Overview

This chapter contains the following sections:

- Cisco UCS Director, page 1
- Setting up Non-Secure Connection to the Cisco UCS Director User Interface, page 8
- Initial Login, page 9
- Recommended Order of System Setup, page 10
- Configuring the Host Name for Cisco UCS Director, page 12
- Working with Ciphers, page 12

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 network 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, as needed, basis.

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

Features and Benefits

The features and benefits of Cisco UCS Director are as follows:

Feature	Benefit
Central management	• Provides a single interface for administrators to monitor, provision, and manage the system across physical, virtual, and bare metal environments • Provides unified dashboards, reports, and heat maps, which reduce troubleshooting and performance bottlenecks
Self-service catalog	• Allows end users to order and deploy new infrastructure instances following IT-prescribed policies and governance

Feature	Benefit
Adaptive provisioning	• Provides a real-time available capability, internal policies, and application workload requirements to optimize the availability of your resources
Dynamic capacity management	• Provides continuous monitoring that indicates real-time infrastructure consumption to improve capacity planning and management • Identifies underutilized and overutilized resources
Multiple hypervisor support	• Supports VMware ESX, ESXi, Microsoft Hyper-V, and Red Hat hypervisors
Computing management	• Monitors, manages, and provisions physical, virtual, and bare metal servers, as well as blades • Allows end users to implement virtual machine life-cycle management and business continuance through snapshots • Allows administrators to access server utilization trending analysis
Network management	• Provides policy-based provisioning of physical and virtual switches and dynamic network topologies • Allows administrators to configure VLANs, virtual network interface cards (vNICs), port groups and port profiles, IP and Dynamic Host Control Protocol (DHCP) allocation, and access control lists (ACLs) across network devices
Storage management	• Provides policy-based provisioning and management of filers, virtual filers (vFilers), logical unit numbers (LUNs), and volumes • Provides unified dashboards that allow administrators comprehensive visibility into organizational usage, trends, and capacity analysis details.

Physical and Virtual Management Features

Physical Server Management • Discover and collect configurations and changes • Monitor and manage physical servers • Perform policy-based server provisioning • Manage blade power • Manage the server life cycle • Perform server use trending and capacity analysis • Perform bare metal provisioning using preboot execution environment (PXE) boot management	**Virtual Computing Management** • Discover, collect, and monitor virtual computing environments • Perform policy-based provisioning and dynamic resource allocation • Manage the host server load and power • Manage the VM life cycle and snapshots • Perform analytics to assess VM capacity, sprawl, and host utilization
Physical Storage Management • Discover, collect, and monitor storage filers • Perform policy-based provisioning of vFilers • Provision and map volumes • Create and map Logical Unit Number (LUN) and iGroup instances • Perform SAN zone management • Monitor and manage network-attached storage (NAS) and SAN-based storage • Implement storage best practices and recommendation	**Virtual Storage Management** • Discover, collect, and monitor storage of vFilers and storage pools • Perform policy-based storage provisioning for thick and thin clients • Create new datastores and map them to virtual device contexts (VDCs) • Add and resize disks to VMs • Monitor and manage organizational storage use • Perform virtual storage trend and capacity analysis
Physical Network Management • Discover, collect, and monitor physical network elements • Provision VLANs across multiple switches • Configure Access Control Lists (ACLs) on network devices • Configure the storage network • Implement dynamic network topologies	**Virtual Network Management** • Add networks to VMs • Perform policy-based provisioning with IP and DHCP allocation • Configure and connect Virtual Network Interface Cards (vNICs) to VLANs and private VLANs • Create port groups and port profiles for VMs • Monitor organizational use of virtual networks

Model-Based Orchestration

Cisco UCS Director includes a task library containing over 1000 tasks and out-of-the-box workflows. Model-based orchestration and a workflow designer enable you to customize and automate the infrastructure administrative and operational tasks. You can extend and customize the system to meet individual needs.

The following table shows the maintenance and update activities of the task library from day1 through day 3:

Day-1	Day-2	Day-3
• Add tenants • Migrate or add applicants • Integrate with enterprise systems • Use End User Portal	• Monitor performance • Start meeting and billing • Manage tenant change • Self-service Infrastructure as a Service (IaaS)	• Add/upgrade hardware • Repurpose

Guided Setup Wizards in Cisco UCS Director

Cisco UCS Director includes a set of wizards that guide you through configuring important features. The following are the available guided setup wizards:

- Device Discovery—This wizard enables you to discover devices and assign them to a pod.
- Initial System Configuration—This wizard helps you complete initial tasks to set up Cisco UCS Director, such as uploading licenses, and setting up SMTP, NTP, and DNS servers.
- vDC Creation—This wizard enables you to configure the policies required to provision VMs in private clouds.
- FlexPod Configuration—This wizard helps you set up a FlexPod account.
- Vblock Pod Configuration—This wizard enables you to discover and assign accounts to Vblock pods.
- VSPEX Pod Configuration—This wizard enables you to discover and assign accounts to VSPEX pods.
- Virtual SAN Pod Configuration—This wizard enables you to set up a Virtual SAN Pod and add devices.

When you first log into Cisco UCS Director, a **Wizard Explorer** window is displayed. From this window, you can view the details of the available guided setup wizards and choose to launch any of them. If you do not want this **Wizard Explorer** to appear every time you log in, you can check the **Do not show this page again** checkbox. To launch these wizards later on, click **Administration** > **Guided Setup**.

In addition to these system-provided wizards, you can create a wizard from a workflow that you have previously configured. For more information, see Creating a Wizard from a Workflow, on page 5.

Creating a Wizard from a Workflow

You can convert valid workflows into wizards, and save them in Cisco UCS Director.

Before You Begin

You must have created valid workflows in Cisco UCS Director.

Step 1 On the menu bar, choose **Administration** > **Guided Setup**.

Step 2 Click **Create from Workflow**.

Step 3 In the **Create Wizard from Workflow** dialog box, complete the following fields:

Name	Description
Select Workflow field	Click **Select** to check the check box of the workflow that you want to convert to a wizard.
Label field	The name of the wizard. This is the primary name of the wizard.
Second Label field	A secondary name of the wizard.
Description field	A description of the wizard.
Icon Image field	Click **Select** to check the check box of the icon that you want to associate with this workflow.

Step 4 Click **Submit**.

Step 5 Click **OK**.

What to Do Next

You can perform the following tasks:

- Launch the wizard.
- Edit the wizard.
- View details of the wizard.
- Re-order the wizard in the interface.
- Delete the wizard.

Common User Interface Options

The following table describes the options that are available on all pages of the application user interface. These options perform the same task on every page.

Icon	Label	Description
	**Refresh**	Refreshes the reported data on the page.
	**Favorite**	Adds a page to the **Favorites** menu. You can use this option to view frequently accessed pages more quickly.
	**Add**	Brings up the **Add** dialog box, from which you can add a new resource.
	**Edit**	Brings up the **Edit** dialog box, from which you can edit a resource.
	**Customize Table**	Brings up the **Customize Report Table** dialog box, in which you choose what columns you want to include on the screen.
	**Export Report**	Brings up the **Export Report** dialog box, from which you download a report to your system. You can generate a report in one of the following formats: • PDF • CSV • XLS
	**Expand**	Expands all the folders that are displayed on the page.
	**Collapse**	Collapses all the folders that are displayed on the page.
	**Add Advanced Filter**	Provides extra filtering parameters on the page.

Icon	Label	Description
	**Search Field**	Accepts a keyword to filter for specific records on the page.

Setting up Non-Secure Connection to the Cisco UCS Director User Interface

By default, the Cisco UCS Director user interface launches in the secure mode. If you want to bypass the secure mode, and launch the user interface in a non-secure mode (HTTP), you must follow this procedure.

Step 1 Log in as root.

Step 2 Make the following changes in the `/opt/infra/web_cloudmgr/apache-tomcat/conf/server.xml` file:

a) Comment out the existing port 8080 Connector tag

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
redirectPort="443" maxHttpHeaderSize="65536"
URIEncoding = "UTF-8"/>
-->
```

b) Add the following as a new port 8080 Connector tag:

```
<Connector port="8080" protocol="HTTP/1.1"
maxThreads="150" minSpareThreads="4"
connectionTimeout="20000"
URIEncoding = "UTF-8" />
```

Step 3 Comment the <security-constraint> tag in the `/opt/infra/web_cloudmgr/apache-tomcat/webapps/app/WEB-INF/web.xml` file.

```
<!--
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
-->
```

Step 4 Restart the services.

Step 5 Launch the user interface and log in to the system.
You can now log into the system in the non-secure mode using the following URL format:

http://<IP-Address>:8080 or http://<IP-Address>

You can launch the user interface in both, secure and non-secure modes.

Initial Login

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

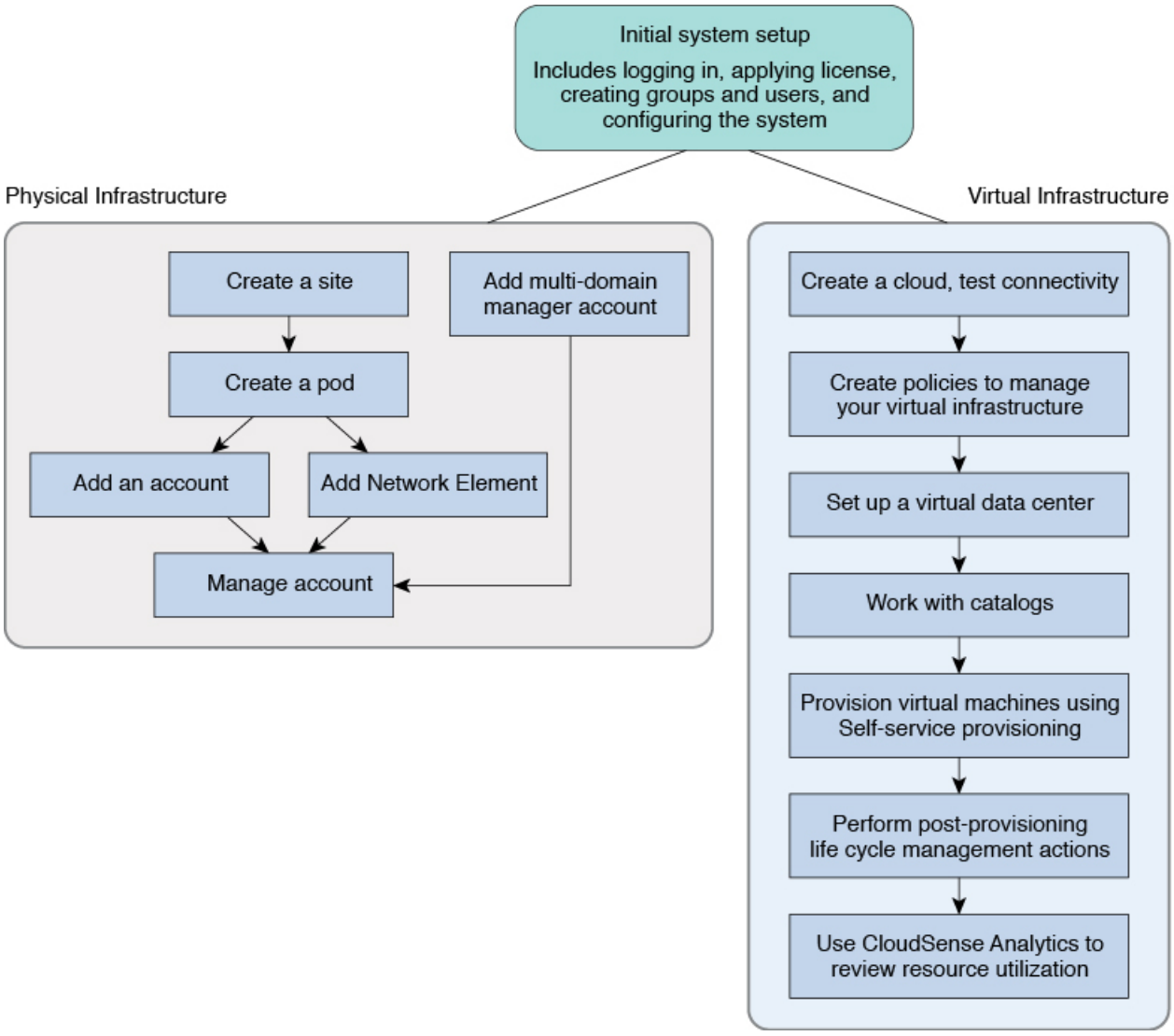
- Username: admin
- Password: admin

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.

Recommended Order of 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



The following table describes the chapters available in this book using which you can complete setting up your environment.

Name	Chapter	Description
Initial set up	2, 3, 4 and 5	Describes how to apply a license, set up the Admin profile, create groups, and create users. You will learn how to access language support, apply portal customization, and system settings

Name	Chapter	Description
Physical Infrastructure	6	Describes how to optionally add a pod and physical account, add network elements, test the connections, and verify account discovery. **Note** You can create the virtual infrastructure before the physical infrastructure if you want.
Virtual Infrastructure	7	Describes how to create a cloud, verify cloud discovery and connectivity, test the connections, and view vCenter plug ins.
Policies	8	Describes how to create and manage computing policies, storage policies, network policies, and system policies. You will learn how to add OS licenses for Microsoft Windows catalogs.
Virtual Data Centers	9	Describes how to set up VDCs to manage specific environments for groups. policies, and cost models, and how resource limits are configured and managed at the VDC level.
Catalogs	10	Describes how to set up catalog items, attach groups with access to a catalog, and publish catalog items.
Self-Service Provisioning	11	Describes how you can create and manage provisioning service requests.
Multi-Disk Provisioning	12	Describes how to configure VM disk provisioning on a preferred single datastore or multiple datastores. It also provides instructions on how to configure individual disk policies for each additional disk in a template.
Chargeback	13	Describes how to create chargeback summary reports, detailed reports, and resource accounting reports. It shows how cost models are defined and assigned to policies within departments and organizations.
Cloud Management	14	Describes how you can get complete cloud visibility, monitor resource usage, and manage the cloud stack—clouds, clusters, host servers, and virtual machines.
Life Cycles	15	Describes how to perform post provisioning life cycle management actions on VMs, such as VM power management, VM resizing, VM snapshot management, and other VM actions.
CloudSense	16	Describes the analytical reports about the underlying physical and virtual infrastructure that Cisco UCS Director can generate.

Configuring the Host Name for Cisco UCS Director

If you changed the default host name of the appliance of Cisco UCS Director using the command prompt, then you must follow this procedure to ensure that the name is updated in the `/etc/hosts` file.

Step 1 SSH to the appliance using the root account.

Step 2 Edit the `/etc/hosts` to update the new host name.
In a single node environment, you must update the file in the following format:

```
vi /etc/hosts
198.51.100.1 new_hostname
```

In a multi-node environment, if the host names of other nodes are changed, then you must update the IP address and the new host name on the primary node, service nodes and database nodes. For example:

```
vi /etc/hosts
198.51.100.1 new_hostname
Ex:
198.51.100.2 UCSD_Primary
198.51.100.3 UCSD_Service
198.51.100.4 UCSD_Inv_DB
198.51.100.5 UCSD_Mon_DB
```

Step 3 Restart the appliance services.

Working with Ciphers

As an administrator in Cisco UCS Director, you have the capability to enable or disable ciphers from the property file. In the event that you enable a cipher with a potential security risk, a warning message is logged in the Cisco UCS Director log file. By default, all ciphers that pose a risk are disabled. You can configure specific ciphers from the `defaultEnabledCipherSuites.properties` file, located in the `/opt/infra/inframgr` folder. For more information, see Editing Cipher Usage, on page 12.

In addition, you can change the preference order of the standard set of ciphers, based on your system requirements. By default, the standard ciphers are listed according to the preference order.

Cisco UCS Director currently supports the use of "limited" and "strong" Java Cryptograpy Extension (JCE) Policy files for Java SE Runtime Environment. If you want to change these policies to "unlimited" and "strong" JCE policies, then you must download and install the latest JCE policy files from the Oracle website. For more information, see Installing the Latest Java Cryptograpy Extension (JCE) Policy Files , on page 13.

Editing Cipher Usage

CipherSuites are maintained in the `defaultEnabledCipherSuites.properties` file. You can edit the list of ciphers in this file, based on the application requirements for your network.

We recommend that you always use the standard ciphers and not enable any broken or risky ciphers for your application.

Step 1 Open the `defaultEnabledCipherSuites.properties` file.
It is available in the `opt/infra/inframgr/` directory.

Step 2 To use a broken cipher, locate the cipher in the file, and uncomment it.

Step 3 Save the file.

Step 4 Restart the service.

Installing the Latest Java Cryptograpy Extension (JCE) Policy Files

Complete the following procedure to download and install the latest JCE policy files:

Step 1 Take a backup of the following files in the `$JAVA_HOME/jre/lib/security` folder:

- `local_policy.jar`
- `US_export_policy.jar`

Step 2 Access the oracle Java SE download page at http://www.oacle.com/technetwork/java/javase/downloads.index.html.

Step 3 Scroll to the **Additional Resources** section to locate the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File.

Step 4 Download the `Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8` zipped file.

Step 5 Extract the contents of the zipped file.

Step 6 Replace the `local_policy.jar` and `US_export_policy.jar` in the `$JAVA_HOME/jre/lib/security` folder.

Step 7 Restart the application.