

# Deploying an Application

- Prerequisites
- Process
- Cloud-Specific Configuration
- One-Click Deployment

## Prerequisites

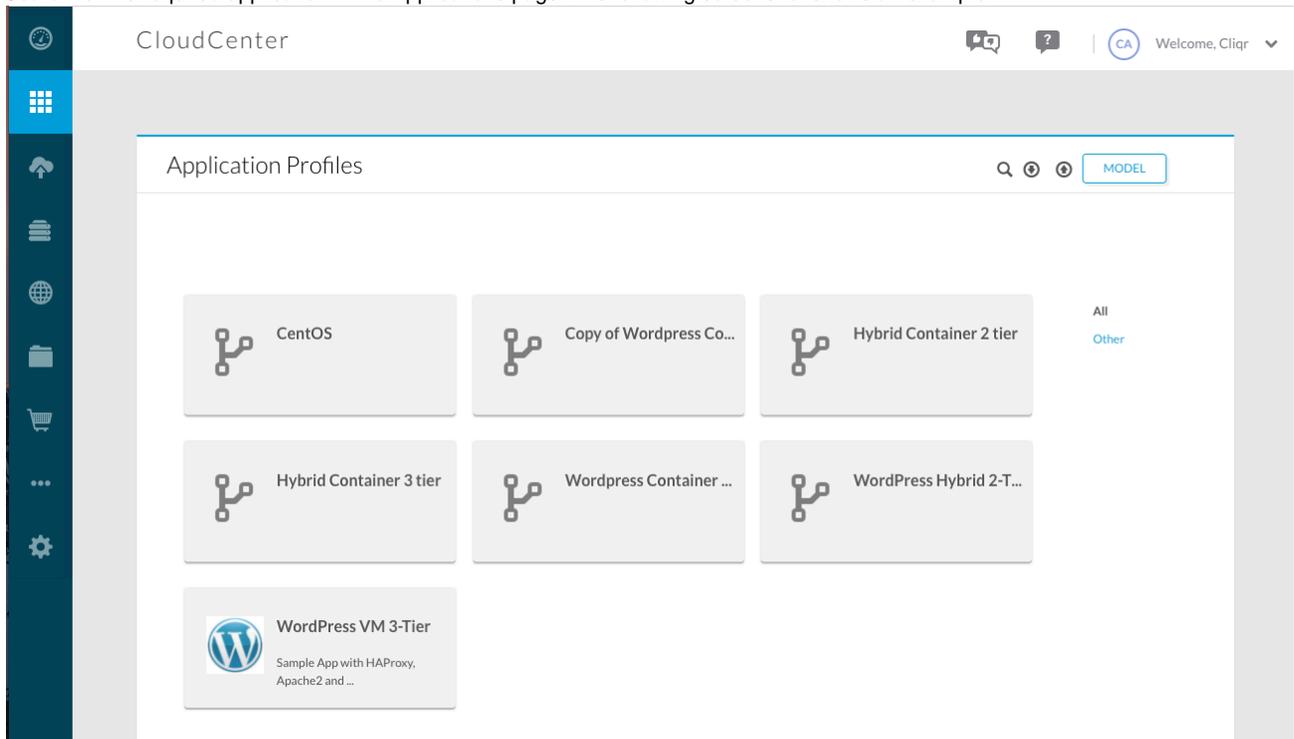
To deploy an application, you should have already performed the following tasks:

- Created an application: See [Model a New Application](#) for additional context.
- Created a deployment environment: See [Deployment Environments](#) for additional context.

## Process

To deploy an application, follow this process:

1. Access the application from the CCM UI and click **Applications**.
2. Search for the required application in the Applications page. The following screenshot shows an example.



3. To deploy an application, left click on it. This brings up Page 1 of the Deploy form, as shown in the following screenshot.

The screenshot shows the 'General Settings' section of a deployment form. It includes fields for 'DEPLOYMENT NAME' (DocDeploy), 'APPLICATION VERSION' (6), and 'DEPLOYMENT ENVIRONMENT' (CCQA\_deploy\_env, kubernetes, sidenv). Below these are sections for 'AGING POLICY' (aging\_policy\_time), 'SUSPENSION POLICY' (suspension\_policy\_BA\_11P), 'TIMEZONE' ((GMT-07:00) Mountain Standard Time/Pacific Daylight Tim-), and 'TAGS'. A tooltip for 'KUBERNETES default' is visible over the 'kubernetes' environment card.

The 'Metadata' section contains a table with columns 'NAME', 'VALUE', and 'ACTIONS'.

NAME	VALUE	ACTIONS
META_EDIT	Editable	
META_MAND	Mandatory	
META_MAND_EDIT	Mandatory and Editable	
Name	%JOB_NAME%	

At the bottom of the Metadata section is a button labeled '+ ADD METADATA'.

In the **General Settings** section, you must give the deployment a name. You can also optionally select a deployment environment, policy or policies, timezone, tags, terminate/suspend protection, and add metadata as required. The deployment environment boards display the name, description, and list of clouds available in this environment.

Tags do not influence the application of policies and users can enter custom tags in the deploy form in addition to selecting from the pre-populated tags for both the application profile and the deployment environment. Additionally, users can delete tags if they are not locked.

While the Aging, Suspension, and Security policies dropdown options are populated based on the deployment environment, the Scaling policies dropdown options are populated based on the application profile. See [Policies](#) for additional context.

The tags are populated based on both the deployment environment and the application profile. You can also add on custom tags for the entire deployment and for each tier in the deploy form at deploy time. See [System Tags](#) for additional context.

4. Scroll down to the enter any global parameters, if defined in the [Application Profile](#), and any per tier settings. The following screenshot shows an example.

The screenshot displays two configuration sections: 'Global Parameters' and 'Tier Settings'.

**Global Parameters**

- GLOBAL\_PARAM\_STRING**: Input field containing 'Global String Param Value'.
- \* GLOBAL\_PARAM\_NUMBER**: Input field containing '1'.
- \* GLOBAL\_PARAM\_LIST**: Dropdown menu showing '123'.
- \* GLOBAL\_PARAM\_PWDWC**: Password field with masked characters '\*\*\*\*\*'.
- \* CONFIRM PASSWORD**: Password field with masked characters '\*\*\*\*\*'.
- \* GLOBAL\_PARAM\_WS**: Dropdown menu showing 'Param 1'.
- GLOBAL\_PARAM\_PATH**: A dropdown menu labeled 'Select a Location' and an adjacent input field containing 'auto/record\_results.sh'.
- \* GLOBAL\_PARAM\_TEXT**: Text area containing the regex pattern: `|@m a T3xt Area with '-:|@#5%^&_-=+[]|:'",.<->/?`

**Tier Settings**

**CentOS\_1**

- \* NUMBER OF NODES**: Input field containing '1' with a 'max:10' label.
- STORAGE SYSTEM**: Text label 'None available'.
- TAGS**: Text label with a help icon.

You can optionally provide per-tier settings for each tier in your application. Keep scrolling down to see all tiers. Some tiers will have settings for other parameters based on the [Application Profile](#) requirements.

### Tier Settings

#### CentOS\_1

\* NUMBER OF NODES

 max:10

STORAGE SYSTEM

None available

TAGS ⓘ

PARAMETERS

\* TIER\_PARAM\_NUMBER ⓘ

TIER\_PARAM\_LIST ⓘ

\* TIER\_PARAM\_PWDWC ⓘ

\* CONFIRM PASSWORD

TIER\_PARAM\_PWD ⓘ

\* TIER\_PARAM\_TEXT ⓘ

TIER\_PARAM\_WS ⓘ

ENVIRONMENT VARIABLES

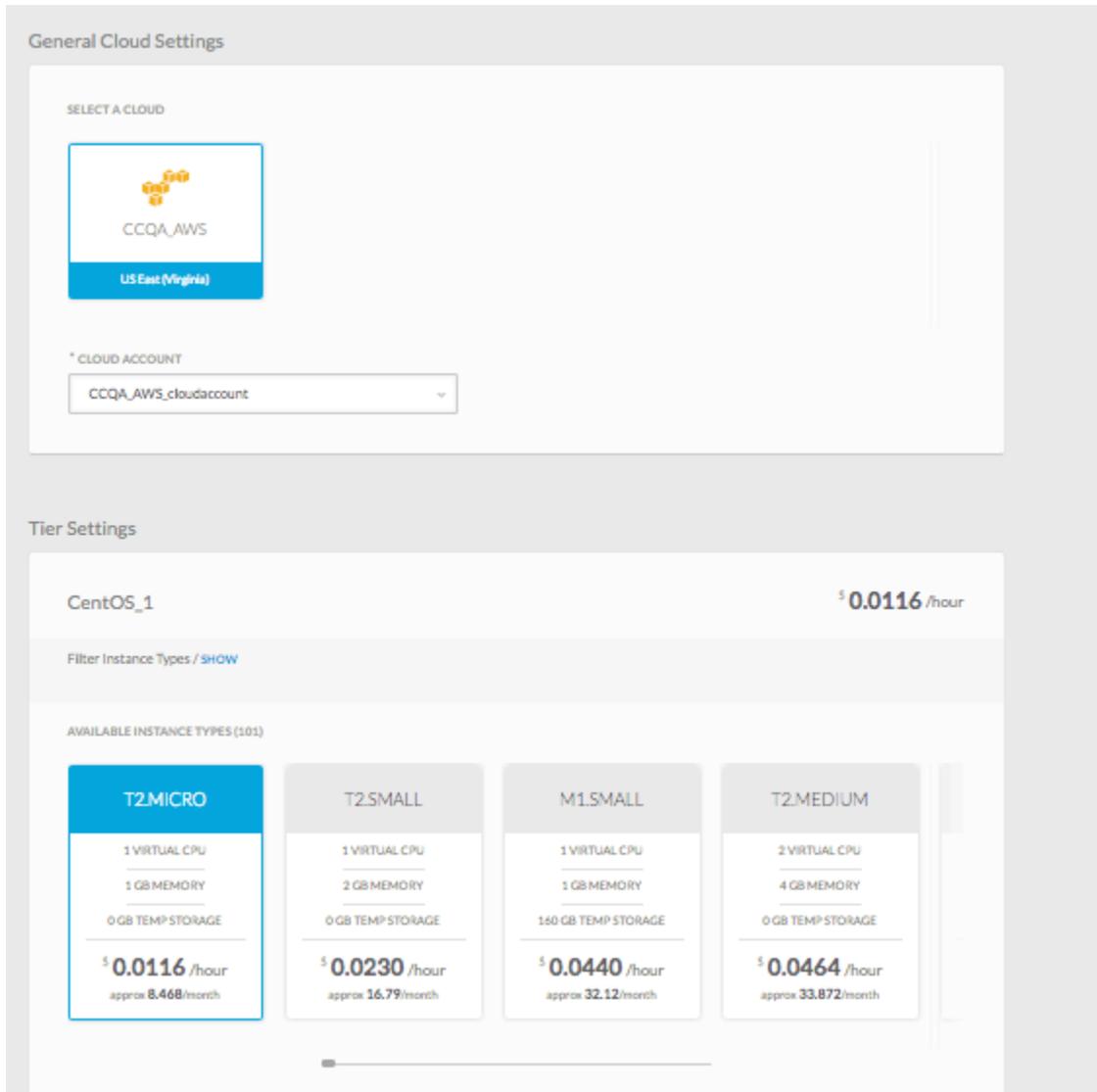
ENV\_PARAM\_VISIBLE

\* ENV\_PARAM\_EDITABLE

\* ENV\_PARAM\_OPTIONAL

NEXT

1. Click **Next** to go to Page 2 of the Deploy form and select the cloud provider and then the cloud account, as shown in the following screenshot.



2. Scroll down further to specify the tier settings for each tier. What is shown in the tier settings of the deploy form is determined by the corresponding Default Tier Cloud Settings in the Deployment Environment form. These include instance type and volume settings as shown above. Scrolling down further will display the the cloud settings and SSH options, as shown in the following screenshot.

Tier Settings

CentOS\_1 \$ 0.0116 /hour

Filter Instance Types / SHOW

AVAILABLE INSTANCE TYPES (101)

T2.MICRO	T2.SMALL	M1.SMALL	T2.MEDIUM
1 VIRTUAL CPU 1 GB MEMORY 0 GB TEMP STORAGE	1 VIRTUAL CPU 2 GB MEMORY 0 GB TEMP STORAGE	1 VIRTUAL CPU 1 GB MEMORY 160 GB TEMP STORAGE	2 VIRTUAL CPU 4 GB MEMORY 0 GB TEMP STORAGE
\$ 0.0116 /hour approx 8.468/month	\$ 0.0230 /hour approx 16.79/month	\$ 0.0440 /hour approx 32.12/month	\$ 0.0464 /hour approx 33.872/month

Volumes

VOLUME	PRICE	SIZE	TYPE
Root Disk ⓘ	\$0.10/month	GB	General Purpose SSD
Additional Volume1	\$2.00/month	20 GB	General Purpose SSD

Cloud Settings

INSTANCE PROFILE ARN ⓘ

arnaws:iam::123456789012:instance-profile/my-instance

\* VPC

vpc-3e41595b (vpc-default-us-east-1) | CIDR 172.31.0.0/16

NIC 1

\* NETWORK

subnet-1fafee46 | us-east-1a | CIDR 172.31.16.0/20

\* PRIVATE IP ALLOCATION

DHCP

ASSIGN PUBLIC IP

ON

[NETWORK INTERFACE CONTROLLER](#)

SSH Options

Adjust any settings as required and click the Deploy button to deploy this application immediately, or click the clock icon to the right of the Deploy button to schedule deploying this application in the future.

## Cloud-Specific Configuration

This section provides details on configuring the **Cloud Settings** section and the **Network Settings** section for each cloud.

If you do not see the required instance type listed in this section, be sure to add the instance type first. See [Manage Instance Types](#) for additional context.

Once you configure the cloud settings, you have two control options to identify if the **Cloud Settings** should be:

- **Visible** (Default) to your end users by toggling the control switch.
- **Configurable** (Default) by your end users by toggling the control switch.

Toggle the required settings as required for your deployment environment defaults.

- [VMware - Cloud and Network Settings](#)

### VMware Network Settings

1. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to use preconfigured ACI extensions.
    1. Select the Network in the NIC section. See [IP Allocation Mode](#) for additional context on NIC configuration.
    2. Add additional NICs, if required.
  - **ON:** End users are allowed to use preconfigured ACI extensions.
    1. Select the required extension, the corresponding options are displayed in the dropdown list for the remaining fields (see [Extensions](#) for additional details):
    2. Select the **APIC Extension** from the dropdown list (see [ACI Extensions](#) for additional details).
    3. Select the **APIC Virtual Machine Manager (VMM)** associated with this APIC Extension from the filtered dropdown list .
    4. Select the **APIC Tenant** associated with this APIC Extension from the filtered dropdown list.
2. Select the Network in the NIC section.
  - If you select **VMware**, select the Network in the NIC section. See [IP Allocation Mode](#) for additional context on NIC configuration.
  - If you select **Cisco ACI**, select the type in the **End Point Group (EPG) Type** field.
    1. **Existing EPG:** If you select this type, you must further select a pre-existing EPG (that is already connected to one of the Bridge Domains) from the **Existing EPG** dropdown, which appears if you select this type.
    2. **New EPG:** If you select this type, you must further select a pre-existing Bridge Domain (to which this EPG must connect) from the **Bridge Domain** dropdown list.
    3. **Bridge Domain Template:** See [Extensions](#) for additional context.
3. Add additional NICs, if required.

### SSH Options

See [SSH Options](#) for additional context.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)

- [vCD - Cloud and Network Settings](#)

### vCD Network Settings

1. Select the Network in the NIC section. If you select **vCD**, select the OrgVdcNetwork in the NIC section. See [IP Allocation Mode](#) for additional context on NIC configuration
2. Add additional NICs, if required.

### SSH Options

See [SSH Options](#) for additional context.

**Back to:**

- [Deploying an Application](#)

- [Deployment Environments](#)

- [OpenStack - Cloud and Network Settings](#)

### OpenStack Network Settings

1. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to associate the public IP with the NIC.
  - **ON:** End users are allowed to associate the public IP with the NIC.
2. Select the required **Network** in the NIC section.
3. Select the **Private IP Allocation** mode in the NIC section. See [IP Allocation Mode](#) for additional context on NIC configuration.
  1. **DHCP:** (Default) This strategy allows the IP to be allocated by the DHCP server to the instance on server boot up. This IP address is not known prior to server boot up.
  2. **Preallocate IP:** This strategy allows the cloud infrastructure IP allocation to be dynamically provided before the server boots up.
4. Add additional NICs, if required.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)
- [OpenStack Configurations](#)

- [IBM BlueMix \(SoftLayer\) - Cloud and Network Settings](#)

### IBM Cloud Network Settings

The Default Private VLAN & Default Public VLAN fields are not available as region-level settings when you [Configure an IBM Cloud](#). Instead, you can configure the following settings.

You have the option to configure these details:

1. Select the required **Private VLAN and Subnet** fields in the Cloud Settings section. These fields specify the default private cloud network to which this CloudCenter instance must be launched.
2. Toggle the **Visibility** switch to determine if you want to allow your end users to configure the Public IP settings.
  1. **OFF:** (Default) End users are not allowed to assign the public IP.
  2. **ON:** End users are allowed to assign the public IP.
3. Select the required **Public VLAN and Subnet** fields. These fields specify the default public cloud network to which this CloudCenter instance must be launched.

**Back to:**

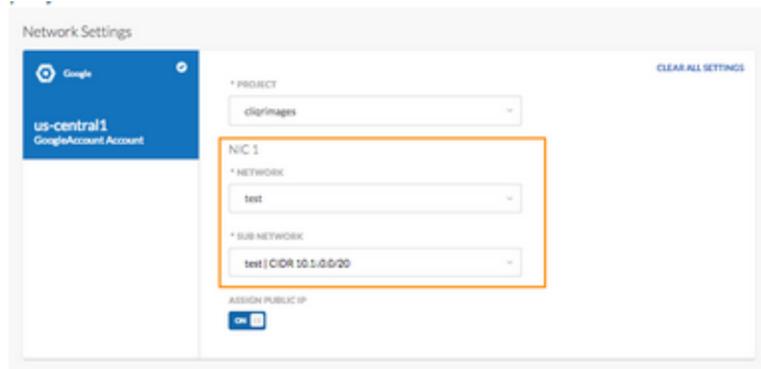
- [Deploying an Application](#)
- [Deployment Environments](#)

- [Google - Cloud and Network Settings](#)

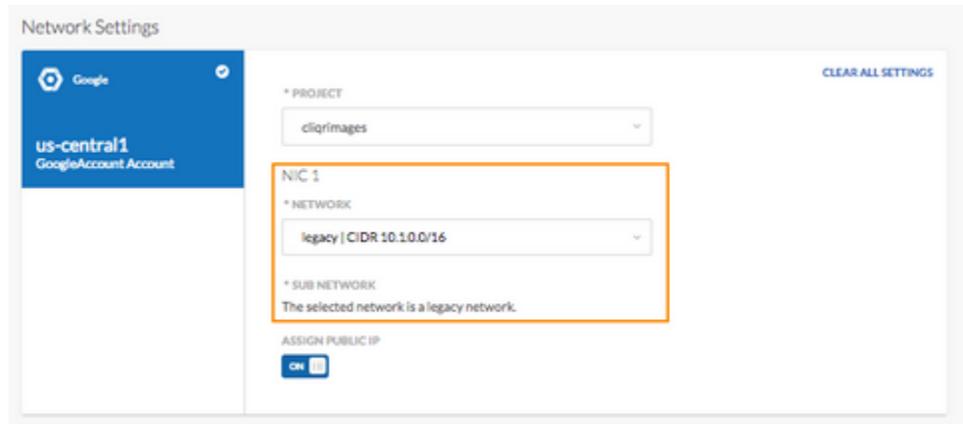
### Google Network Settings

The NIC configuration and Simplified Networks configuration is available for both networks and sub-networks. The CloudCenter platform only supports a single NIC configuration.

1. Select one of the configured networks retrieved from Google cloud:
  - **Non-legacy Networks** – Select the required network and then select the sub-network-based Google project (or the CloudCenter-specific Shared VPC host project) contained within that network.



- **Legacy Networks** – Select the legacy network and the sub-network selection is no longer available.



2. Select the checkbox to indicate if a public IP in the NIC section. See [IP Allocation Mode > Cloud-Specific Nuances > Google](#) for additional context.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)

- [Dimension Data Cloud and Network Settings](#)

**AWS Network Settings**

1. Select the required option from the dropdown list for the **Network Domain** field.
2. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to associate the public IP with the NIC.
  - **ON:** End users are allowed to associate the public IP with the NIC.
3. Select the required **VLAN** and **Public IP** in the NIC section.
4. Add additional NICs, if required.

Each NIC must be assigned to a VLAN and only one NIC is allowed per VLAN. Firewall rules and security policies are applied to all NICs.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)

- [Container Cloud - Kubernetes Cloud Settings](#)

**Kubernetes Cloud Settings**

Select the **Kubernetes Settings** from the **Namespace** dropdown list, if applicable. The list is automatically populated and only requires a selection to be made. Go back to the following pages for related details.

- [Container Clouds](#) for additional cloud-specific details.
- [Deploying an Application](#) for the deployment process

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)

- [Azure Stack - Cloud and Network Settings](#)

### Azure Stack Network Settings

1. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to associate the public IP with the NIC.
  - **ON:** End users are allowed to associate the public IP with the NIC.
2. Select the required **Subnet** in the NIC section.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)
- [Azure Stack Configurations](#)

- [AzureRM - Cloud and Network Settings](#)

### AzureRM Network Settings

Configure the fields described in the table below for AzureRM cloud regions. These fields are configurable for the following features:

- [Deploying an Application](#)
- [Deployment Environments](#)

To configure network settings for AzureRM environments, follow this procedure.

1. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to associate the public IP with the NIC.
  - **ON:** End users are allowed to associate the public IP with the NIC.
2. Select the required **Subnet** in the NIC section.
3. Add additional NICs, if required.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)
- [AzureRM Configurations](#)

- [Azure Pack - Cloud and Network Settings](#)

### Azure Pack Cloud Settings

Configure the fields described in the table below for Azure Pack cloud regions. These fields are configurable for the following features:

- [Deploying an Application](#)
- [Deployment Environments](#)

### Azure Pack Network Settings

1. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to associate the public IP with the NIC.
  - **ON:** End users are allowed to associate the public IP with the NIC.

2. Select the required **Subnet** in the NIC section.
3. Add additional NICs, if required.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)

- [AWS - Cloud and Network Settings](#)

### **AWS Subnet and Deployment Nuances**

#### *Pinning Behavior in AWS Network Settings*

When configuring the Deployment Environments defaults for AWS, be aware of the following nuances:

- You have the option to select multiple subnets for the first NIC (NIC1) and among those subnets you can pin one subnet. The pinned subnet becomes the default network for this VM
- Subsequent NICs (NIC2, NIC3, ...) only list subnets that belong to the availability zone of the pinned subnet of the first NIC. Example, in NIC1 the pinned subnet belongs to the availability zone *us-west-1b*, then subsequent NICs only list subnets belonging to the first NIC's *us-west-1b* zone.

Multiple NICs do not span across different zones.

#### *AWS Availability Sets Behavior*

During a job deployment - If you launch

- A clustered VM setup, the subnet set is passed as the job payload.
- A single VM setup, the VM is launched as the pinned subnet.

### **AWS Network Settings**

Configure the fields described in this section for AWS cloud regions. These fields are configurable for the following features:

- [Deploying an Application](#)
- [Deployment Environments](#)

To configure network settings for AWS environments, follow this procedure.

1. Select the required option from the dropdown list for the **VPC** field. See [AWS Configurations](#) for additional context.
2. Toggle the **Visibility** switch to determine if you want to allow your end users to use pre-configured settings.
  - **OFF:** (Default) End users are not allowed to associate the public IP with the NIC.
  - **ON:** End users are allowed to associate the public IP with the NIC.
3. Select the required **Network** in the NIC section.
4. The **Private IP Allocation** mode in the NIC section defaults to **DHCP**. The DHCP strategy allows the IP to be allocated by the DHCP server to the instance on server boot up. This IP address is not known prior to server boot up. See [IP Allocation Mode](#) for additional context on NIC configuration.
5. Add additional NICs, if required.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)
- [AWS Configurations](#)
- [Availability Sets and Zones](#)

- [Alibaba - Cloud and Network Settings](#)

### **Alibaba Network Settings**

Configure the fields described in the table below for Alibaba cloud regions. These fields are configurable for the following features:

- [Deploying an Application](#)
- [Deployment Environments](#)

To configure network settings for Alibaba environments, follow this procedure.

1. Configure the Instance Password
2. Select the required **Subnet** in the NIC section.

**Back to:**

- [Deploying an Application](#)
- [Deployment Environments](#)

## One-Click Deployment

When you submit the application for deployment, CloudCenter reads the application profile and orchestrates the following tasks with one click:

- Provisions and configures cloud infrastructure and services based on the Application Profile requirements (compute, storage, and network).
- Launches VMs to access the application packages, data, and scripts referenced in the profile and mounts them to the storage repository on the selected cloud.
- Deploys the application components for the various tiers or steps as determined in the application profile.
- Starts each application service in the right order based on service dependencies.

During each orchestration stage, CloudCenter sends status messages to the CCM for users to track the application deployment phase and status.

After the application is deployed in the cloud, it is listed click **Access** *<app name>* to open the IP address where the application is hosted.

### Note

Depending on the context path of the application in the application server, you may need to specify the full path in the browser (for example, `http(s)://<IP address>/app-context-path`).

Configure the Launch URL field with this path when creating the application profile.

Once the application is running, the CloudCenter application provides the ability to securely access cloud VMs using SSH or VNC to directly launch the application from any browser. You can use this method to troubleshoot or run one-off custom commands or scripts.