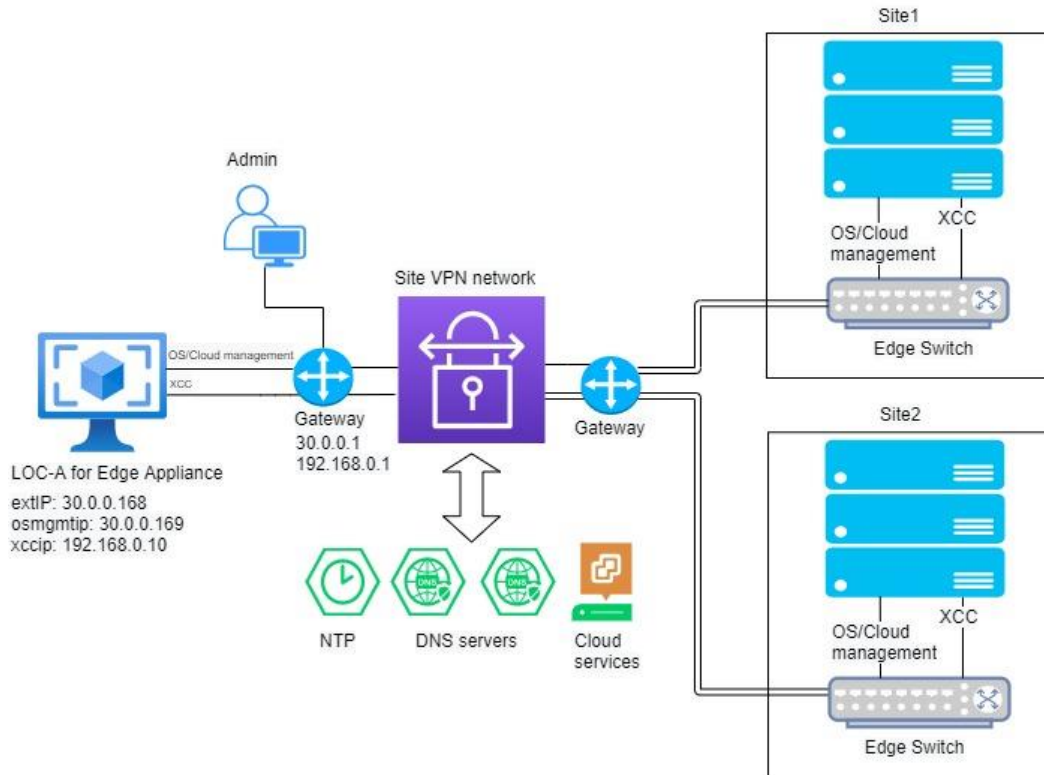
Redfish support must be enabled on the target systems for the deployment to work.

**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 71 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:

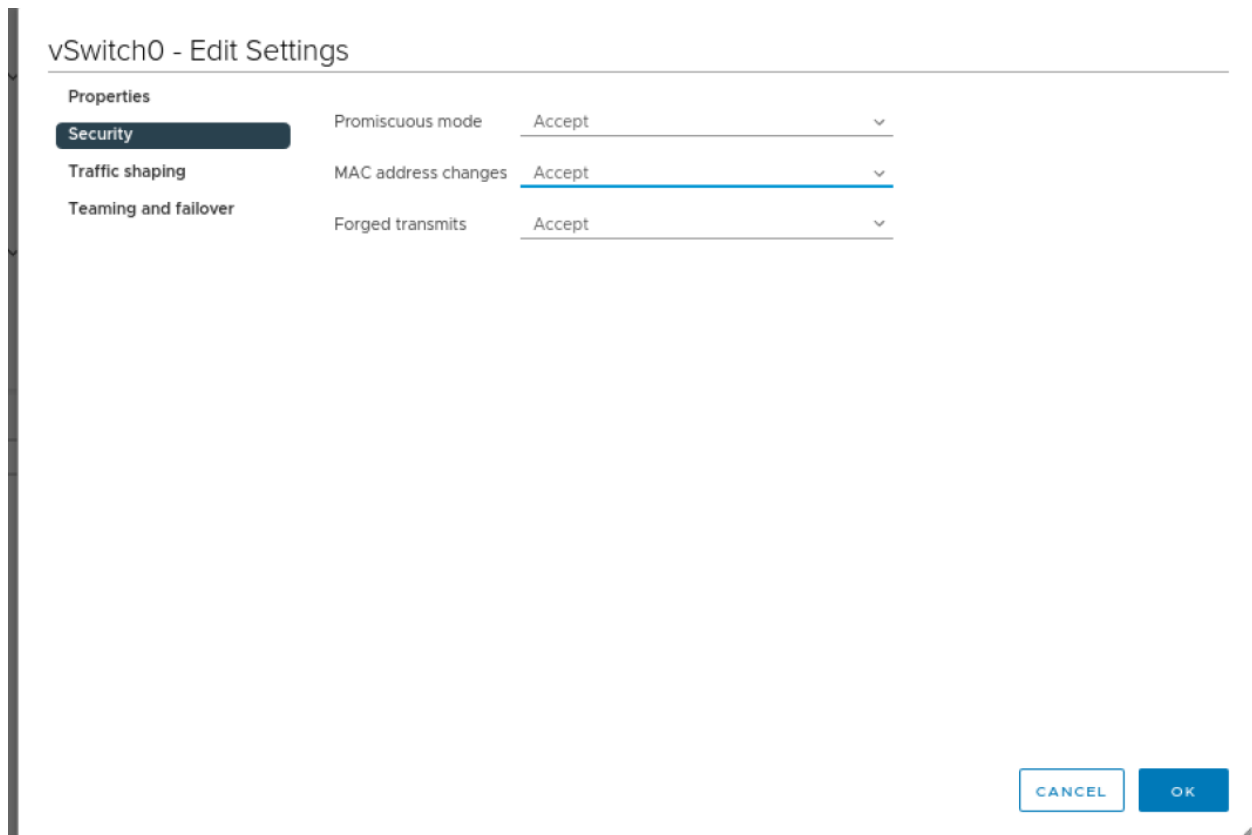


**Figure 1: Network topology of LOC-A Core Framework**

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.

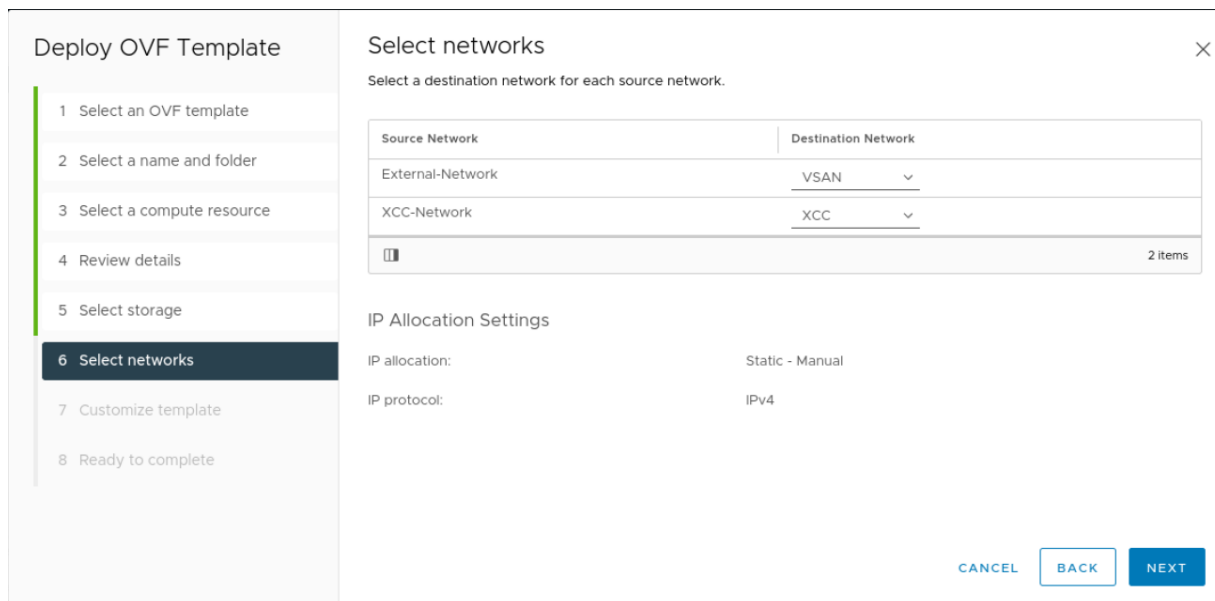
## Step-by-step LOC-A Core Framework appliance installation

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	Loca-edge
External Network IP	Yes	External IPv4 address of the LOC-A appliance portal. You can then access the portal GUI via <a href="https://[External Network IP]">https://[External Network IP]</a>  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 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	192.168.0.10

Parameter	Mandatory	Description	Sample Value
		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. <b>Note:</b> 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 1: 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:

### Deploy OVF Template

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

### Customize template

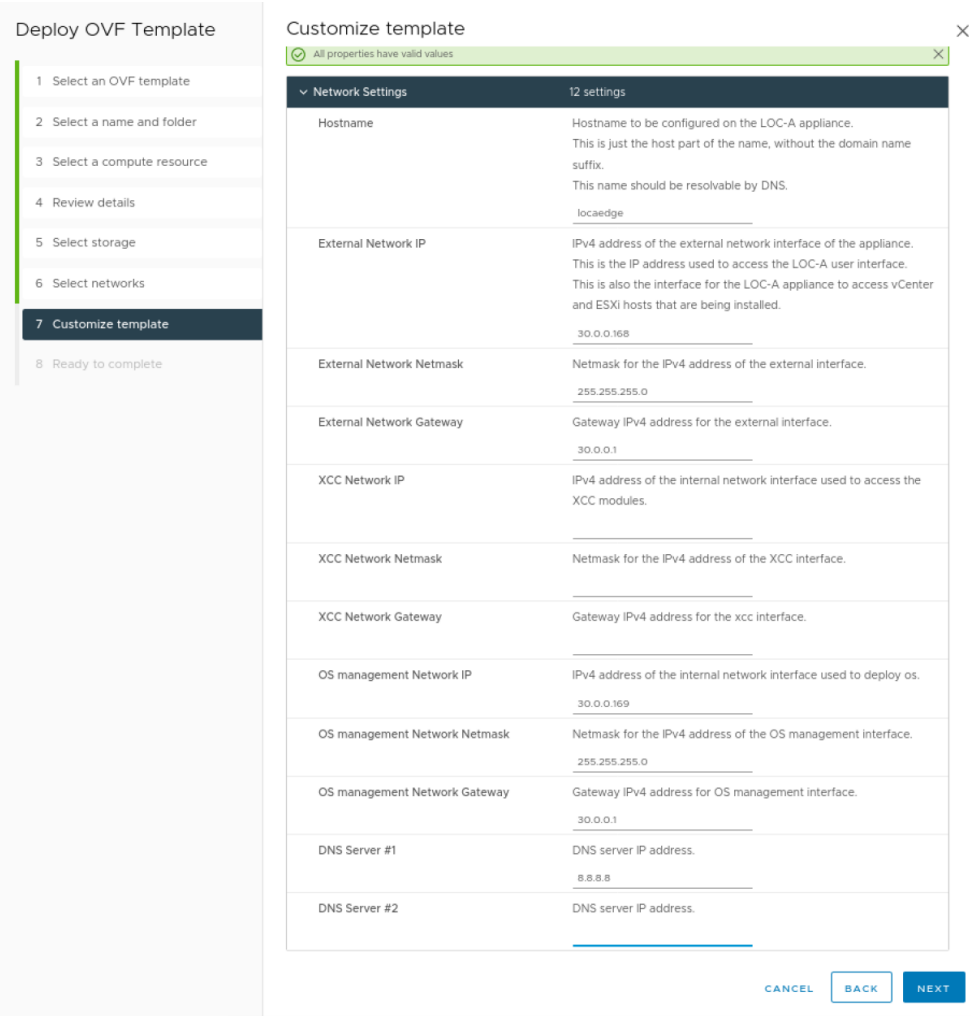
All properties have valid values
✕

Network Settings 12 settings

Hostname	<p>Hostname to be configured on the LOC-A appliance. This is just the host part of the name, without the domain name suffix. This name should be resolvable by DNS.</p> <input style="width: 90%;" type="text" value="locaedge"/>
External Network IP	<p>IPv4 address of the external network interface of the appliance. This is the IP address used to access the LOC-A user interface. This is also the interface for the LOC-A appliance to access vCenter and ESXi hosts that are being installed.</p> <input style="width: 90%;" type="text" value="30.0.0.168"/>
External Network Netmask	<p>Netmask for the IPv4 address of the external interface.</p> <input style="width: 90%;" type="text" value="255.255.255.0"/>
External Network Gateway	<p>Gateway IPv4 address for the external interface.</p> <input style="width: 90%;" type="text" value="30.0.0.1"/>
XCC Network IP	<p>IPv4 address of the internal network interface used to access the XCC modules.</p> <input style="width: 90%;" type="text" value="192.168.0.10"/>
XCC Network Netmask	<p>Netmask for the IPv4 address of the XCC interface.</p> <input style="width: 90%;" type="text" value="255.255.255.0"/>
XCC Network Gateway	<p>Gateway IPv4 address for the xcc interface.</p> <input style="width: 90%;" type="text" value="192.168.0.1"/>
OS management Network IP	<p>IPv4 address of the internal network interface used to deploy os.</p> <input style="width: 90%;" type="text" value="30.0.0.169"/>
OS management Network Netmask	<p>Netmask for the IPv4 address of the OS management interface.</p> <input style="width: 90%;" type="text" value="255.255.255.0"/>
OS management Network Gateway	<p>Gateway IPv4 address for OS management interface.</p> <input style="width: 90%;" type="text" value="30.0.0.1"/>
DNS Server #1	<p>DNS server IP address.</p> <input style="width: 90%;" type="text" value="8.8.8.8"/>
DNS Server #2	<p>DNS server IP address.</p> <input style="width: 90%;" type="text"/>

CANCEL
BACK
NEXT

**Figure 4: Deployment properties for dedicated XCC network**



**Figure 5: Deployment properties for shared network**

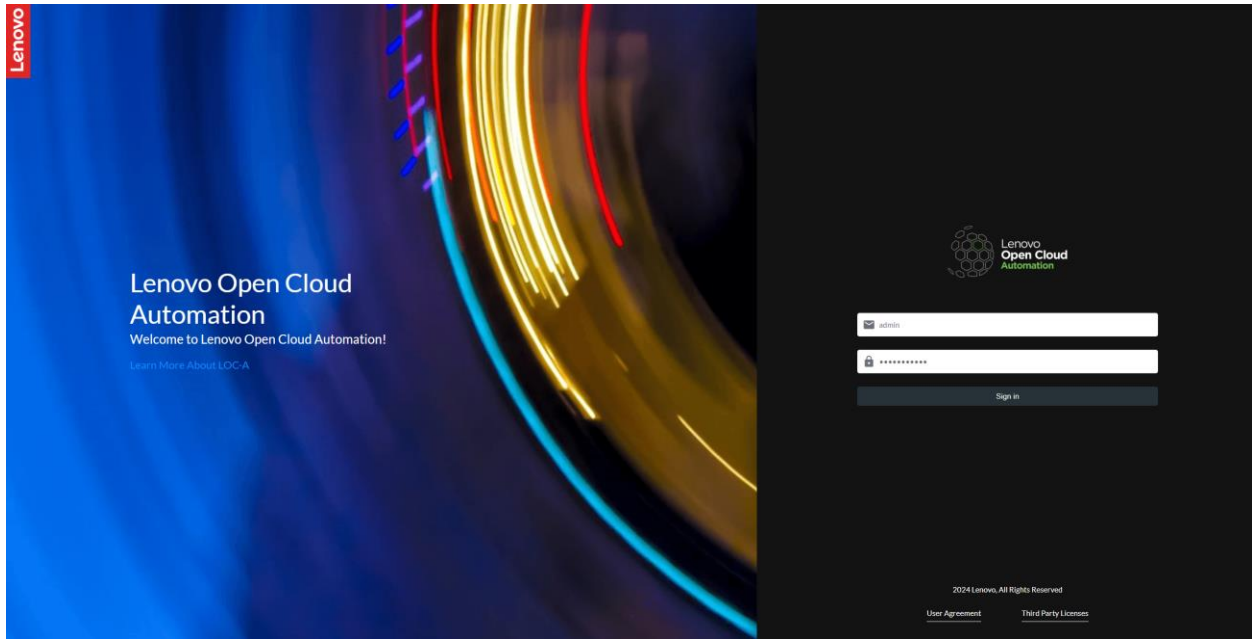
- i. Click **Next** to complete template customization.
- j. Review and accept the OVA installation by clicking **Finish** on the 'Ready to complete' screen. The OVA installation can take quite some time depending on the speed of your network.
- k. After the installation of the OVA completes, ensure 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://\[External Network IP\]](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**. See *User management* on page 86.



## 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
Lenovo Edge Computing Platform (LECP) Single Node	3.0	1

**Table 2: 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:

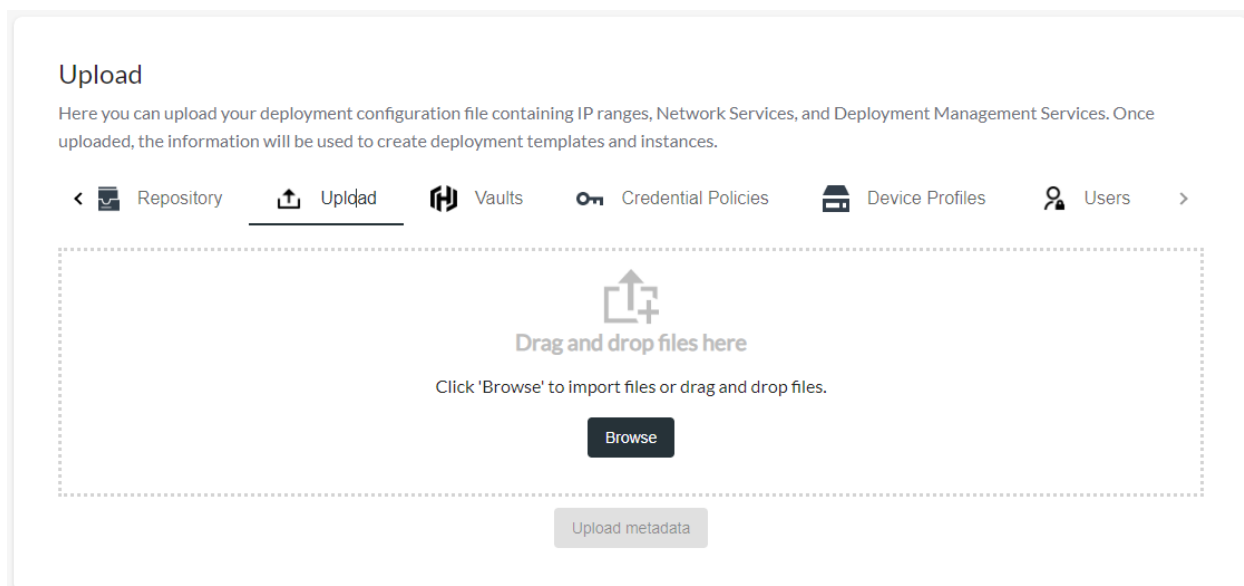
OS Family	Supported Versions	Minimum Nodes
Ubuntu	18.04, 20.04, 22.04	1
ESXi	7.0.3, 8.0.1	1
CentOS	7.9, 8.3	1

**Table 3: OS types supported by LOC-A**

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

Get the sample Excel file “Cloud\_Setup\_sample.xlsx” from Lenovo. Then follow the embedded instructions to fill in the file with the planning data for your edge sites. After filling in the file, upload the spreadsheet to LOC-A

1. From the LOC-A web interface, click **Setup**→**Upload**.
2. Click **Browse** to find the file that you updated.
3. Click **Upload metadata** to upload the template.



**Figure 7: 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 8 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 -> Province → City →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.

<input type="checkbox"/>	Name	Code	City	Province	Country/Region	Geo	Flavor	Deployment Readiness Status
<input type="checkbox"/>	shzj002	shzj002	Pudong	Shanghai	China	Asia	Bare Metal(ESXi)	notReady
<input type="checkbox"/>	buch001	buch001	Pudong	Juneau	USA	North America	VMware ThinkAgile VX Cluster(vSAN)	ready
<input type="checkbox"/>	buch002	buch002	Wuhan	Hubei	China	Asia	Bare Metal(ESXi)	ready
<input type="checkbox"/>	buch003	buch003	Montgomery	Alabama	USA	North America	Bare Metal(Ubuntu)	ready
<input type="checkbox"/>	buch004	buch004	Wuhan	Hubei	China	Asia	RedHat OpenShift Container Platform(OCP)	notReady
<input type="checkbox"/>	buch005	buch005	Pudong	Shanghai	China	Asia	Lenovo Edge Computing Platform(LECP) Single Node	notReady
<input type="checkbox"/>	bgsbuch001	bgsbuch001	Chuo	Tokyo	Japan	Asia	VMware ThinkAgile VX Cluster(vSAN)	notReady
<input type="checkbox"/>	bgsbuch002	bgsbuch002	Morrisville	North Carolina	USA	North America	RedHat OpenShift Container Platform(OCP)	notReady
<input type="checkbox"/>	bgsbuch003	bgsbuch003	Pudong	Shanghai	China	Asia	Lenovo Edge Computing Platform(LECP) Single Node	notReady
<input type="checkbox"/>	bgsbuch004	bgsbuch004	WestSide	Ottawa	Canada	North America	Bare Metal(Oracle)	ready

**Figure 8: 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 9 shows an example of the detailed explanations that can be shown.

<input type="checkbox"/>	Name	Code	City	Province	Country/Region	Geo	Flavor	Deployment Readiness Status
<input type="checkbox"/>	shzj002	shzj002	Pudong	Shanghai	China	Asia	Bare Metal(ESXi)	notReady
<input type="checkbox"/>	buch001	buch001	Pudong	Juneau	USA	North America	VMware ThinkAgile VX Cluster(vSAN)	network BMC doesn't exist network Management doesn't exist

**Figure 10: 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.

## Site Detail

Name	buch003
Site Code	buch003
Address	935 KAREN RD
Region	Montgomery/Alabama/USA/North America
GPS Coordinates	32.361668,-86.279167
Post Code	36109-4740
Time Zone	Dateline Standard Time
<hr/>	
Flavor	Bare Metal(Ubuntu)
Cloud Services	lxco_global,mgmt_hub,lxca_ro_qa,lxca_global,bgs_lxca001,lecp1,new-lxci
Custom Services	bgs_cst001,custom_service
Primary DNS Server	dns001s001buchx
Secondary DNS Server	
Primary NTP Service	pfSense.localdomain
Secondary NTP Service	
<hr/>	
IP Ranges	10.241.8.83/25 — 10.241.8.84/25 31.0.0.21/24 — 31.0.0.30/24 172.16.0.1/24 — 172.16.0.100/24 192.168.0.1/24 — 192.168.0.100/24 10.9.0.6/24 — 10.9.0.10/24

[Close](#)

**Figure 11: Site details**

### 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.

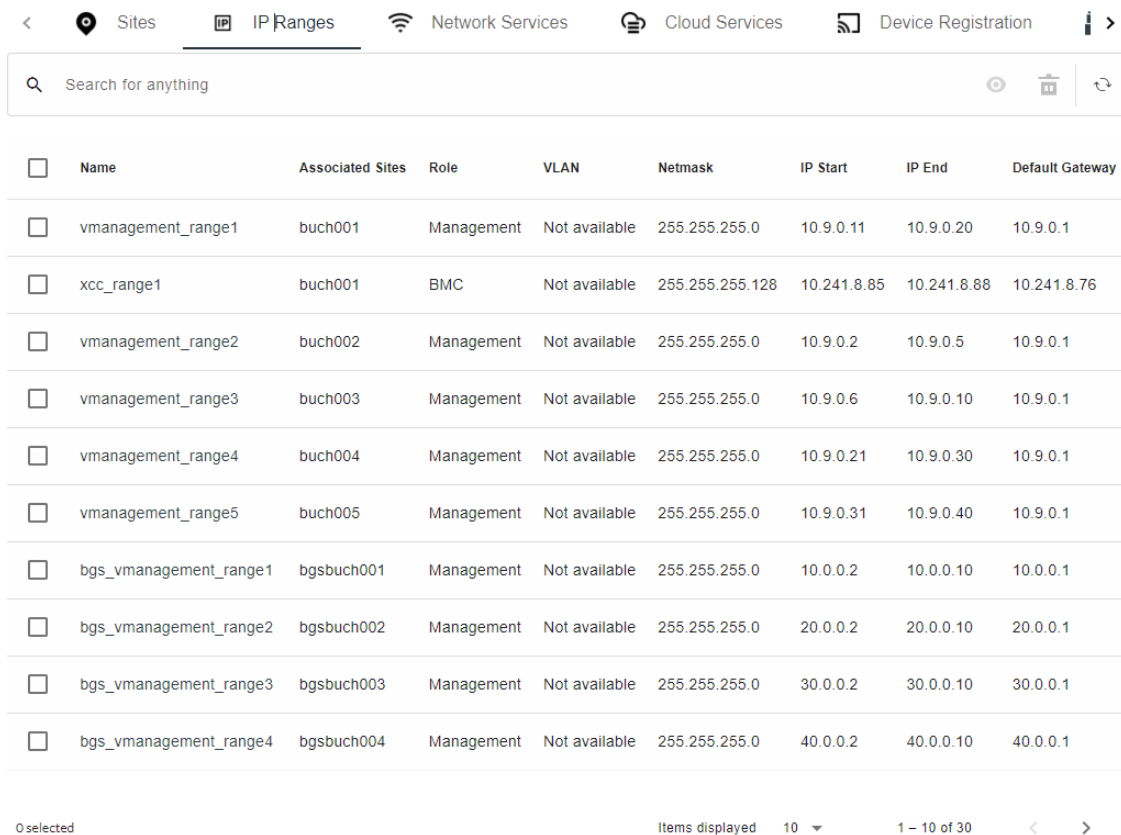
IP ranges will be associated to the site in the order of affinity. An IP range dedicated for a site has a higher affinity than an IP range designated for any site. For example:

- 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.

### IP Ranges

Here you can find the list of IP Ranges that will be used to define templates and configure deployment instances.



<input type="checkbox"/>	Name	Associated Sites	Role	VLAN	Netmask	IP Start	IP End	Default Gateway
<input type="checkbox"/>	vmanagement_range1	buch001	Management	Not available	255.255.255.0	10.9.0.11	10.9.0.20	10.9.0.1
<input type="checkbox"/>	xcc_range1	buch001	BMC	Not available	255.255.255.128	10.241.8.85	10.241.8.88	10.241.8.76
<input type="checkbox"/>	vmanagement_range2	buch002	Management	Not available	255.255.255.0	10.9.0.2	10.9.0.5	10.9.0.1
<input type="checkbox"/>	vmanagement_range3	buch003	Management	Not available	255.255.255.0	10.9.0.6	10.9.0.10	10.9.0.1
<input type="checkbox"/>	vmanagement_range4	buch004	Management	Not available	255.255.255.0	10.9.0.21	10.9.0.30	10.9.0.1
<input type="checkbox"/>	vmanagement_range5	buch005	Management	Not available	255.255.255.0	10.9.0.31	10.9.0.40	10.9.0.1
<input type="checkbox"/>	bgs_vmanagement_range1	bgsbuch001	Management	Not available	255.255.255.0	10.0.0.2	10.0.0.10	10.0.0.1
<input type="checkbox"/>	bgs_vmanagement_range2	bgsbuch002	Management	Not available	255.255.255.0	20.0.0.2	20.0.0.10	20.0.0.1
<input type="checkbox"/>	bgs_vmanagement_range3	bgsbuch003	Management	Not available	255.255.255.0	30.0.0.2	30.0.0.10	30.0.0.1
<input type="checkbox"/>	bgs_vmanagement_range4	bgsbuch004	Management	Not available	255.255.255.0	40.0.0.2	40.0.0.10	40.0.0.1

**Figure 12: 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 4 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
Lenovo LECP Single Node	Management	Node OS/management network	Yes	No	Yes
	BMC	XCC (BMC) management network	Yes	No	Yes
	cluster-mgmt	Cluster management network	Yes	Yes	No
	data	Cluster data network	Yes	Yes	No

**Table 4: 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.

## IP Range Detail

Name	vmanagement_range1
Site	buch001
Role	Management
VLAN	0
IP Start	10.9.0.11
IP End	10.9.0.20
Netmask	255.255.255.0
Default Gateway	10.9.0.1

Close

**Figure 13: IP range detail**

### 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 and LECP Single Node deployment, mandatory network services required for each site are:

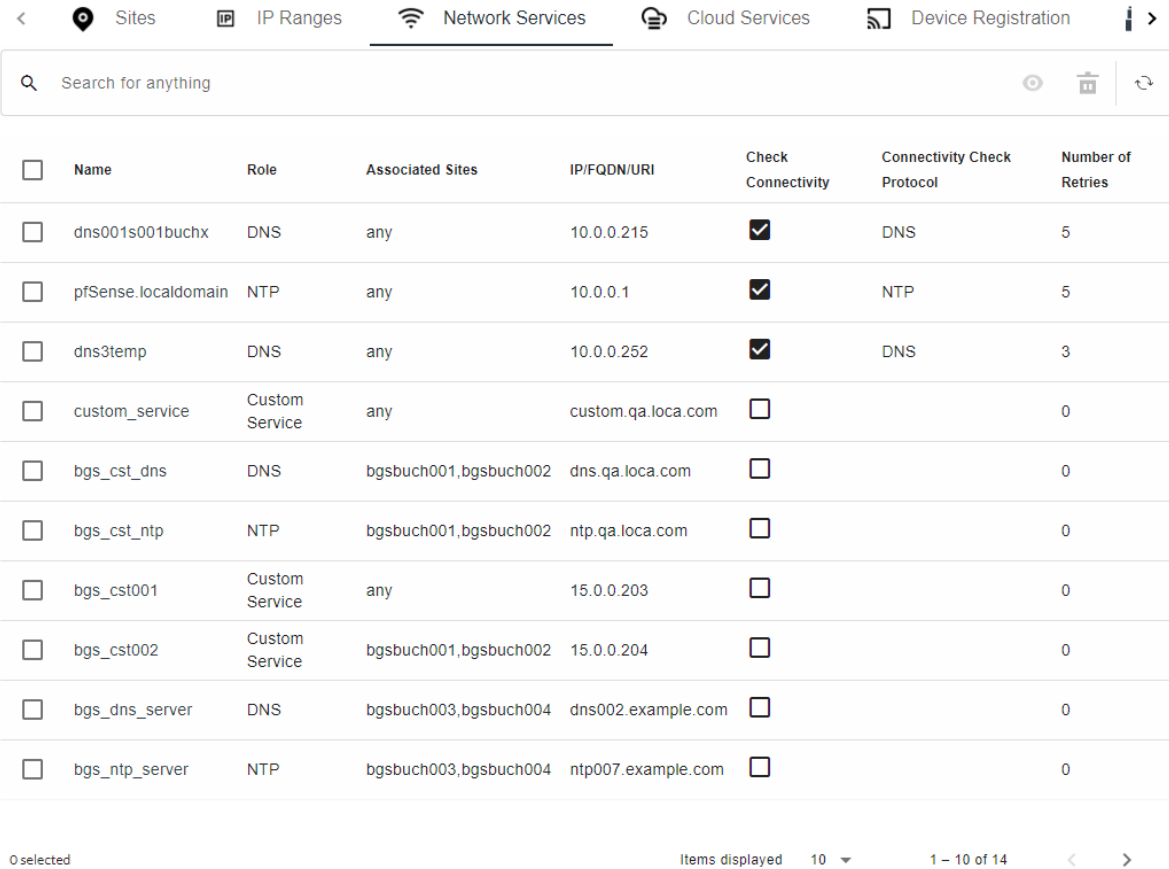
- One DNS server
- One NTP server

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 14 shows an example page that lists network services:

### Network Services

Here you can find the list of Network Services that will be used to define templates and configure deployment instances. The device registration process will check connectivity against the Network Services which have 'Check Connectivity' selected.



<input type="checkbox"/>	Name	Role	Associated Sites	IP/FQDN/URI	Check Connectivity	Connectivity Check Protocol	Number of Retries
<input type="checkbox"/>	dns001s001buchx	DNS	any	10.0.0.215	<input checked="" type="checkbox"/>	DNS	5
<input type="checkbox"/>	pfSense.localdomain	NTP	any	10.0.0.1	<input checked="" type="checkbox"/>	NTP	5
<input type="checkbox"/>	dns3temp	DNS	any	10.0.0.252	<input checked="" type="checkbox"/>	DNS	3
<input type="checkbox"/>	custom_service	Custom Service	any	custom.qa.loca.com	<input type="checkbox"/>		0
<input type="checkbox"/>	bgs_cst_dns	DNS	bgsbuch001,bgsbuch002	dns.qa.loca.com	<input type="checkbox"/>		0
<input type="checkbox"/>	bgs_cst_ntp	NTP	bgsbuch001,bgsbuch002	ntp.qa.loca.com	<input type="checkbox"/>		0
<input type="checkbox"/>	bgs_cst001	Custom Service	any	15.0.0.203	<input type="checkbox"/>		0
<input type="checkbox"/>	bgs_cst002	Custom Service	bgsbuch001,bgsbuch002	15.0.0.204	<input type="checkbox"/>		0
<input type="checkbox"/>	bgs_dns_server	DNS	bgsbuch003,bgsbuch004	dns002.example.com	<input type="checkbox"/>		0
<input type="checkbox"/>	bgs_ntp_server	NTP	bgsbuch003,bgsbuch004	ntp007.example.com	<input type="checkbox"/>		0

0 selected      Items displayed 10      1 - 10 of 14

**Figure 14: Network services list**

View a network service’s details:

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



# Network Service Detail

Name	dns3temp
Type	Network Service
Role	DNS
Site	any
IP/FQDN/URI	10.0.0.252
Check Connectivity	true
Number Of Retries	3

Close

**Figure 15: Network services detail**

## 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 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 <i>Adding devices into external hardware management tools</i> on page 53 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 <i>Adding devices into external hardware management tools</i> on page 53 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 <i>Adding devices into</i>

			<i>external hardware management tools</i> on page 53 for more information.
vCenter	VMware ThinkAgile VX Cluster(vSAN)	Yes, user must be administrator, username can be any	<p>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.</p> <p>vCenter selection policy during a new vSAN cluster deployment:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>
AssistedInstaller	RedHat OpenShift Container Platform(OCP)	No	<p>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.</p> <p>Refer to RedHat documentation on how to setup an AI instance.</p>
LECP Artifact Service	Lenovo Edge Computing Platform(LECP) Single Node	No	LECP Artifact Service is the repository server that hosts cluster deployment bundles. It is mandatory for LECP cluster deployment
LECP Deployer	Lenovo Edge Computing Platform(LECP) Single Node	No	LECP Deployer is the deployer for LECP single node. One LECP Deployer instance can be used to deploy multiple site clusters. It is mandatory for LECP cluster deployment.

**Table 5: Cloud Service Types supported by LOC-A**

Figure 16 shows the listing of cloud services on the Cloud Services page.

## Cloud Services

Here you can find the list of Deployment Management Services that will be used to define templates and configure deployment instances. The device registration process will check connectivity against the Deployment Management Services which have 'Check Connectivity' selected.

< Sites IP Ranges Network Services  **Cloud Services** Device Registration Repository Upload Vaults >

🔍 Search for anything

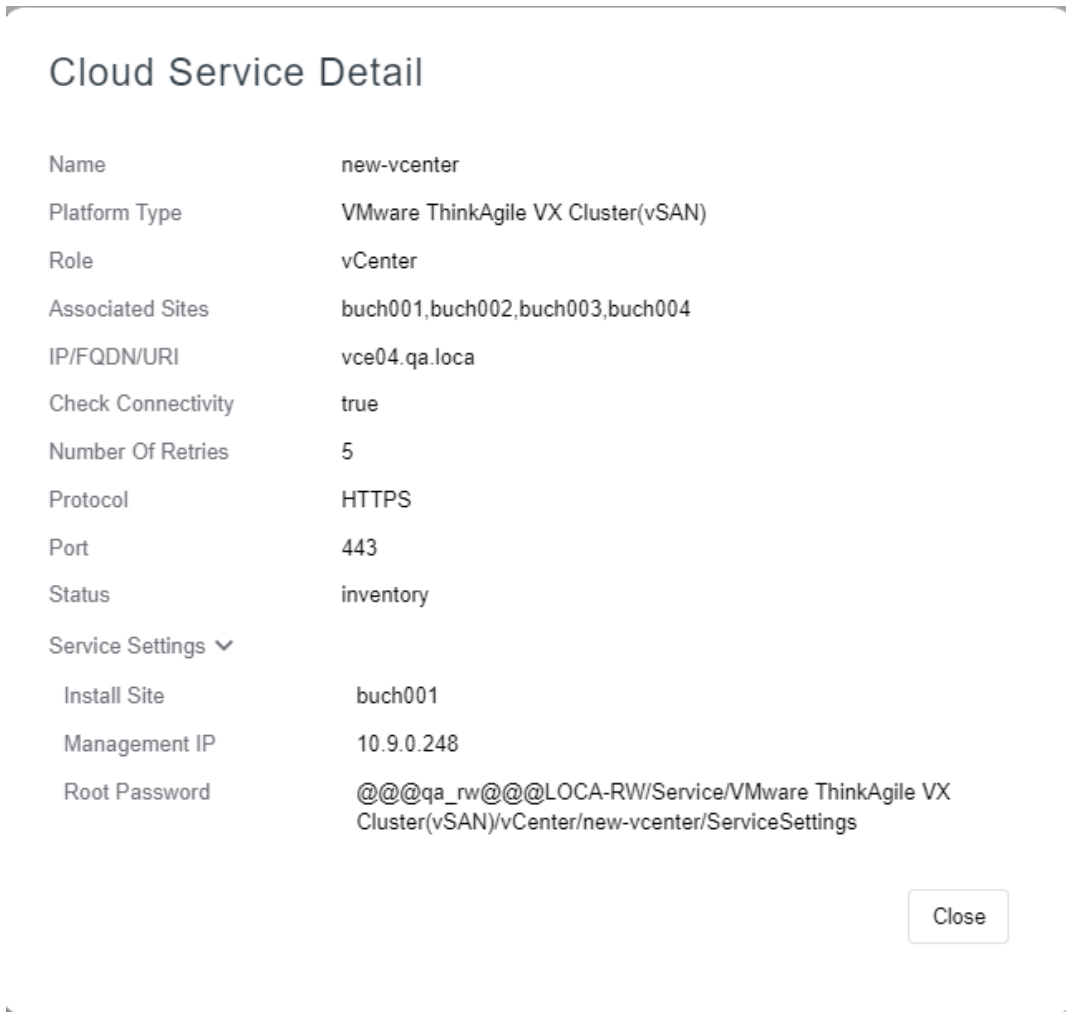
<input type="checkbox"/>	Name	Platform Type	Role	Associated Sites	IP/FQDN/URI	Check Connectivity	Credentials	Number of Retries	Status	Usage
<input type="checkbox"/>	lecp artifact services	Lenovo Edge Computing Platform(LECP) Single Node	LECP Artifact Service	bgsbuch003	10.121.16.36	<input checked="" type="checkbox"/>		3	active	Used in 0 instance
<input type="checkbox"/>	lecp deployer	Lenovo Edge Computing Platform(LECP) Single Node	LECP Deployer	bgsbuch003	30.0.100.10	<input checked="" type="checkbox"/>		3	active	Used in 0 instance
<input type="checkbox"/>	ocpai003	RedHat OpenShift Container Platform(OCP)	AssistedInstaller	buch004,bgsbuch002	10.240.207.115	<input checked="" type="checkbox"/>		3	active	Used in 0 instance
<input type="checkbox"/>	new-vcenter	VMware ThinkAgile VX Cluster(vSAN)	vCenter	buch001,buch002,buch003,buch004	vce04.qa.loc	<input checked="" type="checkbox"/>		5	inventory	Used in 0 instance
<input type="checkbox"/>	new-lxci	VMware ThinkAgile VX Cluster(vSAN)	Lenovo LXCI	buch001,buch002,buch003,buch004	lxci01.qa.loc	<input checked="" type="checkbox"/>		5	inventory	Used in 0 instance
<input type="checkbox"/>	lxca_ro_qa	Hardware management	Lenovo LXCA	buch001,buch002,buch003,buch004	10.0.0.217	<input checked="" type="checkbox"/>		2	active	Used in 0 instance
<input type="checkbox"/>	bgs_lxca	Hardware management	Lenovo LXCA	bgsbuch001,bgsbuch002	16.0.0.201	<input type="checkbox"/>		0	active	Used in 0 instance
<input type="checkbox"/>	bgs_vcenter	VMware ThinkAgile VX Cluster(vSAN)	vCenter	bgsbuch001,bgsbuch002	16.0.0.202	<input type="checkbox"/>		0	active	Used in 0 instance
<input type="checkbox"/>	bgs_lxca001	Hardware management	Lenovo LXCA	any	16.0.0.203	<input type="checkbox"/>		0	active	Used in 0 instance
<input type="checkbox"/>	bgs_lecp	Lenovo Edge Computing Platform(LECP) Single Node	LECP Deployer	any	16.0.0.204	<input type="checkbox"/>		0	active	Used in 0 instance

0 selected Items displayed 10 1 - 10 of 19 < >

**Figure 16: Cloud services list**

View a cloud service's details:

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



**Figure 17: Cloud service detail**

**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, Software Version, IP/FQDN/URI, Check Connectivity, Number of Retries, Protocol, Port, Credentials, Service Settings
Active	No	No	Any value	Site List, Software Version, IP/FQDN/URI, Check Connectivity, Number of Retries, Protocol, Port, Credentials, Service Settings
Active	Yes	Yes	Onboarded, Failed	Software Version, IP/FQDN/URI, Check Connectivity, Number of

				Retries, Protocol, Port, Credentials, Service Settings
--	--	--	--	--

**Table 6: 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.

Name	Platform Type	Role	Associated Sites	IP/FQDN/URI	Check Connectivity	Credentials	Number of Retries	Status	Usage
<input type="checkbox"/> lecp artifact services	Lenovo Edge Computing Platform(LECP) Single Node	LECP Artifact Service	bgsbuch003	10.121.16.36	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	active	Used in 0 instance
<input type="checkbox"/> lecp deployer	Lenovo Edge Computing Platform(LECP) Single Node	LECP Deployer	bgsbuch003	30.0.100.10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	active	Used in 0 instance
<input type="checkbox"/> ocpai003	RedHat OpenShift Container Platform(OCP)	AssistedInstaller	buch004,bgsbuch002	10.240.207.115	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	active	Used in 0 instance
<input checked="" type="checkbox"/> new-vcenter	VMware ThinkAgile VX Cluster(vSAN)	vCenter	buch001,buch002,buch003,buch004	vce04.qa.loca	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5	inventory	Used in 0 instance

**Figure 18: 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.

**Edit Cloud Service: new-vcenter**

Associated Sites\*  
buch001, buch002, buch003, buch004

IP/FQDN/URI\*  
vce04.qa.loca

Check Connectivity\*  
true

Number of Retries\*  
5

Protocol\*  
HTTPS

Port\*  
443

**Credentials**

Type  
APP

Account\*  
administrator@vsphere.

Password\*

**Service Settings**

Root Password\*  
@@@qa\_rw@@@LOCA-RW/Service/VMware ThinkAgile VX Cluster(v

Install Site\*  
buch001

Management IP\*  
10.9.0.248

Close Save

**Figure 19: Cloud Service editing page**

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

### Edit Cloud Service: new-vcenter

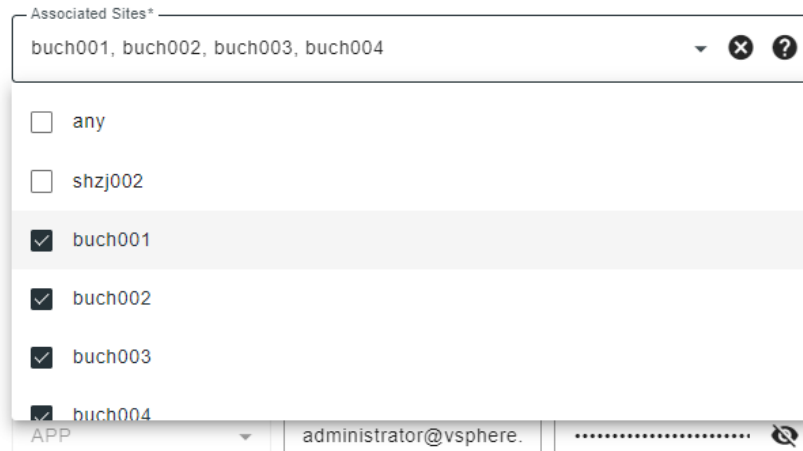


Figure 20: Site List of the cloud service

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

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



Figure 21: 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 **Software Version**:

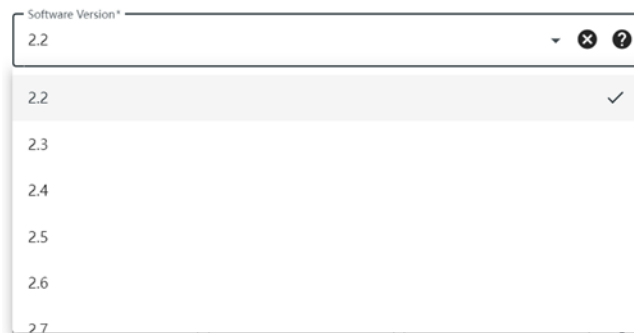


Figure 22: Software Version of the cloud service

**Note:** You can edit this field only when the cloud service role is **Lenovo LECP CMO**. The **Software Version** dropdown menu will not display for other types of cloud services.

6. Edit **Check Connectivity**:

A screenshot of a web form showing a dropdown menu for the field 'Check Connectivity\*'. The dropdown is open, and the value 'true' is selected. Below the dropdown, the labels 'Number of Retries\*', 'Protocol\*', and 'Port\*' are visible.

**Figure 23: 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.

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

A screenshot of the 'Number of Retries\*' input field. The field contains the number '3'. To the right of the input field are up and down arrow icons and a question mark icon.

**Figure 24: 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**.

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

A screenshot of the 'Protocol\*' dropdown menu. The dropdown is open, showing a list of protocols: DNS, NTP, HTTP, HTTPS, SSH, and PING. The 'HTTPS' option is selected and highlighted, with a checkmark icon next to it. Above the dropdown, the text 'Protocol\*' and 'HTTPS' are visible, along with a clear (X) icon and a question mark icon.

**Figure 25: Protocol of the cloud service**

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

9. Edit **Port**:



**Figure 26: 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**.

10. Edit **Credentials**:

**Figure 27: Credentials of the cloud service**

- You will only be allowed to edit credentials for the type supported by this cloud service. The value of **Type** can be **OS** or **APP**.
- Click the input of the account field to edit the **Account** for the specified credential.
- 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.



11. Edit **Service Settings**:

**Figure 28: 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.

Service Settings


Root Password\*

@@@qa\_rw@@@LOCA-RW/Service/VMware ThinkAgile VX Cluster(v)  

Install Site\*

buch001  

Management IP\*



**X** This field is required

**Figure 29: Service Settings check**

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

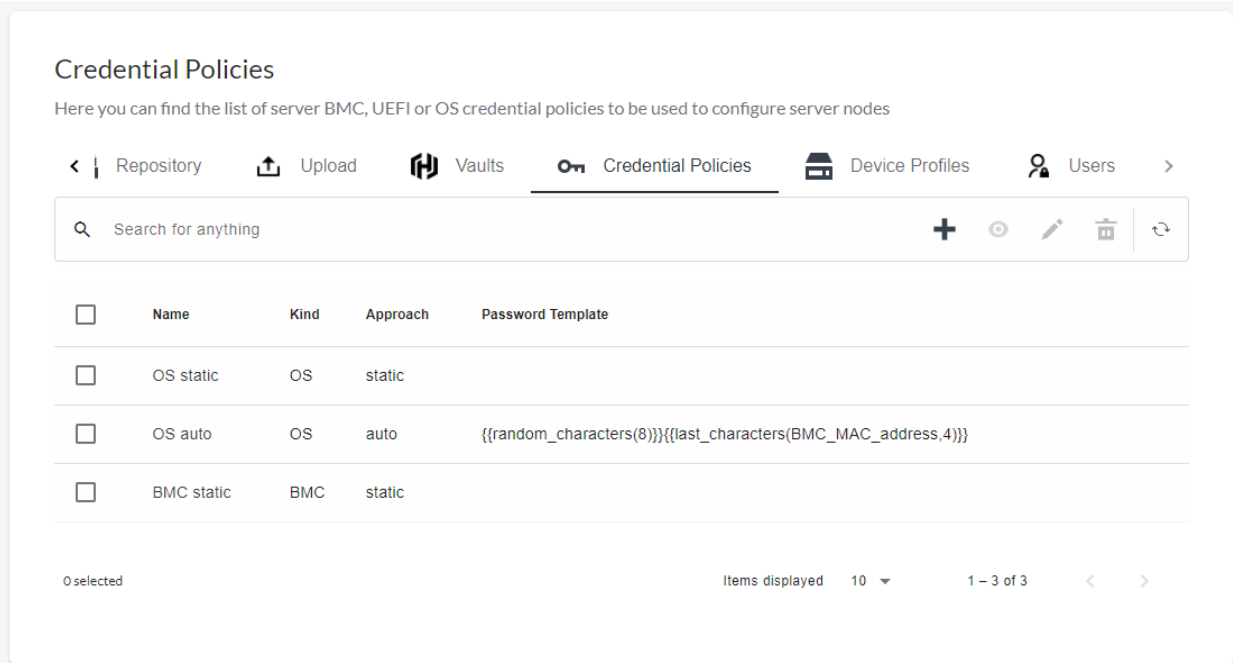
**Note:**

- 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 30: 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.

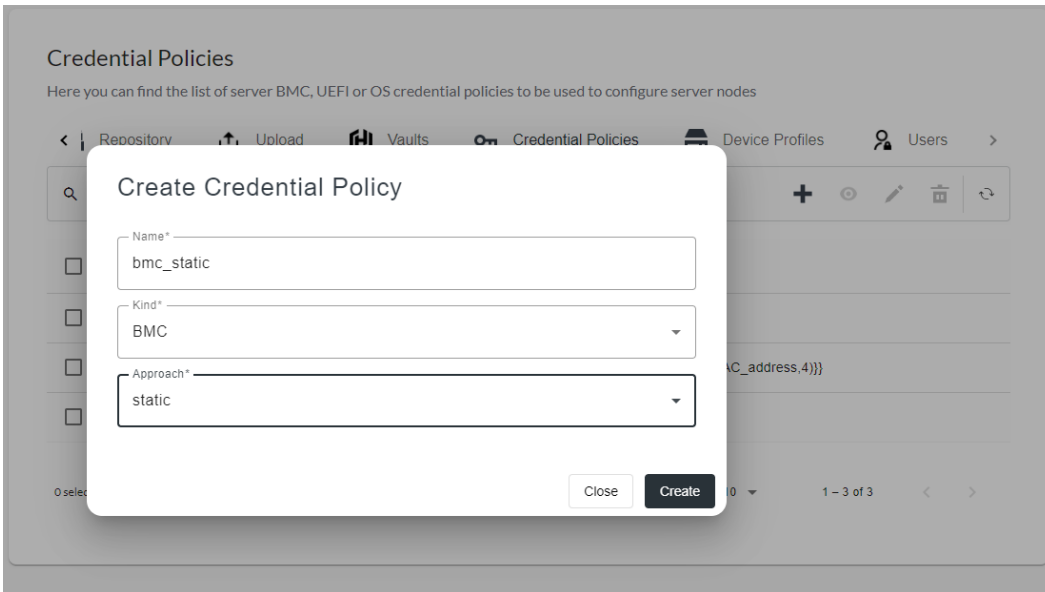
Note: **Kind** is a dropdown list that includes three types, which are **BMC**, **UEFI** and **OS**.

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

Note:

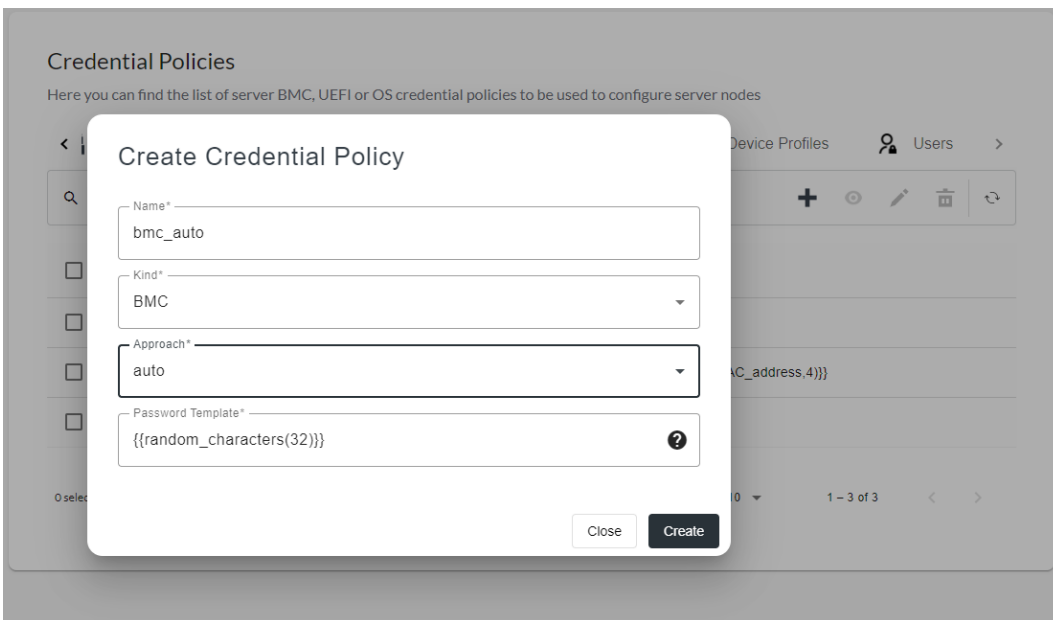
- a. **Approach** includes **static**, **auto**, and **publicKey**. **Static** indicates the need for manual password input, **auto** requires the input of password template, and **publicKey** indicates the use of public key.
  - b. Starting from LOC-A 3.1, you will not be allowed to create **auto** 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 31: Credential Policy creation with the approach of static**

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



**Figure 32: 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:

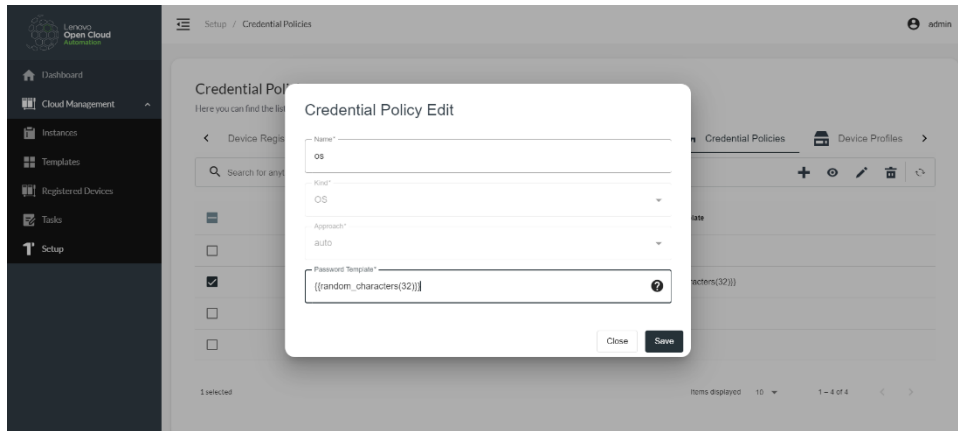
- Supported built-in template variables that can be used are:
  - `{{random_characters(N)}}`: where N is the length of the random string. For example `{{random_characters(32)}}` will be a random string of 32 characters.
  - `{{last_characters(BMC_MAC_address,N)}}`: where N is the length of the last characters 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 33: 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:

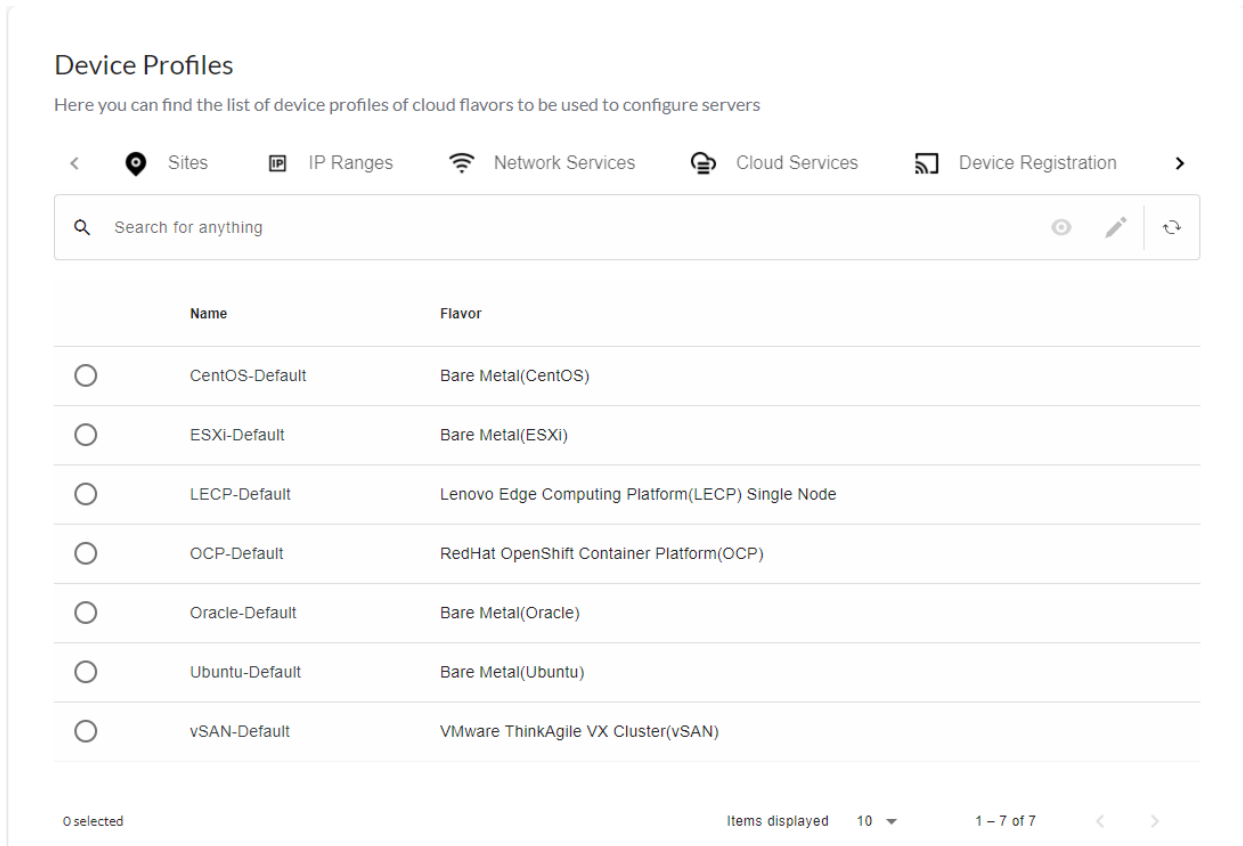
1. Click **Setup** → **Credential Policies**, select a credential policy, click on the **Delete** icon in the upper right corner.
2. Click Delete button to confirm deletion.

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 has built-in default device profiles for each flavor. A device profile defines the server BMC and UEFI configurations for the cloud flavor. Device profile can be optionally specified when creating templates and the BMC/UEFI configurations defined in the device profile will be applied when deploying the cloud/OS instances.

LOC-A does not support creating or deleting a device profile, but the BMC/UEFI configuration settings in the device profile can be partially customized by the users.



**Figure 34: Device Profiles list**

### 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, and then click save.

**Figure 35: Device Profile edit**

**Note:**

- After modifying the device profile, the template currently using that device profile will also be updated but deployed instances will continue to use the old device profile.
- For the SE455 v3 model, configuring Server Operating Mode in the device profile is not supported. Please remove the Server Operating Mode setting from the device profile before you attempt to apply it to ThinkEdge SE455 v3 servers.
- When deploying Centos8.3 on SE350v2, SE360v2, SE455v3, SE350 models, it is not supported to enable secure boot configuration. So it is necessary to turn off the secure boot in the device profile in advance.
- When deploying RedHat OCP on the SE450 model, it is not supported to enable secure boot configuration. So it is necessary to turn off secure boot in advance in the device profile.
- When deploying Ubuntu18.04 on SE450 models, it is not supported to enable secure boot configuration. So it is necessary to turn off the secure boot in the device profile in advance.

## 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 37.

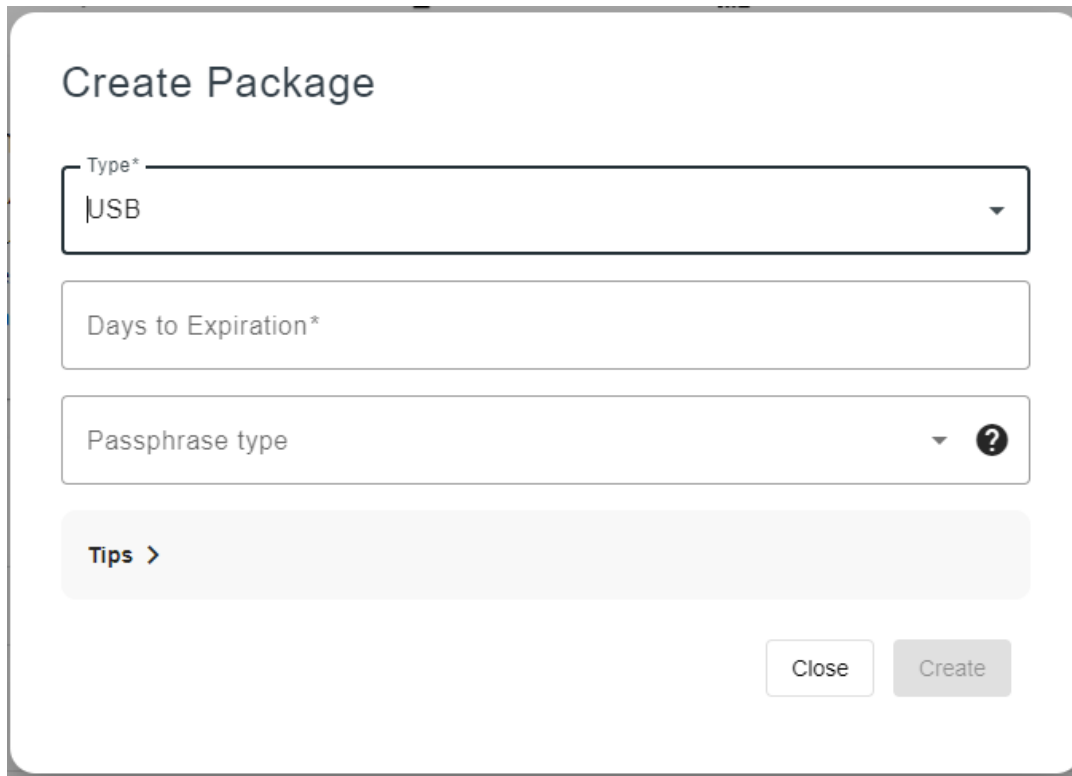
The LOC-A registration package contains site metadata information and other necessary artifacts for nZTP device registration. After importing the edge sites resources metadata, you can generate and then download the LOC-A registration package to facilitate edge-site server node registration.

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.



The screenshot shows a 'Create Package' form with the following elements:

- Title:** Create Package
- Type\*:** A dropdown menu with 'USB' selected.
- Days to Expiration\*:** An empty text input field.
- Passphrase type:** A dropdown menu with a question mark icon.
- Tips >:** A link to view tips.
- Buttons:** 'Close' and 'Create' buttons at the bottom right.

**Figure 36: 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 37 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.



## Registration Package List

Name	Type	Expire Time	Passphrase	Create Time	BMC Password Policy	UEFI Password Policy
<input type="radio"/> Register-Mini-Image	ThinkShield	2024-07-18		2024-06-15 17:30:38	BMC auto	
<input type="radio"/> Register-Mini-Image	USB	2024-06-14		2024-06-13 18:10:02		

0 selected Items displayed 10 1 - 2 of 2

**Figure 37: 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.

## Create Package

Type\*  
ThinkShield

Days to Expiration\*  
31

Passphrase type  
Auto-generate passphrase

BMC New Password Policy\*  
BMC static

BMC New Password\*  
.....

Confirm New Password  
.....

UEFI New Password Policy\*

Preload OS image to XCC

Tips >

Close Create

**Figure 38: 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 37 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 Sideload* section below for more details.

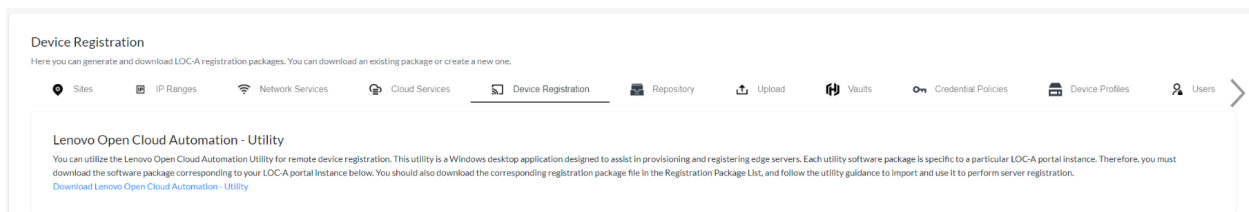
Click **Create** to start generating the package. It usually takes several minutes for the task to complete.

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 39: 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 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.

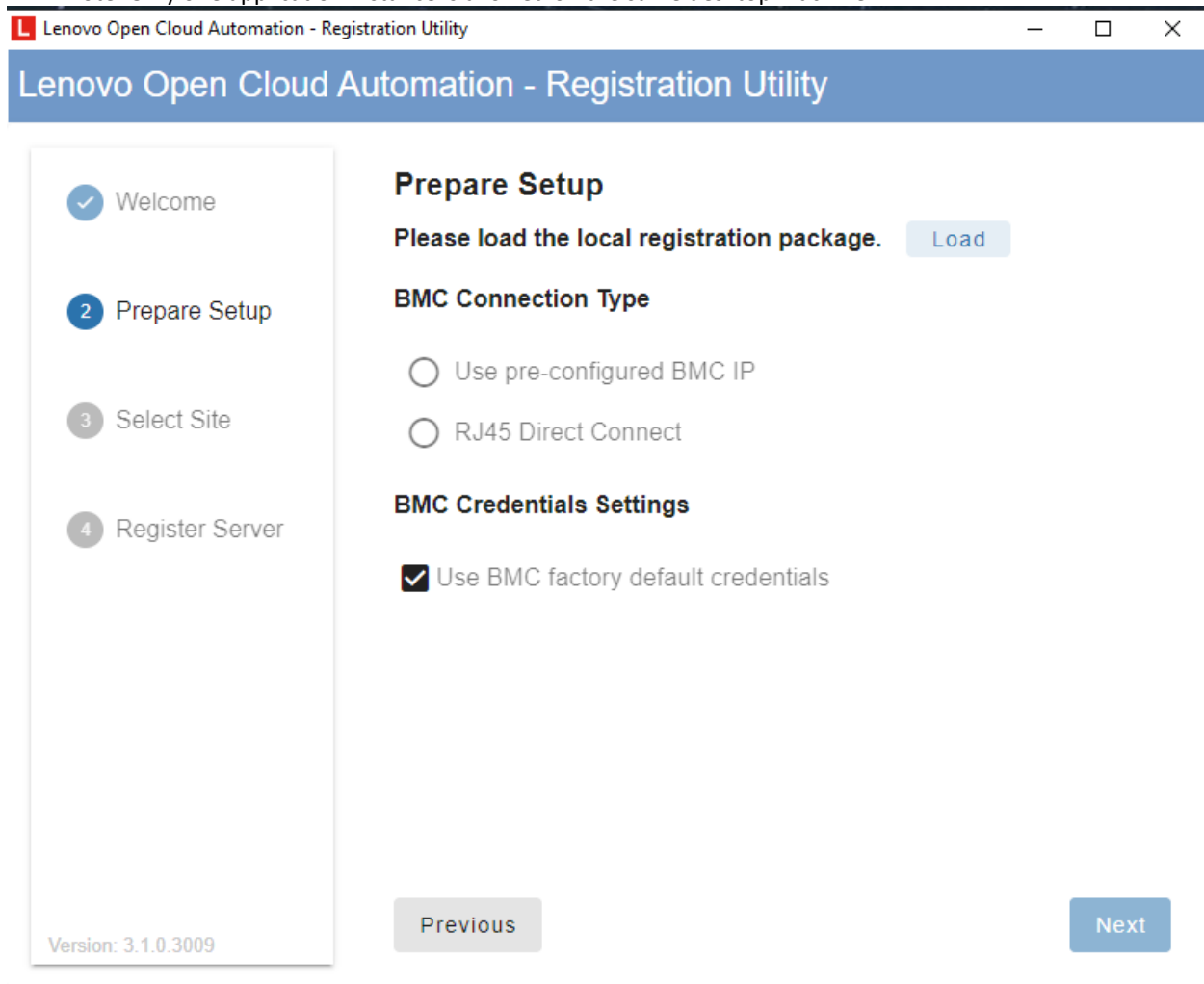
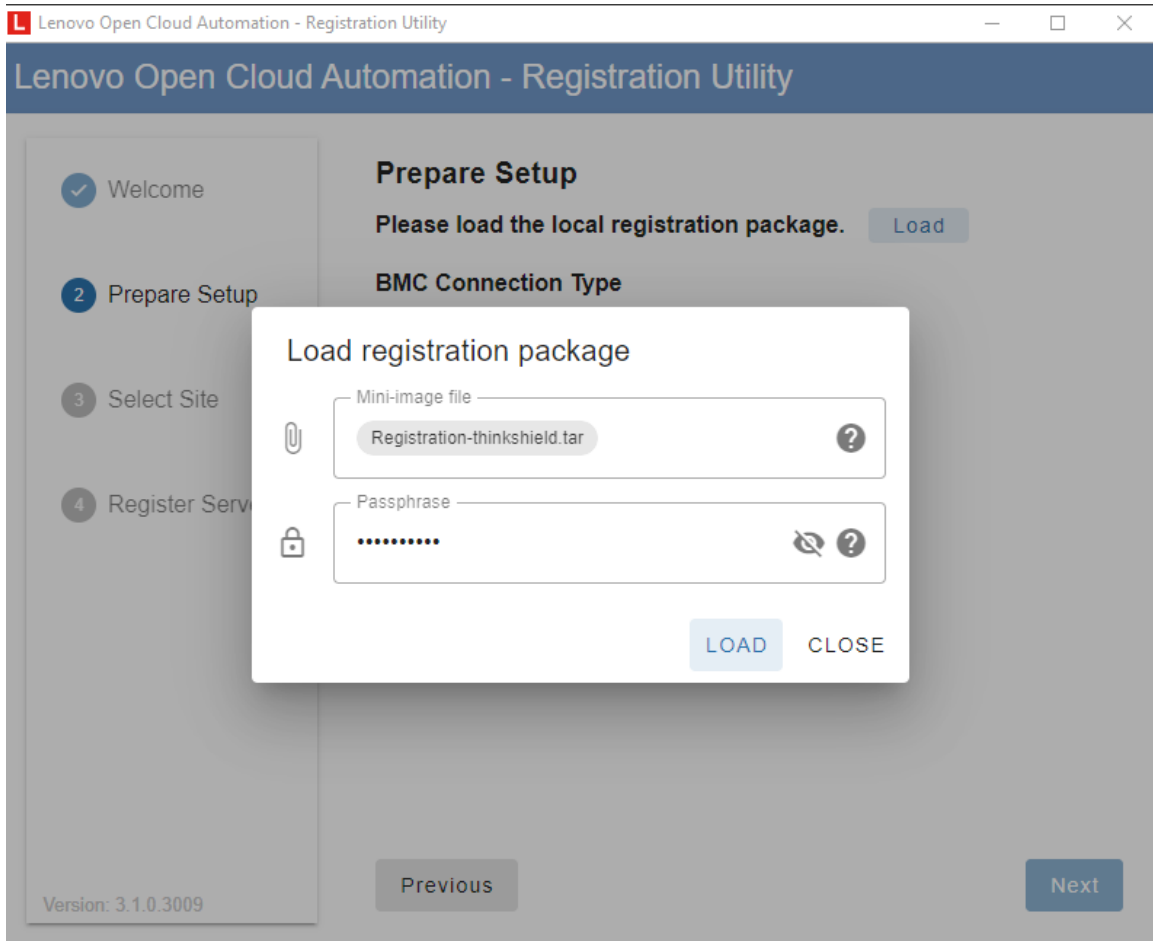


Figure 40: LOC-A Utility - Prepare Setup

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 41: 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.

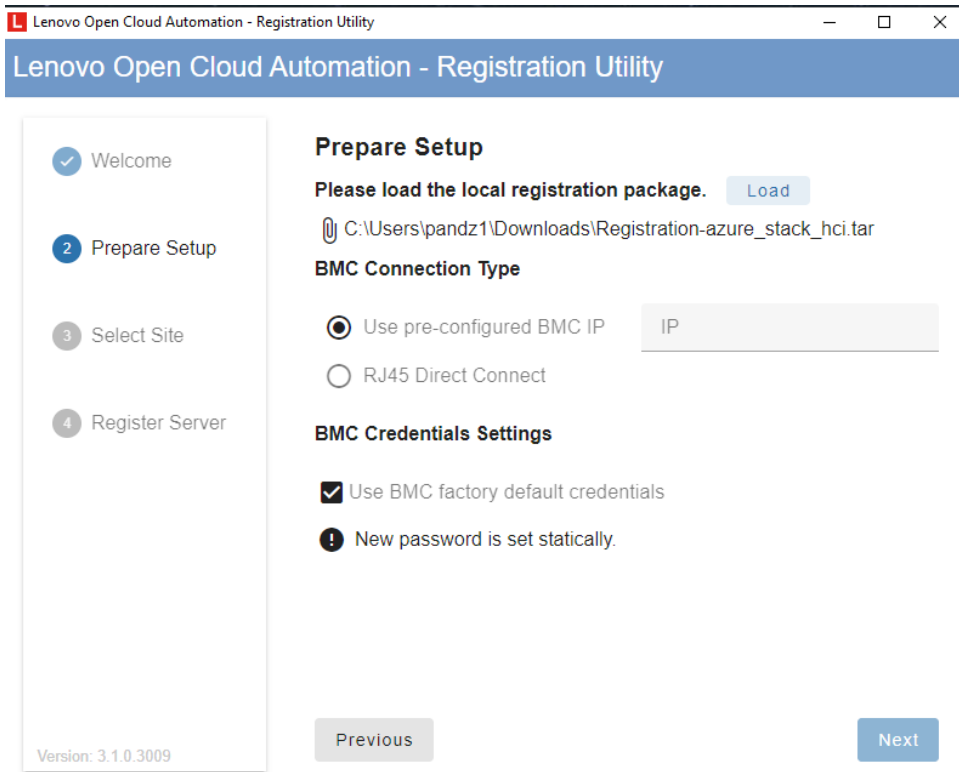


Figure 42: Use pre-configured BMC IP

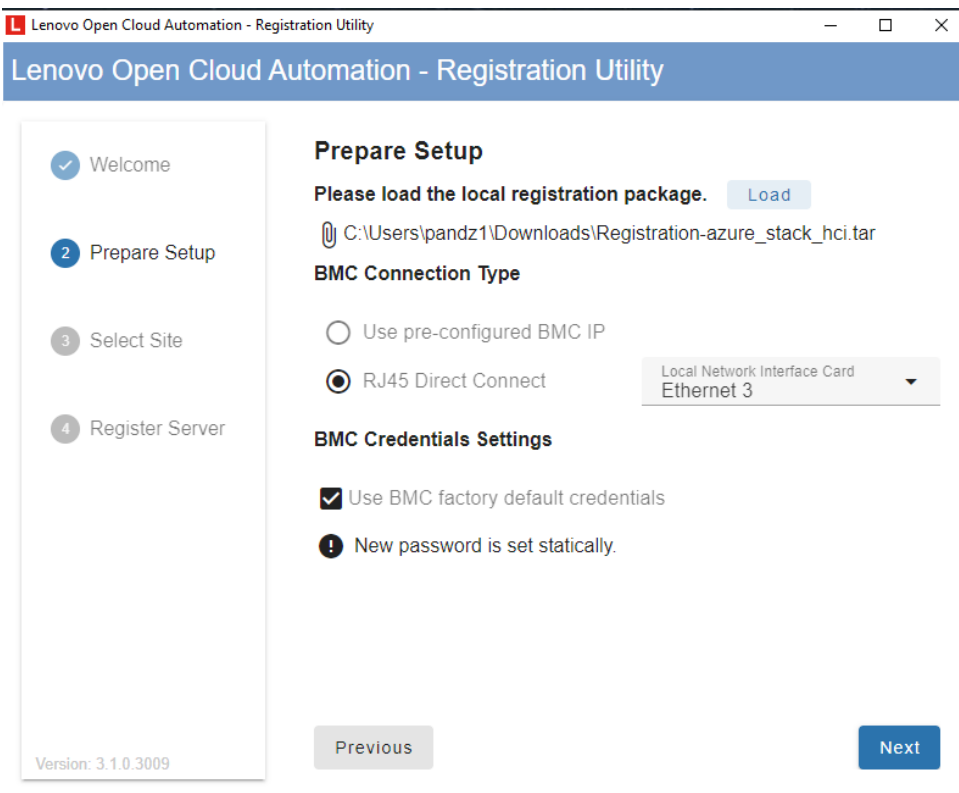


Figure 43: RJ45 Direct Connect

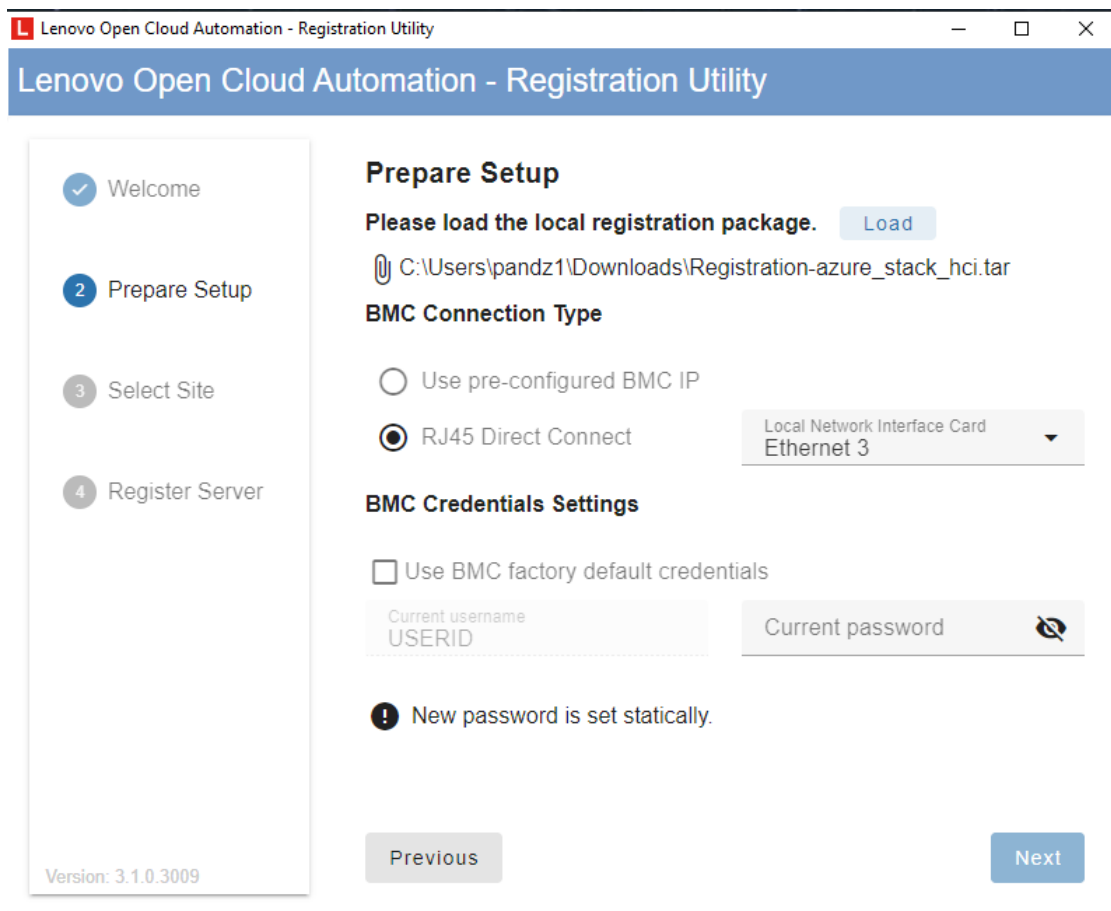
#### 4. Configure BMC Credentials Settings

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 PASSWORD (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 44: 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.

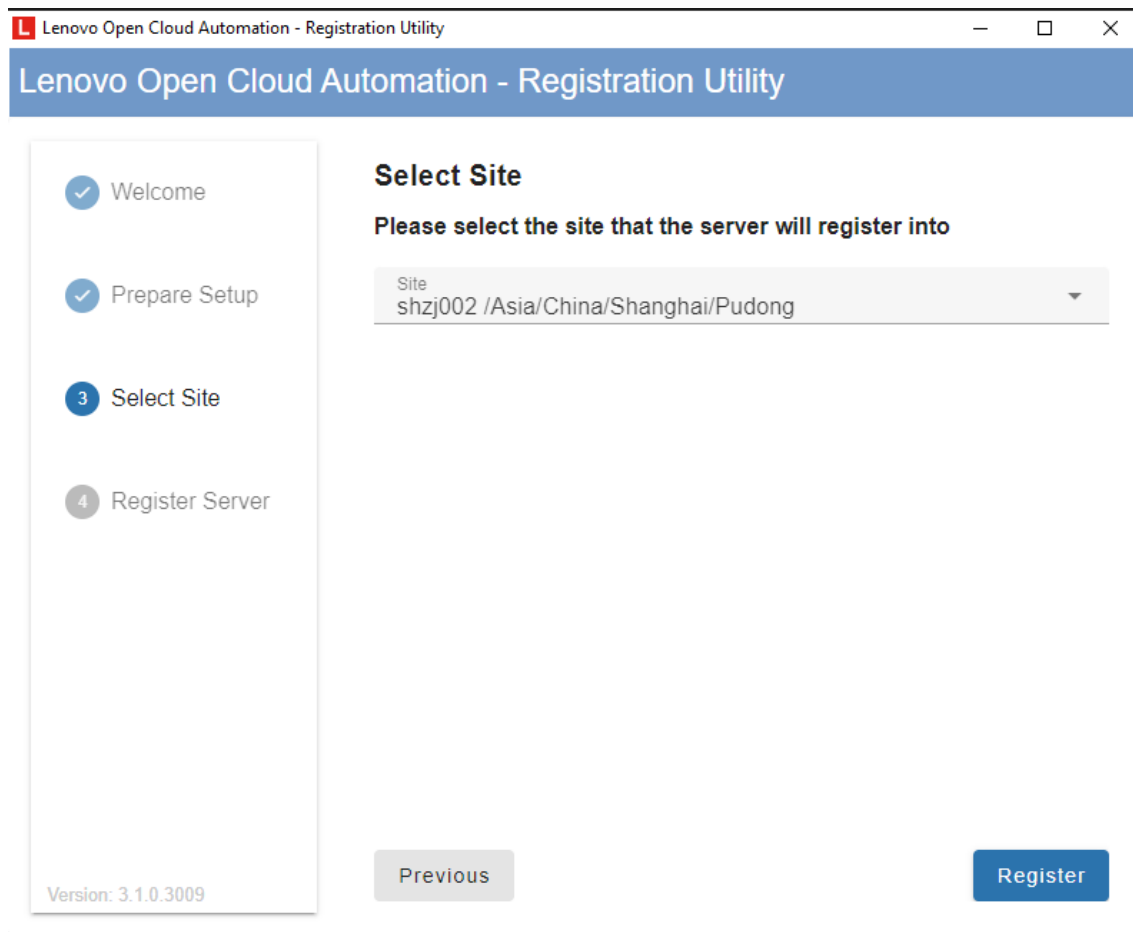


Figure 45: Select Site

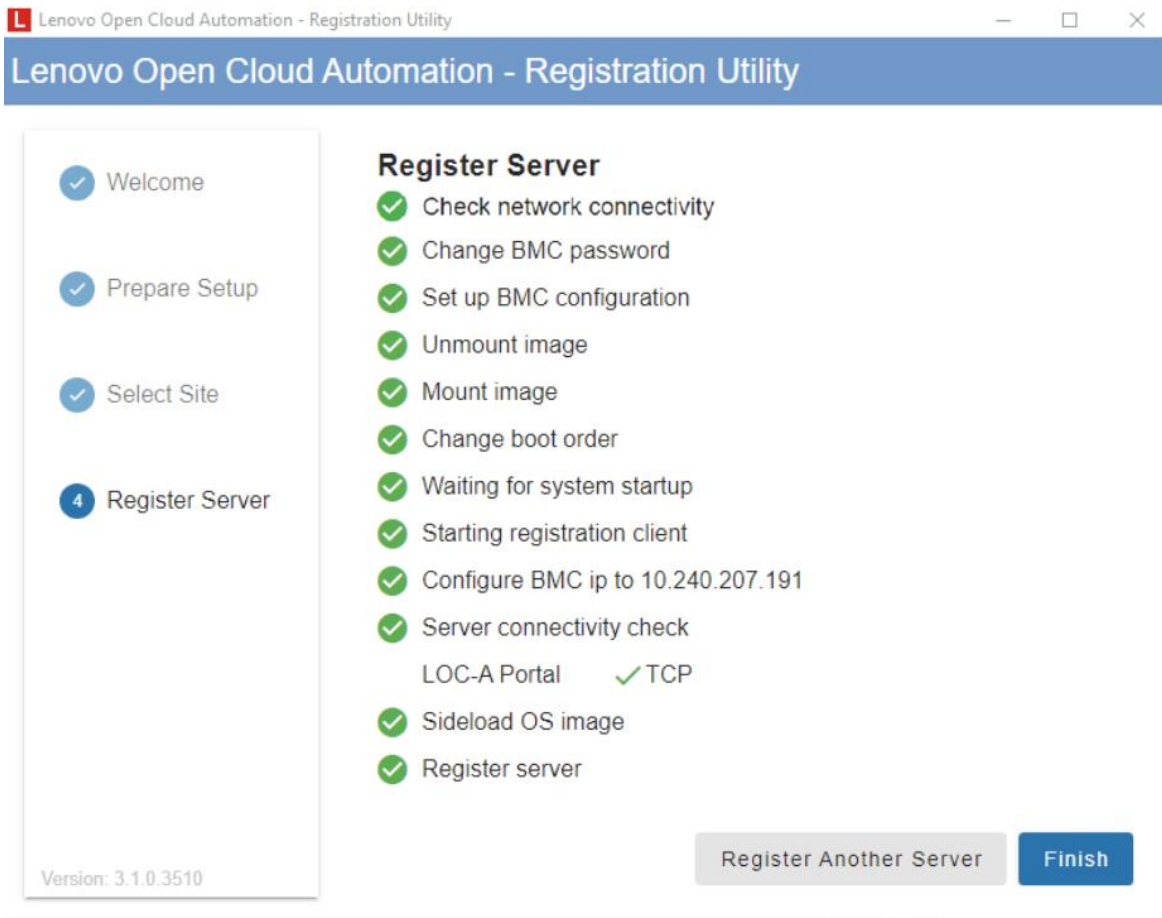
## 6. Server Registration

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.

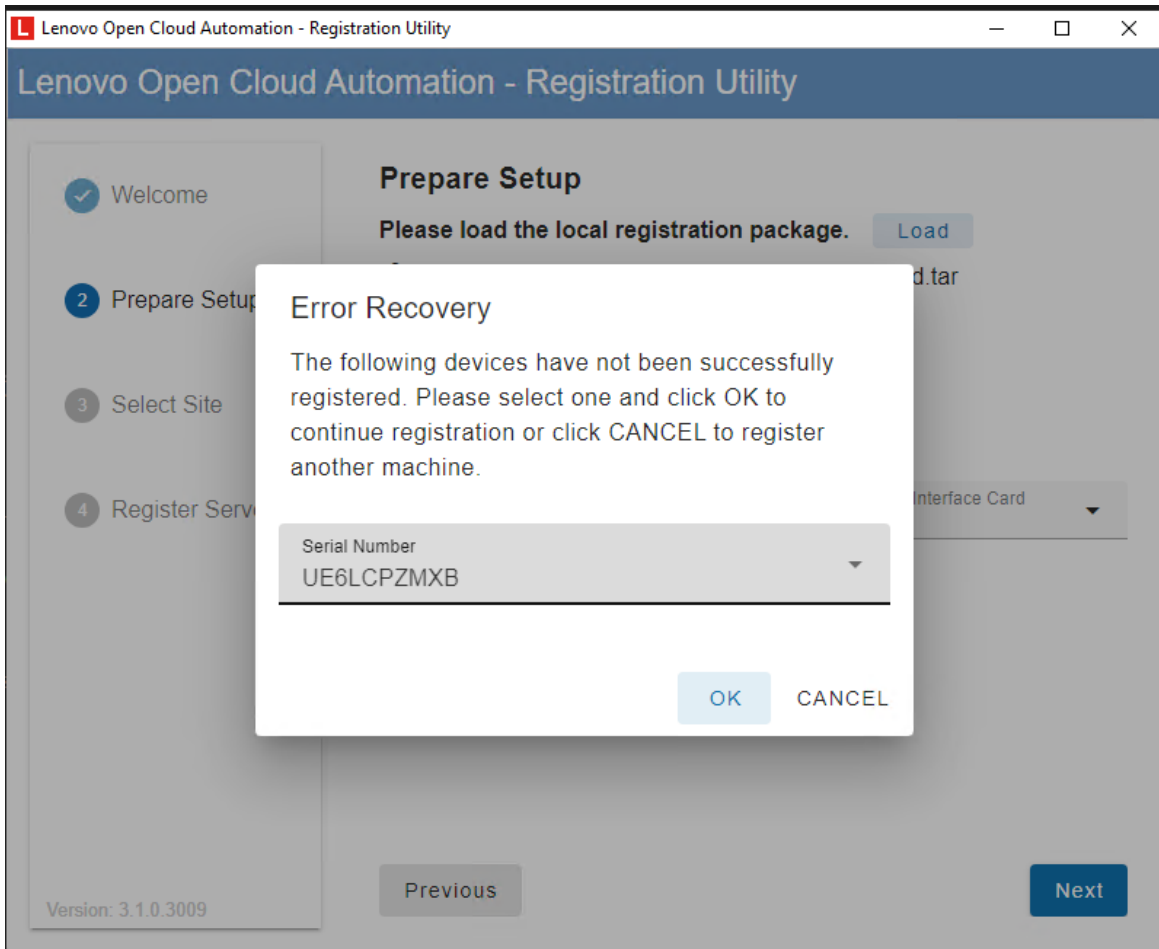




**Figure 46: Register server through LOC-A Utility**

## 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 47: Error recovery**

## Log

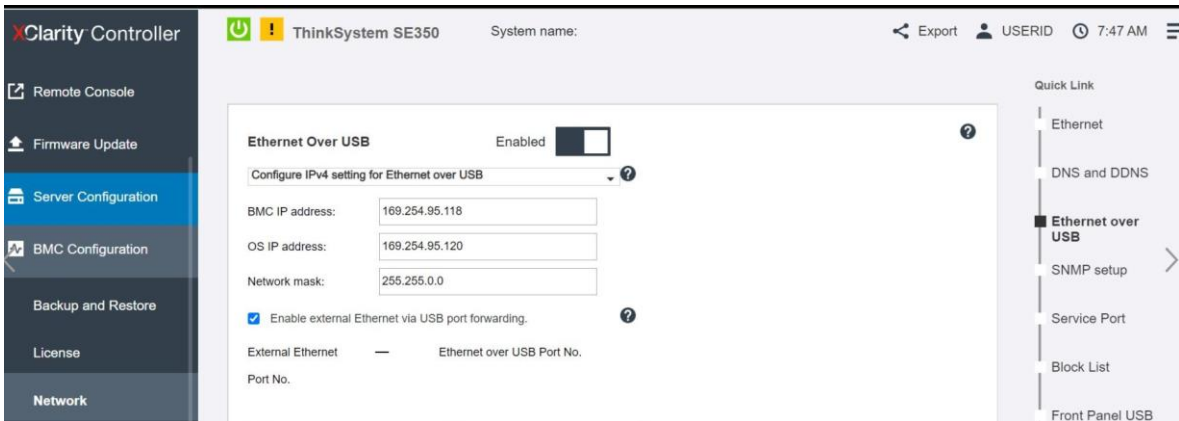
The logs for the LOC-A Utility are located at: `C:\Users\%USERPROFILE%\Documents\LOCA_UTILITY_logs\xxx.log`. In case you need Lenovo Support, please send the log file to the Lenovo support team. Max size of the log file is 1M, when the max size is reached, it will be backed up to `xxx.old.log`. Only 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 48: Ethernet Over USB shows an example configuration through the XCC user interface.



**Figure 48: 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 49: 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.

```

Welcome to Lenovo Registration Client
input encryption password[*****]:*****
Please input BMC password:*****
Please input new BMC password:*****
Site: buch001   Geo: /North America/USA/Juneau/Pudong
Site: buch002   Geo: /Asia/China/Hubei/Wuhan
Site: buch003   Geo: /North America/USA/Alabama/Montgomery
Site: buch004   Geo: /Asia/China/Hubei/Wuhan
Site: buch005   Geo: /Asia/China/Shanghai/Pudong
Site: bgsbuch001   Geo: /Asia/Japan/Tokyo/Chuo
Site: bgsbuch002   Geo: /North America/USA/North Carolina/Morrisville
Site: bgsbuch003   Geo: /Asia/China/Shanghai/Pudong
Site: bgsbuch004   Geo: /North America/Canada/Ottawa/
Site: bgsbuch005   Geo: /Asia/Japan/Osaka/Fukushima
input site location[site]:buch001_

```

Figure 50: 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).

```

Please select an action:1
Site: buch001   Geo: /North America/USA/Juneau/Pudong
Site: buch002   Geo: /Asia/China/Hubei/Wuhan
Site: buch003   Geo: /North America/USA/Alabama/Montgomery
Site: buch004   Geo: /Asia/China/Hubei/Wuhan
Site: buch005   Geo: /Asia/China/Shanghai/Pudong
Site: bgsbuch001   Geo: /Asia/Japan/Tokyo/Chuo
Site: bgsbuch002   Geo: /North America/USA/North Carolina/Morrisville
Site: bgsbuch003   Geo: /Asia/China/Shanghai/Pudong
Site: bgsbuch004   Geo: /North America/Canada/Ottawa/
Site: bgsbuch005   Geo: /Asia/Japan/Osaka/Fukushima
input site location[site]:buch001
input BMC ip[169.254.95.118]:
input BMC password [*****]:*****

1. config the server
2. connectivity check
3. register the server
4. update customer site
5. config BMC ip
0. exit
Please select an action:

```

Figure 51: 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.

```
UDP Port:53 Protocol:dns Status:success
Target: 10.0.0.1 pfSense.localdomain
UDP Port:123 Protocol:ntp Status:success
Target: 10.9.0.222 LOC-A Portal
TCP Port:443 Protocol:https Status: success

1. config the server
2. connectivity check
3. register the server
4. update customer site
5. config BMC ip
0. exit
Please select an action:3
Registration is started, please be patient
-> Successfully registered the server to LOCA: https://10.9.0.222

1. config the server
2. connectivity check
3. register the server
4. update customer site
5. config BMC ip
0. exit
```

Figure 52: 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.

```
5. config xcc ip
0. exit
Please select an action:4
Trying to update site infomation from registration server, please be patient
Site information is updated

1. config the server
2. connectivity check
3. register the server
4. update customer site
5. config xcc ip
0. exit
Please select an action:5
('gateway': '10.240.206.1', 'ip': '10.240.206.228', 'netmask': '255.255.255.0')
set xcc ip to :10.240.206.228

1. config the server
2. connectivity check
3. register the server
4. update customer site
5. config xcc ip
0. exit
Please select an action:
```

Figure 53: Config the server

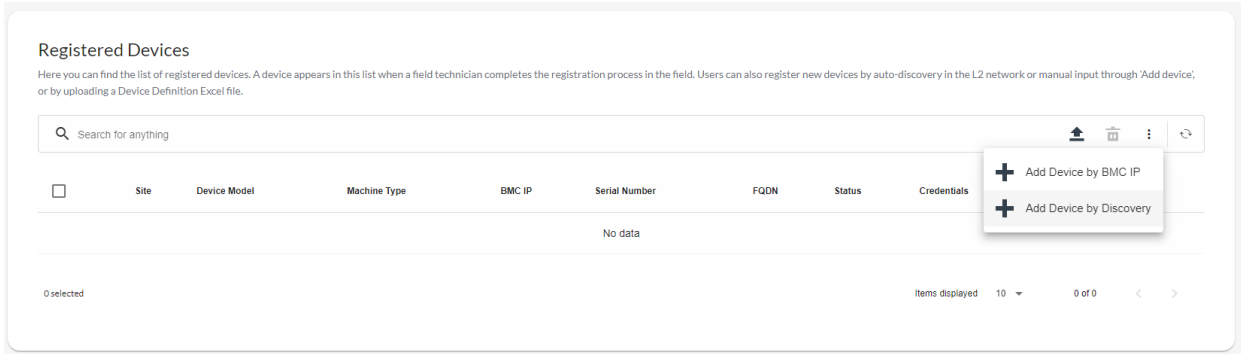
- f. Reconfigure the server (optional).  
If the server registration failed because of an incorrect configuration, such as selecting the wrong site or entering the wrong credentials, use action 1 (config the server) to reconfigure the server.
- g. Update customer site (optional)  
If the site information 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 and add them into LOC-A inventory. Complete the following steps to register devices through automatic discovery:

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

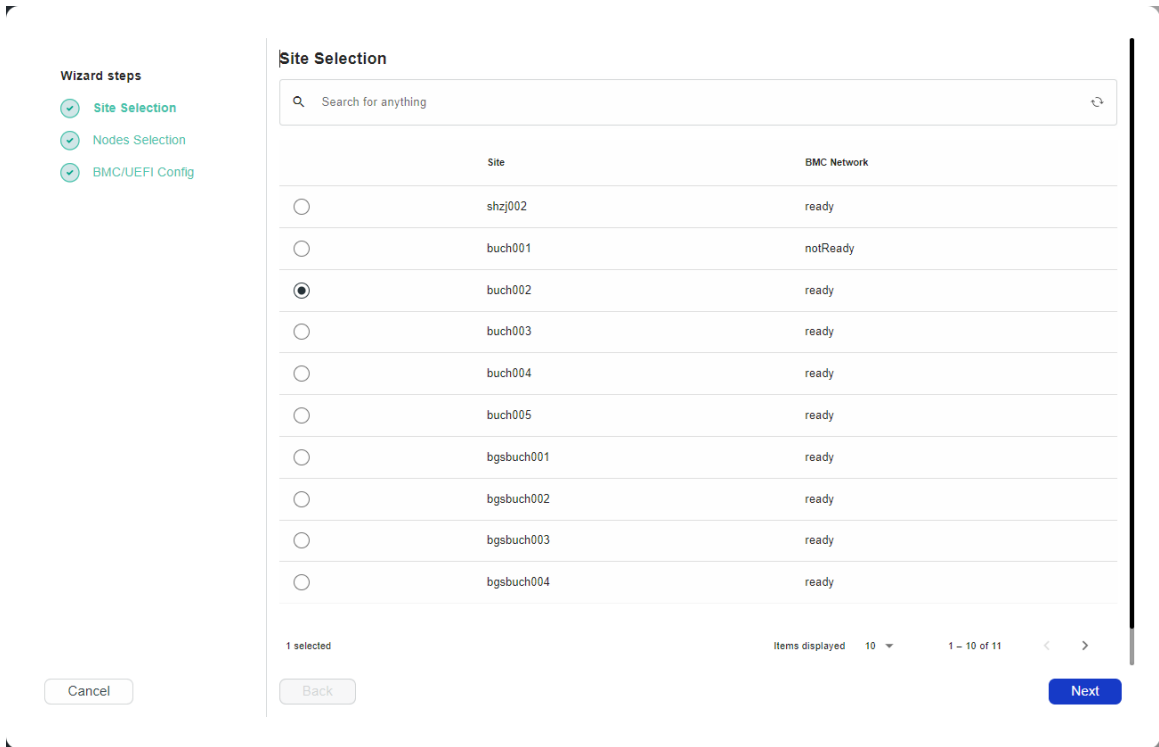


**Figure 54: Add devices by discovery**

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.

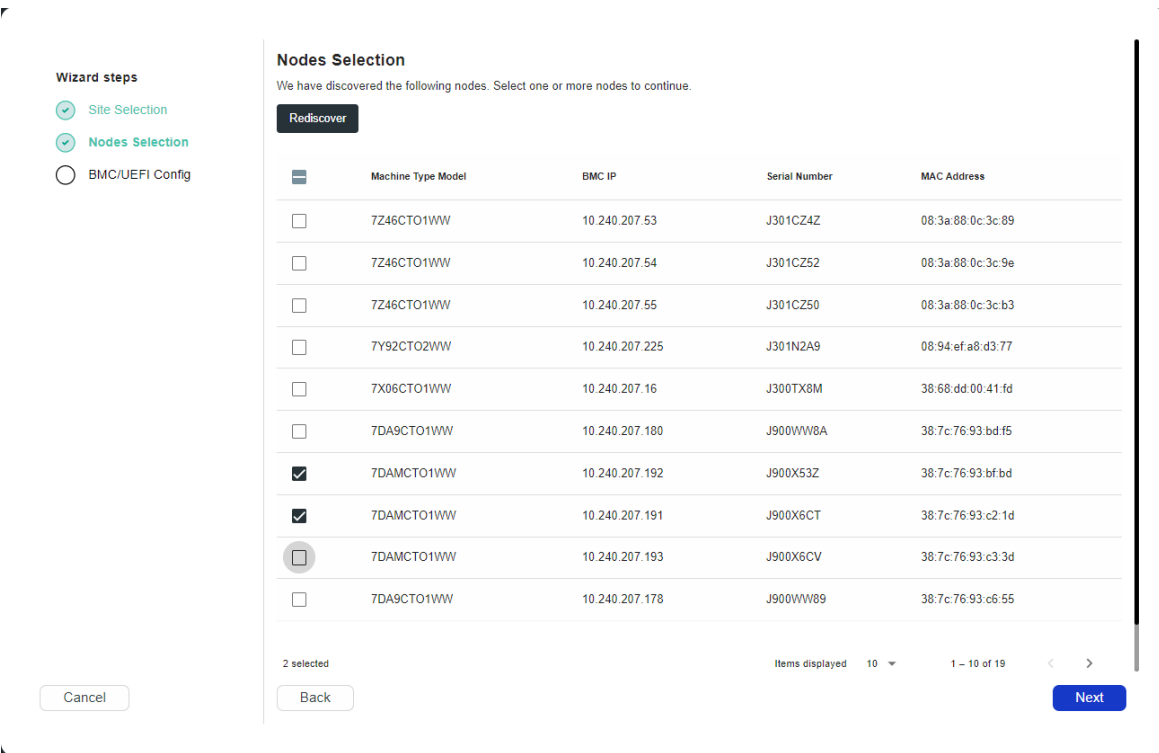
**Note:** If the value shown in the BMC Network column is not **'ready'**, it indicates that the BMC(XCC) network was not properly planned, and you will not be able to select that site.

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



**Figure 55: Add devices by discovery - site selection**

- 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 56: Add devices by discovery - nodes selection from discovered list**

- 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.

**Wizard steps**

- Site Selection
- Nodes Selection
- BMC/UEFI Config**

**BMC/UEFI Config**

Each physical host has a BMC, which is used for hardware management. To simplify management without sacrificing security, please choose a credential policy to be used for all hosts. In addition, you must specify the current BMC passwords. The factory default password is listed for the current BMC password, but note that logging into an BMC for the first time forces a password change.

Specify BMC IP Address, Current BMC Password and Current UEFI Administrator Password

Use the same BMC password for all devices

Serial Number	Site	BMC Original IP	BMC Assigned IP	BMC Username	BMC Current Password	UEFI Administrator Current Password
J900X53Z	buch002	10.240.207.192	10.241.8.81/25	USERID	.....	.....
J900X6CT	buch002	10.240.207.191	10.241.8.82/25	USERID	.....	.....

Items displayed 10 1 - 2 of 2

**Specify BMC and UEFI credential policies**

BMC New Password Policy\*  
No changes

UEFI New Password Policy\*  
No changes

Cancel Back Done

**Figure 57: Add devices by discovery - BMC/UEFI config**

- 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.

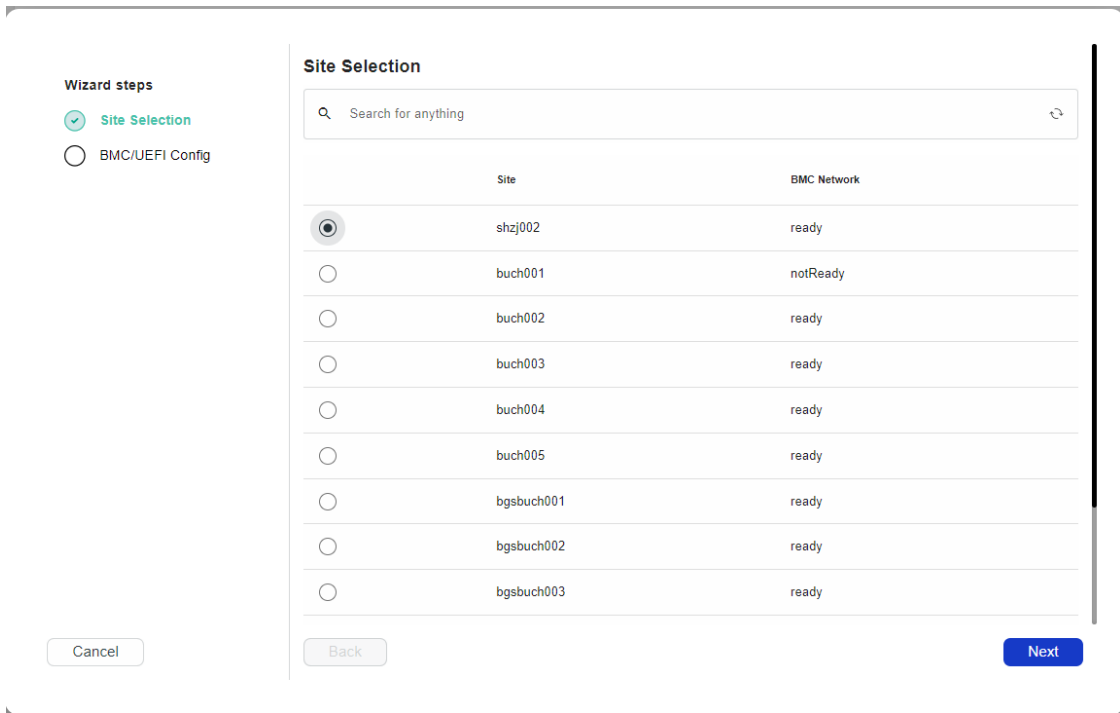
### Add device by BMC IP

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:

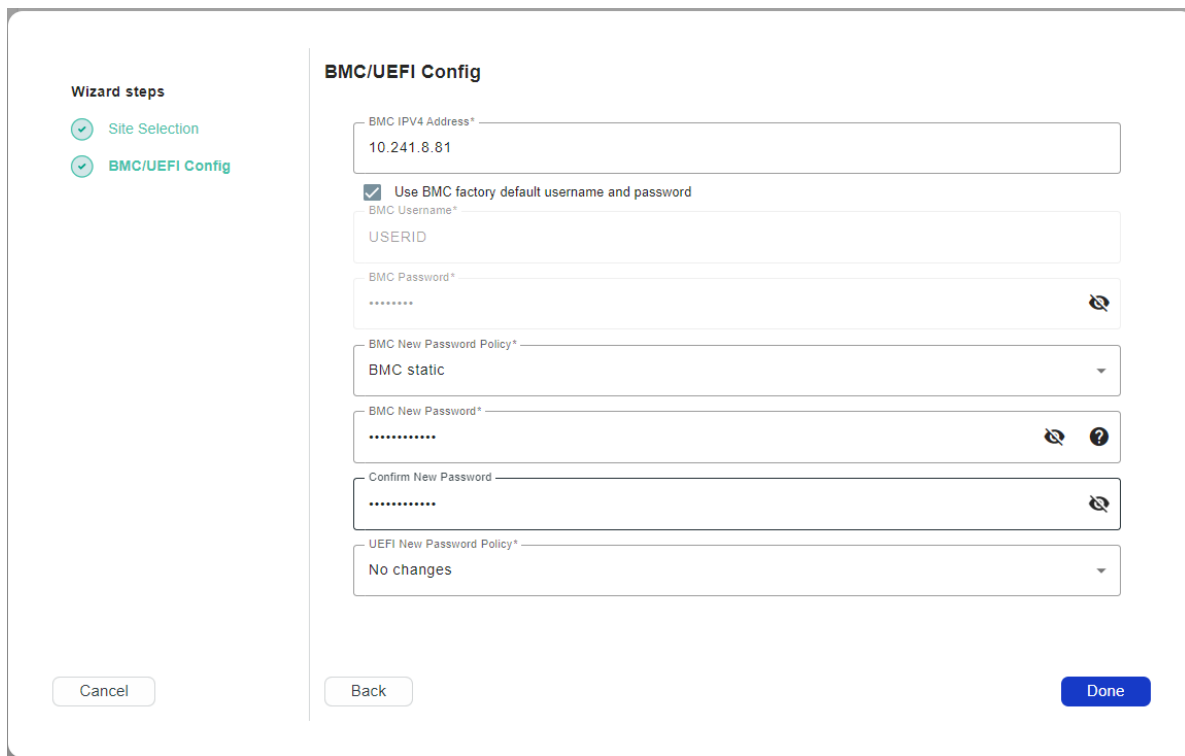
- Click **Registered Devices** → **Add Device** → **Add Device by BMC IP**.
- Select the site to which the BMC will be added and click **Next**.
- In BMC configuration page, enter the BMC IP address, the BMC user ID, the existing BMC passwords.
- Select BMC New Password Policy or keep it as “No changes” which means do not change BMC password.
- Select UEFI New Password Policy or keep it as “No changes” which means do not change UEFI password.
- 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 58: Add device by BMC IP – select site**







**Figure 59: Add device by IP – BMC/UEFI Config**

## Tasks

[Download All Service Logs](#)

Here you can find the list of tasks executed by the system and their status.




<input type="checkbox"/>	Name	Status	Created By	Start Time	Stop Time
<input type="checkbox"/>	Add Devices By IP	 50%	admin	2024-06-15 18:01:14	Not available
<input type="checkbox"/>	Remove Devices	 successful	admin	2024-06-15 17:57:10	2024-06-15 17:58:06
<input type="checkbox"/>	Add Devices By Excel	 successful	admin	2024-06-15 17:42:24	2024-06-15 17:52:41
<input type="checkbox"/>	Discover Devices	 successful	admin	2024-06-15 17:49:56	2024-06-15 17:50:40

**Figure 60: Task of add devices**

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

### Registered Devices

Here you can find the list of registered devices. A device appears in this list when a field technician completes the registration process in the field. Users can also register new devices by auto-discovery in the L2 network or manual input through 'Add device', or by uploading a Device Definition Excel file.

<input type="checkbox"/>	Site	Server Model	Machine Type	BMC IP	Serial Number	FQDN	Status	Credentials	Preload Image
<input type="checkbox"/>	shzj002	ThinkEdge SE360 V2	7DAM	10.240.207.191	J900X6CT		Inventory		Not available
<input type="checkbox"/>	shzj002	ThinkEdge SE360 V2	7DAM	10.240.207.192	J900X53Z		Inventory		Not available
<input type="checkbox"/>	shzj002	ThinkEdge SE360 V2	7DAM	10.240.207.193	J900X6CV		Inventory		Not available

0 selected Items displayed 10 1 - 3 of 3

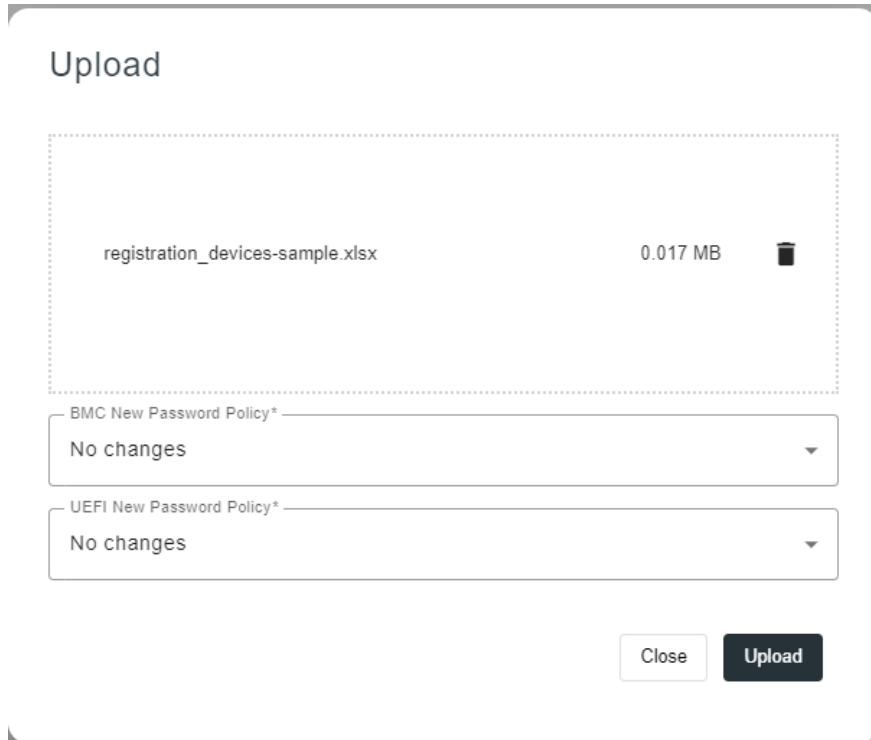
**Figure 61: Registered device list**

### 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. Before you begin, get the sample Excel file “registration\_devices-sample.xlsx” from Lenovo, and follow the embedded instructions to fill in the file with the planning data for your devices. From the LOC-A web interface, click **Registered 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.
6. Click **Upload** to upload the file.



**Figure 62: 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.cus tom.local	xxx	xxxxx	Yes	HTTPS, Port 443	3

**Figure 63: LXCA cloud service of Hardware management type**

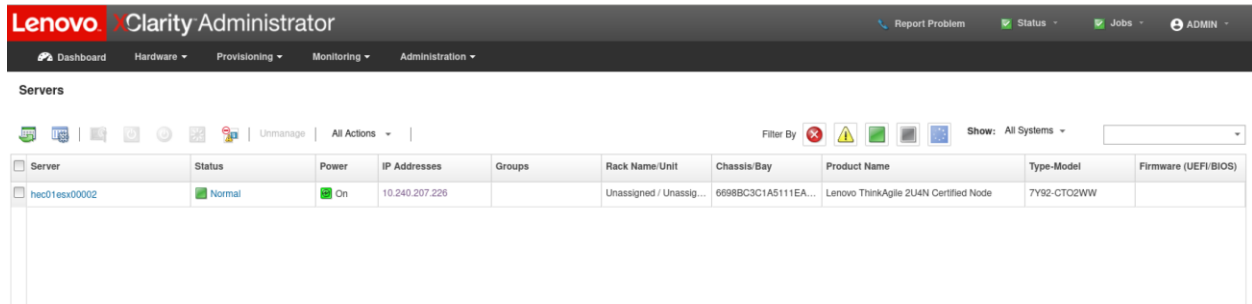
The LXCA or LXCO instance can either be an IP address or an FQDN that is resolvable by the DNS configured for the LOC-A Core Framework appliance. If you specify a site list, all nodes from those sites will be added to this LXCA instance.

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 64: Devices added into LXCA instance**

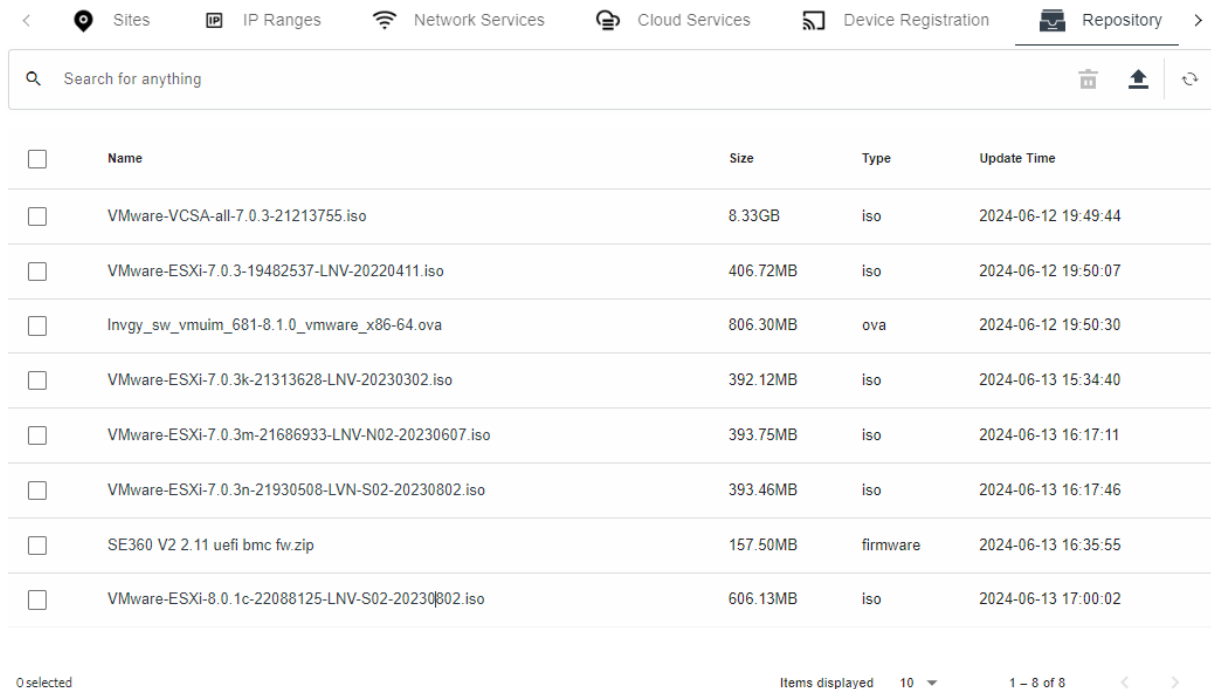
## Repository management

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.

### Repository

Here you can upload the required files for deployment.



**Figure 65: 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 66 shows an example of the ISO image details.

## Image Detail

Name	VMware-ESXi-7.0.3-19482537-LNV-20220411.iso
Size	406.72MB
Type	iso
Update Time	2024-03-20 13:57:24

Details ▾

### MD5

2c2642037f6b2715b68ffcd160ba6a9d

Close

**Figure 66: 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.

## Image Detail

Name Invgy\_fw\_xcc\_tei3f2z-6.35\_anyos\_noarch2.zip  
Size 125.51MB  
Type firmware  
Update Time 2024-03-21 16:48:28

Details ▾

Device Type	Firmware Type	Release Date	Version	Build
7Y65	xcc	2024-03-18 00:00:00	6.35	tei3f2z

Close

**Figure 67: 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.

Upload File to Server

Choose file type  
OS Image(iso)

Drag and drop files here

Click 'Browse' to import files or drag and drop files.

Browse

Upload

**Figure 68: 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.

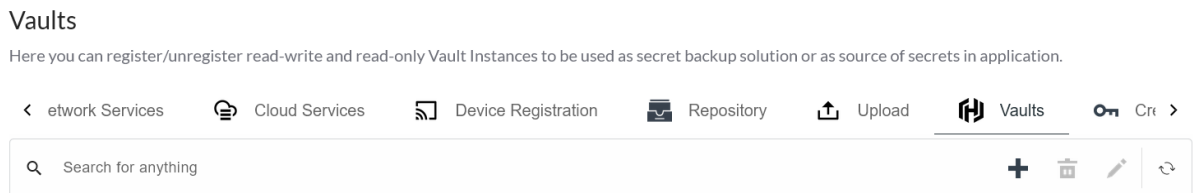
Hashicorp Vault instance can be used as a user owned backup solution for the LOC-A user's secrets, or as a user owned secrets source for LOC-A's user's secrets. This feature integrates LOC-A with the HashiCorp Vault application. Users can opt to centralize all secrets in a HashiCorp Vault server. This 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

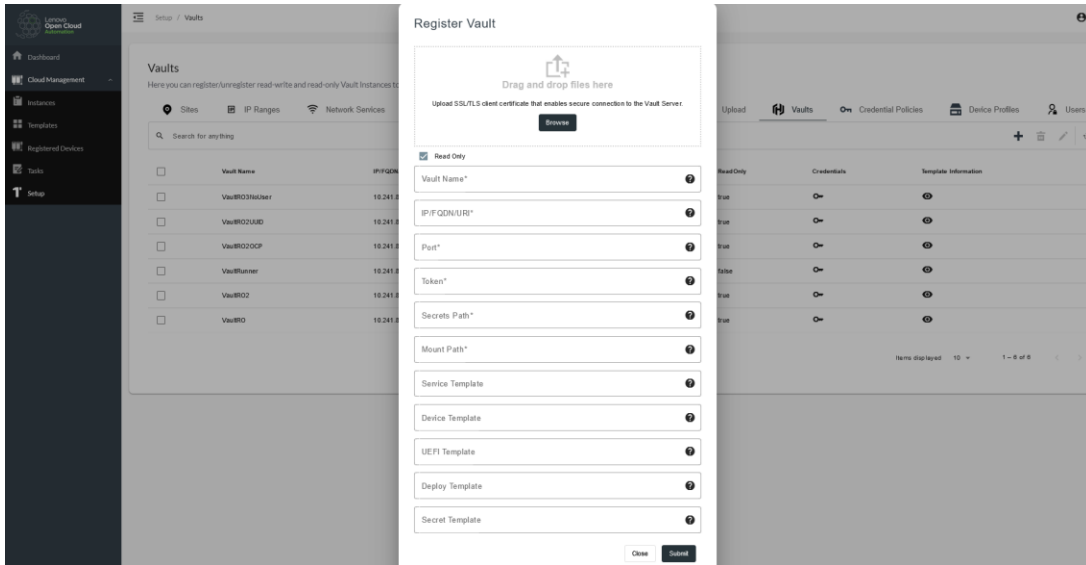
Navigate to **Setup → Vaults** and click the **Add** icon:



**Figure 69: Vaults list**

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





**Figure 70: 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.local	@@@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 71: 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.local	administrator@lenovo	@@@VaultRO2	
lxca_global	Hardware management	Lenovo LXCA		buch002	10.240.207.131	admin	@@@VaultRO2	
lxco_global	Hardware management	Lenovo LXCO		buch002	10.240.159.188	USERID	@@@VaultRO2	

Figure 72: 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 73: Configure to use Vault with secret path template

**Figure 74: 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:

	Vault Name	IP/FQDN/URI	Mount Path	Secrets Path	ReadOnly	Credentials	Template Information
<input type="checkbox"/>	VaultRO3NoUser	10.241.8.53	kv-v1/	RO3/	true	🔒	👁️
<input type="checkbox"/>	VaultRO2UID	10.241.8.53				🔒	👁️
<input type="checkbox"/>	VaultRO2OCP	10.241.8.53				🔒	👁️
<input checked="" type="checkbox"/>	VaultRunner	10.241.8.53				🔒	👁️
<input type="checkbox"/>	VaultRO2	10.241.8.53				🔒	👁️
<input type="checkbox"/>	VaultRO	10.241.8.53				🔒	👁️

**Figure 75: 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.

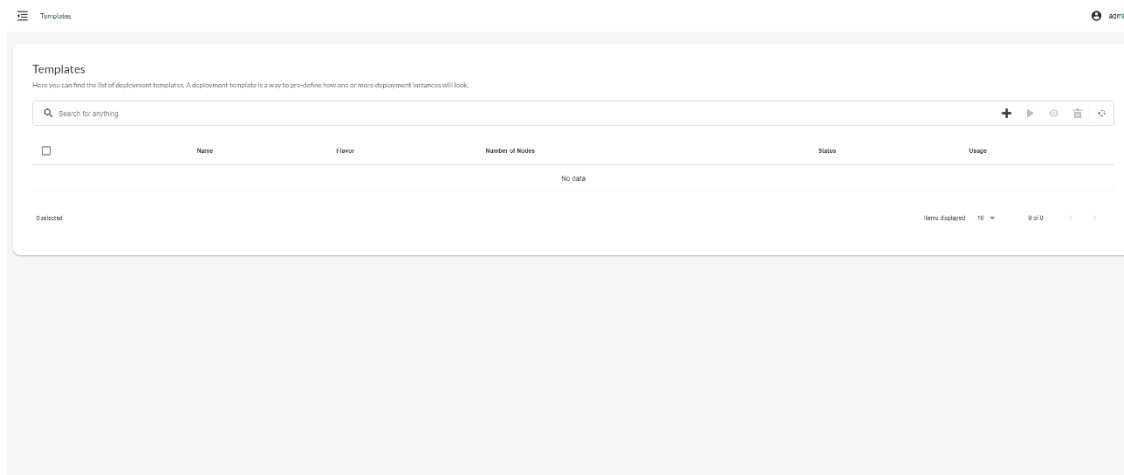
A vault instance can be registered at any time during LOC-A usage, so if the user has chosen by mistake to delete the secrets pushed by LOC-A in a read-write vault, the user can re-register the vault and the secrets will be pushed back by LOC-A.

## 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 76: Templates page**

2. Select a cloud flavor for the template.

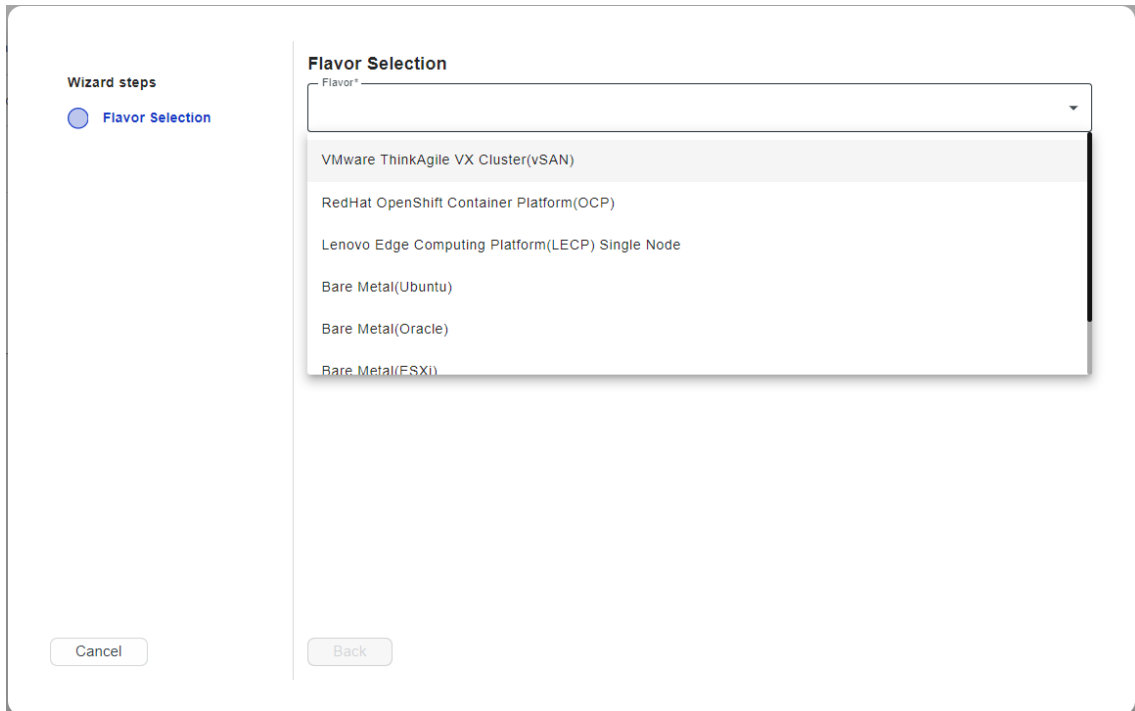


Figure 77: Flavor selection

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

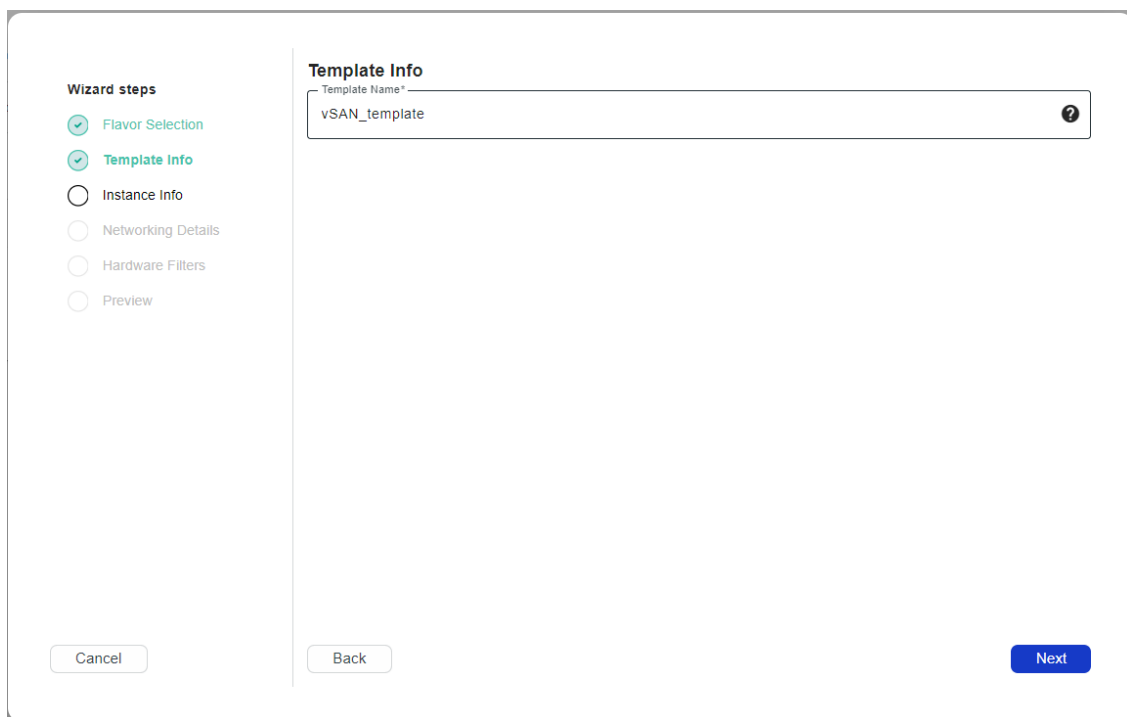


Figure 78: Cloud template wizard

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 79: 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": "xxxxxxxxxxxxxxxx",
      "email": "example@abc.com"
    },
    "quay.io": {
      "auth": "xxxxxxxxxxxxxxxx",
      "email": " example@abc.com"
    },
    "registry.connect.redhat.com": {
      "auth": "xxxxxxxxxxxxxxxx",
      "email": "example@abc.com"
    }
  },
}
```

```

    "registry.redhat.io": {
      "auth": "xxxxxxxxxxxxxxxx",
      "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 11 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

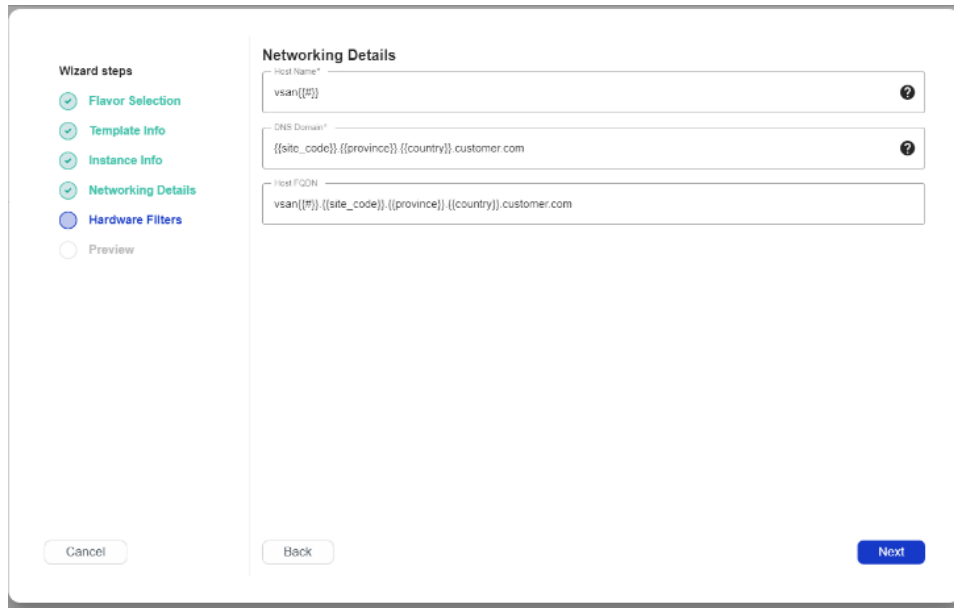
```

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 80: 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.

**Wizard steps**

- ✓ Flavor Selection
- ✓ Template Info
- ✓ Instance Info
- ✓ Networking Details
- Hardware Filters**
- Preview

**Hardware Filters**

Device Model\* ThinkEdge SE450

Number of Devices\* 3

Device Profile vSAN-Default

Select a firmware package which will be used to update firmware during deployment

OS Credential Policy\* os-static

Root Password\*

Confirm Root Password

Cancel Back Next

**Figure 81: 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.

**Wizard steps**

- ✓ Flavor Selection
- ✓ Template Info
- ✓ Instance Info
- ✓ Networking Details
- Hardware Filters**
- Preview

**Hardware Filters**

Device Model\* ThinkEdge SE450

Number of Devices\* 3

Device Profile vSAN-Default

Select a firmware package which will be used to update firmware during deployment

OS Credential Policy\* os-auto

Cancel Back Next

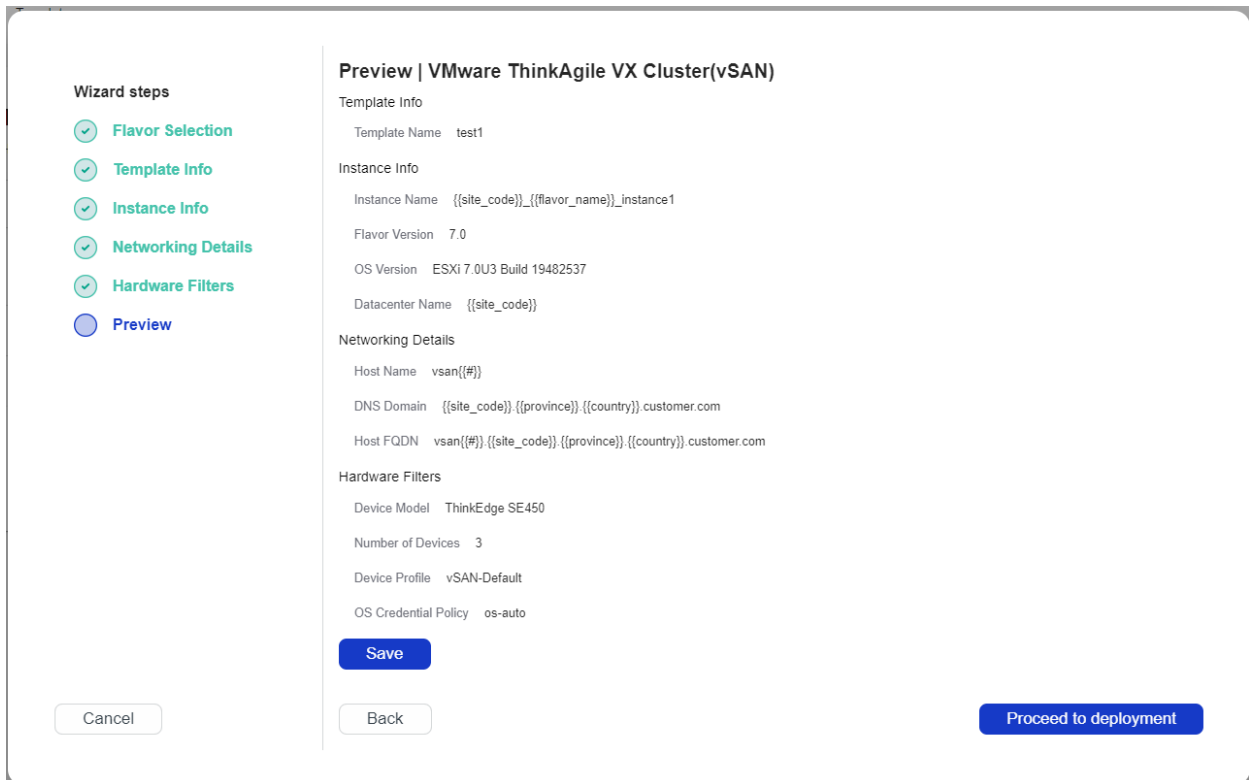
**Figure 82: Cloud template - define hardware filter and auto root password policy**

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	<ul style="list-style-type: none"> <li>• public key</li> </ul>
VMware vSAN	<ul style="list-style-type: none"> <li>• static password</li> <li>• password template string</li> </ul>
Bare metal OS	<ul style="list-style-type: none"> <li>• static password</li> <li>• password template string</li> </ul>
Lenovo Edge Computing Platform	<ul style="list-style-type: none"> <li>• static password</li> <li>• password template string</li> </ul>

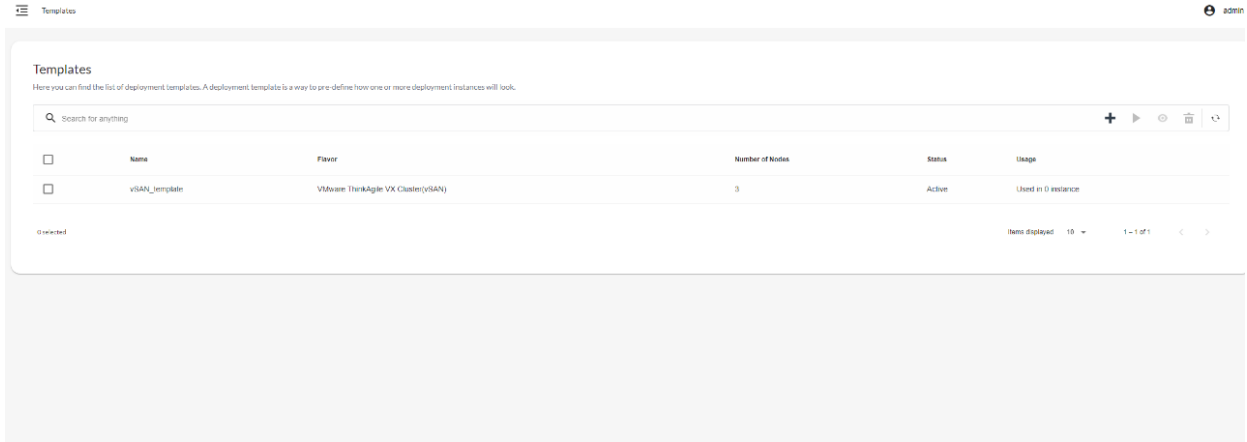
**Table 7: Nodes Authentication Types supported by LOC-A**

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 83: Cloud template summary**

- 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 84: Cloud templates list**

View cloud template details:

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

## Template Detail

Name	vsAN_template
Kind	cloud
Status	active
Usage	Used in 0 instance
Flavor Name	VMware ThinkAgile VX Cluster(vSAN)
Flavor Version	7.0
OS Version	ESXi 7.0U3 Build 19482537
Instance Name	{{site_code}}_{{flavor_name}}_instance1
DNS Domain	{{site_code}}.{{province}}.{{country}}.customer.com
Host FQDN	vsan{{#}}.{{site_code}}.{{province}}.{{country}}.customer.com
Device Profile 	Name vsAN-Default
	BMC
	Power Restore Policy Always On
	UEFI
	Server Operating Mode Efficiency_FavorPerformance
	Secure Boot true
Device Model	ThinkEdge SE455 V3
Number of Devices	3
Firmware Package	Not available
Authentication Type	Use a statically defined password(not recommended)
Authentication Value	..... 
Other Properties 	
Datacenter Name	{{site_code}}_{{flavor_name}}_dc1

Close

**Figure 85: Cloud template detail**

## 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.

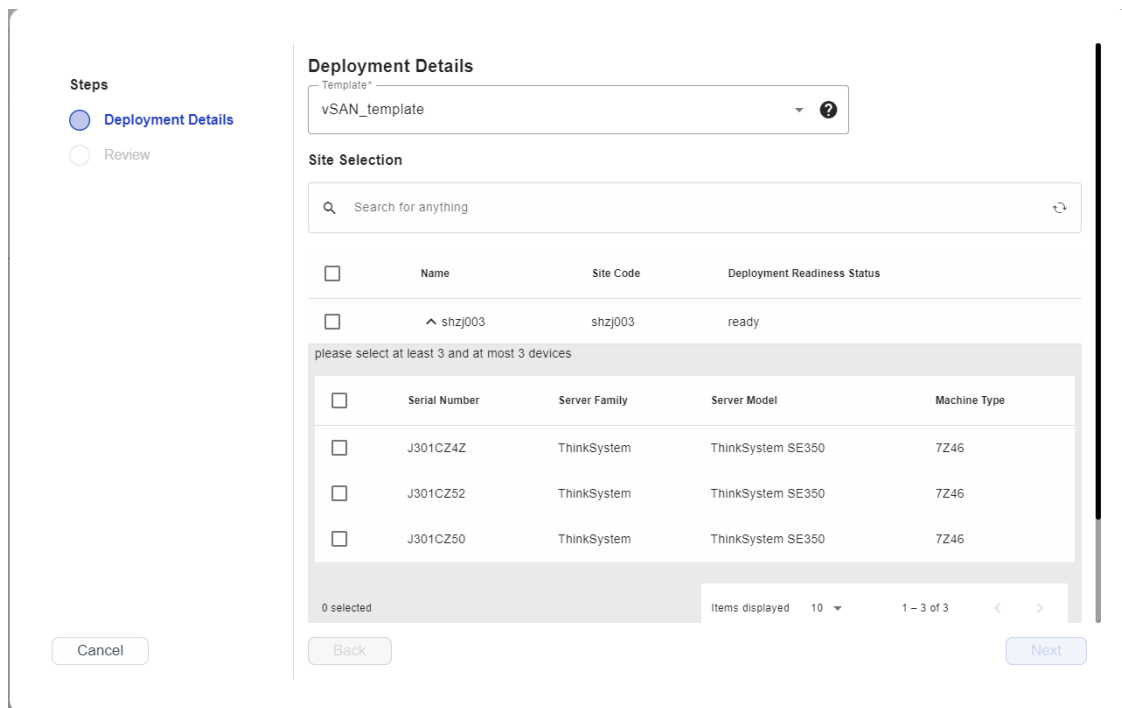


Figure 86: Create new cloud instance via template

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.

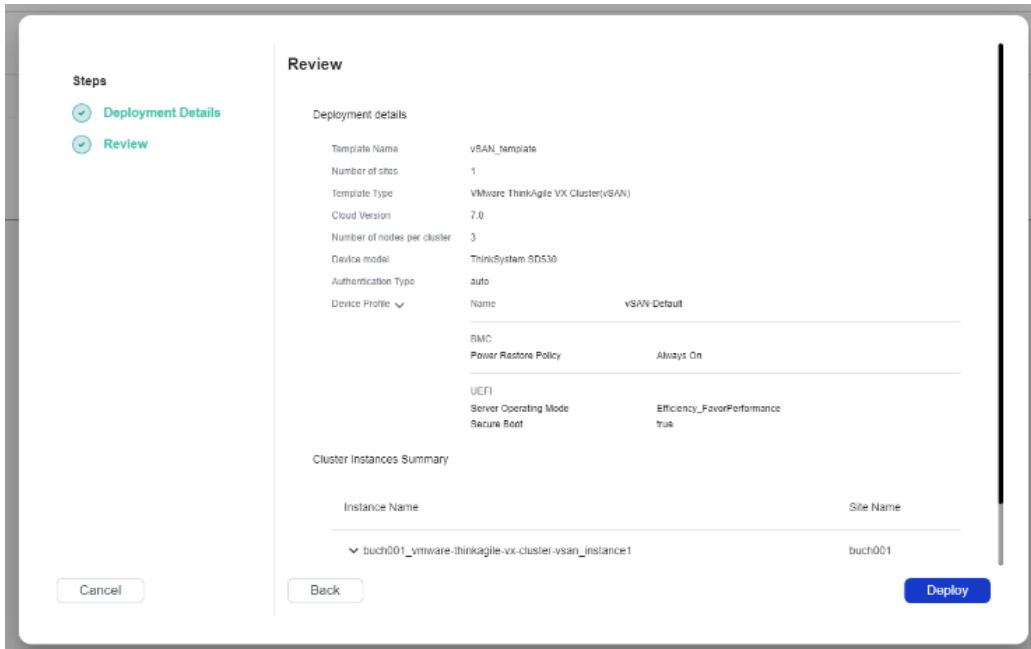


Figure 87: Review cloud deployment

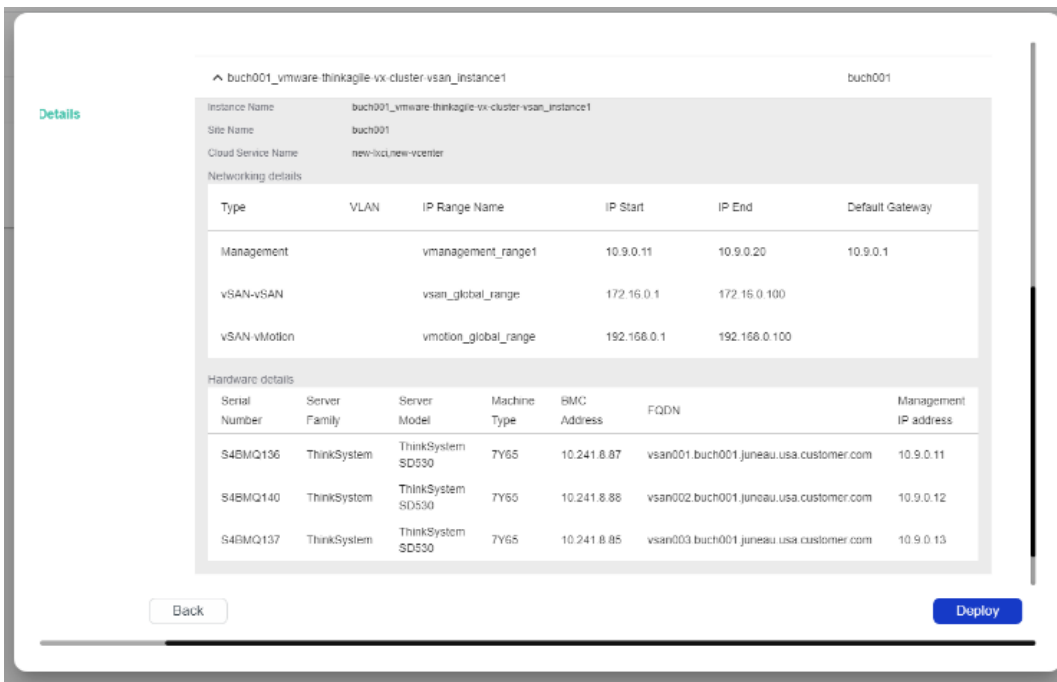


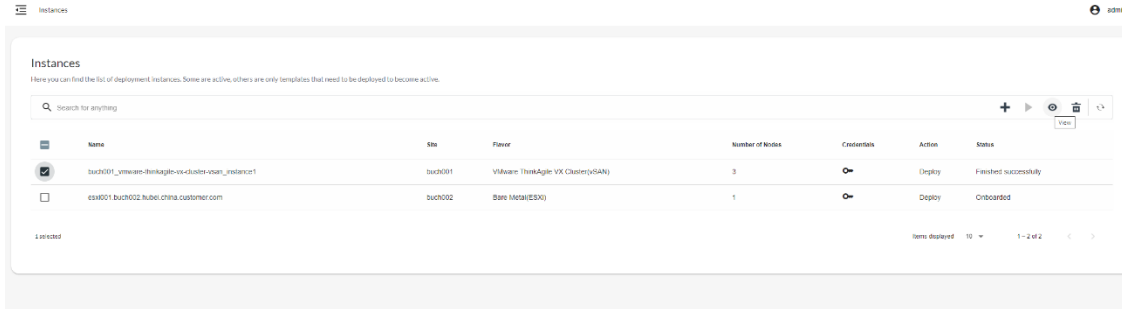
Figure 88: Expand to view cluster details

## 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:

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



**Figure 89: Select installed cluster to expand**

2. 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.

## Instance Detail

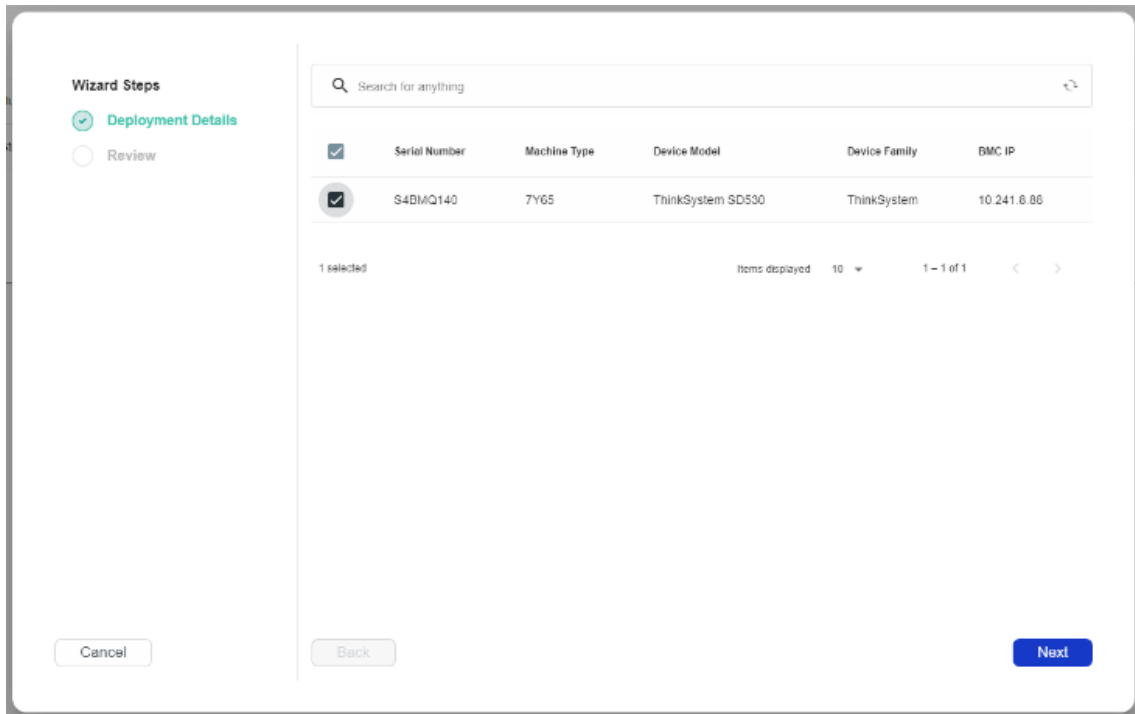
Detail		Hosts
Name	buch001_vmware-thinkagile-vx-cluster-vsan_instance1	
Flavor	VMware ThinkAgile VX Cluster(vSAN)	
Number Of Nodes	3	
Status	Finished successfully	
Site	buch001	
Template	vSAN_template	
Device Model	ThinkSystem SD530	
Cloud Services	new-vcenter	
Network Services	dns3temp,dns001s001buchx pfSense.localdomain	
IP Ranges	10.9.0.11 - 10.9.0.20 192.168.0.1 - 192.168.0.100 172.16.0.1 - 172.16.0.100	
Device Profile	Name vSAN-Default	
BMC		
Power Restore Policy	Always On	
UEFI		
Server Operating Mode	Efficiency_FavorPerformance	
Secure Boot	true	

Close Add Hosts

**Figure 90: View cluster details**

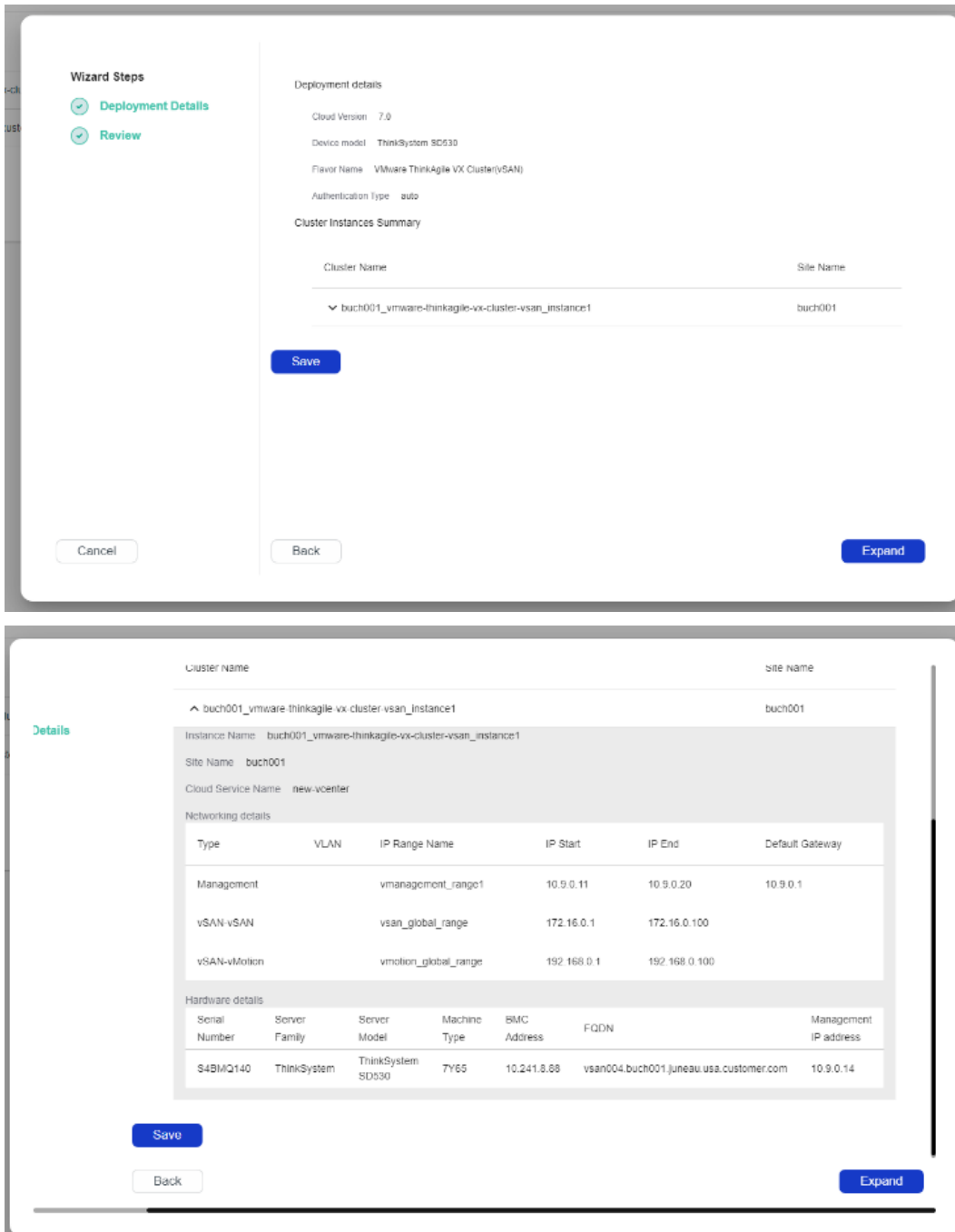


3. The cloud expansion operation will apply the original cloud template settings that were used for cloud deployment. All free devices in this site that meet the device filtering requirement will be listed. You can select the devices that you want to add into the cluster, then click **Next**.



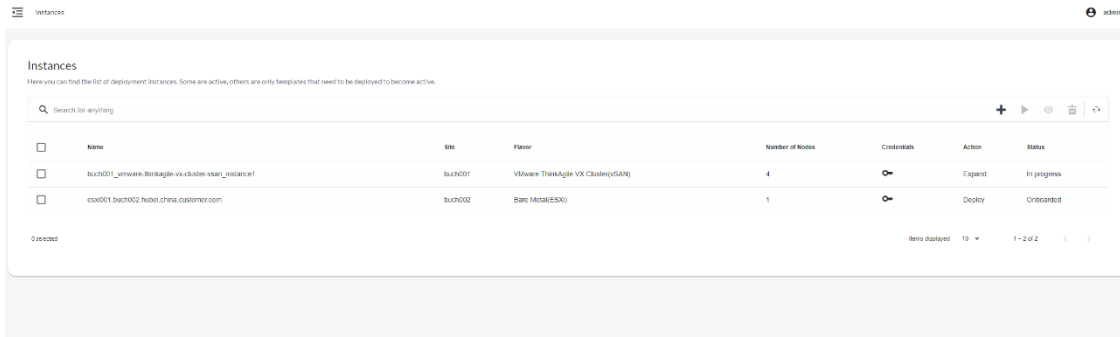
**Figure 91: Cloud expansion wizard**

4. 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.



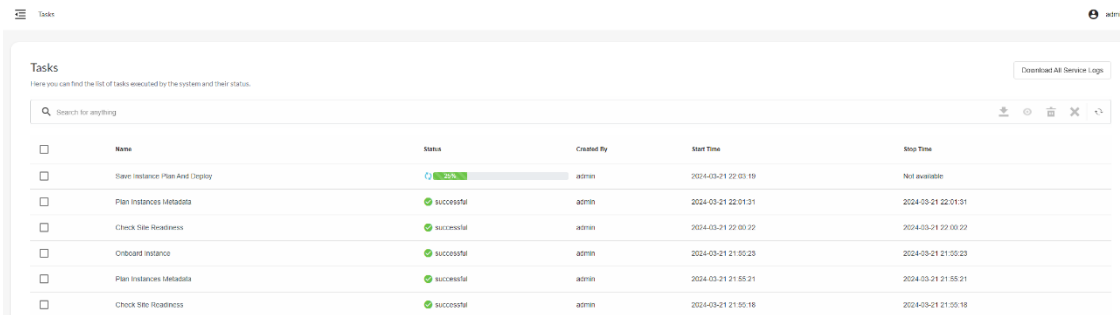
**Figure 92: View cloud expansion details**

- 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 93: Instance during expansion**

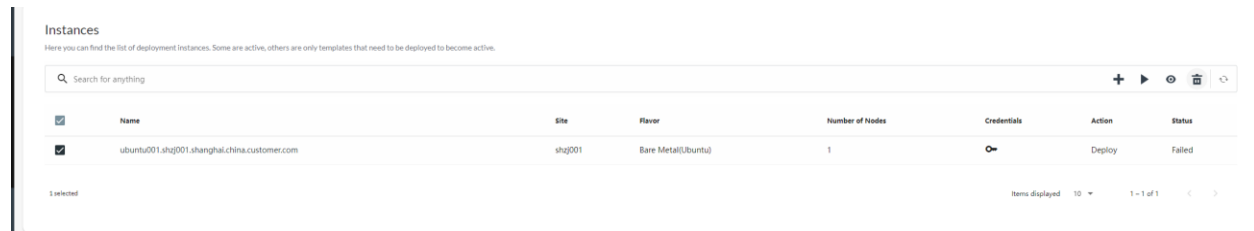
Alternatively, you can click **Save** to save the plan, but the cloud expansion will not be started immediately. The cluster instance will be displayed on the **Instances** page with status of “Onboarded” and action of “Expand”. You can select the site and click **All Actions**→**Run** to kick off the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



**Figure 94: 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 95: Instance deletion**

## Create an OS template

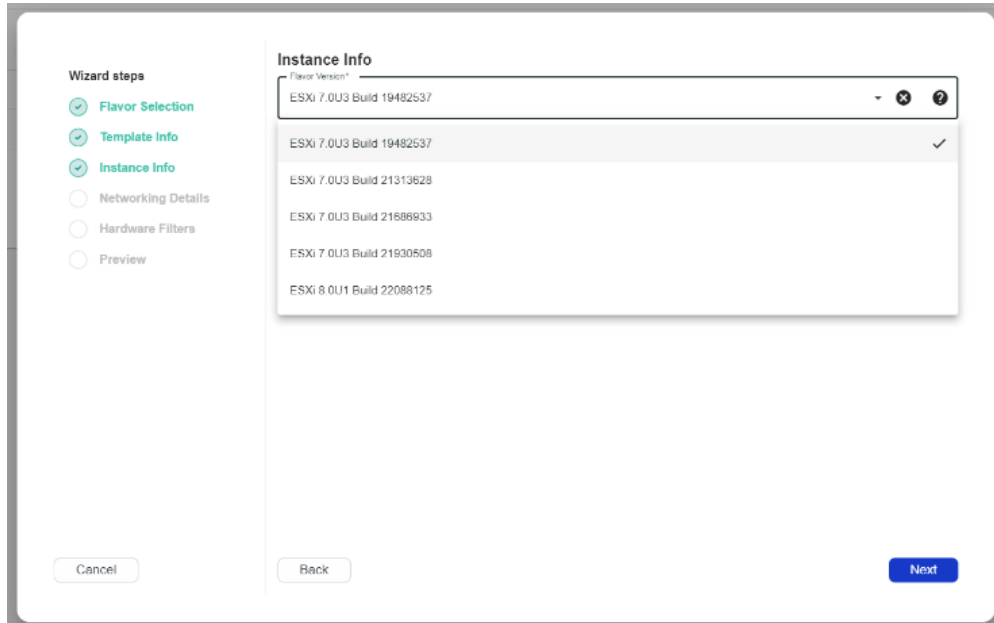
Creating an OS template is like creating a cloud template; it facilitates bare metal OS deployment for multiple devices in batches. In this release, only Ubuntu 18.04/20.04/22.04, VMware ESXi 7/ 8, and CentOS 7.9/8.3 OS deployments are verified and supported by LOC-A.

**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:

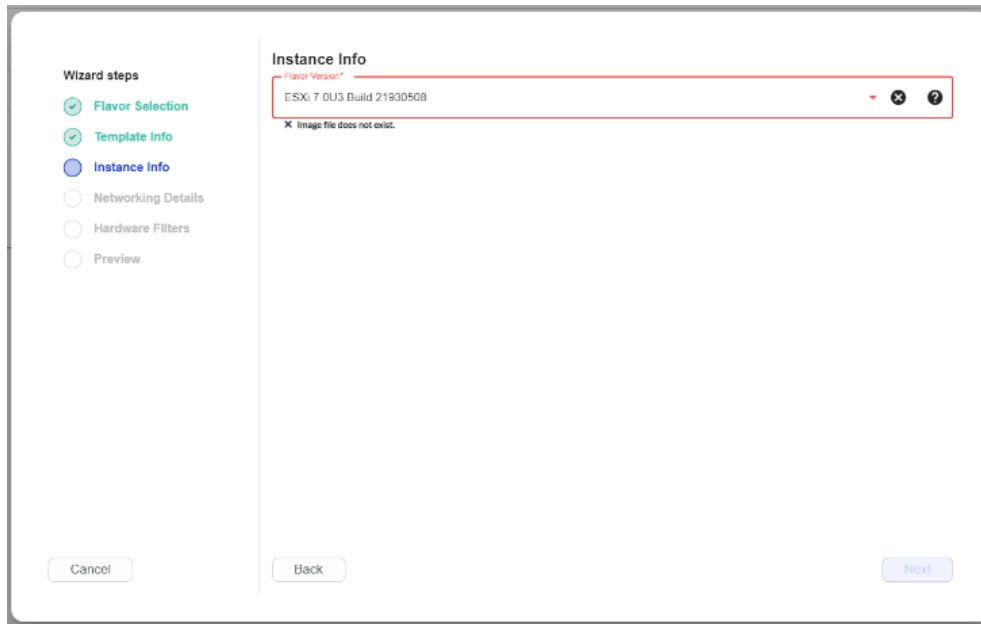
1. From the LOC-A portal, click **Templates**. Then click **+** (**Add**) to start the template creation process.
2. Select the OS flavor from the dropdown list of Flavor Selection page and click **Next**.
3. On Template Info page, fill in the desired template name.

4. On the Instance Info page, choose the OS version from the dropdown Flavor Version list.



**Figure 96: 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.



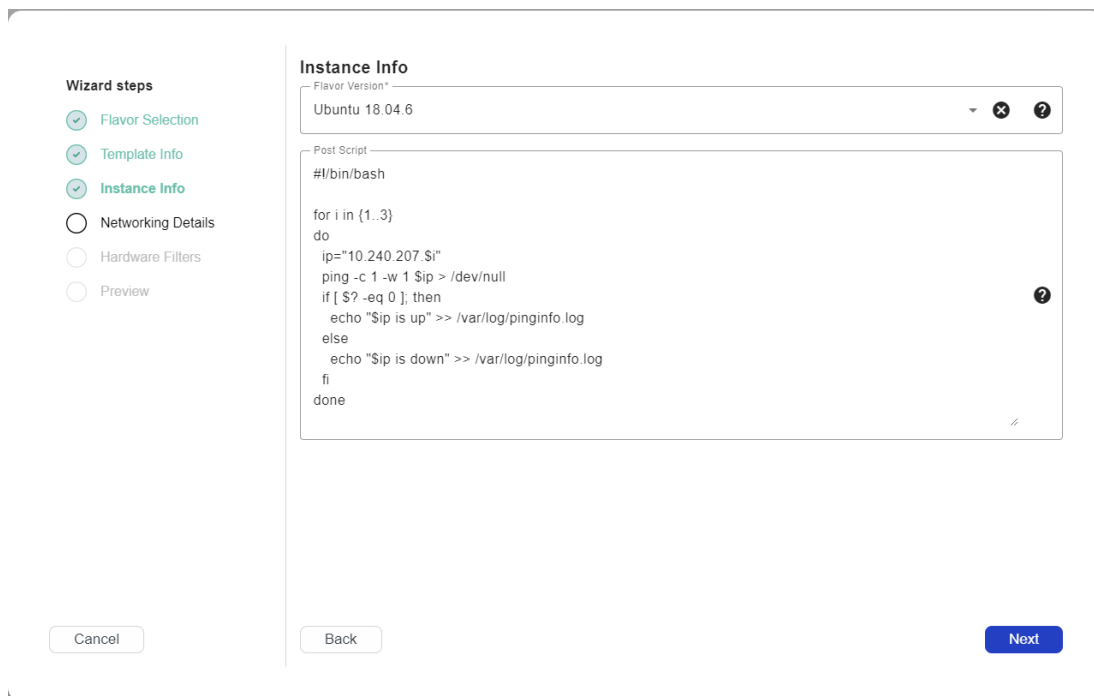
**Figure 97: Missing image file in LOC-A repository**

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

Flavor	Version	Download Link
BareMetal (Ubuntu)	18.04.6	<a href="http://www.cdimage.ubuntu.com/ubuntu/releases/18.04/release/ubuntu-18.04.6-server-amd64.iso">http://www.cdimage.ubuntu.com/ubuntu/releases/18.04/release/ubuntu-18.04.6-server-amd64.iso</a>
	20.04.6	<a href="https://ftp.ulak.net.tr/ubuntu-releases/20.04.6/ubuntu-20.04.6-live-server-amd64.iso">https://ftp.ulak.net.tr/ubuntu-releases/20.04.6/ubuntu-20.04.6-live-server-amd64.iso</a>
	22.04.3	<a href="https://ftp.ulak.net.tr/ubuntu-releases/22.04.3/ubuntu-22.04.3-live-server-amd64.iso">https://ftp.ulak.net.tr/ubuntu-releases/22.04.3/ubuntu-22.04.3-live-server-amd64.iso</a>
BareMetal (CentOS)	7.9	<a href="http://centos.turhost.com/7.9.2009/isos/x86_64/CentOS-7-x86_64-DVD-2009.iso">http://centos.turhost.com/7.9.2009/isos/x86_64/CentOS-7-x86_64-DVD-2009.iso</a>
	8.3	<a href="https://vault.centos.org/8.3.2011/isos/x86_64/CentOS-8.3.2011-x86_64-dvd1.iso">https://vault.centos.org/8.3.2011/isos/x86_64/CentOS-8.3.2011-x86_64-dvd1.iso</a>
BareMetal (ESXi)	ESXi 7.0U3 Build 19482537	<a href="https://vmware.lenovo.com/content/2022_05/Lenovo_Custom_ISO/7.0u3/VMware-ESXi-7.0.3-19482537-LNV-20220411.iso">https://vmware.lenovo.com/content/2022_05/Lenovo_Custom_ISO/7.0u3/VMware-ESXi-7.0.3-19482537-LNV-20220411.iso</a>
	ESXi 7.0U3 Build 21930508	<a href="https://vmware.lenovo.com/content/2023_08/Lenovo_Custom_ISO/7.0u3/s/VMware-ESXi-7.0.3n-21930508-LNV-S02-20230802.iso">https://vmware.lenovo.com/content/2023_08/Lenovo_Custom_ISO/7.0u3/s/VMware-ESXi-7.0.3n-21930508-LNV-S02-20230802.iso</a>
	ESXi 7.0U3 Build 21686933	<a href="https://vmware.lenovo.com/content/2023_08/Lenovo_Custom_ISO/7.0u3/n/VMware-ESXi-7.0.3m-21686933-LNV-N02-20230607.iso">https://vmware.lenovo.com/content/2023_08/Lenovo_Custom_ISO/7.0u3/n/VMware-ESXi-7.0.3m-21686933-LNV-N02-20230607.iso</a>
	ESXi 7.0U3 Build 21313628	<a href="https://vmware.lenovo.com/content/2023_03/Lenovo_Custom_ISO/7.0u3/VMware-ESXi-7.0.3k-21313628-LNV-20230302.iso">https://vmware.lenovo.com/content/2023_03/Lenovo_Custom_ISO/7.0u3/VMware-ESXi-7.0.3k-21313628-LNV-20230302.iso</a>
	ESXi 8.0U1 Build 22088125	<a href="https://vmware.lenovo.com/content/custom_iso/8.0/8.0u1/s/VMware-ESXi-8.0.1c-22088125-LNV-S02-20230802.iso">https://vmware.lenovo.com/content/custom_iso/8.0/8.0u1/s/VMware-ESXi-8.0.1c-22088125-LNV-S02-20230802.iso</a>

**Table 8: 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 currently supported.



**Figure 98: 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 63 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.

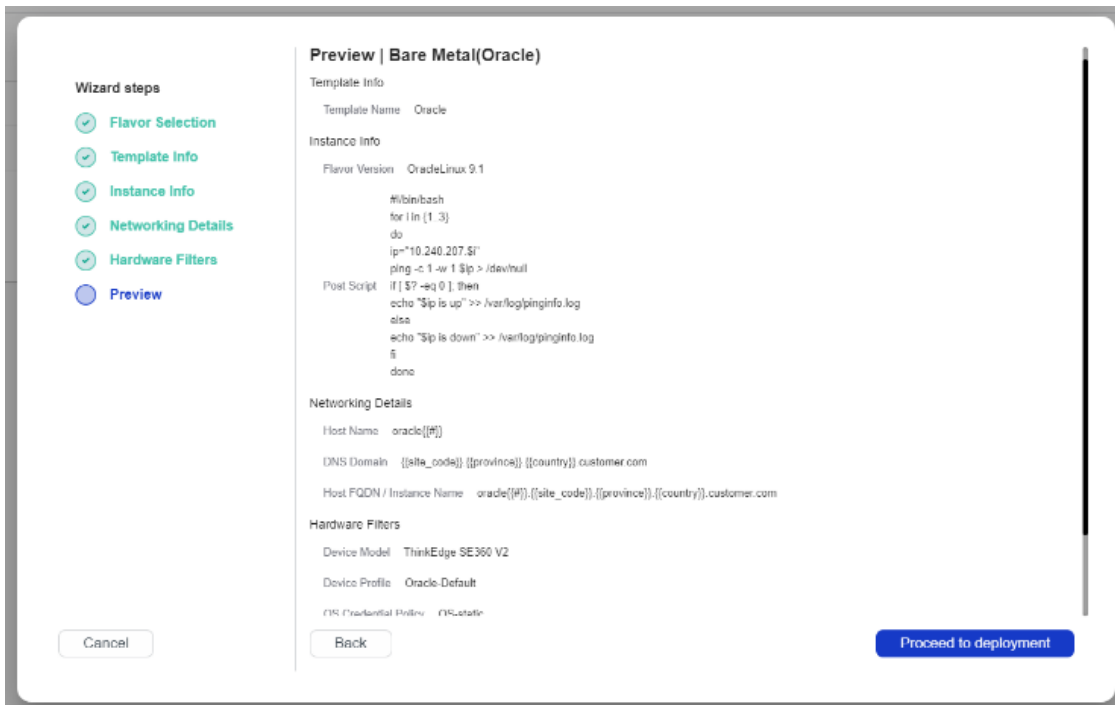


Figure 99: Review OS template

## 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 71 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.

The screenshot shows the 'Review' page in the LOC-A portal. On the left, a 'Steps' sidebar shows 'Deployment Details' and 'Review' as completed steps. The main content area is titled 'Review' and contains the following information:

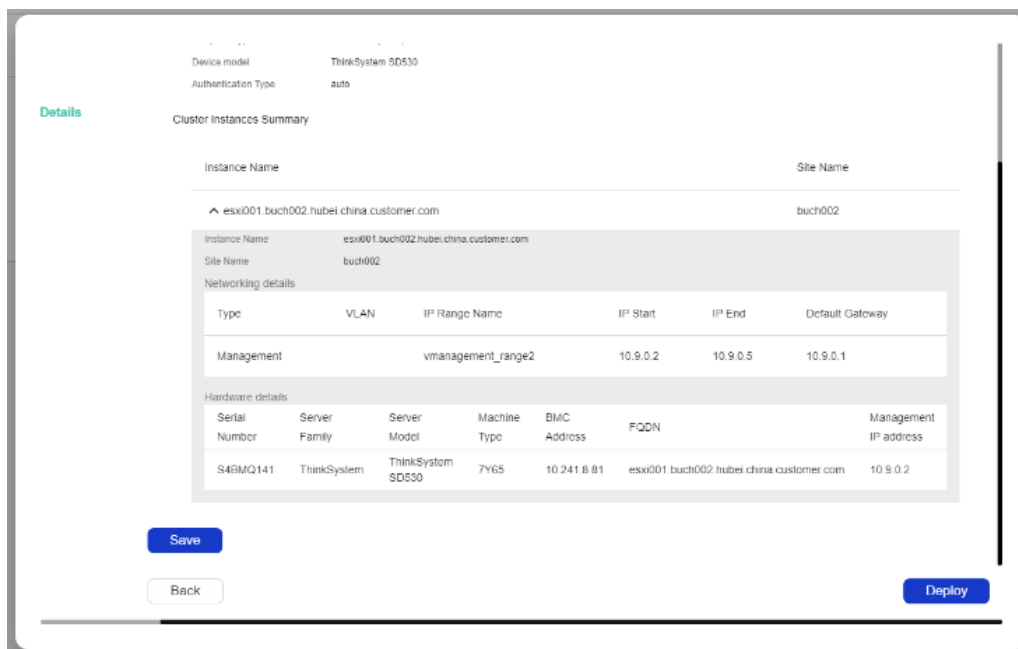
**Deployment details**

Template Name	ESXi_imp
Number of sites	1
Template Type	Bare Metal(ESXi)
Device model	ThinkSystem SD530
Authentication Type	auto

**Cluster Instances Summary**

Instance Name	Site Name
esxi001 buch002 hubei.china.customer.com	buch002

At the bottom of the page, there are three buttons: 'Cancel' (left), 'Back' (middle), and 'Deploy' (right). A 'Save' button is also visible above the 'Cluster Instances Summary' table.



**Figure 100: Review bare metal OS deployment details**

## 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 101: Optional server SD card slot example**

### **Supported server list:**

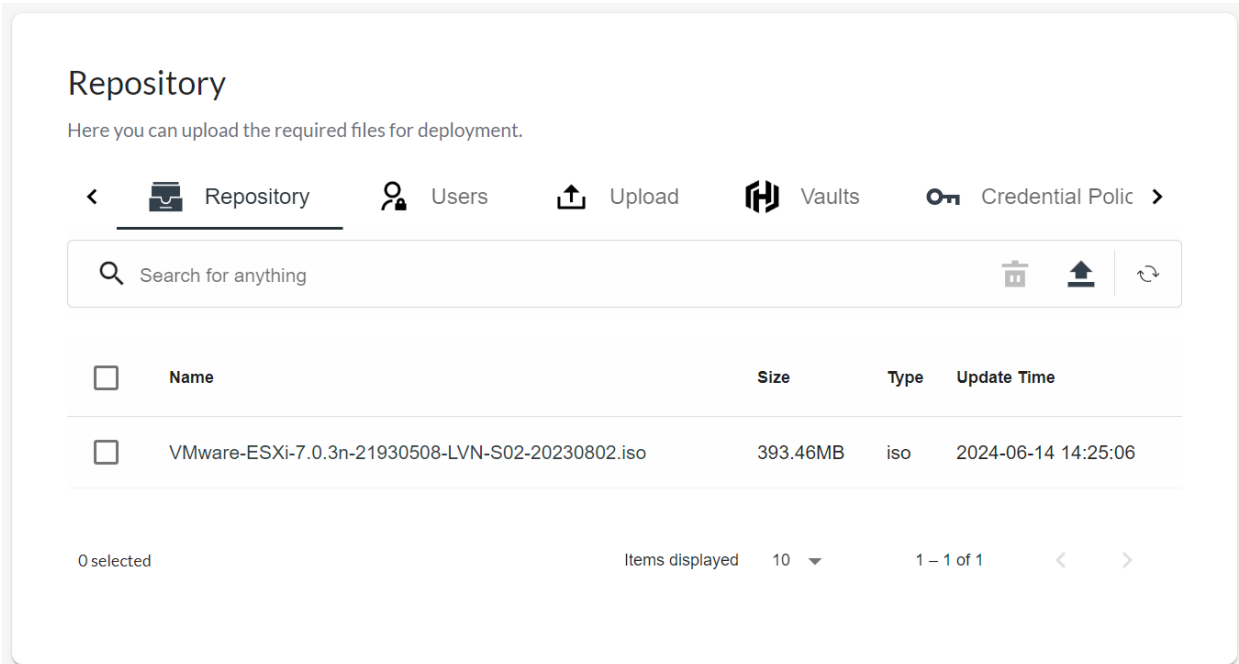
- ThinkEdge SE350 V2
- ThinkEdge SE360 V2



**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 sideload 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 102: 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.

## Lenovo Open Cloud Automation - Registration Utility

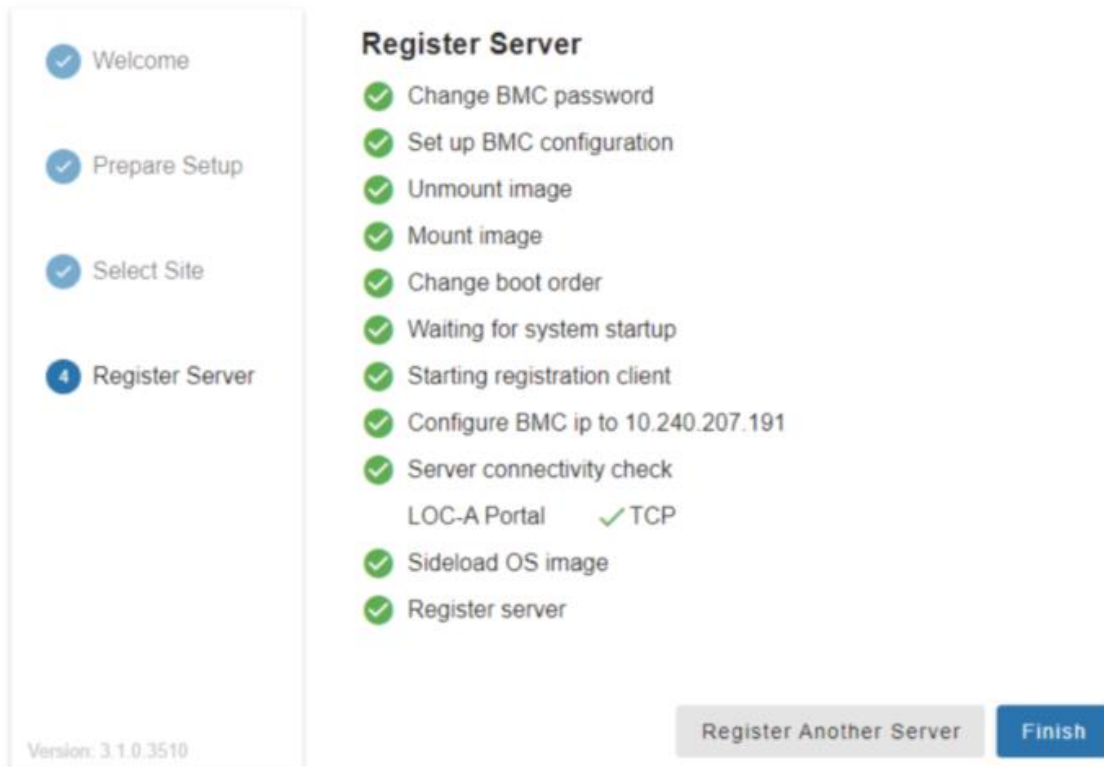


Figure 103: Sideload OS image during server registration

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

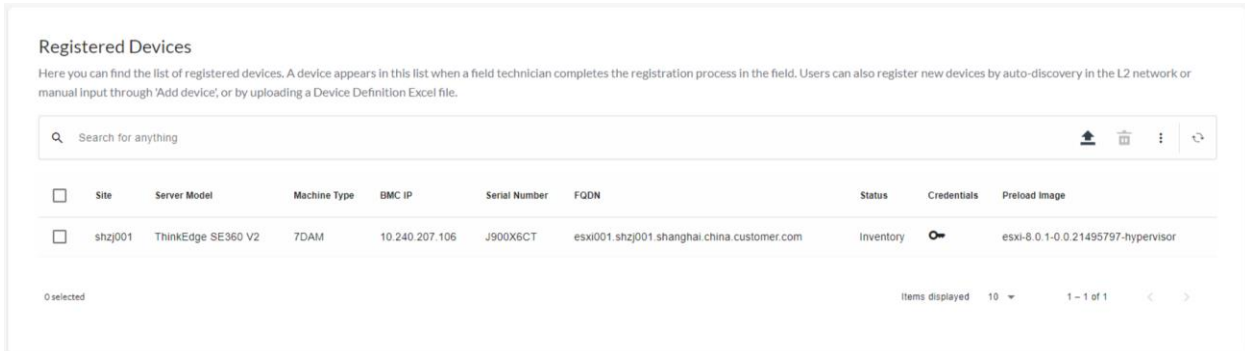
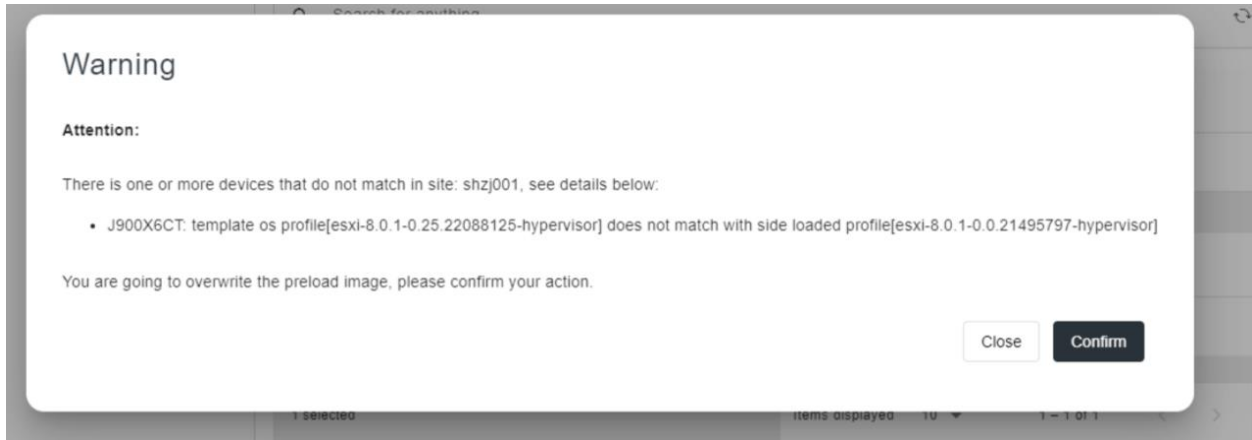


Figure 104: Registered device with preload image

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 105: 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.

Tasks Download All Service Logs

Here you can find the list of tasks executed by the system and their status.

Q Search for anything 📄 👁 🗑 ✕ ↺

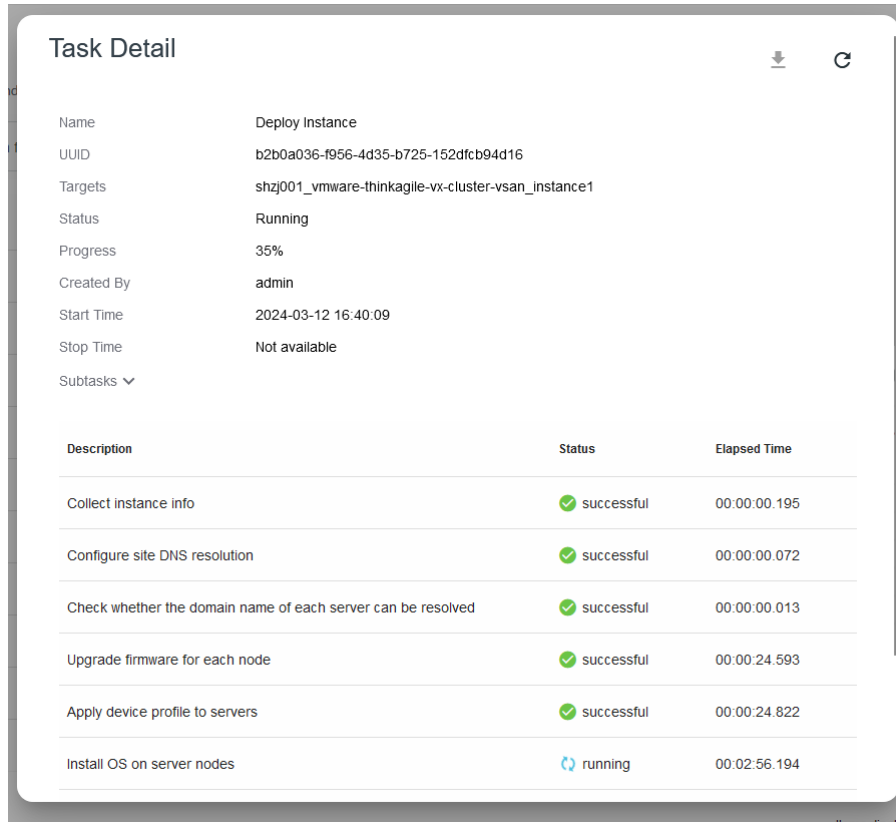
<input type="checkbox"/>	Name	Status	Created by	Start Time	Stop Time
<input type="checkbox"/>	Deploy Instance	<span style="color: blue;">🔄</span> 35%	admin	2024-03-12 16:40:09	Not available
<input type="checkbox"/>	Onboard Instance	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:09:29	2024-03-12 16:09:29
<input type="checkbox"/>	Plan Instances Metadata	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:09:27	2024-03-12 16:09:27
<input type="checkbox"/>	Check Site Readiness	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:09:24	2024-03-12 16:09:24
<input type="checkbox"/>	Add Devices By Excel	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:01:10	2024-03-12 16:05:34
<input type="checkbox"/>	Onboard Inventory	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:03:27	2024-03-12 16:03:27
<input type="checkbox"/>	Onboard Inventory	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:03:07	2024-03-12 16:03:07
<input type="checkbox"/>	Onboard Inventory	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:03:01	2024-03-12 16:03:02
<input type="checkbox"/>	Onboard Inventory	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:02:25	2024-03-12 16:02:26
<input type="checkbox"/>	Onboard Inventory	<span style="color: green;">✔</span> successful	admin	2024-03-12 16:02:21	2024-03-12 16:02:21

0 selected Items displayed 10 1 - 10 of 15 < >

**Figure 106: 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 107: Task detail with subtasks**

## 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.

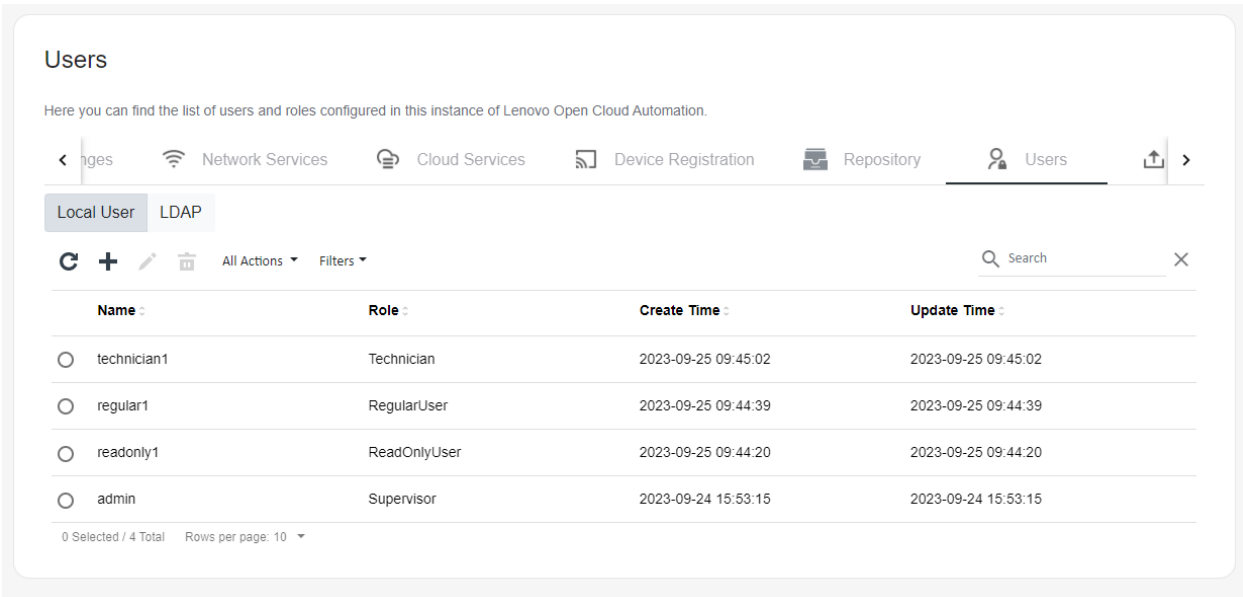
User passwords must meet the following rules:

- 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 108: 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.

1. 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.
2. 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 109 shows an example LDAP configuration page.

**Users**

Here you can find the list of users and roles configured in this instance of Lenovo Open Cloud Automation.

[Sites](#)
[IP Ranges](#)
[Network Services](#)
[Cloud Services](#)
[Device Registration](#)
[Repository](#)
[Users](#)

LDAP IP \* 
Allow Logins from:

LDAP Port \*

Enable TLS \*

LDAP Username \*

LDAP Password \*

LDAP Root DN \*

User Search \*

User Search Attribute \*

Group Search

Group Search Attribute

Select User Role \*

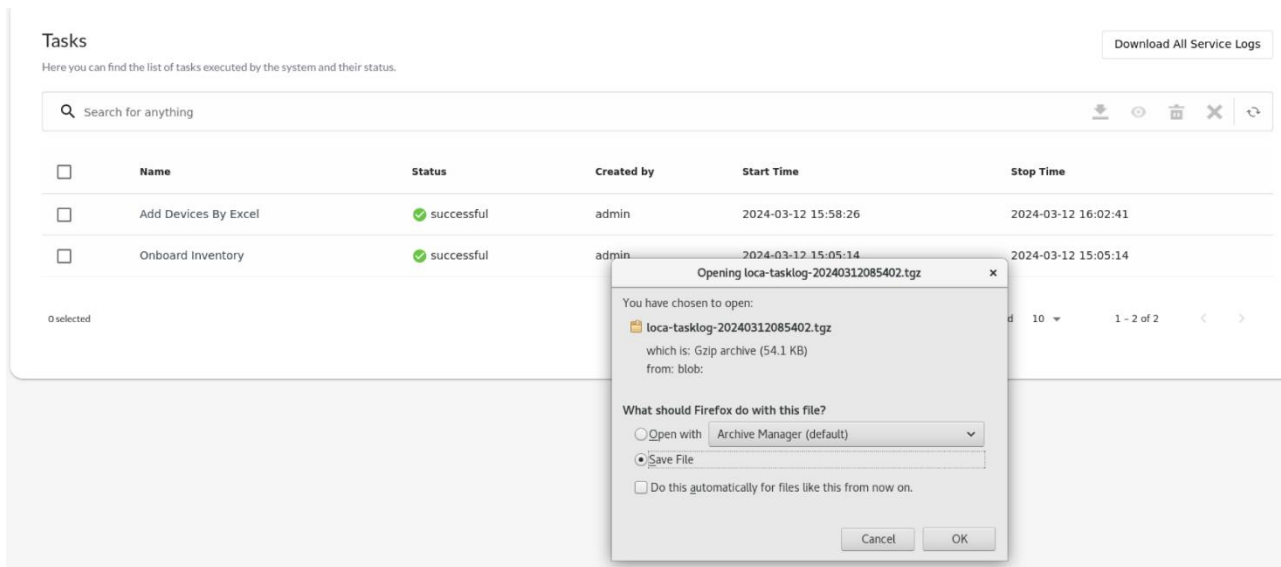
**Figure 109: LDAP authentication configuration**

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

## 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 110: 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 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.

```
[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
36352030302066322063382038342D306620373520386120643520323620616420623820
64300A564D776172652D34322033312038362036352030302066322063382038342D3066
2037352038612064352032362061642062382064300A36353836333134322D663230302D
383463382D306637352D3861643532366164623864300A4E410A41667571627142326C53
724B4D52740A323032342D30362D32305430383A30343A35330A4B3D313B443D320AFEED
FACE

Please input response message:(press Ctrl+D to finish):

```

**Figure 111: 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

```
[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
36352030302066322063382038342D306620373520386120643520323620616420623820
64300A564D776172652D34322033312038362036352030302066322063382038342D3066
2037352038612064352032362061642062382064300A36353836333134322D663230302D
383463382D306637352D3861643532366164623864300A4E410A41667571627142326C53
724B4D52740A323032342D30362D32305430383A30343A35330A4B3D313B443D30AFEEED
FACE

Please input response message:(press Ctrl+D to finish):
DEADC0DE000000040000020071A429F37C96CD47DCD181FAB3F6B4ACE7A4F248133C2445
075AB9FC1549EAFDDBE156E2E90F8514B702BB68B121567D354AC55509265025856A6EC0
929BA9AEBDFE353E20FDCE43EC006F04E95E52275CABC10734DC17607DB2041E308B0ACC
FDD8124B7529D595418E4DDAD00FF17B04A1BF8AFB3718F7F784BFF1D04C4790F32175A4
D8B032AD0410E352F4216188137C1EEA9AF20B928B166C36EAC32E1EC3460F2793FFD410
61B0A851A96CD1D1EACF147C4C897870B1B76AD9CEE6E07B251DCAF29025557D5F983EFF
A7AB46BD5C33AA12FF3BA249E9492075BE747A3377AC04B7D13DD183DE2E246B7267660
4AA340B35970E37BACB3E85C670612C1DAC47F6EE6986A4479F619055E1CDFA5467DF02C
947DC5E0A6681D069337A76BA66189FA9F843410CB46608825508D7EDA458D7733A10331
485033A0542FEA91A5ECB0F938BDCFC4BD3C026D42D51E60D86246FD576F23EF1EB97E49
D289C38A9BEBFA94918DD753574EC46F45156D5541BA462E5927383A0A40EE7096802F8E
32F6FD04E09A645D7BDEE4871E89E1EC2EA6B8BD229292373CB0E9A68986C087E1A900ED
445978A22ACBA03A002193808F93411320F250A45444DB704EDB026B390EEE21D423583F
1F2F51A6AE7E9F9595D8B1CA26CFCE7606931A657091EE49BBAD47B91D3EE5A6E47D6244
722BB05D8557298D51FC0FEA1308D26D7F7EF86C0000000000000000
```

**Figure 112: Input response text**

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



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 115: 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 116: Disable debug shell**

## Known issues and limitations

This release has the following issues and limitations:

- A failed task 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.
- ThinkSystem SD530 and ThinkAgile 2U4N Certified Node models do not support configuring bmc.powerRestorePolicy even if device profile defined it.

- For the ThinkEdge SE455 v3 model, configuring Server Operating Mode in the device profile is not supported. Please remove the Server Operating Mode setting from the device profile before you attempt to apply it to ThinkEdge SE455 v3 servers.
- When deploying Centos8.3 on SE350v2, SE360v2, SE455v3, SE350 models, it is not supported to enable secure boot configuration. So when deploying Centos8.3 on these models, it is necessary to turn off the secure boot in the device profile in advance.
- When deploying RedHat OCP on the SE450 model, it is not supported to enable secure boot configuration. So when deploying HedHat OCP on this model, it is necessary to turn off secure boot in advance in the device profile.
- When deploying Ubuntu18.04 on SE450 models, it is not supported to enable secure boot configuration. So when deploying Ubuntu18.04 on this model, it is necessary to turn off the secure boot in the device profile in advance.
- When running a Baremetal OS deployment task, the subtask “Install OS on server nodes” is not the indicator for OS deployment progress, real OS deployment job is executed in subtask “Execute cloud flavor plugin deployment job”. Example as below:

## Task Detail



Name	Deploy Instance
UUID	095ccf4d-089b-4820-a75d-69d69479311a
Targets	ubuntu001.buch003.alabama.usa.customer.com
Status	Successful
Progress	100%
Created By	regular
Start Time	2024-03-20 17:06:51
Stop Time	2024-03-20 17:31:49

### Subtasks ▼

Configure site DNS resolution	✓ successful	00:00:00.047
Check whether the domain name of each server can be resolved	✓ successful	00:00:00.008
Upgrade firmware for each node	✓ successful	00:00:24.052
Apply device profile to servers	✓ successful	00:00:23.914
Install OS on server nodes	✓ successful	00:00:00.000
Execute pre cloud services deployment	✓ successful	00:00:00.003
Execute cloud flavor plugin deployment job	✓ successful	00:23:45.914
Execute post script after flavor operated	✓ successful	00:00:00.009
Execute post cloud services deployment	✓ successful	00:00:00.006

Close

**Figure 117: OS deployment subtasks**

- 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.

OnBoard	Onboard LAN 1 Port1	Ethernet	OnBoard	N/A
▼ PCI Summary				
Segment Number	0	Bus Number	4	
Device Number	0	Function Number	0	
Vendor ID	0x8086	Device ID	0x125D	
Sub Vendor ID	0x8086	Sub Device ID	0x0000	
Slot Designation	Onboard LAN 1 Port1	Support Hot Plug	No	
Revision ID	0x0004			

**Figure 118: Unsupported onboard LAN ports in server inventory**

## 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.