Cisco UCS Director Getting Started Guide, Release 6.5

Revised: July 10, 2017,

Getting Started with Cisco UCS Director

Cisco UCS Director

Cisco UCS Director is a complete, highly secure, end-to-end management, orchestration, and automation solution for a wide array of Cisco and non-Cisco data infrastructure components, and for the industry's leading converged infrastructure solutions based on the Cisco UCS and Cisco Nexus platforms. For a complete list of supported infrastructure components and solutions, see the Cisco UCS Director Compatibility Matrix.

Cisco UCS Director is a 64-bit appliance that uses the following standard templates:

- Open Virtualization Format (OVF) for VMware vSphere
- Virtual Hard Disk (VHD) for Microsoft Hyper-V

Management through Cisco UCS Director

Cisco UCS Director extends the unification of computing and networking layers through Cisco UCS to provide you with comprehensive visibility and management of your data center infrastructure components. You can use Cisco UCS Director to configure, administer, and monitor supported Cisco and non-Cisco components. The tasks you can perform include the following:

- Create, clone, and deploy service profiles and templates for all Cisco UCS servers and compute applications.
- Monitor organizational usage, trends, and capacity across a converged infrastructure on a continuous basis. For example, you can view heat maps that show virtual machine (VM) utilization across all your data centers.
- Deploy and add capacity to converged infrastructures in a consistent, repeatable manner.
- Manage, monitor, and report on data center components, such as Cisco UCS domains or Cisco Nexus network devices.
- Extend virtual service catalogs to include services for your physical infrastructure.
- Manage secure multi-tenant environments to accommodate virtualized workloads that run with non-virtualized workloads.

Automation and Orchestration with Cisco UCS Director

Cisco UCS Director enables you to build workflows that provide automation services, and to publish the workflows and extend their services to your users on demand. You can collaborate with other experts in your company to quickly and easily create policies. You can build Cisco UCS Director workflows to automate simple or complex provisioning and configuration processes.

Once built and validated, these workflows perform the same way every time, no matter who runs the workflows. An experienced data center administrator can run them, or you can implement role-based access control to enable your users and customers to run the workflows on a self-service basis, as needed.

With Cisco UCS Director, you can automate a wide array of tasks and use cases across a wide variety of supported Cisco and non-Cisco hardware and software data center components. A few examples of the use cases that you can automate include, but are not limited to:

- VM provisioning and lifecycle management
- Network resource configuration and lifecycle management

- Storage resource configuration and lifecycle management
- Tenant onboarding and infrastructure configuration
- Application infrastructure provisioning
- Self-service catalogs and VM provisioning
- Bare metal server provisioning, including installation of an operating system

Obtaining a License

About Licenses

You must obtain a license to use Cisco UCS Director, as follows:

1. Before you install Cisco UCS Director, generate the Cisco UCS Director license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in Fulfilling the Product Access Key, on page 3.
3. After you install Cisco UCS Director, update the license in Cisco UCS Director as described in Updating the License, on page 6.
4. After the license has been validated, you can start to use Cisco UCS Director.

Fulfilling the Product Access Key

Before You Begin

You need the PAK number.

Procedure

Step 1 Navigate to the Cisco Software License website.

Step 2 If you are directed to the Product License Registration page, you can take the training or click **Continue to Product License Registration**.

Step 3 On the Product License Registration page, click **Get New Licenses from a PAK or Token**.

Step 4 In the **Enter a Single PAK or TOKEN to Fulfill** field, enter the PAK number.

Step 5 Click **Fulfill Single PAK/TOKEN**.

Step 6 Complete the additional fields in **License Information** to register your PAK:

Name	Description
Organization Name	The organization name.
Site Contact Name	The site contact name.
Street Address	The street address of the organization.

Name	Description
City or Town	The city or town.
State or Province	The state or province.
Zip or Postal Code	The zip code or postal code.
Country	The country name.

Step 7 Click **Issue Key**.
The features for your license appear, and you receive an email with the Digital License Agreement and a zipped license file.

Installing Cisco UCS Director

Cisco UCS Director can be hosted on a VMware vSphere or vCenter, or on a HyperV environment. For more information on system requirements, prerequisite, and installation procedure, refer the Cisco UCS Director Installation on VMware vSphere Guide and Cisco UCS Director Installation on Microsoft Hyper-V Manager Guide.

The multi-node setup is supported for Cisco UCS Director on a 64-bit operating system only. With a multi-node setup, you can scale Cisco UCS Director to support a larger number of VMs than is supported by a single installation of Cisco UCS Director. For more information on installation and configuration of Cisco UCS Director on multi-node setup, refer the Cisco UCS Director Multi-Node Installation and Configuration Guide.

Configuring the Network Interface in ShellAdmin

This procedure is optional.

Procedure

Step 1 Log in to the Cisco UCS Director VM console with the shelladmin user credentials:
If this is the first time you have logged into the ShellAdmin after deployment, you will be prompted to change the default password.

Step 2 Choose `Configure Network Interface`.

Step 3 At the `Do you want to Configure DHCP/STATIC IP [D/S]` prompt, enter one of the following choices:

- If DHCP is enabled, enter D (IP addresses are assigned automatically)
- To configure static IP, enter S, and then choose the interface you want to configure at the next prompt followed by the option to select IPv4 or IPv6. This is followed by the confirmation of the interface selected and the version of IP for which you select **Y** to continue. Then enter the following details:
  - IP address

- Netmask
- Gateway
- DNS Server 1
- DNS Server 2

Step 4 Confirm when prompted.

Accessing the Cisco UCS Director GUI

Initial Login

Log into Cisco UCS Director by hostname or IP address with the following credentials:

- Username: admin
- Password: admin

Note We recommend that you delete the startup admin account after you create the first admin account or, at least, change the default password. To access the End User Portal, you must have a valid email address.

Changing the Admin Password

You are prompted to change the default admin user password after you log into Cisco UCS Director for the first time. On Subsequent login, you can follow these steps to change the admin user password.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.
Step 2 On the **Users and Groups** page, click **Users**.
Step 3 Click the row with the administration user for which you want to change the default password.
Step 4 From the **More Actions** drop-down list, choose **Change Password**.
Step 5 On the **Change Password** screen, enter the old password and then the new password and confirm it.
Step 6 Click **Save**.

Updating the License

Before You Begin

If you received a zipped license file by an email, extract and save the license (.lic) file to your local machine.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Keys**.

Step 3 Click **Update License**.

Step 4 On the **Update License** screen, do the following:

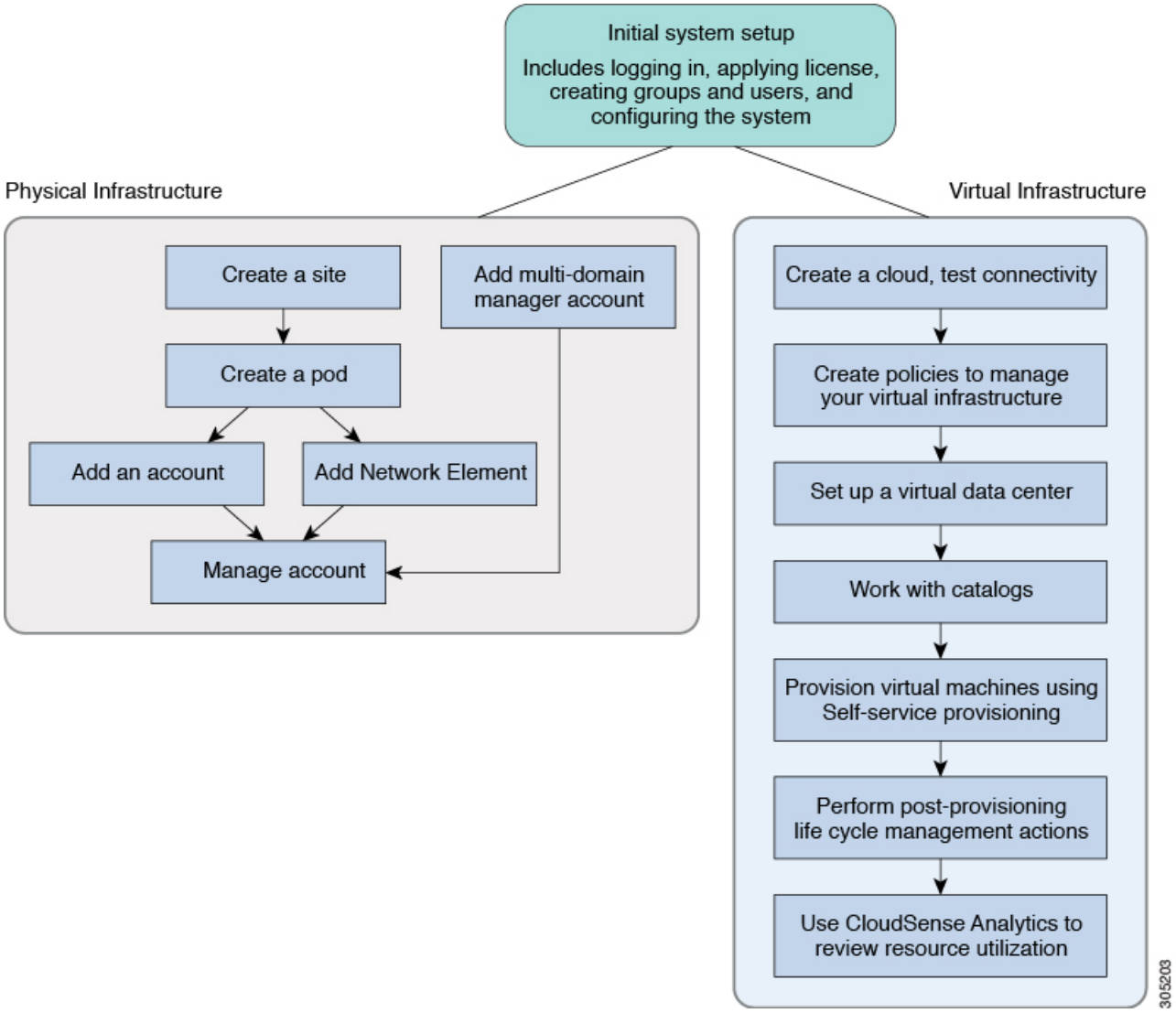
a) Drop the `.lic` file from your local system or click **Select a File** and navigate to the location where you stored the `.lic` file.
To enter license text instead of file upload, check the **Enter License Text** checkbox and enter the license text in the **License Text** field.

b) Click **Submit**.
The license file is processed, and a message appears confirming the successful update.

Cisco UCS Director System Setup

The following figure illustrates the workflow to set up your environment using Cisco UCS Director:

Figure 1: Sample Workflow to Set up Your Environment



Initial System Setup

Procedure

Step 1 Log into Cisco UCS Director.

Step 2 Choose **Administration** > **Guided Setup**.

Step 3 On the **Guided Setup** page, double-click **Initial System Configuration**.

Note Although the Guided Setup wizard allows you to uncheck and skip steps, the recommended approach is to perform all steps in the process.

Step 4 Drop the license file or Click **Select a File** to specify the location of the license file for the Cisco UCS Director software that you downloaded from the Cisco website.
To enter the license text, check the **Enter License Text** checkbox and enter the license text in the **Licese Text** field.

Note If you have uploaded license file already as per the Updating the License, on page 6 procedure, click **Skip**.

Step 5 After the upload is complete, click **Next**.

Step 6 From the **Language** drop-down list, choose your preferred language setting.

Note After completing all the tasks in the wizard, you must log out and log back into the system for the locale changes to take effect.

Step 7 Click **Next**.

Step 8 In the **DNS Server** screen, enter the IP address of the one or more DNS servers.

Step 9 Click **Next**.

Step 10 Iin the **Mail Server** screen, configure the mail server settings. This configuration allows Cisco UCS Director to send email notifications to administrators and users.
Check the **Send a Test Email** check box in the **Mail Server** screen, to send a test message to verify that Cisco UCS Director can communicate with the mail server. In the **Test Email Address** field, enter the email address to receive notification and approval messages from Cisco UCS Director.

Note Consider naming the outgoing email address with Cisco UCS Director nomenclature so that administrators and users can easily identify the source of email messages.

Step 11 Click **Next**.

Step 12 In the **NTP Server** screen, enter the name or IP address of one or more Network Time Protocol (NTP) servers.

Step 13 Click **Next**.
Cisco UCS Director displays a summary of the configurations.Review the settings and modify them as needed.

Step 14 Click **Next** to view the recommended next steps.

Step 15 Click **Close** to save the configurations.

Creating a User Group

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Click **Add**.

Step 4 On the **Add Group** screen, complete the following fields:

Field Name	Description
Name field	The name of the group or the customer organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '@
Description field	The description of the group or the customer organization, if required.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.
Phone field	The contact's phone number.
Address field	The contact's address.
Group Share Policy drop-down list	Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies.
Allow Resource Assignment To Users check box	If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

What to Do Next

Repeat this procedure if you want to add more groups. For each group that you add, you can edit resource limits, manage tags, and customize the logo and application labels.

Adding Users

Before You Begin

Ensure that you have created a group before you add a user to it.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Click **Add**.

Step 4 On the **Add User** screen, complete the required fields, including the following:

Field Name	Description
User Role drop-down list	Choose the role type for the user.
User Group drop-down list	Select the group that the user will have access to. You can either select a group already available, or you can add a new group. **Note** This field is visible only when you select Service End-User or Group Admin as the user role.
MSP Organization drop-down list	Select the MSP organization that the user will manage. You can either select an organization that is currently available, or you can add a new organization. **Note** This field is visible only when you select **MSP Admin** as the user role.
Login Name field	The login name. You can include special characters such as ( ). & - _ `~ $% ^ {}! ' @
Password field	The password. **Note** If Lightweight Directory Access Protocol (LDAP) authentication is configured for the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	The password is entered again for confirmation.

Field Name	Description
User Contact Email field	The email address. **Note** The email address is required to notify the group owner about the service request status and to request approval.
First Name field	The first name.
Last Name field	The last name.
Phone field	The phone number of the user.
Address field	The office address of the user.
Set user disable date check box	Check to set the date and time when the user account must be disabled in the system. Disabling a user account means that the user can no longer log in into the system. A week prior to this date, an email message stating that the account will be disabled is sent to the user. This automatic email message is generated and sent by the **PeriodicNotificationToUserTask** system task. On the specified date and time, the user account is disabled automatically. If the user is logged in to the system on the date specified, then the login session is terminated automatically.
Locale drop-down list	Choose a language for the system specifically for this user. By default, the language is set to English. When this user logs in, the user interface is displayed in the language you selected. This locale selection applies only to this user.
Login with Classic View check box	Check to launch the Classic View user interface when this user logs in to the system. The capability to set the system to launch the Classic View for other users is available only in Release 6.5. The Classic View will be removed in a subsequent release.

Step 5 Click **Add**.

What to Do Next

Click a row with a user and click **Manage Profiles**, to optionally assign multiple roles for that user.

Setup for Physical Infrastructure

About Managing a Physical Infrastructure

Cisco UCS Director enables you to manage both physical and virtual infrastructures. While managing a physical account, you would need to first create a site, and add a pod to the site. After you create this account, Cisco UCS Director discovers all components within the newly created physical account. Typically, the discovery process takes about 5 minutes. In the system, you can either add a new pod or you can use the default pod that is available. A physical account can be associated with the default pod or with one that you add.

Note As an administrator, you can create either a physical account or a virtual account first in the system. A physical account in Cisco UCS Director has no dependency on a virtual (cloud) account.

Adding a Site

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Site Management**.

Step 3 Click **Add**.

Step 4 On the **Add Site** screen, complete the following fields:

Name	Description
Site Name field	A descriptive name for the site.
Description field	The description of the site, such as the location, significance, and so on.
Contact Name field	The name of the person responsible for this site.

Step 5 Click **Submit**.

Adding a Pod

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Pods**.

Step 3 Click **Add**.

Step 4 On the **Add Pod** screen, complete the following fields:

Name	Description
Name field	A descriptive name for the pod.
Type drop-down list	Choose the type of pod that you want to add. This can be one of the following: • **Flexpod** • **VersaStack** • **Generic** • **ExpressPod Medium** • **VSPEX** • **ExpressPod Small** • **Vblock** • **HyperFlex** • **Virtual SAN Pod** The nongeneric pod types accommodate only specific physical and virtual components. A generic pod does not require a specific pod license. You can add any type of physical or virtual component to a generic pod. For more information about bundled pod licenses (FlexPod, Vblock, and VSPEX), which include the necessary individual device licenses to run a pod, see the Cisco UCS Director Installation and Upgrade Guides. **Note** Only VersaStack and Generic pods are supported in the IBM accounts in Cisco UCS Director.
Site drop-down list	Choose the site where you want to add the pod. If your environment does not include sites, you can omit this step.
Description field	(Optional) A description of the pod.
Address field	The physical location of the pod. For example, this field could include the city or other internal identification used for the pod.

Name	Description
Hide Pod check box	Check to hide the pod if you do not want it to show in the Converged Check View. You can continue to add or delete accounts from the pod. For example, you can use this check box to ensure that a pod that does not have any physical or virtual elements is not displayed in the Converged View.

Step 5 Click **Add**.

What to Do Next

Add one or more accounts to the pod.

Adding a Physical Account

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Physical Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which this physical account belongs.
Category drop-down list	Choose the category type (Computing or Storage). If you chose Storage, continue to Step 6.
Account Type drop-down list	Choose from the following account types for this physical account: • **UCSM** • **HP ILO** • **Cisco Rack Server (CIMC)** • **IPMI**

Step 5 Click **Submit**.

Step 6 On the **Add Account** screen, complete the following fields:

Name	Description
Authentication Type drop-down list	Choose from the following authentication types to be used for this account: • **Locally Authenticated—**A locally authenticated user account is authenticated directly through the fabric interconnect and can be enabled or disabled by anyone with admin or AAA privileges. • **Remotely Authenticated—**A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.
Server Management drop-down list	Choose how servers are managed by this account by selecting one of the following options: • **All Servers** • **Selected Servers**
Account Name field	A unique name for the physical account that you want to add.
Server Address field	The IP address of the server.
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	The username for accessing this account. This field is not displayed if you choose to use a credential policy.
Password field	The password associated with the username. This field is not displayed if you choose to use a credential policy.
Transport Type drop-down list	Choose the transport type that you want to use for the account. This can be one of the following: • **HTTP** • **HTTPS** This field is not displayed if you choose to use a credential policy.

Name	Description
Port field	The server port number. This field is not displayed if you choose to use a credential policy.
Description field	The description of the account.
Contact Email field	The contact email address for the account.
Location field	The location.
Service Provider field	The service provider's name, if any.

Step 7 If this account is Storage, choose the appropriate account type: **NetApp ONTAP**, **NetApp OnCommand**, **EMC VNX**, **EMC VMAX Solutions Enabler** or **WHIPTAIL**.

Step 8 Click **Add**.

Adding a Network Element

In order to create a virtual server that supports load balancing, first add a network element in Cisco UCS Director. After a Load Balancer is added as a network element in Cisco UCS Director, it appears on the **Managed Network Element** screen.

Before You Begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Managed Network Elements**.

Step 3 Click **Add Network Element**.

Step 4 On the **Add Network Element** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which the network element belongs.
Device Category drop-down list	Choose the device category for this network element. For example: **F5 Load Balancer**.
Device IP field	The IP address for this device.

Name	Description
Protocol drop-down list	Choose the protocol to be used. The list may include the following: • Telnet • SSH • HTTP • HTTPS **Note** When working with an F5 load balancer device, HTTP and HTTPS are the only valid selections.
Port field	The port to use.
Login field	The login name.
Password field	The password associated with the login name.

Step 5 Click **Submit**.

Adding the F5 Load Balancer triggers the system task inventory collection. The polling interval configured on the **System Tasks** screen specifies the frequency of inventory collection.

What to Do Next

To modify or edit a virtual server, choose the server, and then click **Modify**. To remove a virtual server, choose the server, and then click **Delete**.

Adding a Multi-Domain Manager Account

You can add the following types of multi-domain manager accounts:

- PNSC—Cisco Prime Network Services Controller account
- DCNM—Cisco Prime Data Center Network Manager account
- UCS Central—Cisco UCS Central account
- APIC—Cisco Application Policy Infrastructure Controller account
- EMC RecoverPoint account
- EMC VPLEX account

Before You Begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, choose the account type from the drop-down list.

Step 5 Click **Submit**.

Step 6 On the **Multi-Domain Manager Account** screen, complete the following fields:

Name	Description
Account Name field	Choose the account name to which this multi-domain manager account belongs.
Description field	(Optional) The description of the account.
Server Address field	Enter the IP address of the server managing the multi-domain manager account.
Account Name field	A unique name for the physical account that you want to add.
Server Address field	The IP address of the server.
User ID field	The username for accessing this account.
Password field	The password associated with the username.
Transport Type drop-down list	Choose the transport type that you want to use for the account. This can be one of the following: • http • https
Port field	The server port number. The default port is 443.
Contact Email field	(Optional) The contact email address for the account.
Location field	(Optional) The location.

Step 7 Click **Submit**.

Setup for Virtual Infrastructure

About Managing Virtual Infrastructure

To manage virtual infrastructure, create virtual accounts in Cisco UCS Director. A virtual account represents a supported hypervisor or cloud service to communicate with vCenter or Microsoft Virtual Machine Managers. The virtual account is termed as cloud.

Managing Policies

A policy is a group of rules that determine where and how a new resource, be it a virtual machine or a bare metal server, is provisioned within the infrastructure, based on available system resources. Create required policie for the virtual infrastructure by referring the *Managing Policies* chapter of the Cisco UCS Director Administration Guide.

Adding a Virtual Data Center

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, click **VDC**.

Step 3 Click **Add**.

Step 4 On the **VDC Add** screen, select an account type from the drop-down list.
The account type that you select determines the list of cloud names that are displayed on the **Add VDC** screen.

Step 5 Click **Submit**.

Step 6 On the **Add VDC** screen, complete the following fields:

Name	Description
VDC Name field	The name of the VDC. You can include special characters such as ( ). & - _ `~ $% ^ {}! ' @ **Note** A name cannot be edited after it is entered.
VDC Locked check box	Check the check box to deny the use of the VDC for any further deployments. Uncheck the check box to allow the use of the VDC for further deployments.
VDC Description field	The VDC-specific description.
Group drop-down list	Click **Select** to check the check box of the group for which the VDC is being set up.
Cloud Name drop-down list	Choose the cloud on which the VDC is being set up. The options available in this drop-down list are determined by the account type you specified.

Name	Description
Approvers and Contacts	
First Level Approver(s) field	The users who must approve the service request at the first level. Click **Select** and check the check boxes of the users. You can select multiple users.
Second Level Approver(s) field	The users who must approve the service request at the second level. Click **Select** and check the check boxes of the users. You can select multiple users.
Approval Required from all users check box	Check this check box to indicate that approval is required from all users who have been selected as first-level and second-level approvers.
Number of Approval Requests Reminders field	The number of times the reminder email to approve the service request is sent to the approvers. By default, the system sends a reminder email once in every 24 hours until the service request is approved or rejected.
Reminder Interval (Hours) field	The time interval between the reminder emails that are sent to the approvers. By default, the system sends a reminder email every 24 hours.
Provider Support Email Address field	The contact or user's email address. The person who is notified about VM provisioning using this VDC.
Copy Notifications to Email Address field	The second contact's email address for copying notifications about this VDC.
Policies	
System Policy drop-down list	Choose the system policy applicable to the VDC.
Computing Policy drop-down list	Choose the computing policy applicable to the VDC.
Network Policy drop-down list	Choose the network policy applicable to the VDC.
Storage Policy drop-down list	Choose the storage policy applicable to the VDC.
ISO Image Mapping Policy drop-down list	Choose the ISO image mapping policy applicable to the VDC.
Cost Model drop-down list	Choose the cost model applicable to the VDC.

Name	Description
Disable displaying cost details check box	Check the check box to disable displaying cost details in the following pages for this VDC: • Create Service Request wizard The cost information is not displayed in the **Deployment Configuration** pane, **Custom Specification** pane and the **Summary** pane. • Specific VM action pages - VM resize, Resize VM disk, and Create VM disk. • Email notifications
User Action Policy drop-down list	Choose the policy that is used for execution of orchestration workflow post provisioning of the VMs. The chosen workflow appears as an action button for VMs within the VDC.
VM Management Policy drop-down list	Choose the VM management policy for the VDC. This policy defines how VMs are managed in the VDC.
Enable Storage Efficiency check box	Check the check box to clone the VM using RCU. This option is only available for some VDC types.
End User Self-Service Policy	Select a self-service policy for the VDC. The policy defines the tasks or actions that can be performed on the VDC. **Note** This drop-down list is populated with policies that are relevant to the account type that you are creating the VDC for. The tasks that a user can perform on a VDC are defined by the role that the user is mapped to and by the end user self-service policy assigned to the VDC. If you have upgraded to the current release, then the permissions to perform VM management tasks are retained in any pre-existing end user self-service policy. However, the permissions defined in the user role to which the user belongs takes precedence.

Step 7 Click **Add**.

Note The following tasks can no longer be performed by users on a VM:

- Migrate a VM
- Use Stack View
- Assign a VM

What to Do Next

After adding a VDC, you can edit, clone, or delete it by selecting the respective option in the user interface.

Working with Catalogs

You can self-provision virtual machines (VMs) and bare metal (BM) servers using predefined catalog items. Only a system administrator can create a catalog. A catalog defines parameters, such as the cloud name and the group name to which the VM is bound.

You have to create and publish a catalog to make it available for use. See the *Managing Catalogs* chapter of the Cisco UCS Director Administration Guide.

Provisioning VMs using Self-Service Provisioning

You can provision virtual machines (VMs) or applications through self-service provisioning. To provision a VM or an application using self-service provisioning, you must create a service request. The service request workflow includes allocation of required resource to VM, approval of VM provisioning (if required), creation and provisioning of VM, schedule VM lifecycle setup, and VM creation notification to user. See the *Using Self-Service Provisioning* chapter of Cisco UCS Director Administration Guide.

Managing Post-Provisioning Life Cycle

You can manage the lifecylce of VMs using Cisco UCS Director, such as power on or off a VM, configure lease time for a VM, and apply tag to a VM. See the *Managing Lifecycles* chapter of Cisco UCS Director Administration Guide.

Using Cloud Sense Analytics

CloudSense Analytics in Cisco UCS Director provide visibility into the infrastructure resources utilization, critical performance metrics across the IT infrastructure stack, and capacity in real time. CloudSense significantly improves capacity trending, forecasting, reporting, and planning of virtual and cloud infrastructures. See the *Managing CloudSense Analytics* chapter of Cisco UCS Director Administration Guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands