

# CX Cloud Agent Overview v2.4

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Deployment Requirements](#)

### [Accessing Critical Domains](#)

[Domains Specific to the CX Cloud Agent Portal](#)

[Domains Specific to CX Cloud Agent OVA](#)

### [Catalyst Center Supported Version](#)

[Supported Browsers](#)

[Supported Product List](#)

[Upgrading/Installing CX Cloud Agent v2.4](#)

[Upgrading Existing VMs to Large and Medium Configuration](#)

### [Upgrade CX Cloud Agent v2.4](#)

### [Adding CX Cloud Agent](#)

### [Adding Catalyst Center as Data Source](#)

### [Adding Other Assets as Data Sources](#)

[Discovery Protocols](#)

[Connectivity Protocols](#)

[Telemetry Processing Limitation for Devices](#)

### [Adding Other Assets Using a Seed File](#)

[Add Other Assets Using a New Seed File](#)

[Add Other Assets Using a Modified Seed File](#)

### [Add Other Assets Using IP Ranges](#)

[Adding Other Assets by IP Ranges](#)

[Editing IP Ranges](#)

[Deleting IP Range](#)

[About Devices Discovered from Multiple Controllers](#)

[Scheduling Diagnostics Scans](#)

### [Upgrading CX Cloud Agent VMs to Medium and Large Configurations](#)

[Reconfiguring Using VMware vSphere Thick Client](#)

[Reconfiguring Using Web Client ESXi v6.0](#)

[Reconfiguring Using Web Client vCenter](#)

### [Deployment and Network Configuration](#)

[OVA Deployment](#)

[ThickClient ESXi 5.5/6.0 Installation](#)

[WebClient ESXi 6.0 Installation](#)

[WebClient vCenter Installation](#)

[OracleVirtual Box 5.2.30 Installation](#)

[MicrosoftHyper-V Installation](#)

[Network Configuration](#)

[Alternative Approach to Generate Pairing Code Using CLI](#)

---

[Configure Cisco Catalyst Center To Forward Syslog to CX Cloud Agent](#)

[Prerequisites](#)

[Configure Syslog Forward Setting](#)

[Configure Other Assets to Forward Syslog to CX Cloud Agent](#)

[Existing Syslog Servers with Forward Capability](#)

[Existing Syslog Servers without Forward Capability OR without Syslog Server](#)

[Enable Information Level Syslog Settings](#)

## **[Back Up and Restore the CX Cloud VM](#)**

[Back Up](#)

[Restore](#)

## **[Security](#)**

[Physical Security](#)

[Account Security](#)

[Network Security](#)

[Authentication](#)

[Hardening](#)

[Data Security](#)

[Data Transmission](#)

[Logs and Monitoring](#)

[Cisco Telemetry Commands](#)

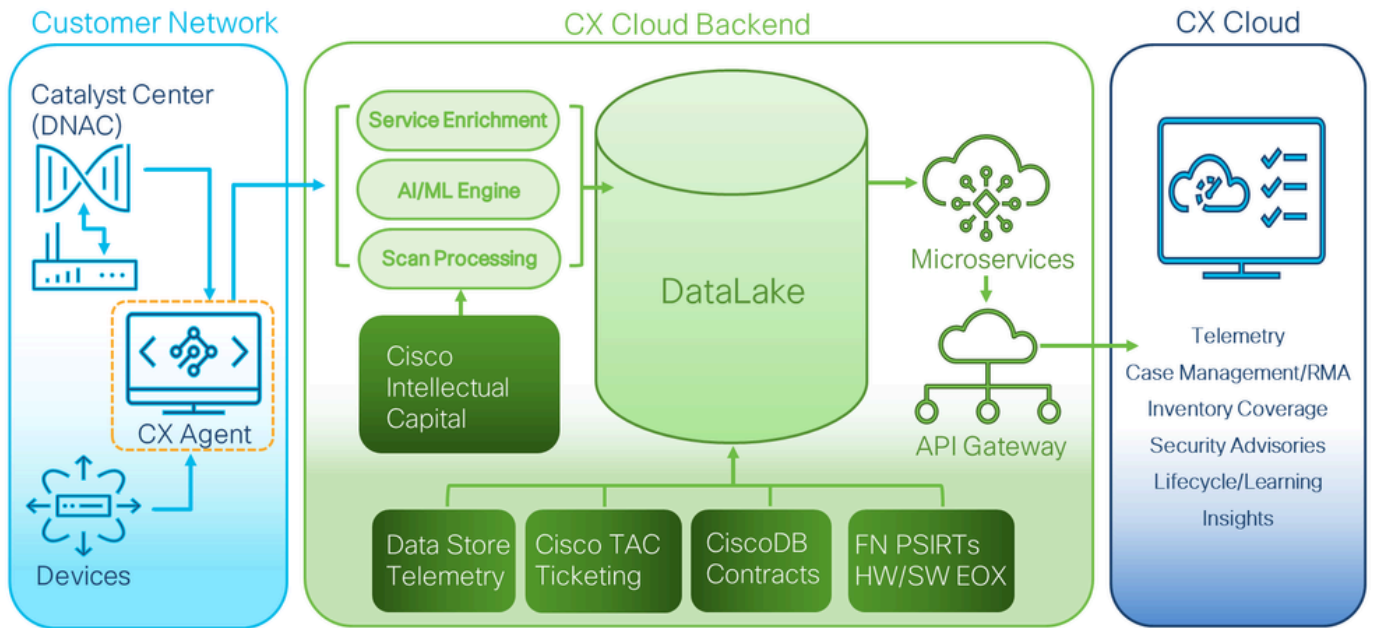
[Security Summary](#)

---

# **Introduction**

This document describes Cisco's Customer Experience (CX) Cloud Agent. Cisco's CX Cloud Agent is a highly scalable platform that collects telemetry data from customer network devices to deliver actionable insights for customers. CX Cloud Agent enables the Artificial Intelligence (AI)/Machine Learning (ML) transformation of active running configuration data into proactive and predictive insights displayed in CX Cloud.

# CX Cloud Architecture



CX Cloud Architecture

This guide is specific to CX Cloud Agent v2.4. Refer to the [Cisco CX Cloud Agent](#) page to access prior versions.



**Note:** Images in this guide are for reference purposes only. Actual content can vary.

## Prerequisites

CX Cloud Agent runs as a Virtual Machine (VM) and is available for download as an Open Virtual Appliance (OVA) or a Virtual Hard Disk (VHD).

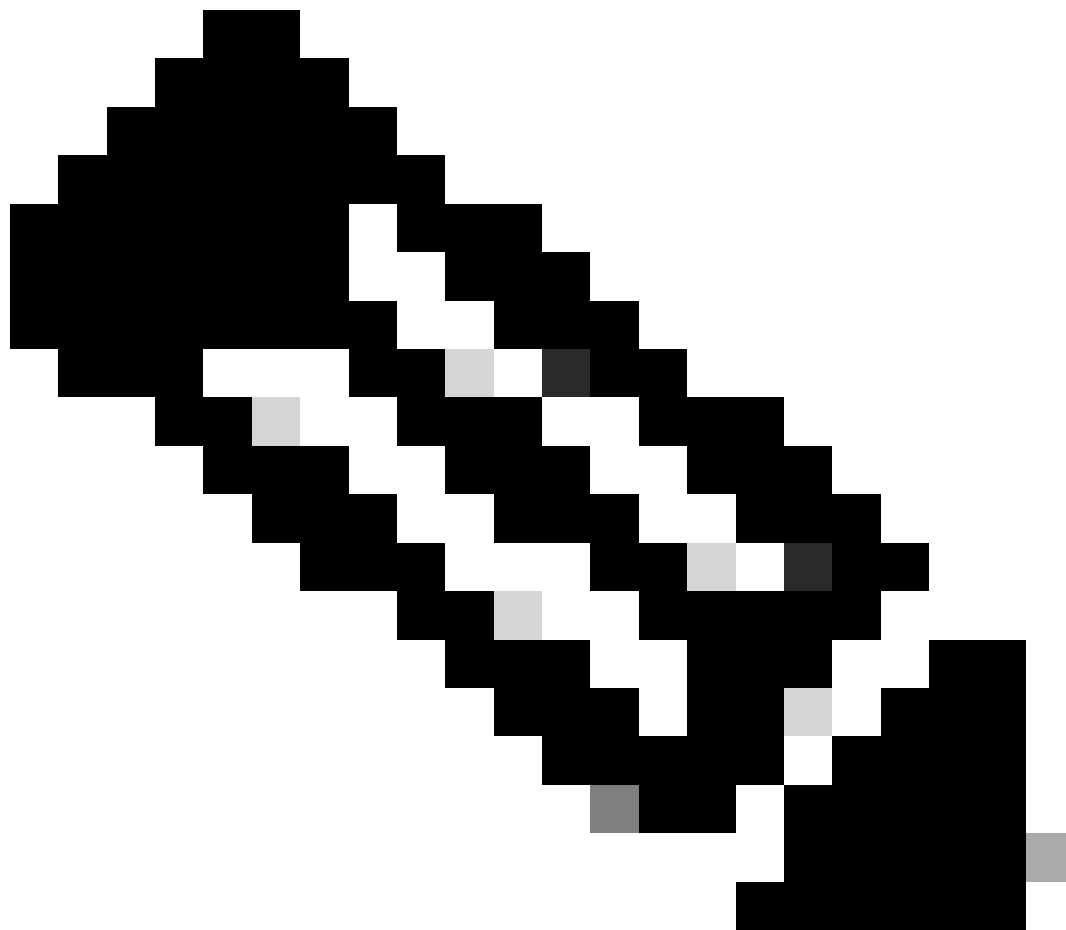
## Deployment Requirements

- One of the following hypervisors is required for a new install:
  - VMware ESXi v5.5 or later
  - Oracle Virtual Box v5.2.30 or later
  - Windows Hypervisor version 2012 to 2022
- The configurations in the following table are required for deploying VM:

CX Cloud Agent Deployment Type	Number of CPU Cores	RAM	Hard Disk	*Maximum number of Assets directly connected to CX Cloud

				Agent
Small OVA	8C	16GB	200GB	10,000
Medium OVA	16C	32GB	600GB	20,000
Large OVA	32C	64GB	1200GB	50,000 :

\*In addition to connecting 20 Cisco Catalyst Center (Catalyst Center) non-clusters or 10 Catalyst Center clusters for each CX Cloud Agent instance.



**Note:** Flexible OVA/Patch 2.4 for medium and large configurations is available only for the VMware ESXi VMs. The Oracle VirtualBox and Windows Hyper-V cannot be used for medium and large configurations.

- For customers using designated US data centers as the primary data region to store CX Cloud data, the

CX Cloud Agent must be able to connect to the servers shown here, using the Fully Qualified Domain Name (FQDN), and using HTTPS on TCP port 443:

- FQDN: agent.us.cisco.cloud
- FQDN: ng.acs.agent.us.cisco.cloud
- FQDN: cloudsso.cisco.com
- FQDN: api-cx.cisco.com
- For customers using designated Europe data centers as the primary data region to store CX Cloud data: the CX Cloud Agent must be able to connect to both of the servers shown here, using the FQDN, and using HTTPS on TCP port 443:
  - FQDN: agent.us.cisco.cloud
  - FQDN: agent.emea.cisco.cloud
  - FQDN: ng.acs.agent.emea.cisco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- For customers using designated Asia Pacific data centers as the primary data region to store CX Cloud data: the CX Cloud Agent must be able to connect to both of the servers shown here, using the FQDN, and using HTTPS on TCP port 443:
  - FQDN: agent.us.cisco.cloud
  - FQDN: agent.apjc.cisco.cloud
  - FQDN: ng.acs.agent.apjc.cisco.cloud
  - FQDN: cloudsso.cisco.com
  - FQDN: api-cx.cisco.com
- For customers using designated Europe and Asia Pacific data centers as their primary data region, connectivity to FQDN: agent.us.cisco.cloud is required only for registering the CX Cloud Agent with CX Cloud during initial setup. After the CX Cloud Agent is successfully registered with CX Cloud, this connection is no longer required.
- For local management of the CX Cloud Agent, port 22 must be accessible.
- The following table provides a summary of the ports and protocols that must be opened and enabled for CX Cloud Agent to function correctly:

CX Cloud Agent Traffic					
Source	Destination	Protocol	Port	Purpose	Type
CX Cloud Agent	<u>All regions:</u> cloudsso.cisco.com api-cx.cisco.com agent.us.cisco.cloud DNA Center <u>AMER region:</u> ng.acs.agent.us.cisco.cloud <u>EMEA region:</u> agent.emea.cisco.cloud ng.acs.agent.emea.cisco.cloud <u>APJC region:</u> agent.apjc.cisco.cloud ng.acs.agent.apjc.cisco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers	Bi-directional to Cisco AWS regional data centers and DNA Center
CX Cloud Agent	Network Devices	SNMP	UDP/161	Initial discovery Ongoing inventory collections	Outbound to LAN
CX Cloud Agent	Network Devices	SSH	TCP/22	Collection of telemetry from CLI commands	Outbound to LAN
CX Cloud Agent	Network Devices	Telnet	TCP/23	Collection of telemetry from CLI commands	Outbound to LAN
Network Devices	CX Cloud Agent	Syslog	UDP/514	Transfer syslogs for Alert Fault Management	Inbound from LAN
Workstation	CX Cloud Agent	SSH	TCP/22	CX Cloud Agent Maintenance	Inbound from LAN

- An IP is automatically detected if the Dynamic Host Configuration Protocol (DHCP) is enabled in the VM environment; Otherwise, a free IPv4 address, Subnet mask, Default Gateway IP address, and Domain Name Service (DNS) server IP address must be available.
- Only IPv4 is supported.

- The certified single node and High Availability (HA) Cluster Catalyst Center versions are 2.1.2.x to 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x and Catalyst Center Virtual Appliance and Catalyst Center Virtual Appliance.
- If the network has SSL interception, permit-list CX Cloud Agent's IP address.
- For all directly connected assets, SSH privilege level 15 is required.
- Use only the provided hostnames; static IP addresses cannot be used.

## Accessing Critical Domains


To start the CX Cloud journey, users require access to the following domains. Use only the hostnames provided; do not use static IP addresses.

### Domains Specific to the CX Cloud Agent Portal

Major Domains	Other Domains
cisco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

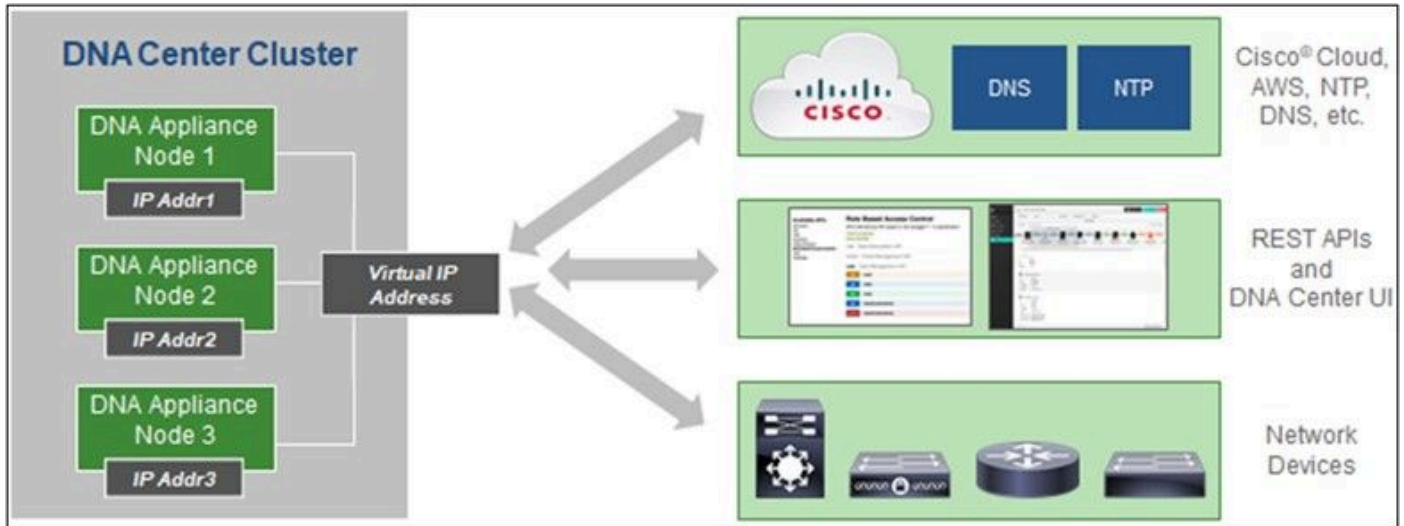
### Domains Specific to CX Cloud Agent OVA

AMERICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.cisco.cloud	agent.us.cisco.cloud	agent.us.cisco.cloud
ng.acs.agent.us.cisco.cloud	agent.emea.cisco.cloud	agent.apjc.cisco.cloud
	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

 **Note:** The outbound access must be allowed with redirection enabled on port 443 for the specified FQDN's.

## Catalyst Center Supported Version

Supported single node and HA Cluster Catalyst Center versions are 2.1.2.x to 2.2.3.x, 2.3.3.x, 2.3.5.x, 2.3.7.x and Catalyst Center Virtual Appliance and Catalyst Center Virtual Appliance.



*Multi-Node HA Cluster Cisco DNA Center*

## Supported Browsers

For the best experience on Cisco.com, the latest official release of these browsers is recommended:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

## Supported Product List

To view the list of products supported by CX Cloud Agent, refer to the [Supported Product List](#).

## Upgrading/Installing CX Cloud Agent v2.4

- Existing customers upgrading to the new version should refer to [Upgrade CX Cloud Agent v2.4](#).
- New customers implementing a fresh flexible OVA v2.4 install should refer to [Adding CX Cloud Agent as Data Source](#).

## Upgrading Existing VMs to Large and Medium Configuration

Customers can upgrade their existing VM configuration to medium or large using Flexible OVA options based on their network size and complexity.

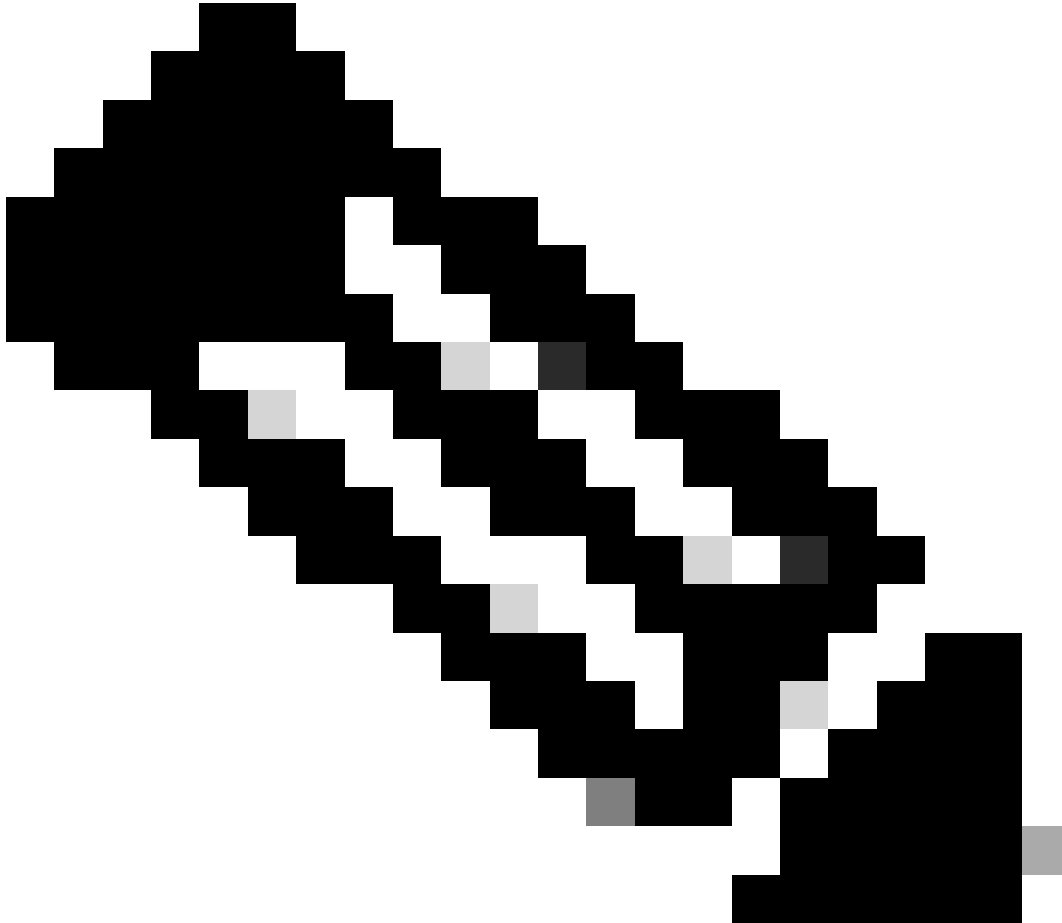
To upgrade the existing VM configuration from small to medium or large, refer to section [Upgrading CX Cloud Agent VMs to medium and large configuration](#).



# Upgrade CX Cloud Agent v2.4

Customers running CX Cloud Agent v2.3.x and above can follow the steps in this section to directly upgrade to v2.4.

---

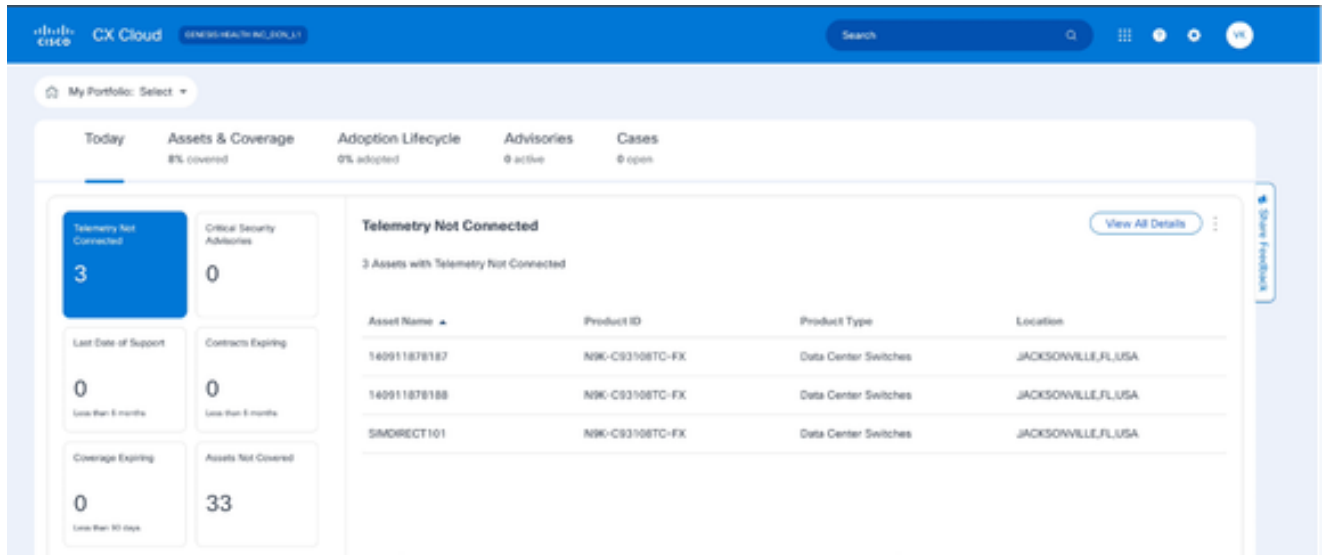


**Note:** Customers on CX Cloud Agent v2.2.x should upgrade to v2.3.x before upgrading to v2.4 or install the v2.4 as fresh OVA install.

---

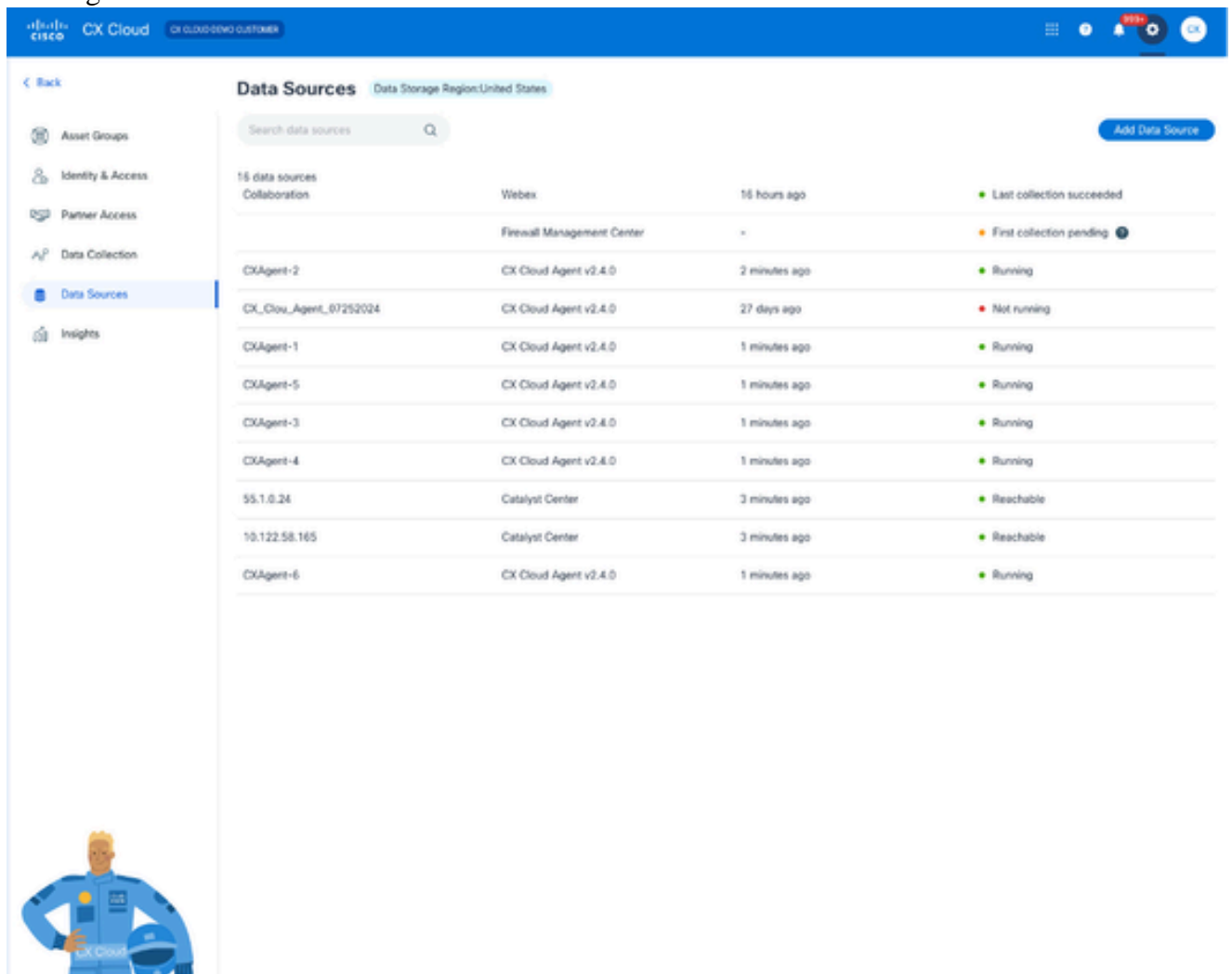
To install the CX Cloud Agent upgrade v2.4 from CX Cloud:

1. Log in [CX Cloud](#). The **Home** page displays.



CX Cloud Home Page

2. Click the **Admin Center** icon. The **Data Sources** window opens displaying CX Cloud Agent as an existing data source.



Data Sources

3. Click the **CX Cloud Agent** data source. The **CX Cloud Agent** details window opens.

Name	Type	Last Collection	Status
Collaboration	Webex	16 hours ago	Last collection success
Practical Management Center	-	-	File collection pending
CCAgent-2	CX Cloud Agent v2.4.0	2 minutes ago	Running
CX_Cloud_Agent_0702020	CX Cloud Agent v2.4.0	27 days ago	Not running
CCAgent-1	CX Cloud Agent v2.4.0	1 minute ago	Running
CCAgent-5	CX Cloud Agent v2.4.0	1 minute ago	Running
CCAgent-3	CX Cloud Agent v2.4.0	1 minute ago	Running
CCAgent-4	CX Cloud Agent v2.4.0	1 minute ago	Running
SI.1.0.24	Catalyst Center	3 minutes ago	Reachable
10.122.18.105	Catalyst Center	3 minutes ago	Reachable
CCAgent-9	CX Cloud Agent v2.4.0	1 minute ago	Running

Data Sources Detail View

4. Click the **Software** tab.

Name	Type	Data Last
Contract	Assets with coverage	17 days
Data Center Networking	Intersight	8 hours
Data Center Compute	Intersight	10 hours
Monski	Monski	-
		-
	Catalyst Center	233 days
CX Cloud Agent 1	CX Cloud Agent v2.3.0	233 days

CX Cloud Agent Detail View

5. Select the software version **2.4.0** from **Choose a software version to update to** drop-down.
6. Click **Install Update** to install CX Cloud Agent v2.4.0.



**Note:** Customers can schedule the update for later by clearing the **Install Now** check box which displays scheduling options.

---

## Adding CX Cloud Agent

Customers can add up to twenty (20) CX Cloud Agent instances in CX Cloud.

To add a CX Cloud Agent:



**Note:** Repeat the following steps to add additional CX Cloud Agent instances as a data source.

- 
1. Log in to [CX Cloud](#). The **Home** page displays.

The screenshot displays the Cisco CX Cloud dashboard. At the top, the navigation bar includes the Cisco logo, 'CX Cloud', and a user profile 'DAVID P. HICKLING'. Below this, a 'My Portfolio' dropdown is set to 'Select'. A summary row shows: Today, Assets & Coverage (82% covered), Adoption Lifecycle (54% adopted), Advisories (14 active), and Cases (2310 open).

The main content area is divided into several sections:

- Customize:** A grid of six cards:
  - Telemetry Not Connected: 10882
  - Critical Faults: 0 (Last 7 days)
  - Crashed Assets: 0 (Last 7 days)
  - Critical Security Advisories: 1
  - High Crash Risk Assets: 0
  - Hardware Last Date of Support: 407 (Less than 6 months)
  - Software Last Date of Support: 8 (Less than 6 months)
  - Contracts Expiring: 1 (Less than 6 months)
- Telemetry Not Connected:** A table with 10882 assets. The table has columns: Asset Name, Product ID, Product Type, and Location.
 

Asset Name	Product ID	Product Type	Location
003011866766	CS-DESKMIN-K9	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
003411866767	CS-DESKMIN-K9	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
003611866768	CS-DESKMIN-K9	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
003711866769	CS-DESKMIN-K9	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
003811866770	CS-DESKMIN-K9	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
005811476828	C9200L-48P-4X	Switches	SAN FRANCISCO,CA,USA
005811476829	C9200L-48P-4X	Switches	SAN FRANCISCO,CA,USA
005811476830	C9200L-48P-4X	Switches	SAN FRANCISCO,CA,USA
- Cases:** Shows 'My open cases' as 1935 and 'Action required' as 12. Includes an 'Open Case' button and a link to 'View all open cases (2310) >'. There is also an 'Open Case' button in the top right of this section.
- Adoption Lifecycle:** Shows two progress bars for 'Service Provider Networking' (SR-MPLS Enabled Network and SRv6 Enabled Network), both at 0% complete. Each bar includes an 'Onboard Stage' label and a 'Next task' link: 'Learn about SR-MPLS benefits and network simplification' and 'Learn about SRv6 benefits and network simplification'.

A 'Go to Adoption Lifecycle >' link is located at the bottom of the Adoption Lifecycle section.

CX Cloud Home Page

2. Select the **Admin Center** icon. The **Data Sources** window opens.

**Data Sources** Data Storage Region: United States

Search data sources

15 data sources

Name	Agent	Last Collection	Status
Collaboration	Webex	16 hours ago	Last collection succeeded
	Firewall Management Center	-	First collection pending
CXAgent-2	CX Cloud Agent v2.4.0	2 minutes ago	Running
CX_Cloud_Agent_07252024	CX Cloud Agent v2.4.0	27 days ago	Not running
CXAgent-1	CX Cloud Agent v2.4.0	1 minutes ago	Running
CXAgent-5	CX Cloud Agent v2.4.0	1 minutes ago	Running
CXAgent-3	CX Cloud Agent v2.4.0	1 minutes ago	Running
CXAgent-4	CX Cloud Agent v2.4.0	1 minutes ago	Running
55.1.0.24	Catalyst Center	3 minutes ago	Reachable
10.122.58.165	Catalyst Center	3 minutes ago	Reachable
CXAgent-6	CX Cloud Agent v2.4.0	1 minutes ago	Running









**Add Data Source**

Data Sources

3. Click **Add Data Source**. The **Add Data Source** window opens. The options displayed vary based on customer subscriptions.

## Add Data Source

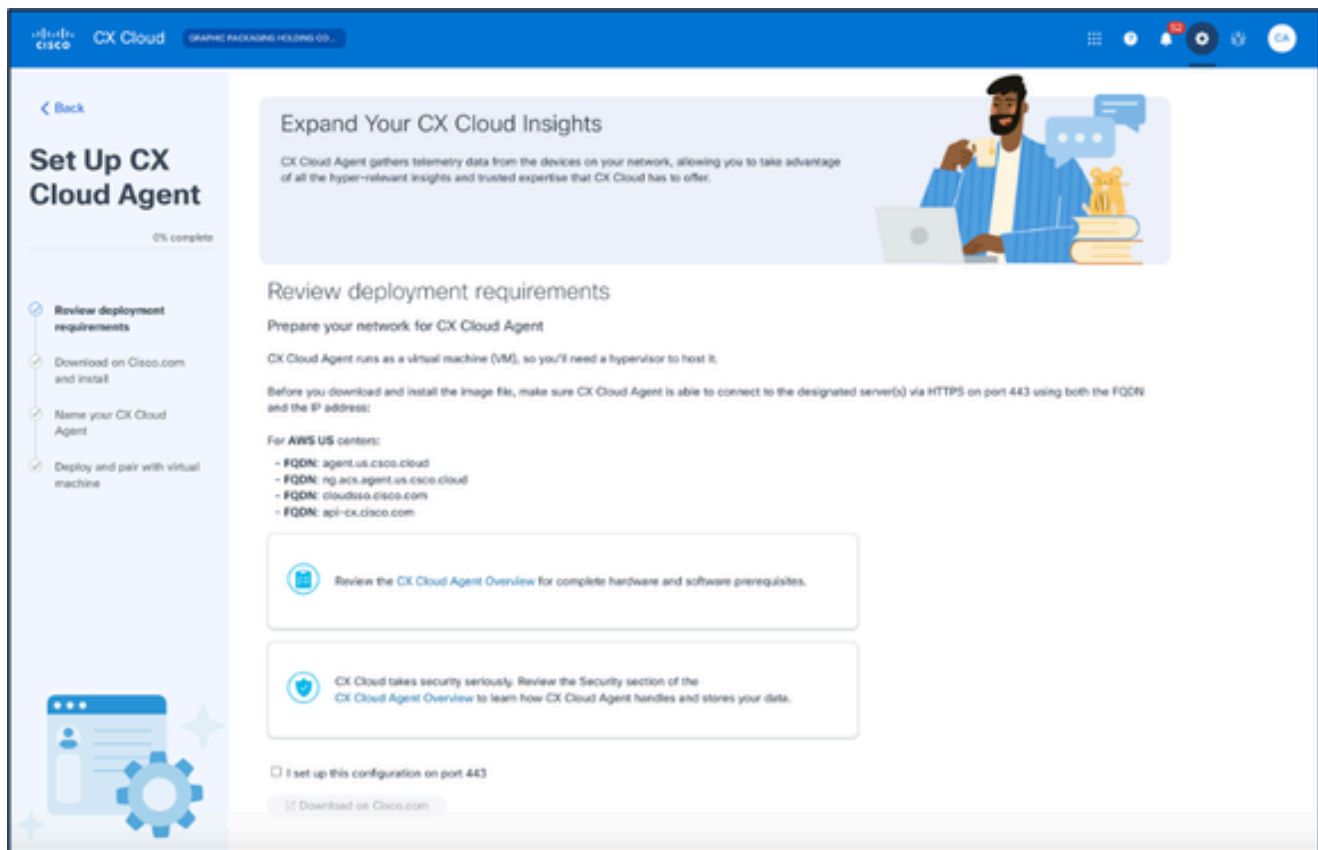
Search data sources Q

-  **Catalyst Center**  
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types) Add Data Source
-  **Cisco Catalyst SD-WAN Manager**  
Supports the Success Track for WAN Add Data Source
-  **Contracts**  
Supports assets associated with a contract Add Data Source
-  **CX Cloud Agent**  
Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks Add Data Source
-  **Firewall Management Center**  
Supports Cisco Secure Firewall Add Data Source
-  **Intersight**  
Supports the Data Center Compute and Data Center Networking Success Tracks Add Data Source
-  **Other Assets by IP Ranges**  
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks) Add Data Source
-  **Other Assets by Seed File**  
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks) Add Data Source

*Add Data Source*

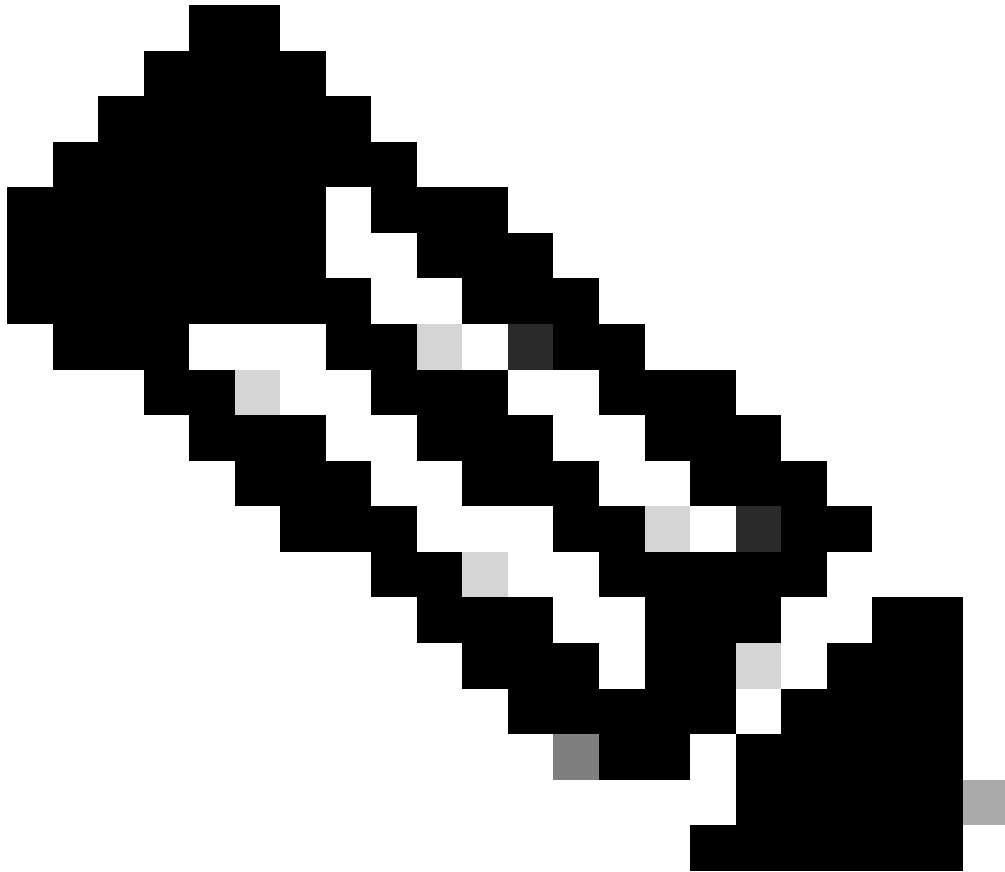
4. Click **Add Data Source** from the **CX Cloud Agent** option. The **Set Up CX Cloud Agent** window opens.





*Set Up CX Cloud Agent*

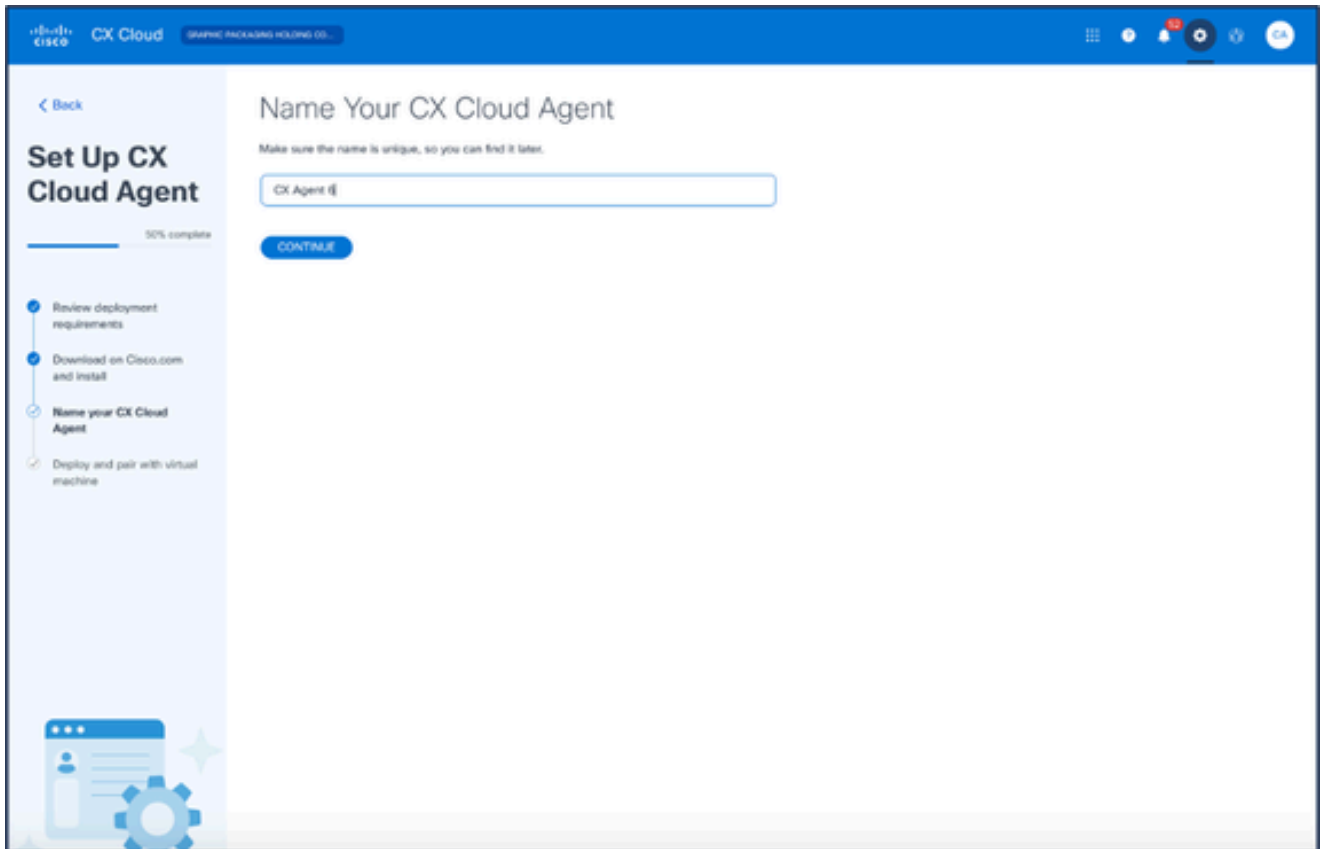
5. Review the **Review deployment requirements** section and select the **I set up this configuration on port 443** check box.
6. Click **Download on Cisco.com**. The **Software Download** page opens.
7. Download the CX Cloud Agent v2.4 OVA file.



**Note:** A Pairing Code, required to complete the setup of the CX Cloud Agent, is generated after deploying the OVA file.

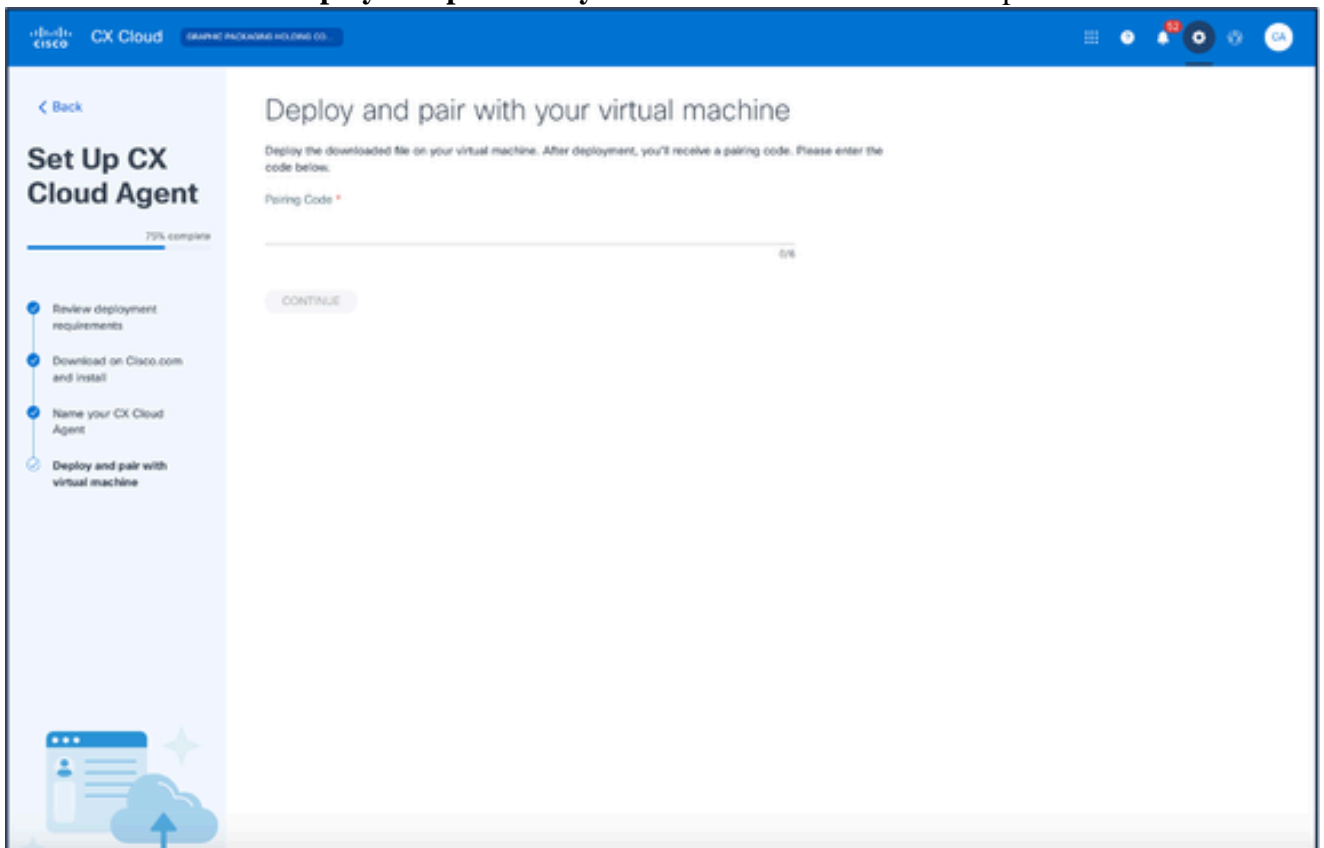
---

8. Enter the CX Cloud Agent name in the **Name Your CX Cloud Agent** field.



*Name Your CX Cloud Agent*

9. Click **Continue**. The **Deploy and pair with your virtual machine** window opens.



*Deploy and Pair with Your Virtual Machine*

10. Enter the **Pairing Code** received after deployment of the downloaded OVA file.

11. Click **Continue**. The registration progress displays, followed by a confirmation.

## Adding Catalyst Center as Data Source

To add Catalyst Center as data source:

1. Click **Add Data Source** in the **Admin Center > Data Sources** window.

The screenshot shows the 'Add Data Source' interface. At the top, there is a search bar labeled 'Search data sources' with a magnifying glass icon. Below the search bar is a list of data sources, each with an icon, a title, a description, and an 'Add Data Source' button. The data sources listed are:

- Catalyst Center**: Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)
- Cisco Catalyst SD-WAN Manager**: Supports the Success Track for WAN
- Contracts**: Supports assets associated with a contract
- CX Cloud Agent**: Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks
- Firewall Management Center**: Supports Cisco Secure Firewall
- Intersight**: Supports the Data Center Compute and Data Center Networking Success Tracks
- Other Assets by IP Ranges**: Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)
- Other Assets by Seed File**: Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

*Add Data Source*

2. Click **Add Data Source** from the **Catalyst Center** option.

## Which CX Cloud Agent Do You Want to Connect to?

Select option ▼



*Select CX Cloud Agent*

3. Select the CX Cloud Agent from the **Which CX Cloud Agent Do You Want to Connect to** drop-down list.
4. Click **Continue**. The **Connect to CX Cloud** window opens.

**Connect to CX Cloud**

Connect a Catalyst Center (3 of 3)

IP Address or FQDN \* City \*

Username \* Password \*

Schedule inventory collection

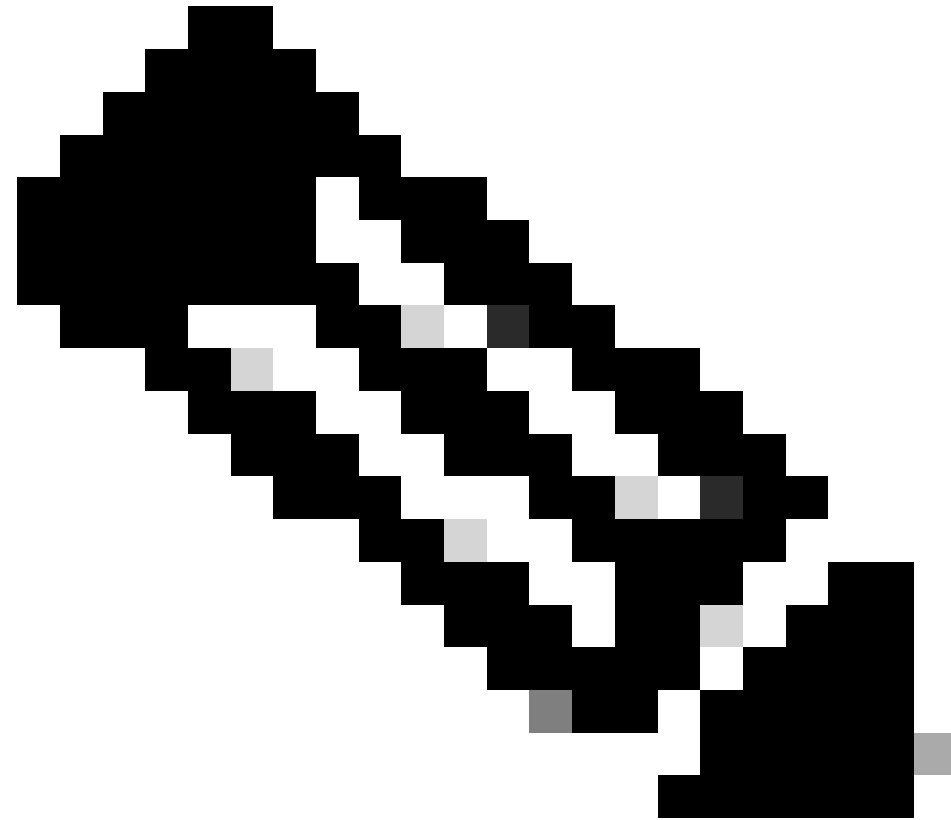
Frequency Select time Time Zone

From... 12:00 AM America/New\_York (UTC ...

Run the first collection now (this may take up to 75 minutes)

*Connect to CX Cloud*

5. Enter the following details:
  - **Virtual IP Address or FQDN** (i.e., Catalyst Center IP Address),
  - **City** (i.e., Catalyst Center's location),
  - **Username**
  - **Password**
  - **Frequency, Time, and Time Zone** to indicate how often the CX Cloud Agent should perform network scans in **Schedule Inventory Collection** sections



**Note:**Select **Run the first collection now** checkbox to run the collection now.

---

6. Click **Connect**. A confirmation displays with the Catalyst Center IP Address.

## Adding Other Assets as Data Sources

Telemetry collection has been extended to devices not managed by the Catalyst Center, enabling customers to view and interact with telemetry-derived insights and analytics for a broader range of devices. After the initial CX Cloud Agent setup, users have the option to configure CX Cloud Agent to connect to 20 additional Catalyst Centers within the infrastructure monitored by CX Cloud.

Users can identify devices to incorporate into CX Cloud by uniquely identifying such devices using a seed file or by specifying an IP range, which can be scanned by CX Cloud Agent. Both approaches rely on Simple Network Management Protocol (SNMP) for the purpose of discovery (SNMP) and on Secure Shell (SSH) for connectivity. These must be properly configured to enable successful telemetry collection.

To add other assets as data sources:

- Upload a seed file using a seed file template.
- Provide an IP address range.

## Discovery Protocols

Both seed file-based direct device discovery and IP range-based discovery rely on SNMP as the discovery protocol. Different versions of SNMP exist, but CX Cloud Agent supports SNMPV2c and SNMP V3 and either or both versions can be configured. The same information, described next in complete detail, must be provided by the user to complete configuration and to enable connectivity between the SNMP-managed device and SNMP service manager.

SNMPV2c and SNMPV3 differ in terms of security and remote configuration model. SNMPV3 uses an enhanced cryptographic security system supporting SHA encryption to authenticate messages and ensure their privacy. It is recommended that SNMPv3 be used on all public and internet-facing networks to protect against security risks and threats. On CX Cloud, it is preferred that SNMPv3 be configured and not SNMPv2c, except for older legacy devices that lack built-in support for SNMPv3. If both versions of SNMP are configured by the user, CX Cloud Agent can, by default, attempt to communicate with each respective device using SNMPv3 and revert to SNMPv2c if the communication cannot be successfully negotiated.

## Connectivity Protocols

As part of the direct device connectivity setup, users must specify details of the device connectivity protocol: SSH (or, alternatively, telnet). SSHv2 can be used, except in the cases of individual legacy assets which lack the appropriate built-in support. Be aware that SSHv1 protocol contains fundamental vulnerabilities. Absent additional security, telemetry data and the underlying assets can be compromised due to these vulnerabilities when relying on SSHv1. Telnet is also insecure. Credential information (usernames and passwords) submitted through telnet are not encrypted and therefore vulnerable to compromise, absent additional security.

## Telemetry Processing Limitation for Devices

The following are limitations when processing telemetry data for devices:

- Some devices may show as reachable in the **Collection Summary** but are not visible in the CX Cloud **Assets** page. Device instrumentation limitations prevent the processing of such devices telemetry.
- If a device from the seed file or IP range collections is also part of the Cisco Catalyst Center inventory, the device is reported only once for the Cisco Catalyst Center entry. The respective devices within the seed file/IP range entry are skipped to avoid duplication.


## Adding Other Assets Using a Seed File

A seed file is a .csv file where each line represents a system data record. In a seed file, every seed file record corresponds to a unique device from which telemetry can be collected by CX Cloud Agent. All error or information messages for each device entry from the seed file being imported are captured as part of job log details. All devices in a seed file are considered managed devices, even if the devices are unreachable at the time of initial configuration. In the event a new seed file is being uploaded to replace a previous one, the date of last upload is displayed in CX Cloud.

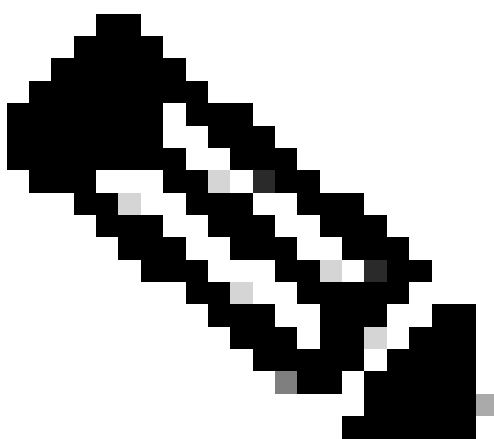
CX Cloud Agent can attempt to connect to the devices but cannot be able to process each one to show in the Assets pages in cases where it is not able to determine the PIDs or Serial Numbers. Any row in the seed file that starts with a semicolon is ignored. The header row in the seed file starts with a semicolon and can be kept as is (recommended option) or deleted while creating the customer seed file.

It is important that the format of the sample seed file, including column headers, not be altered in any way. Click the link provided to view a seed file in PDF format. This PDF is for reference only and can be used to create a seed file that needs to be saved in .csv format.

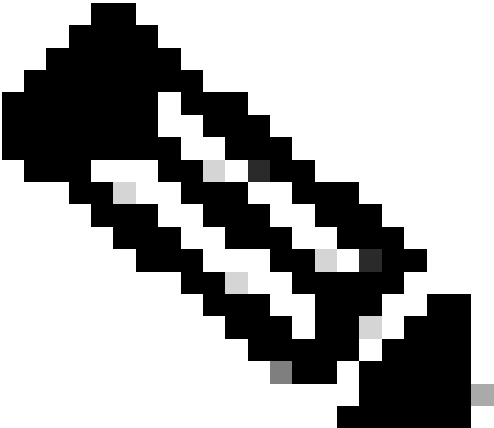
Click this [link](#) to view a seed file that can be used to create a seed file in .csv format.

 **Note:** This PDF is for reference only and can be used to create a seed file that needs to be saved in .csv format.

This table identifies all necessary seed file columns and the data that must be included in each column.

Seed File Column	Column Header / Identifier	Purpose of the Column
A	IP Address or hostname	Provide a valid, unique IP Address or hostname of the device.
B	SNMP protocol version	The SNMP protocol is required by CX Cloud Agent and is used for device discovery within the customer network. Values can be snmpv2c or snmpv3, but snmpv3 is recommended due to security considerations.
C	snmpRo : Mandatory if col#=3 selected as 'snmpv2c'	If the legacy variant of SNMPv2 is selected for a specific device, then snmpRO (read only) credentials for the device SNMP collection must be specified. Otherwise, entry can be blank.
D	snmpv3UserName : Mandatory if col#=3 selected as 'snmpv3'	If SNMPv3 is selected to communicate with a specific device, then the respective login username must be provided.
E	snmpv3AuthAlgorithm : values can be MD5 or SHA	<p>SNMPv3 protocol permits Authentication via either the MD5 or SHA Algorithm. If the device is configured with secure Authentication, then the respective Auth Algorithm must be provided.</p>  <p><b>Note:</b> MD5 is considered insecure, and SHA can be used on all devices that</p>



Seed File Column	Column Header / Identifier	Purpose of the Column
		support it.
F	snmpv3AuthPassword : password	If either a MD5 or a SHA cryptographic algorithm is configured on the device, then the relevant Authentication password needs to be provided for device access.
G	snmpv3PrivAlgorithm : values can be DES , 3DES	<p>If the device is configured with the SNMPv3 privacy algorithm (this algorithm is used to encrypt the response), then the respective Algorithm needs to be provided.</p>  <p><b>Note:</b> 56-bit keys used by DES are considered too short to provide cryptographic security, and that 3DES can be used on all devices that support it.</p>
H	snmpv3PrivPassword : password	If the SNMPv3 privacy algorithm is configured on the device, then its respective privacy password needs to be provided for device connection.
I	snmpv3EngineId : engineID, unique ID representing device, specify engine ID if manually configured on device	The SNMPv3 EngineID is a unique ID representing each device. This engine ID is sent as a reference while collecting the SNMP datasets by CX Cloud Agent. If the customer configures the EngineID manually, then the respective EngineID needs to be provided.

Seed File Column	Column Header / Identifier	Purpose of the Column
J	cliProtocol: values can be 'telnet', 'sshv1', 'sshv2'. If empty can set to 'sshv2' by default	The CLI is intended to interact with the device directly. CX Cloud Agent uses this protocol for CLI collection for a specific device. This CLI collection data is used for Assets and other Insights Reporting within CX Cloud. SSHv2 is recommended; absent other network security measures, in themselves SSHv1 and Telnet protocols do not provide adequate transport security.
K	cliPort : CLI protocol port number	If any CLI Protocol is selected, its respective port number needs to be provided. For example, 22 for SSH and 23 for telnet.
L	cliUser : CLI User name (either CLI username/password or BOTH can be provided, BUT both columns (col#=12 and col#=13) cannot be empty.)	The respective CLI username of the device needs to be provided. This is used by CX Cloud Agent at the time of connecting to the device during CLI collection.
M	cliPassword : CLI user password (either CLI username/password or BOTH can be provided, BUT both columns (col#=12 and col#=13) cannot be empty.)	The respective CLI password of the device needs to be provided. This is used by CX Cloud Agent at the time of connecting to the device during CLI collection.
N	cliEnableUser	If enable is configured on the device, then the device's enableUsername value needs to be provided.
O	cliEnablePassword	If enable is configured on the device, then the device's enablePassword value needs to be provided.
P	Future Support (No Inputs required)	Reserved for Future Use
Q	Future Support (No Inputs required)	Reserved for Future Use
R	Future Support (No Inputs required)	Reserved for Future Use


Seed File Column	Column Header / Identifier	Purpose of the Column
S	Future Support (No Inputs required)	Reserved for Future Use

## Add Other Assets Using a New Seed File

To add other assets using a new seed file:


1. Click **Add Data Source** in the **Admin Center > Data Sources** window.

### Add Data Source




**Catalyst Center**  
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types)

Add Data Source




**Cisco Catalyst SD-WAN Manager**  
Supports the Success Track for WAN

Add Data Source




**Contracts**  
Supports assets associated with a contract

Add Data Source




**CX Cloud Agent**  
Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks

Add Data Source




**Firewall Management Center**  
Supports Cisco Secure Firewall

Add Data Source




**Intersight**  
Supports the Data Center Compute and Data Center Networking Success Tracks

Add Data Source



**Other Assets by IP Ranges**  
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

Add Data Source



**Other Assets by Seed File**  
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks)

Add Data Source

*Add Data Source*

2. Click **Add Data Source** from the **Other Assets by Seed File** option.

## Which CX Cloud Agent Do You Want to Connect to?

Select option ▼



*Select CX Cloud Agent*

3. Select the CX Cloud Agent from the **Which CX Cloud Agent Do You Want to Connect to** dropdown list.
- 

## Which CX Cloud Agent Do You Want to Connect to?

OIC\_Team\_test\_CXCAGENT\_IP\_104 ▼

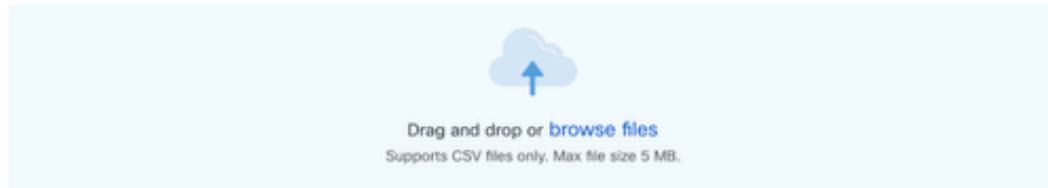


*Continue*

4. Click **Continue**. The **Upload Your Seed File** page displays.

### Upload your seed file

Download the [seed file template](#) and add your device information. Then attach the file below.



### Schedule inventory collection

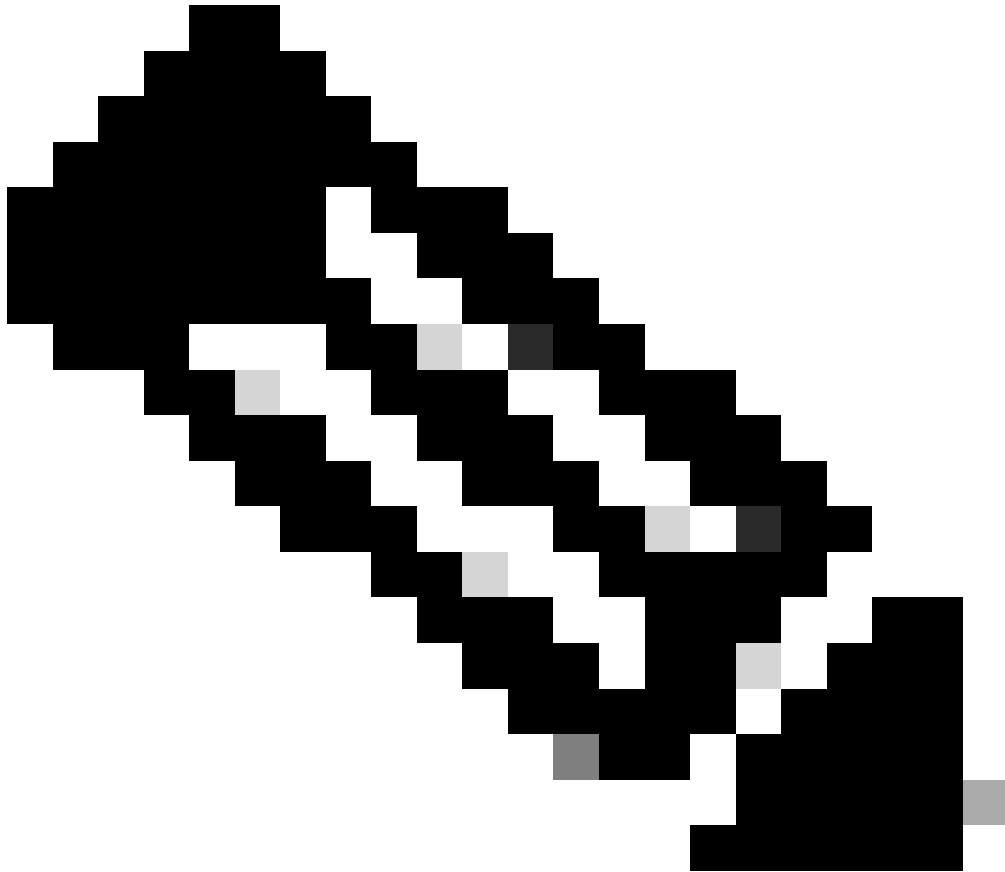
Frequency	Select time	Time Zone	
Frequency ▾	12:00 ▾	AM ▾	Europe/Amsterdam (... ▾

Run the first collection now (this may take up to 75 minutes)

Connect

#### *Upload Your Seed File*

5. Click the hyperlinked **seed file template** to download the template.
6. Manually enter or import data into the file. Once complete, save the template as a .csv file to import the file into CX Cloud Agent.
7. Drag-and-drop or click **browse files** to upload the .csv file.
8. Complete the **Schedule inventory collection** section.



**Note:** Before initial configuration of CX Cloud is completed, CX Cloud Agent must perform the first telemetry collection by processing the seed file and establishing connection with all identified devices. Collection can be initiated on-demand or run according to a schedule defined here. Users can perform the first telemetry connection by selecting the Run the first collection now check box. Depending on the number of entries specified in the seed file and other factors, this process can take a considerable amount of time.

---

9. Click **Connect**. The **Data Sources** window opens, displaying a confirmation message.

## Add Other Assets Using a Modified Seed File

To add, modify, or delete devices using the current seed file:

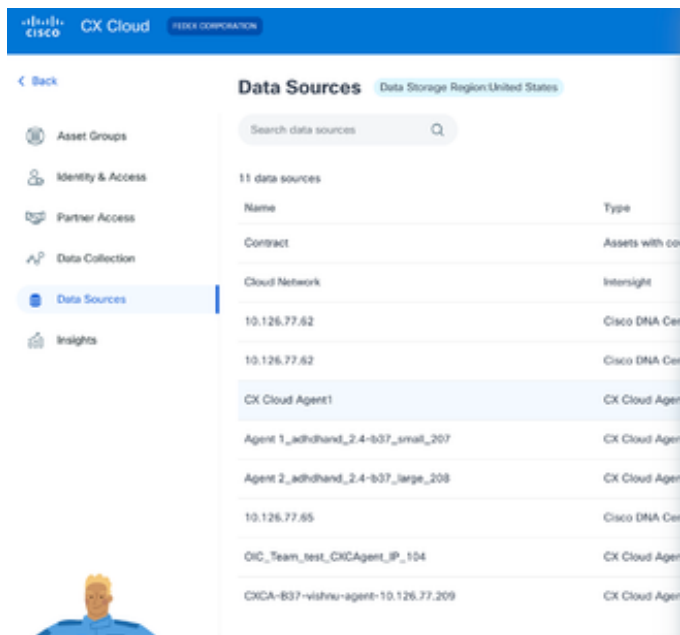
1. **Open** the previously created seed file, make required changes, and **save** the file.



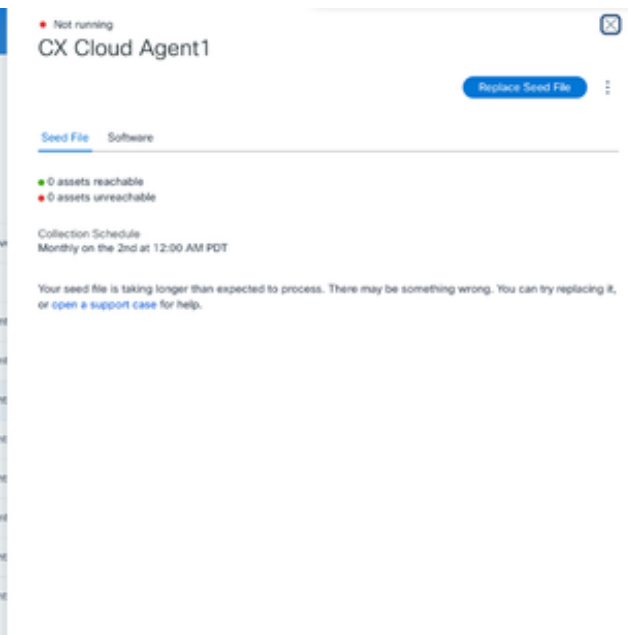
**Note:** To add assets to the seed file, append those assets to the previously created seed file and reload the file. This is necessary since uploading a new seed file replaces the current seed file. Only the latest uploaded seed file is used for discovery and collection.

---

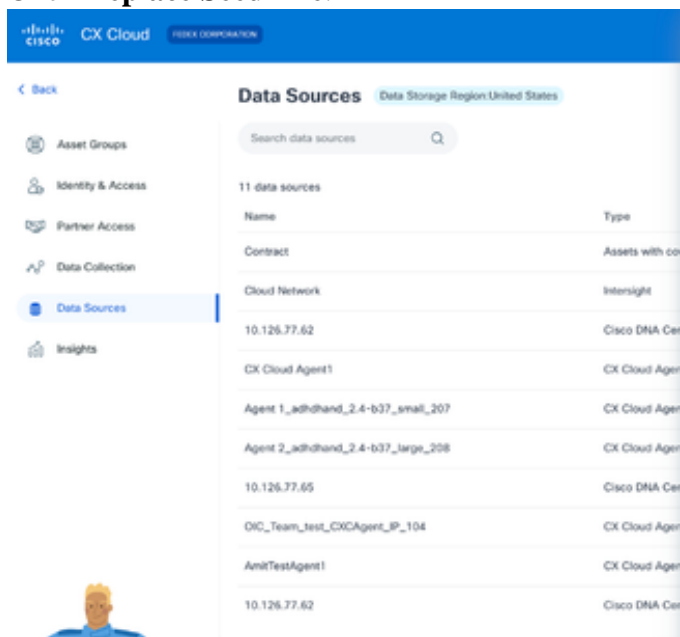
2. From the **Data Sources** page, click the CX Cloud Agent data source that requires an updated seed file. The **CX Cloud Agent** details window opens.



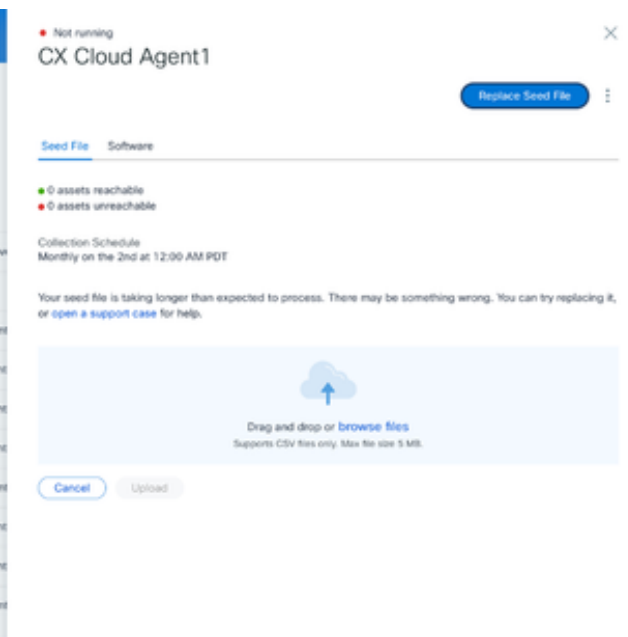
CX Cloud Agent Details window



### 3. Click **Replace Seed File**.



CX Cloud Agent window



### 4. Drag-and-drop or click **browse files** to upload the modified seed file.

### 5. Click **Upload**.

## Add Other Assets Using IP Ranges

IP ranges allow users to identify hardware assets and, subsequently, collect telemetry from those devices based on IP addresses. The devices for telemetry collection can be uniquely identified by specifying a single network-level IP range, which can be scanned by CX Cloud Agent using the SNMP protocol. If the IP range is chosen to identify a directly connected device, the IP addresses that are referenced can be as restrictive as possible, while allowing coverage for all required assets.

- Specific IPs can be provided, or wildcards can be used to replace octets of an IP to create a range.

- If a specific IP address is not included in the IP range identified during setup, CX Cloud Agent does not attempt to communicate with a device that has such an IP address, nor does it collect telemetry from such a device.
- Entering \*.\*.\*.\* allows CX Cloud Agent to use the user-supplied credential with any IP. For example: 172.16.\*.\* allows the credentials to be used for all devices in the 172.16.0.0/16 subnet.
- If there are any changes to the network or Installed Base (IB), the IP range can be modified. Refer to section [Editing IP Ranges](#)

CX Cloud Agent will attempt to connect to the devices but may not be able to process each one to show in the **Assets** view in cases where it is not able to determine the PIDs or Serial Numbers.

---

 **Notes:**

Clicking **Edit IP Address Range** initiates on-demand device discovery. When any new device is added or deleted (within or outside) to a specified IP-range, customer must always click **Edit IP Address Range** (refer to section [Editing IP Ranges](#)) and complete the steps required for initiating the on-demand device discovery to include any newly added device to the CX Cloud Agent collection inventory.

---

Adding devices using an IP range requires users to specify all applicable credentials through the configuration UI. The fields visible vary depending on the protocols selected on the previous windows. If multiple selections are made for the same protocol, for example, selecting both SNMPv2c and SNMPv3 or selecting both SSHv2 and SSHv1, CX Cloud Agent automatically auto-negotiates the protocol selection based on the individual device capabilities.

When connecting devices using IP addresses, customer should ensure all relevant protocols in the IP range along with SSH versions and Telnet credentials are valid or the connections will fail.

## Adding Other Assets by IP Ranges









To add devices using the IP range:

1. Click **Add Data Source** in the **Admin Center** > **Data Sources** window.



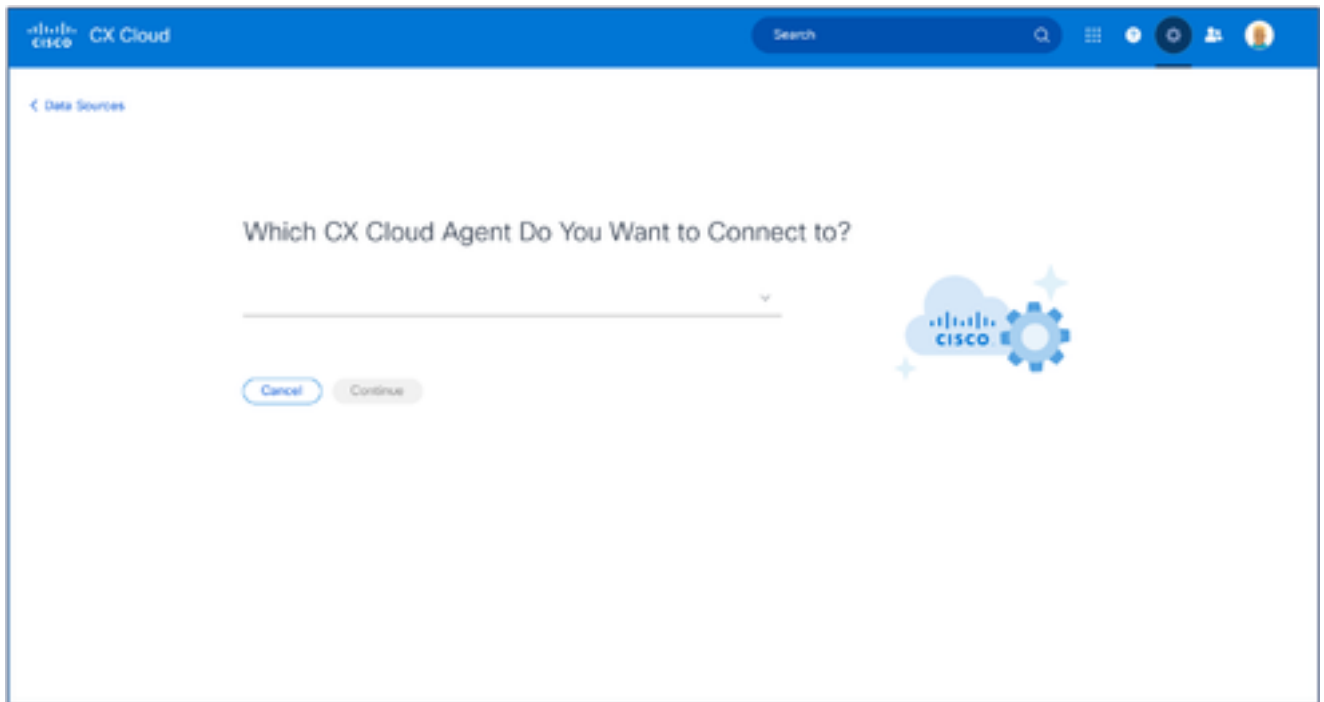
## Add Data Source

Search data sources Q

-  **Catalyst Center**  
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types) Add Data Source
-  **Cisco Catalyst SD-WAN Manager**  
Supports the Success Track for WAN Add Data Source
-  **Contracts**  
Supports assets associated with a contract Add Data Source
-  **CX Cloud Agent**  
Add up to 20 CX Cloud Agents to your network to support a variety of Success Tracks Add Data Source
-  **Firewall Management Center**  
Supports Cisco Secure Firewall Add Data Source
-  **Intersight**  
Supports the Data Center Compute and Data Center Networking Success Tracks Add Data Source
-  **Other Assets by IP Ranges**  
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks) Add Data Source
-  **Other Assets by Seed File**  
Uses CX Cloud Agent to support the Success Track for Campus Network (manual method recommended for smaller networks) Add Data Source

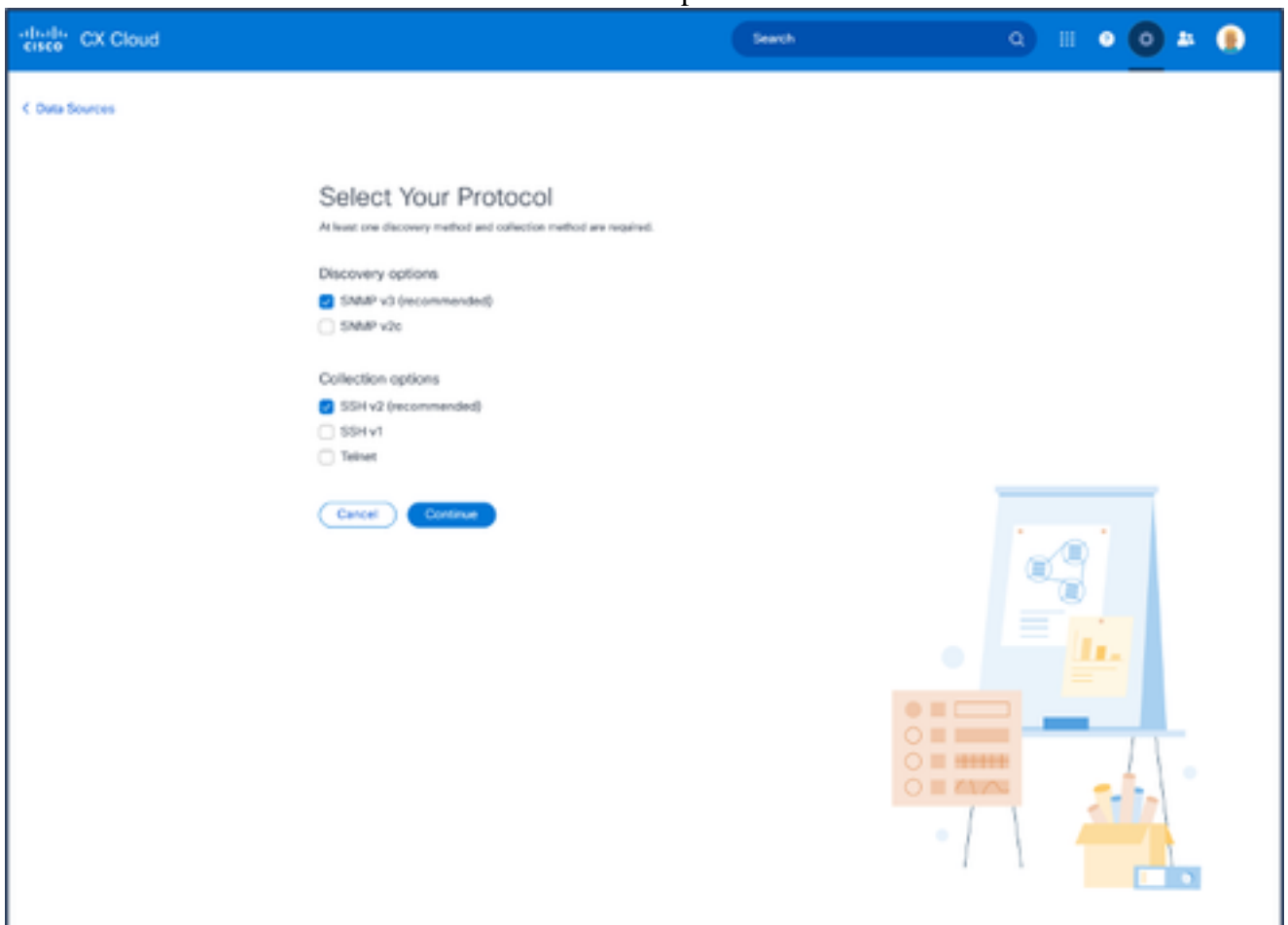
*Add Data Sources*

2. Click **Add Data Source** in the **Other Assets by IP Ranges** option.



*Select CX Cloud Agent*

3. Select the CX Cloud Agent from the **Which CX Cloud Agent Do You Want to Connect to** drop-down list.
4. Click **Continue**. The **Select Your Protocol** window opens.



*Select Your Protocol*

5. Select the applicable check boxes for **Discovery options** and **Collection options**.

6. Click **Continue**.

The screenshot shows the Cisco CX Cloud interface for configuring data sources. The page is titled "Provide Discovery Details" and includes an "Edit protocol" link. The configuration is divided into two main sections: "SNMP v3 credentials" and "SSH v2 credentials".

**SNMP v3 credentials:**

- Starting IP address: 198.89.09.2
- Ending IP address: 198.89.09.10
- Username: Marger1505
- Engine ID: Tuto50102
- Authorization algorithm: MD5
- Privacy algorithm: DES
- Authorization password: [Redacted]
- Authorization password: [Redacted]

**SSH v2 credentials:**

- Username: Marger1505
- Enable username (optional): Tuto50102
- Password: MD5
- Enable password (optional): [Redacted]

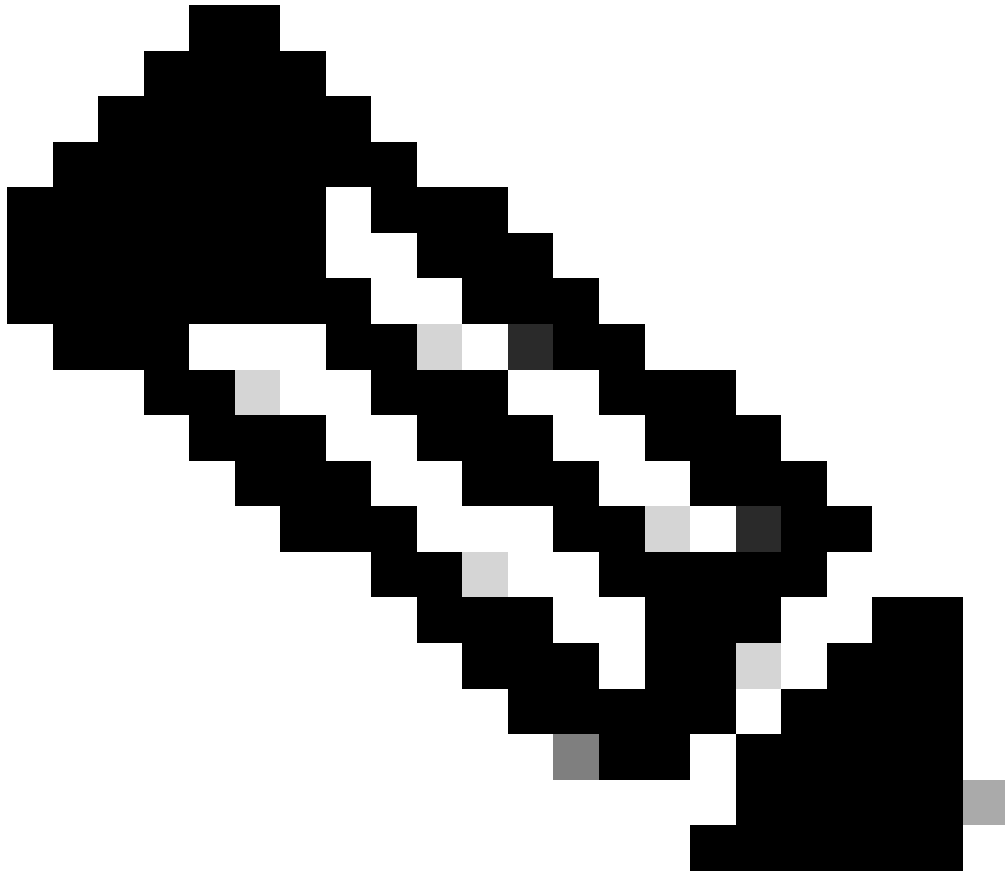
**Schedule Inventory Collection:**

- Frequency: Weekly
- Time: 12:00 AM PST
- Day: Tuesday
- Run the first collection now (may take up to 75 minutes)
- Buttons: Add Another IP Range, Complete Setup, Delete this IP range

An illustration of a presentation board with charts and a person is visible in the bottom right corner of the interface.

*Provide Discovery Details and Schedule Inventory Collection Sections*

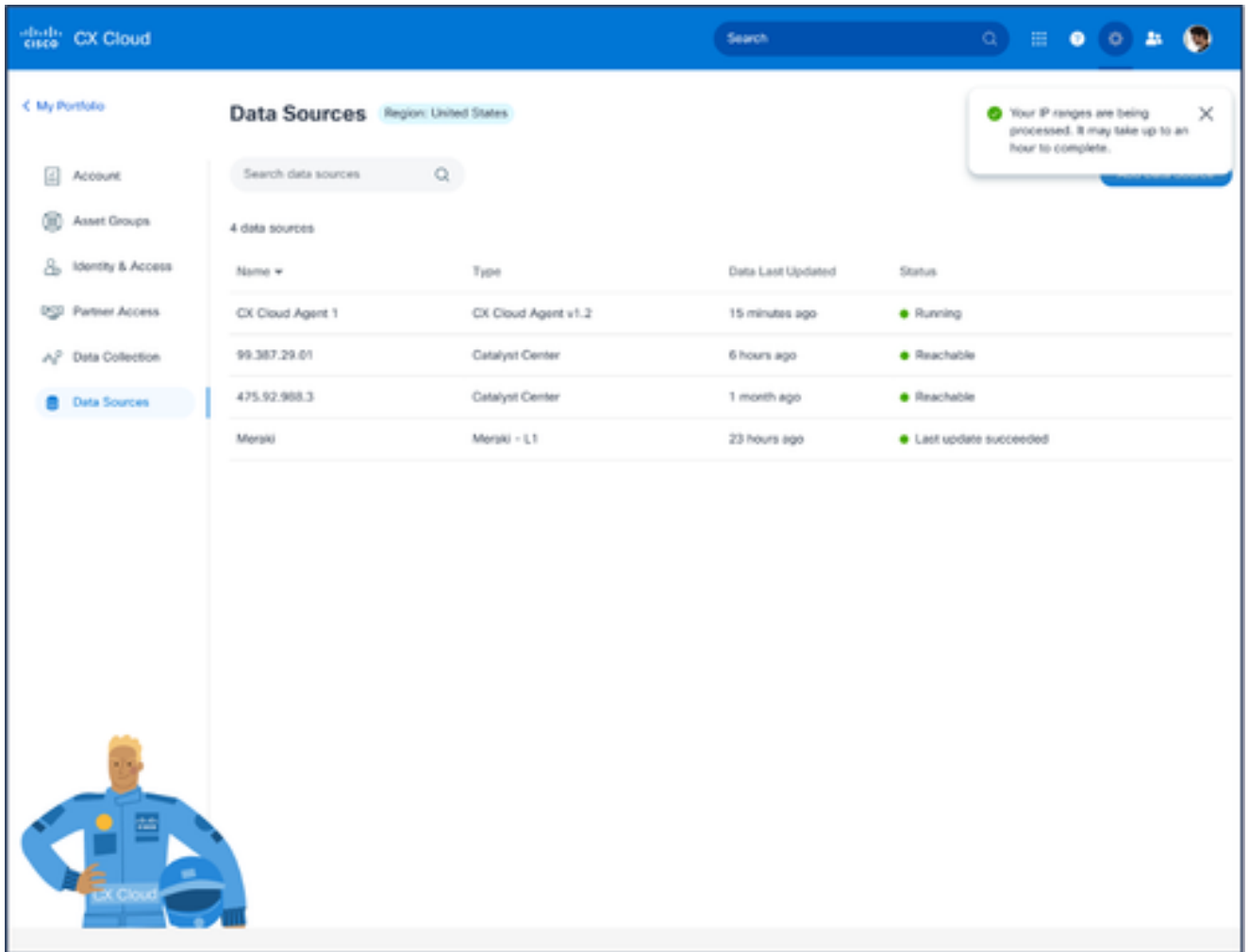
7. Enter the required details in the **Provide Discovery Details** and **Schedule Inventory Collection** sections.



**Note:** To add another IP range for the selected CX Cloud Agent, click Add Another IP Range to navigate back to the Set Your Protocol window and repeat the steps in this section.

---

8. Click **Complete Setup**. A confirmation displays upon successful deployment.

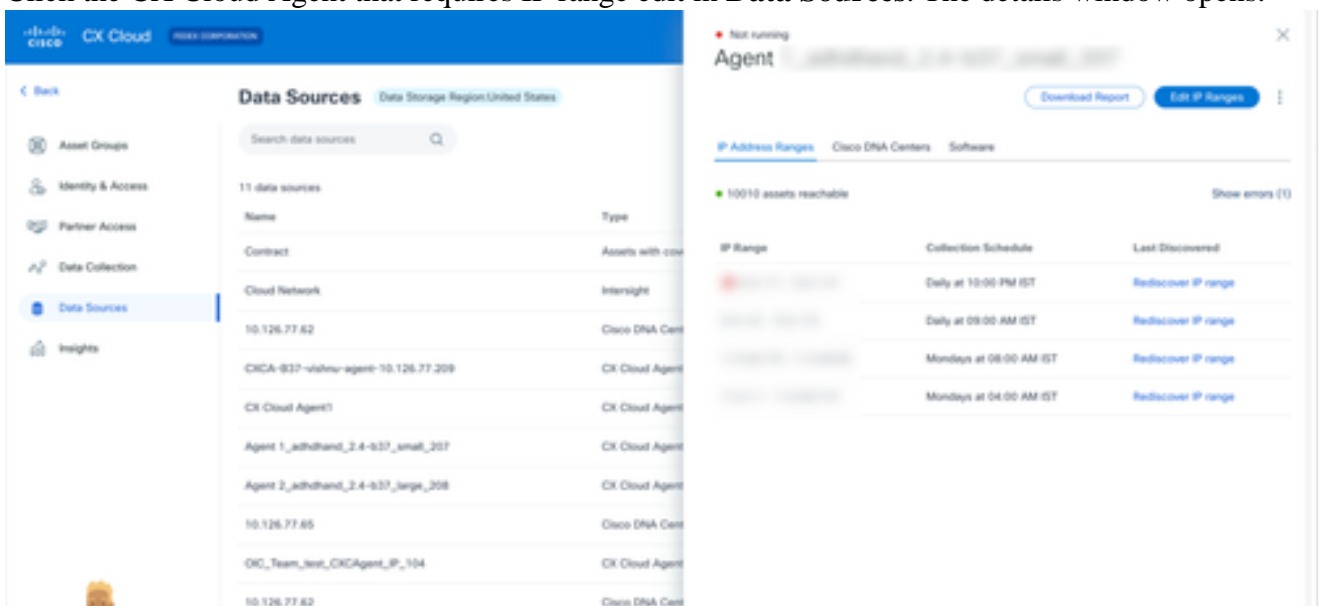


Confirmation Message

## Editing IP Ranges

To edit an IP range:

1. Navigate to the **Data Sources** window.
2. Click the CX Cloud Agent that requires IP range edit in **Data Sources**. The details window opens.

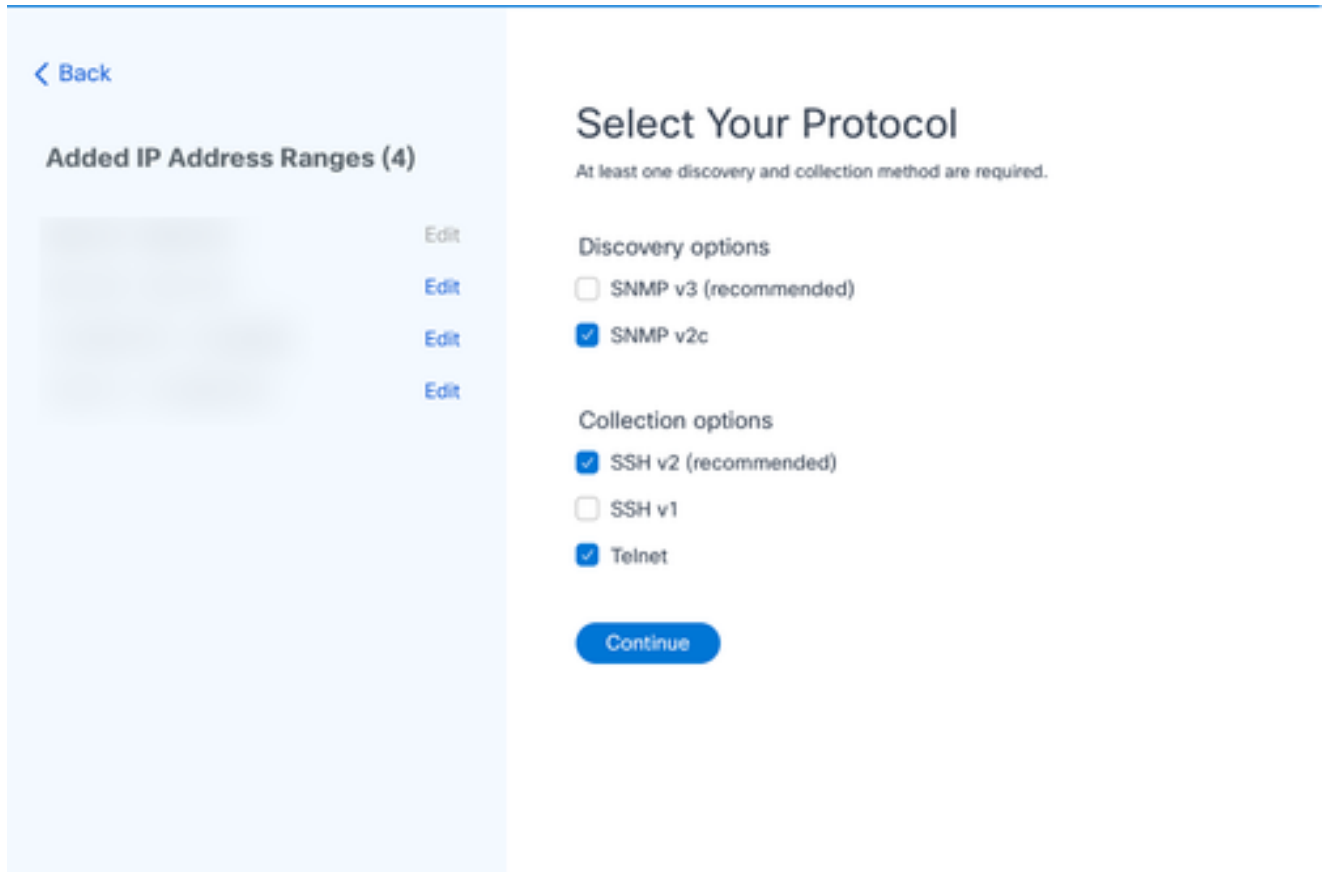


3. Click **Edit IP Address Range**. The Connect to CX Cloud window opens.

The screenshot shows a web interface for configuring discovery details. On the left, a sidebar titled 'Added IP Address Ranges (4)' contains a list of ranges, each with an 'Edit' link. The main area is titled 'Provide Discovery Details' and includes a link 'Edit the protocols' in the top right. The configuration is organized into sections: 'Starting IP Address' (5.0.1.71) and 'Ending IP Address' (5.0.1.72); 'SNMP V2c credentials' with a 'Read Community' field; 'SSHV2 credentials' with 'Username' (cxsuper2020@gmail.com) and 'Password' (masked) fields, and 'Enable Username (Optional)' and 'Enable Password (Optional)' checkboxes; and 'Telnet credentials' with similar 'Username' and 'Password' fields and checkboxes. At the bottom, there are three buttons: 'Delete this IP range', 'Add Another IP Range', and 'Complete Setup'.

*Provide Discovery Details*

4. Click **Edit the protocols**. The **Select Your Protocol** window opens.



*Select Your Protocol*

5. Select the appropriate check boxes to choose applicable protocols and click **Continue** to navigate back to the **Provide Discovery Details** window.

[< Back](#)

**Added IP Address Ranges (4)**

Edit

Edit

Edit

Edit

## Provide Discovery Details [Edit the protocols](#)

Starting IP Address: 5.0.1.71

Ending IP Address: 5.0.1.72

### SNMP V2c credentials

Read Community

---

### SSHV2 credentials

Username:

Enable Username (Optional)

Password:

Enable Password (Optional)

### Telnet credentials

Username:

Enable Username (Optional)

Password:

Enable Password (Optional)

[Delete this IP range](#) [Add Another IP Range](#) [Complete Setup](#)

*Provide Discovery Details*

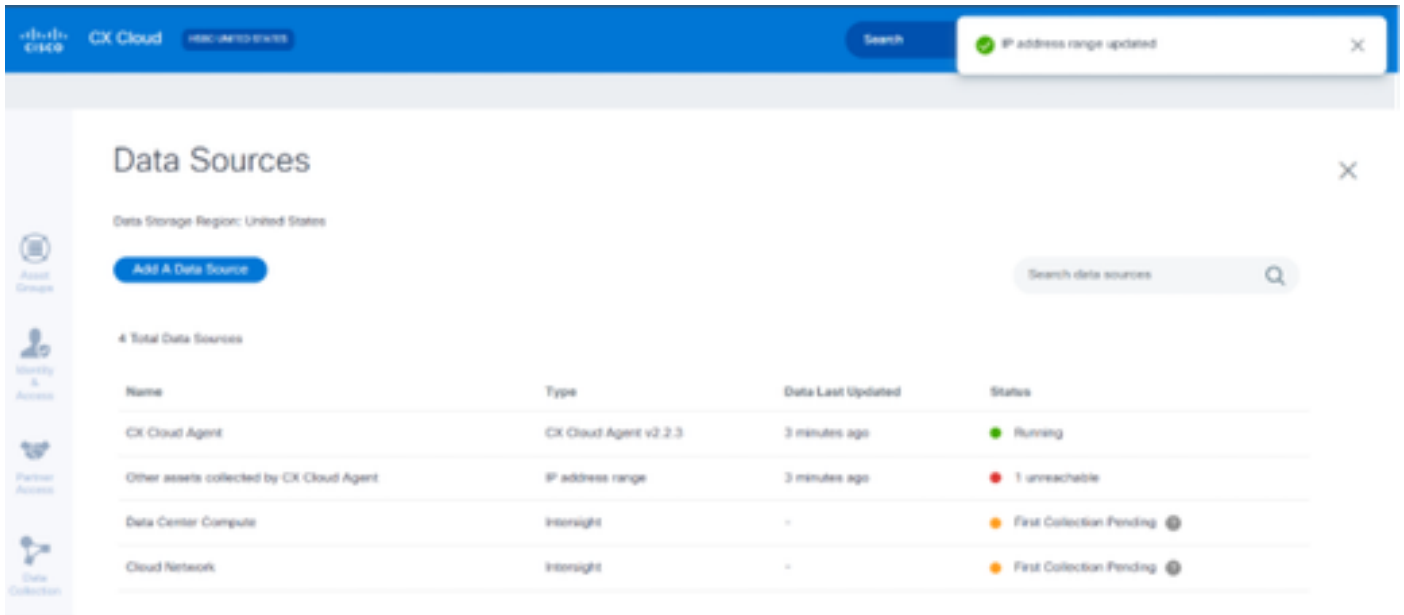
6. Edit the details as required and click **Complete Setup**. The **Data Sources** window opens, displaying a message confirming the addition of newly added IP Address range(s).





**Note:** This confirmation message does not verify whether devices within the modified range are reachable or if their credentials are accepted. This confirmation occurs when the customer initiates the discovery process..

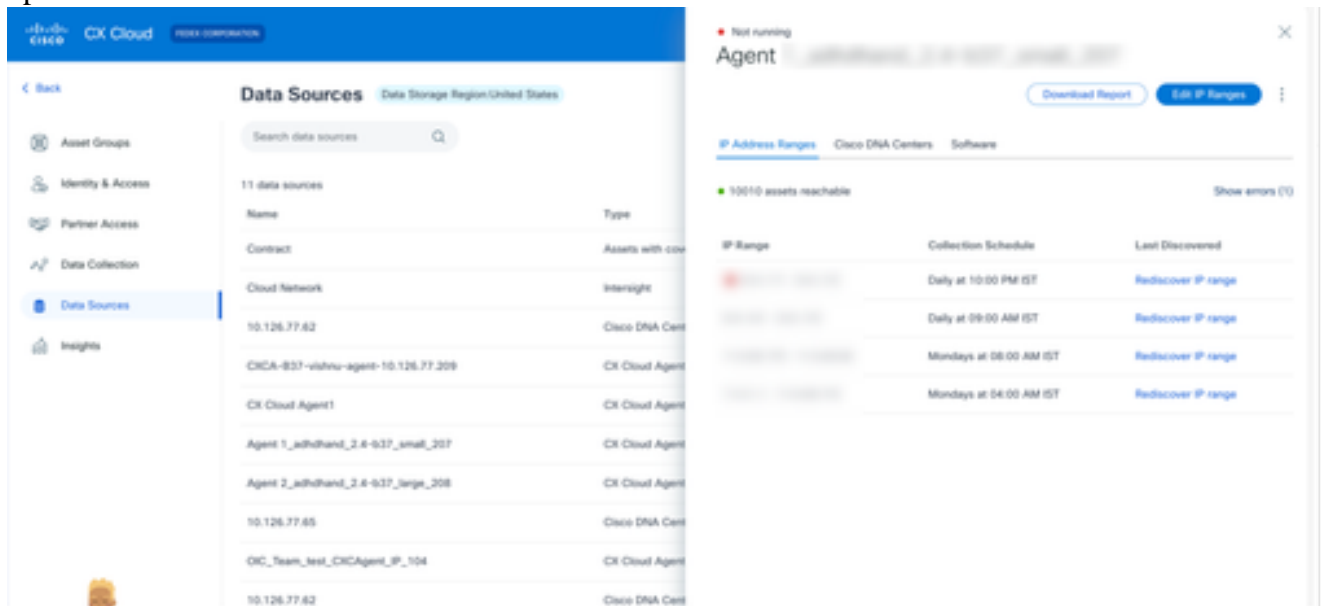
---



## Deleting IP Range

To delete an IP range:

1. Navigate to the **Data Sources** window.
2. Select the respective CX Cloud Agent with the IP range that needs to be deleted. The details window opens.



*Data Sources*

3. Click **Edit IP Ranges**. The **Provide Discovery Details** window opens.

[← Back](#)

**Added IP Address Ranges (4)**

Edit  
Edit  
Edit  
Edit

### Provide Discovery Details [Edit the protocols](#)

Starting IP Address: 5.0.1.71      Ending IP Address: 5.0.1.72

**SNMP V2c credentials**  
Read Community

\_\_\_\_\_

**SSHV2 credentials**

Username:       Enable Username (Optional) \_\_\_\_\_

Password:       Enable Password (Optional) \_\_\_\_\_

**Telnet credentials**

Username:       Enable Username (Optional) \_\_\_\_\_

Password:       Enable Password (Optional) \_\_\_\_\_

[Delete this IP range](#)      [Add Another IP Range](#)      [Complete Setup](#)

*Provide Discovery Details*

4. Click the **Delete this IP range** link. The confirmation message displays.

[✕](#)

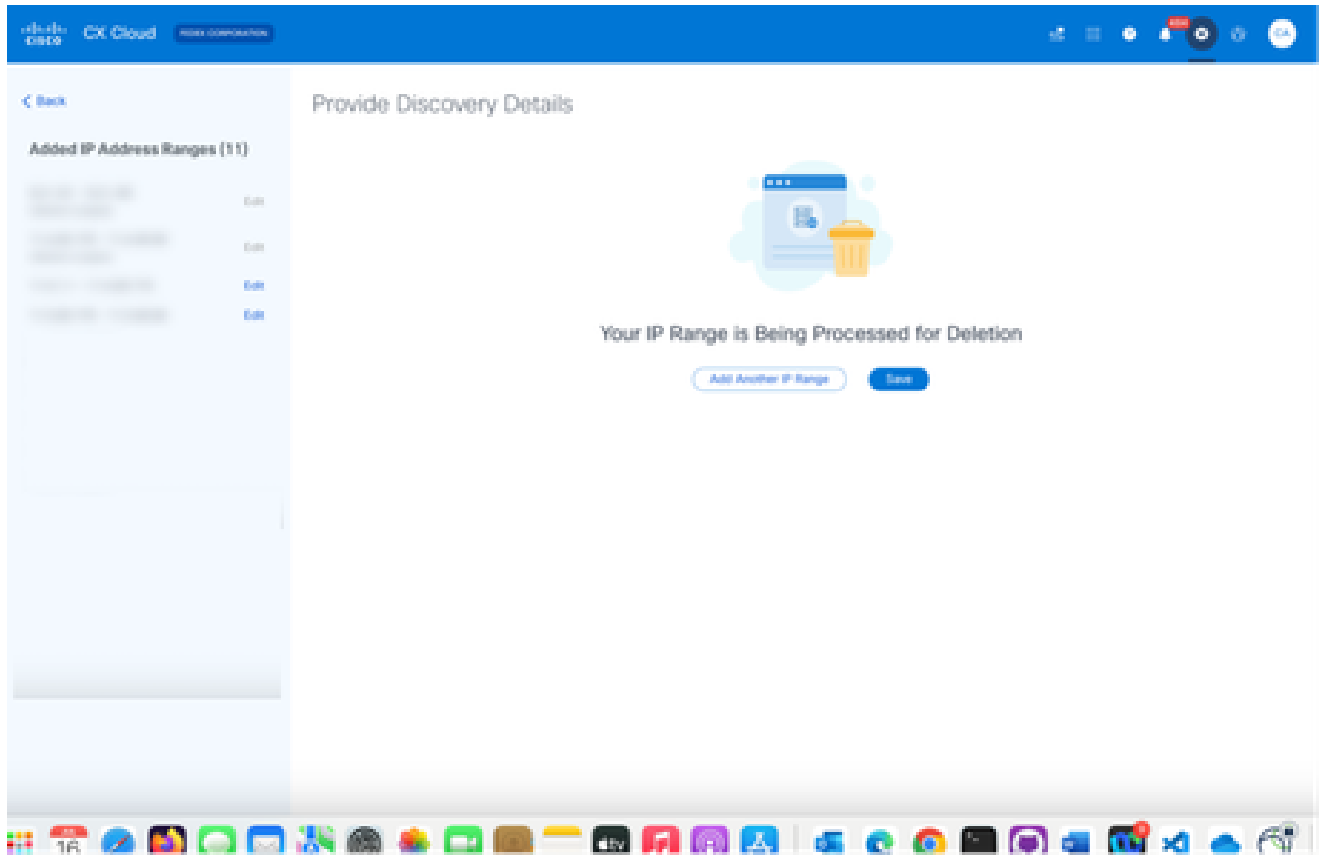
## Delete This IP Range

Any edits you've made won't be saved.

[Continue Editing](#)      [Delete](#)

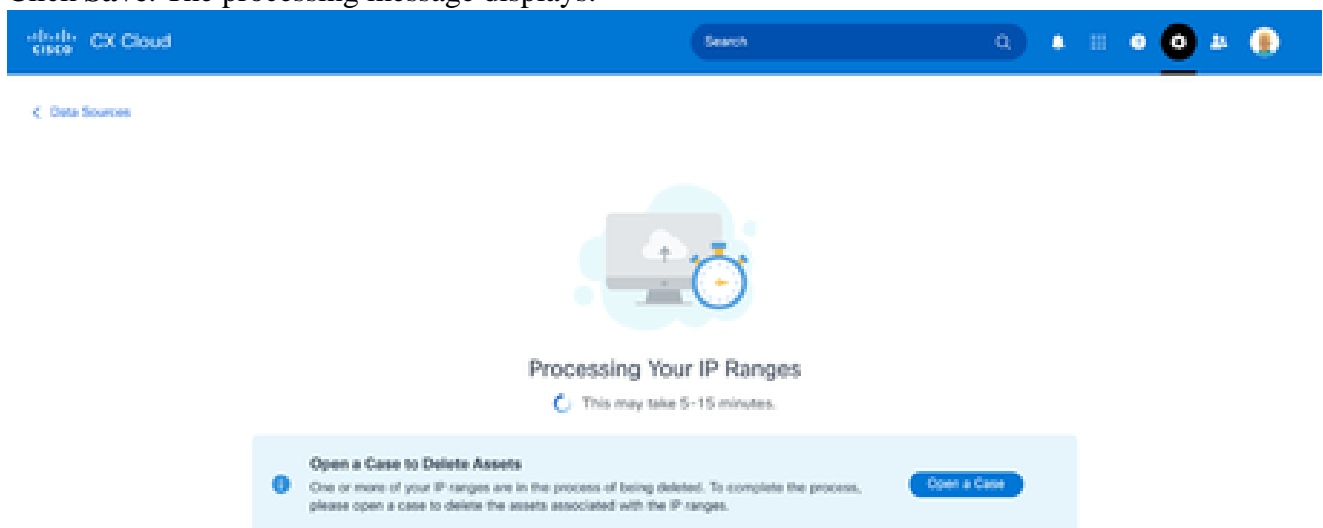
*Confirmation Delete Message*

5. Click **Delete**.



*IP Range Delete*

6. Click **Save**. The processing message displays.



7. Click **Open a Case** to create a case to delete the assets associated with the IP range. The **Data Sources** window opens, displaying a confirmation message.

## **About Devices Discovered from Multiple Controllers**

It is possible that some devices could be discovered by both the Cisco Catalyst Center and direct device connection to CX Cloud Agent causing duplicate data to be collected from those devices. To avoid collecting duplicate data and having only one controller manage the devices, a precedence for which CX Cloud Agent manages the devices needs to be determined.

- If a device is first discovered by Cisco Catalyst Center and then rediscovered by direct device connection (using a seed file or an IP range), Cisco Catalyst Center takes precedence in controlling the device.
- If a device is first discovered by direct device connection to CX Cloud Agent and then rediscovered by Cisco Catalyst Center, Cisco Catalyst Center takes precedence in controlling the device.

## **Scheduling Diagnostics Scans**

Customers can schedule on demand diagnostic scans in CX Cloud.



**Note:** Cisco recommends scheduling diagnostic scans or initiating on-demand scans at least 6-7 hours apart from inventory collection schedules so they do not overlap. Executing multiple diagnostic scans simultaneously can slow the scanning process and potentially result in scan failures.

---

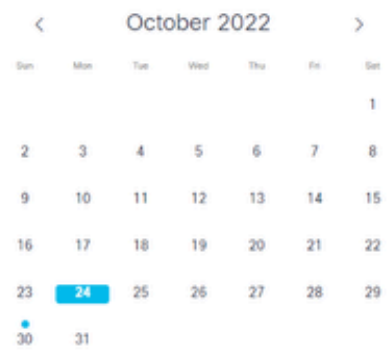
To schedule diagnostic scans:

1. On the **Home** page, click the **Settings** (gear) icon.
2. On the **Data Sources** page, select **Data Collection** in the left pane.
3. Click **Schedule Scan**.

## Data Collection

Diagnostic Scans 3

Schedule Scan



No Diagnostic Scans Found

Inventory Collection 3

3 Collections

Source	Schedule	
Other assets collected by CX Cloud Agent	Monthly on the 30th at 05:30 PM EDT	⋮
10.197.238.127	Monthly on the 30th at 05:00 PM EDT	⋮
22.1.90.1	Monthly on the 30th at 09:00 PM EDT	⋮

Rapid Problem Resolution

Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.

Enable for Campus Network

Data Collection

4. Configure a schedule for this scan.

### Other assets collected by CX Cloud Agent Inventory Collection Details ×

Schedule History

Weekly ▾ on Sunday ▾ at 12:00 am ▾ EDT

Created: Oct 3, 2022

Save Scheduled Collection

Configure Scan Schedule

5. In the devices list, select all devices for the scan and click **Add**.

## New Scheduled Scan

**Data Sources**

Other assets collected by CX Cloud Agent X

**Description (Optional)**

<input type="checkbox"/>	Device	Source IP	IP Address
<input type="checkbox"/>	Device_22_0_2_1	10.127.249.156	22.0.2.1
<input type="checkbox"/>	Device_22_0_32_1	10.127.249.156	22.0.32.1
<input type="checkbox"/>	Device_22_0_36_1	10.127.249.156	22.0.36.1
<input type="checkbox"/>	Device_22_0_41_1	10.127.249.156	22.0.41.1
<input type="checkbox"/>	Device_22_0_51_1	10.127.249.156	22.0.51.1
<input type="checkbox"/>	Device_22_0_55_1	10.127.249.156	22.0.55.1
<input type="checkbox"/>	Device_22_0_61_1	10.127.249.156	22.0.61.1
<input type="checkbox"/>	Device_22_0_63_1	10.127.249.156	22.0.63.1
<input type="checkbox"/>	Device_22_0_64_1	10.127.249.156	22.0.64.1
<input type="checkbox"/>	Device_22_0_70_1	10.127.249.156	22.0.70.1

**Schedule**

Frequency ▼ at Time ▼ IST Save Changes

Add >
< Remove

Devices are part of selected list

1 2 Next

### Schedule a Scan

6. Click **Save Changes** when the scheduling is complete.

The Diagnostic Scans and the Inventory Collection schedules can be edited and deleted from the Data Collection page.

Asset Groups  
 Identity & Access  
 Partner Access  
 Data Collection  
 Data Sources  
 Insights  
 Automation

## Data Collection

**Diagnostic Scans** ▼

2 Scans

Asset Count	Source	Schedule
1	10.127.249.152	Not scannable
10	10.127.249.152	Daily at 07:00 PM IST

Schedule Scan

**Inventory Collection** ▼

8 Collections

Source	Schedule
Other assets collected by CX Cloud Agent	Daily at 04:00 AM IST
	Daily at 12:30 AM IST
172.20.224.70/live.cisco.com	Monthly on the 9th at 11:30 PM IST
10.127.249.152	Daily at 02:00 AM IST

October 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
	3	4	5	6	7	8
	10	11	12	13	14	15
	16	17	18	19	20	21
	23	24	25	26	27	28
	30	31				

Edit Schedule

Delete Schedule

**Rapid Problem Resolution**

Automate data collection and diagnostics when a support case is opened. This helps Cisco experts diagnose and troubleshoot problems faster.

Enable for Campus Network

Rapid Problem Resolution for Cloud Network and Data Center Compute is managed in Intersight. Enable or disable tech support bundle collection in Intersight for these Success Tracks.

[View detailed instructions](#)

Data Collection with Edit and Delete Schedule Options

# Upgrading CX Cloud Agent VMs to Medium and Large Configurations



Once VMs are upgraded, it is not possible to:

- Downscale from a large or medium to a small configuration
- Downscale from a large to medium configuration
- Upgrade from a medium to large configuration

Prior to upgrading the VM, Cisco recommends taking a snapshot for the purpose of recovery in case of failure. Refer to [Backing Up and Restoring the CX Cloud VM](#) for more details.

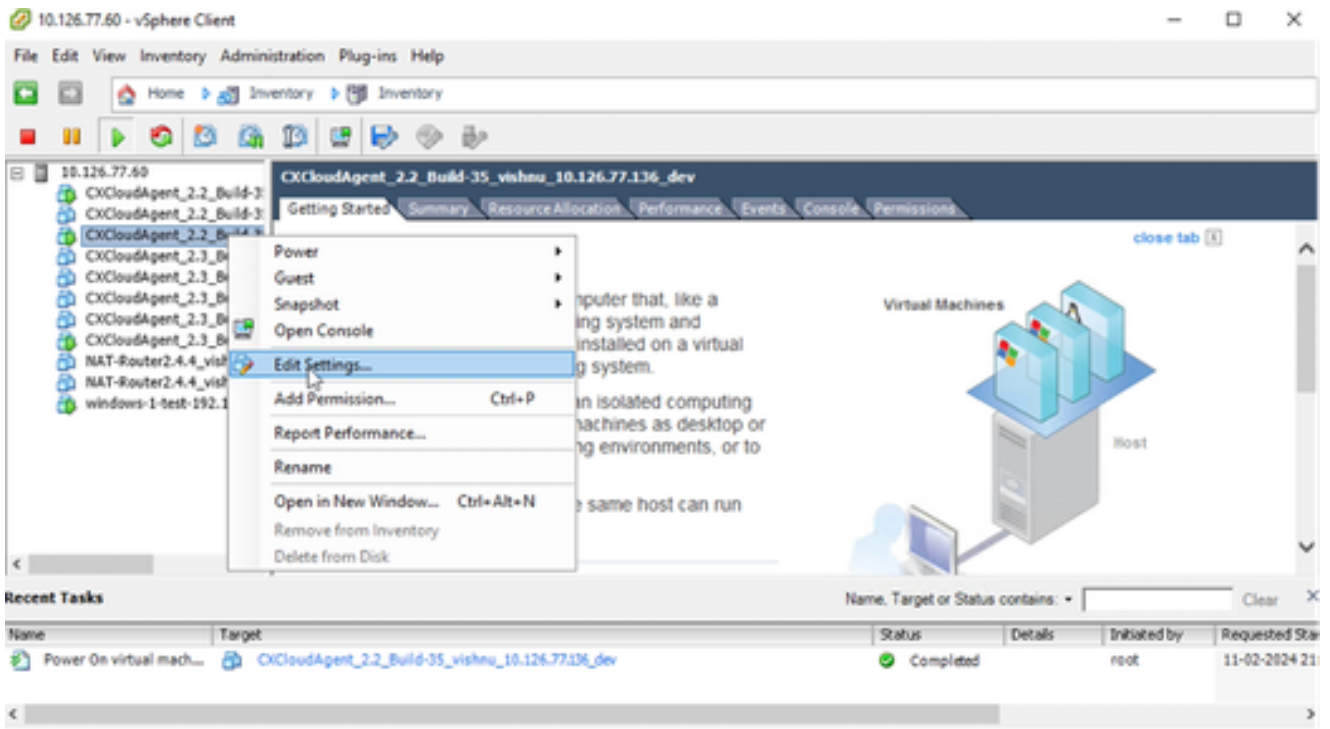
## **Reconfiguring Using VMware vSphere Thick Client**

To upgrade the VM configuration using existing VMware vSphere Thick Client:



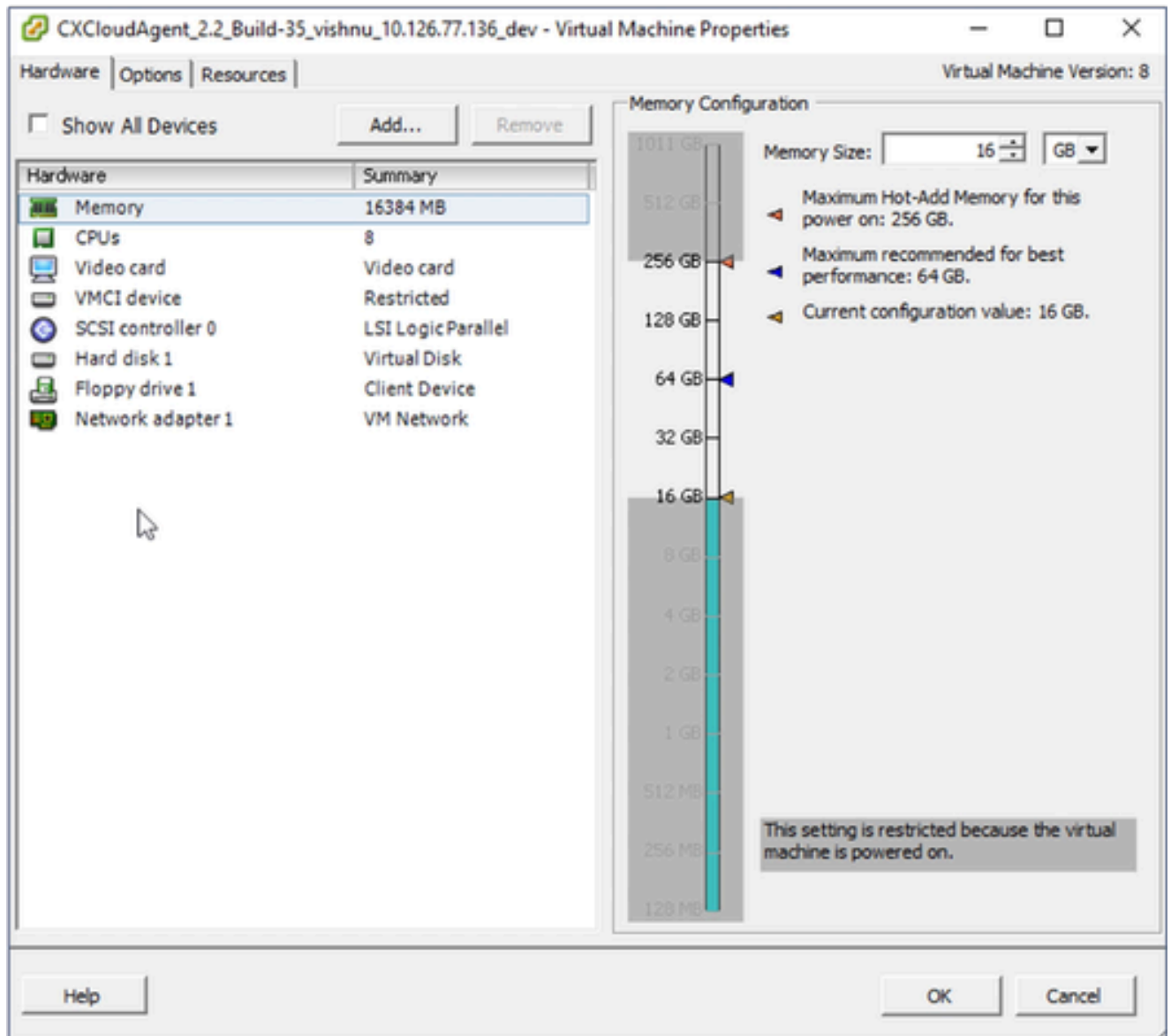
vSphere Client

1. Log in to the VMware vSphere Client. The **Home** page displays a list of VMs.



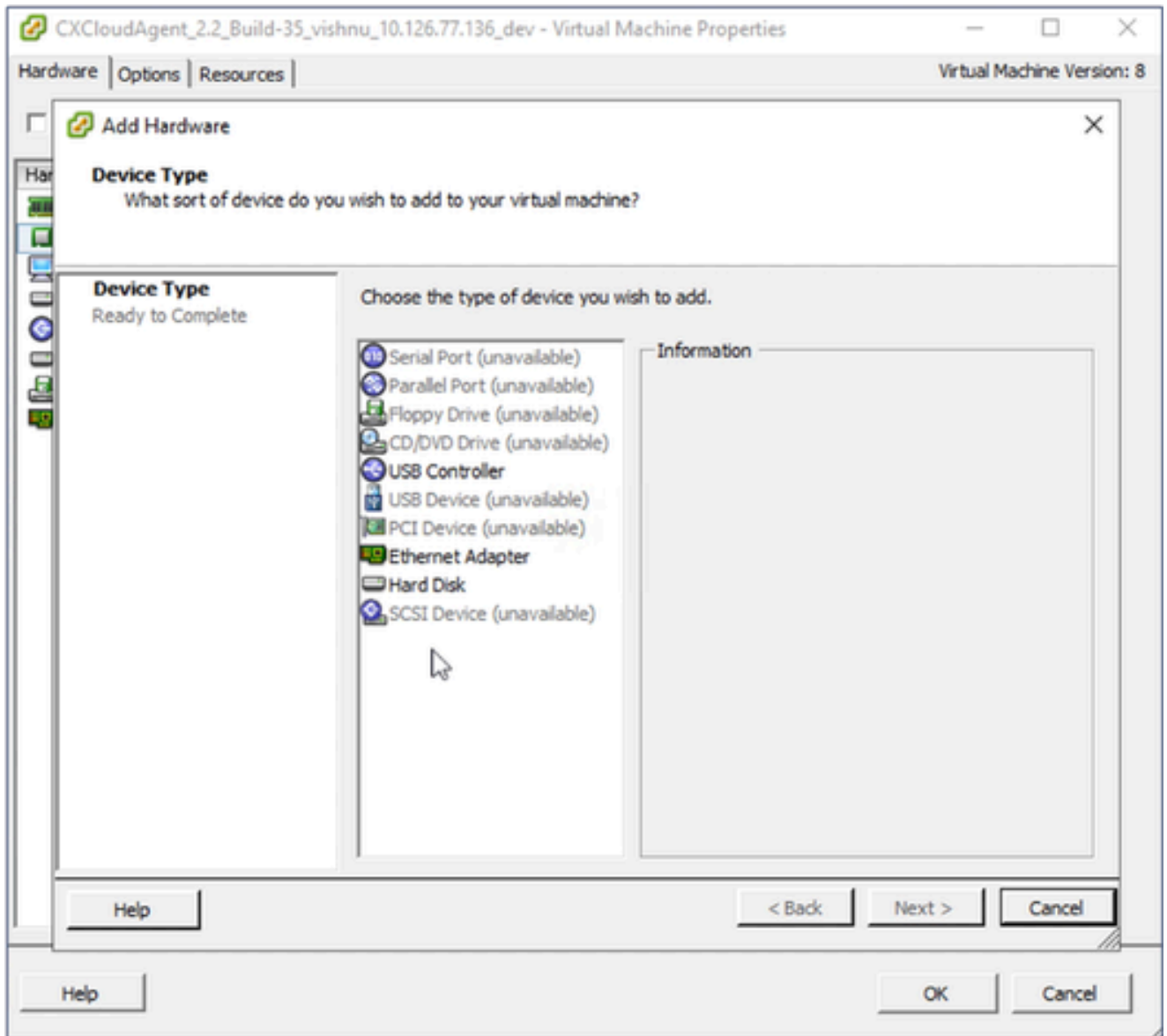
*Edit Settings*

2. Right-click the target VM and select **Edit Settings** from the menu. The **VM Properties** window opens.



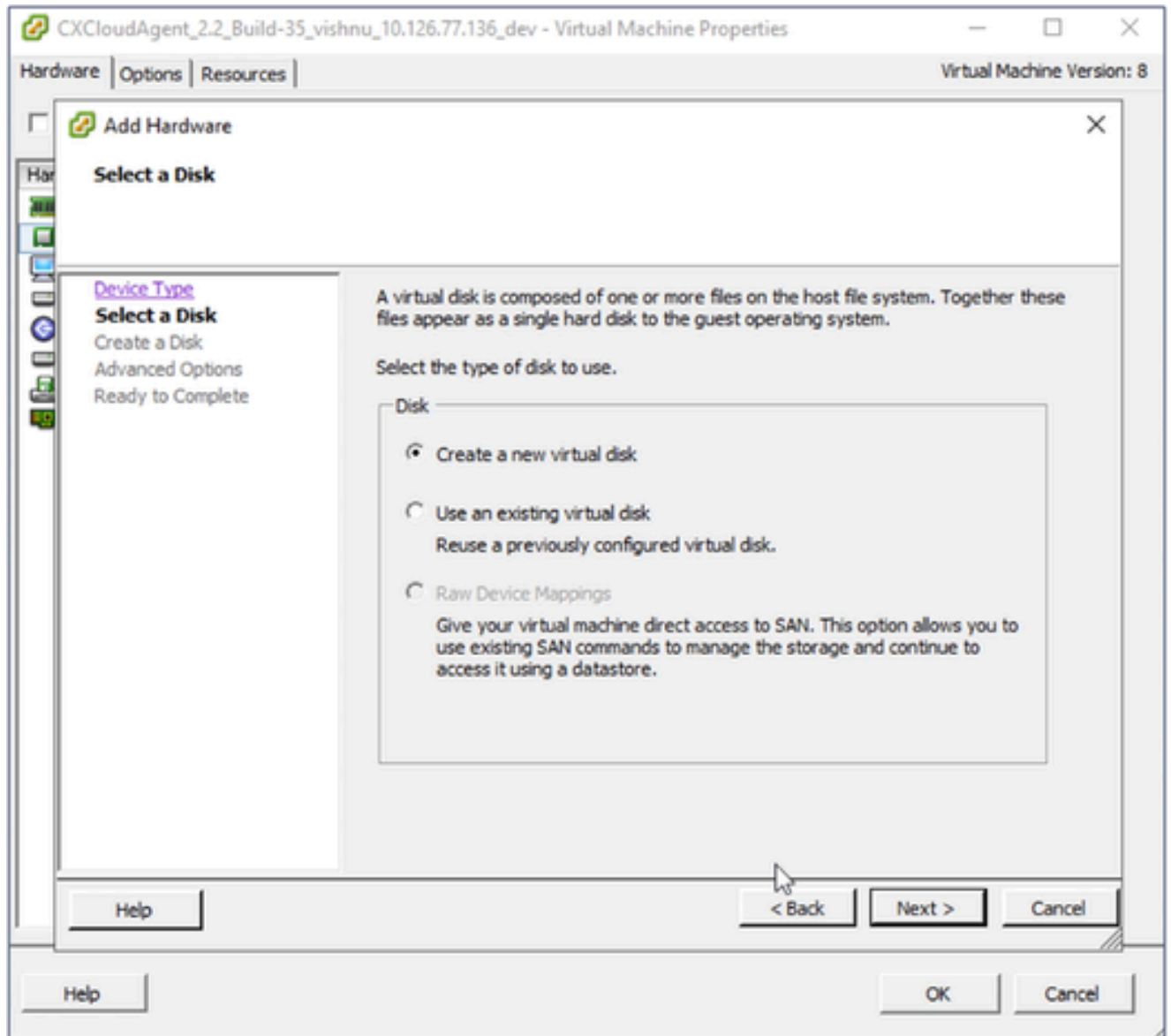
*VM Properties*

3. Update the **Memory Size** values as specified:  
 Medium: 32 GB (32768 MB)  
 Large: 64 GB (65536 MB)
4. Select **CPUs** and update the values as specified:  
 Medium: 16 core (8 sockets \*2 core/socket)  
 Large: 32 core (16 sockets \*2 core/socket)
5. Click **Add**. The **Add Hardware** window opens.



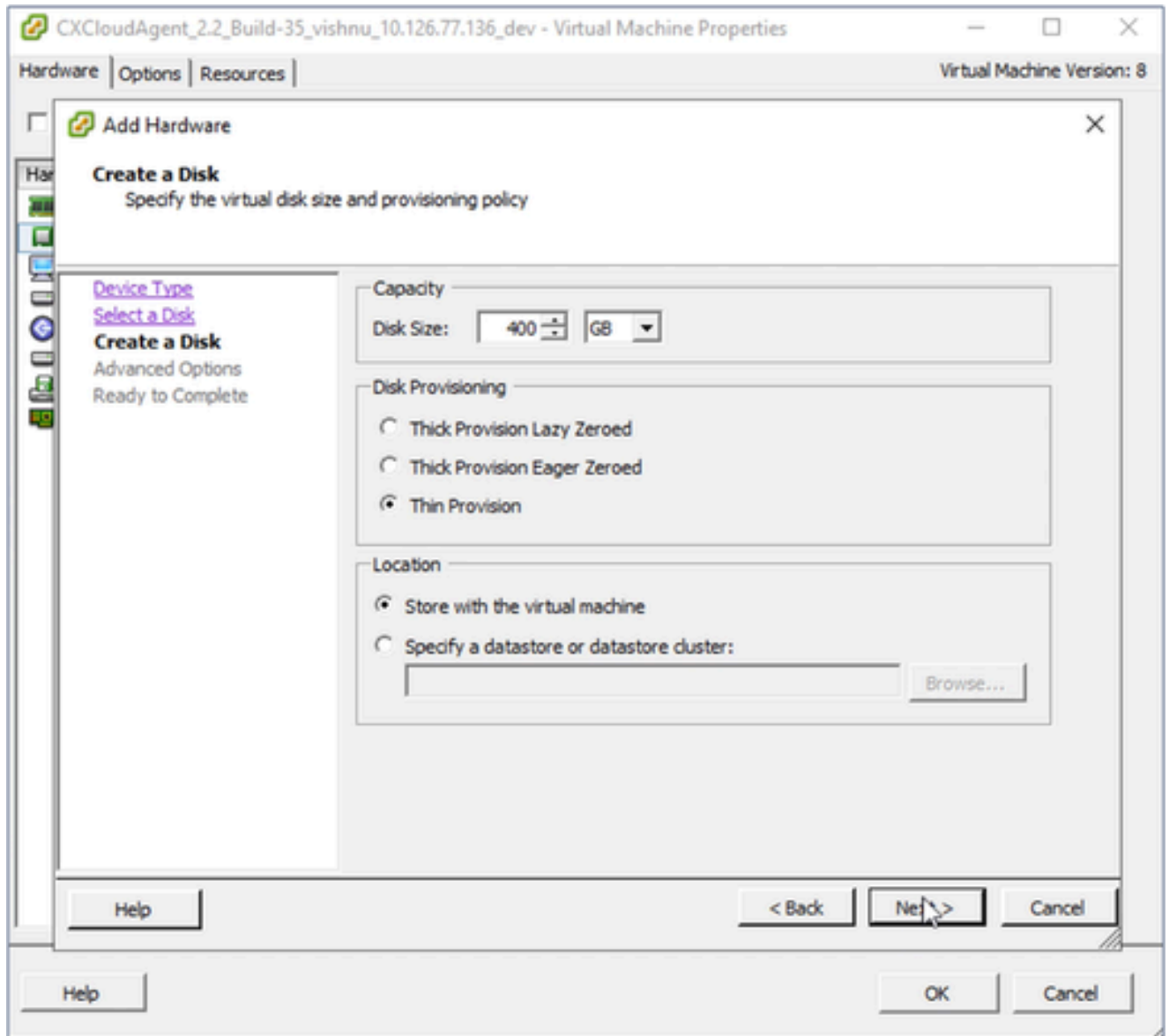
*Device Type*

6. Select **Hard Disk** as the **Device Type**.
7. Click **Next**.



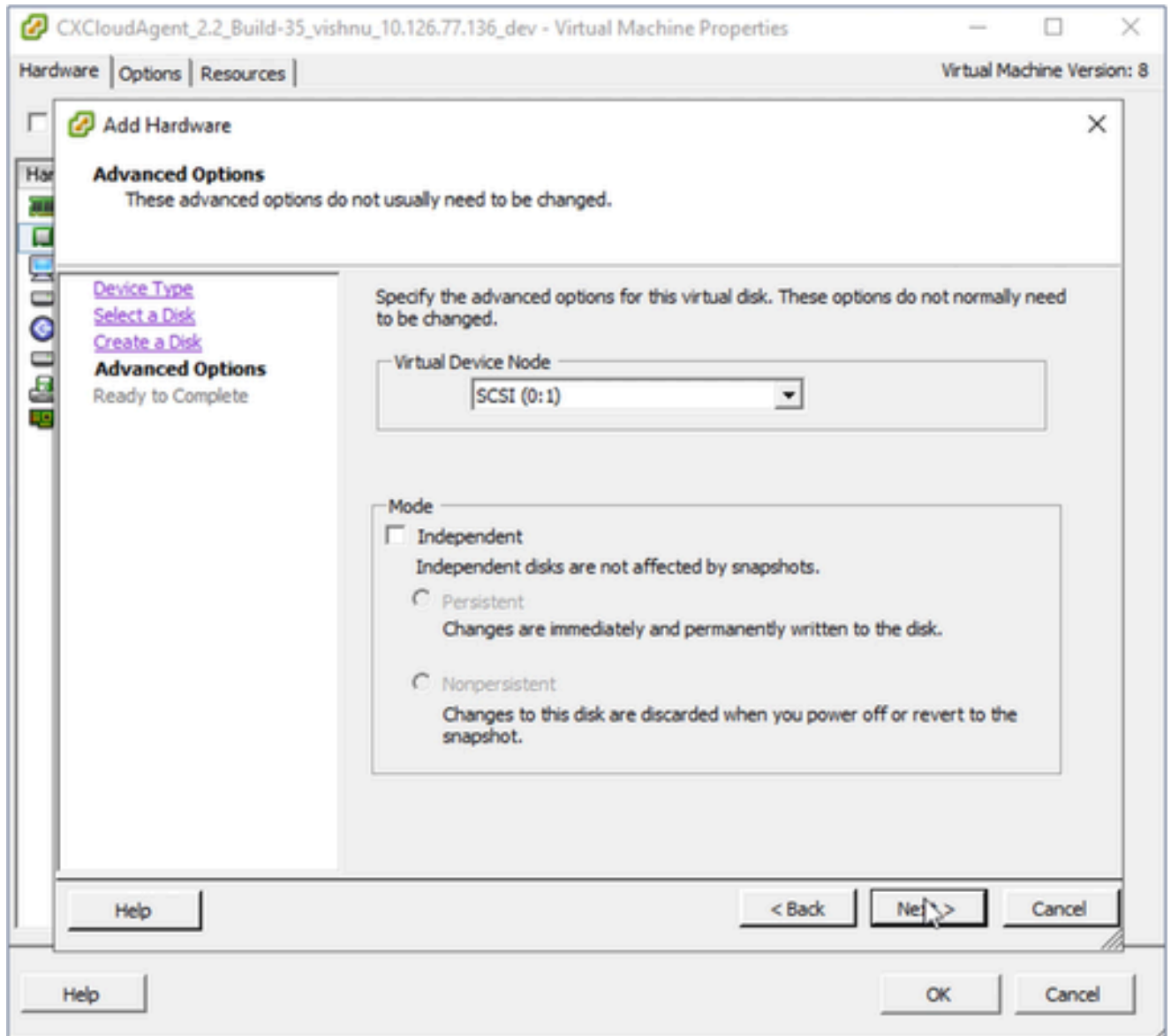
*Select Disk*

8. Select the **Create a new virtual disk** radio button and click **Next**.



*Create Disk*

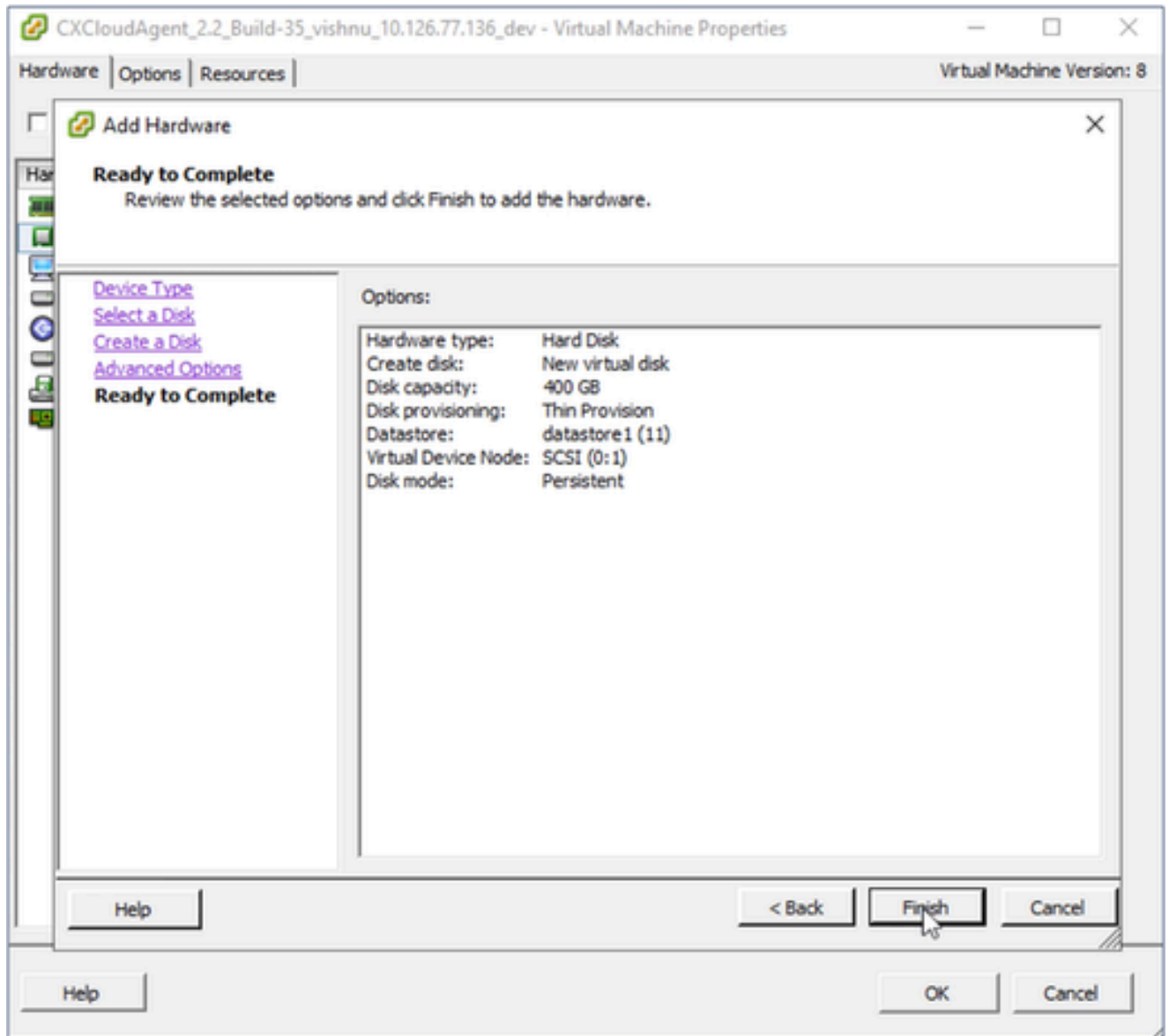
9. Update the **Capacity > Disk Size** as specified:  
Small to Medium: 400 GB, (Initial size 200 GB, increasing total space to 600 GB)  
Small to Large: 1000 GB, (Initial size 200 GB, increasing total space to 1200 GB)
10. Select the **Thin Provision** radio button for **Disk Provisioning**.
11. Click **Next**. The **Advanced Options** window displays.



*Advanced Options*

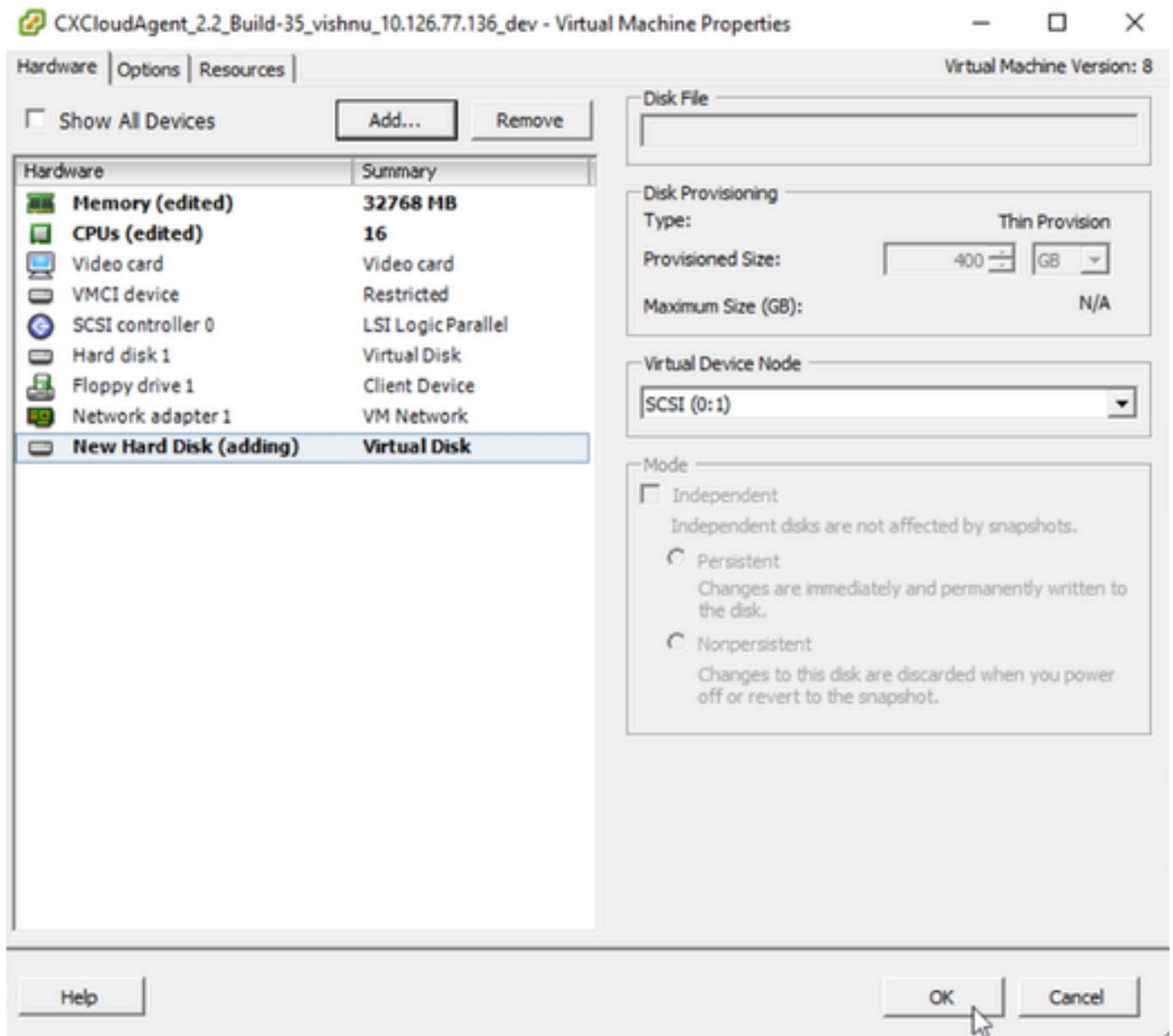
12. Do not make changes. Click **Next** to continue.





*Ready to Complete*

13. Click **Finish**.



Hardware

14. Click **OK** to complete the reconfiguration. The completed reconfiguration displays in the **Recent Tasks** panel.

10.126.77.60 - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home Inventory Inventory

10.126.77.60

- CXCloudAgent\_2.2\_Build-3
- CXCloudAgent\_2.2\_Build-3
- CXCloudAgent\_2.2\_Build-3
- CXCloudAgent\_2.3\_Build-7
- CXCloudAgent\_2.3\_Build-7
- CXCloudAgent\_2.3\_Build-7
- CXCloudAgent\_2.3\_Build-7
- CXCloudAgent\_2.3\_Build-7
- NAT-Router2.4.4\_vishnu\_1
- NAT-Router2.4.4\_vishnu\_1
- windows-test-192.168.77

CXCloudAgent\_2.2\_Build-35\_vishnu\_10.126.77.136\_dev

Getting Started Summary Resource Allocation Performance Events Console Permissions

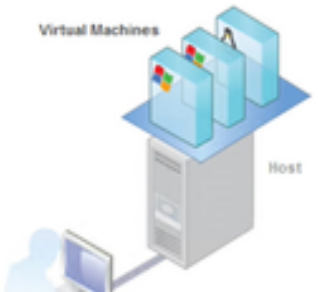
close tab

### What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.



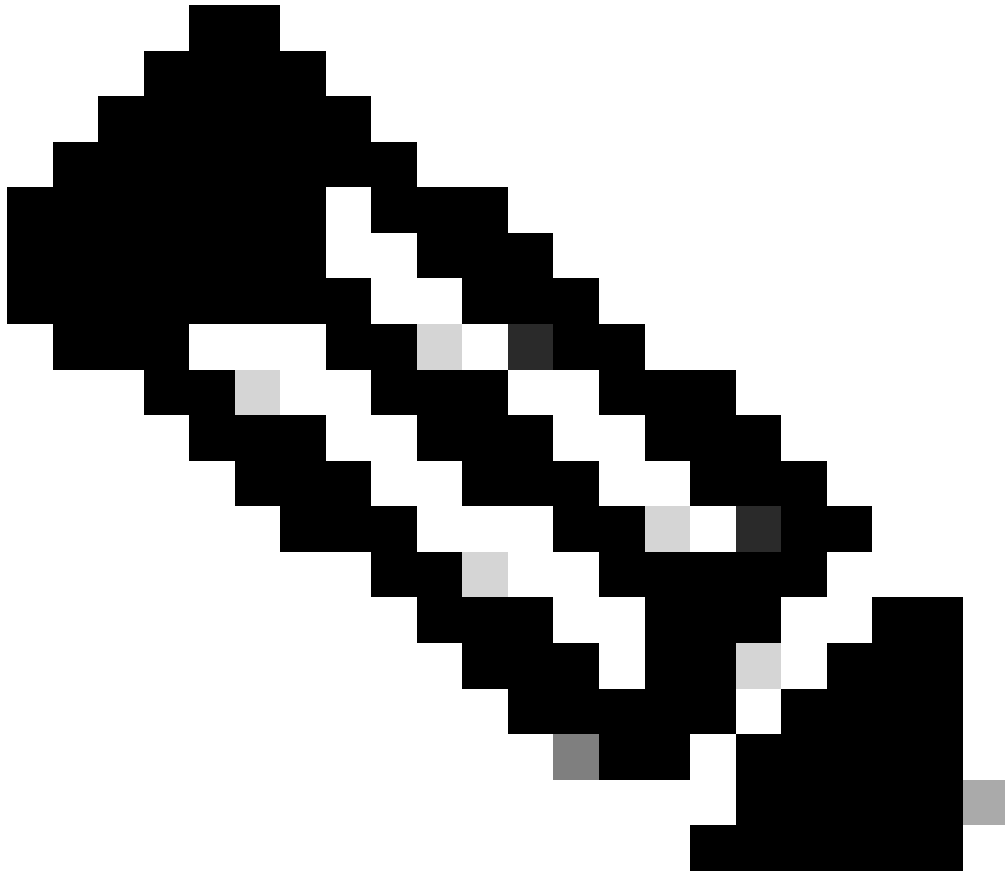
Recent Tasks

Name, Target or Status contains: Clear

Name	Target	Status	Details	Initiated by
Reconfigure virtual machine	CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev	Completed		root
Power On virtual machine	CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev	Completed		root

Tasks root

Recent Tasks



**Note:** Configuration changes take approximately five minutes to complete.

---

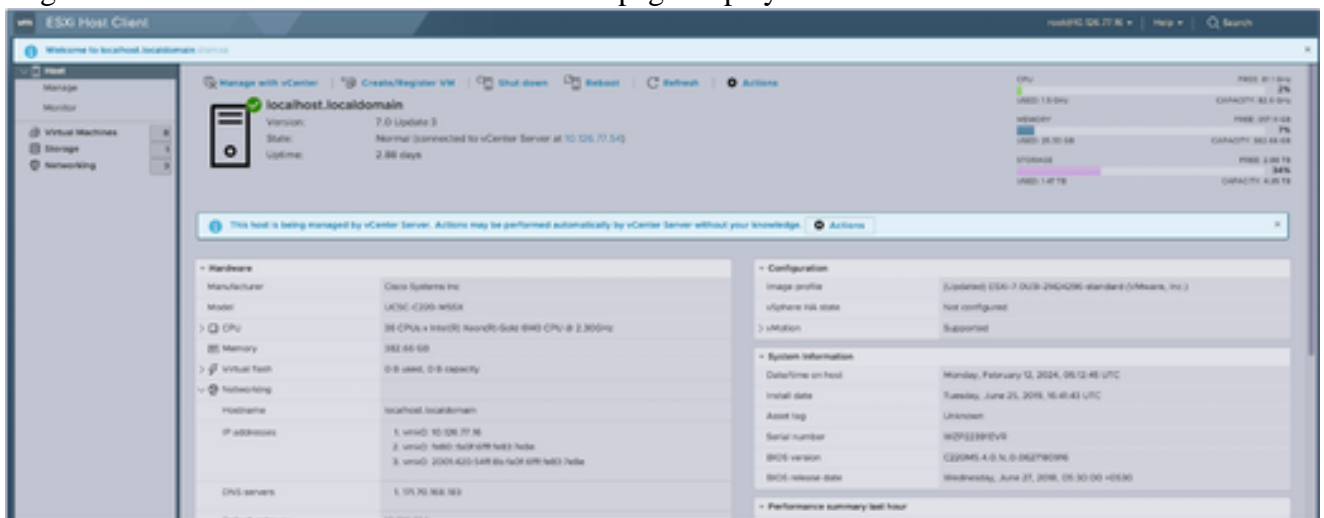
## Reconfiguring Using Web Client ESXi v6.0

To update VM configurations using Web Client ESXi v6.0:



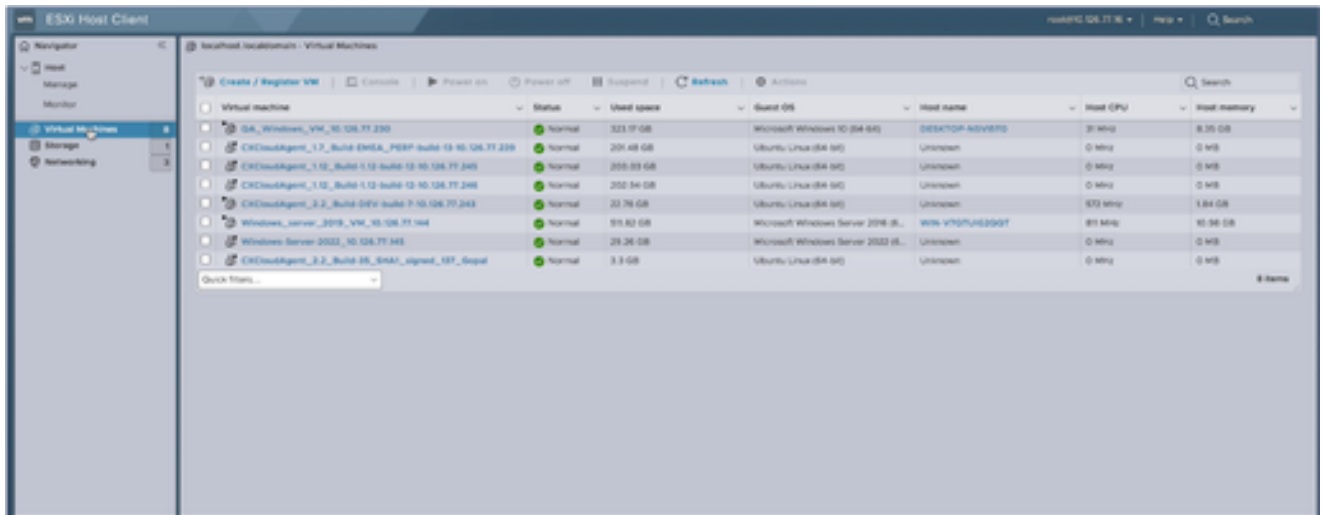
ESXi Client

1. Log in to the VMware ESXi Client. The **Home** page displays.



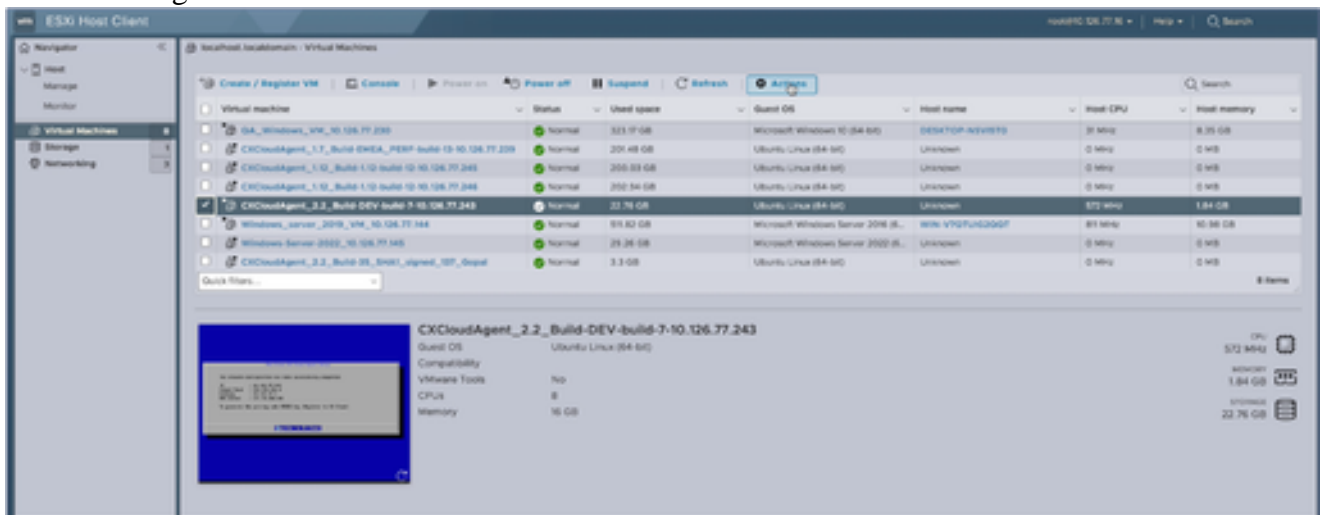
ESXi Home Page

2. Click **Virtual Machine** to display a list of VMs.



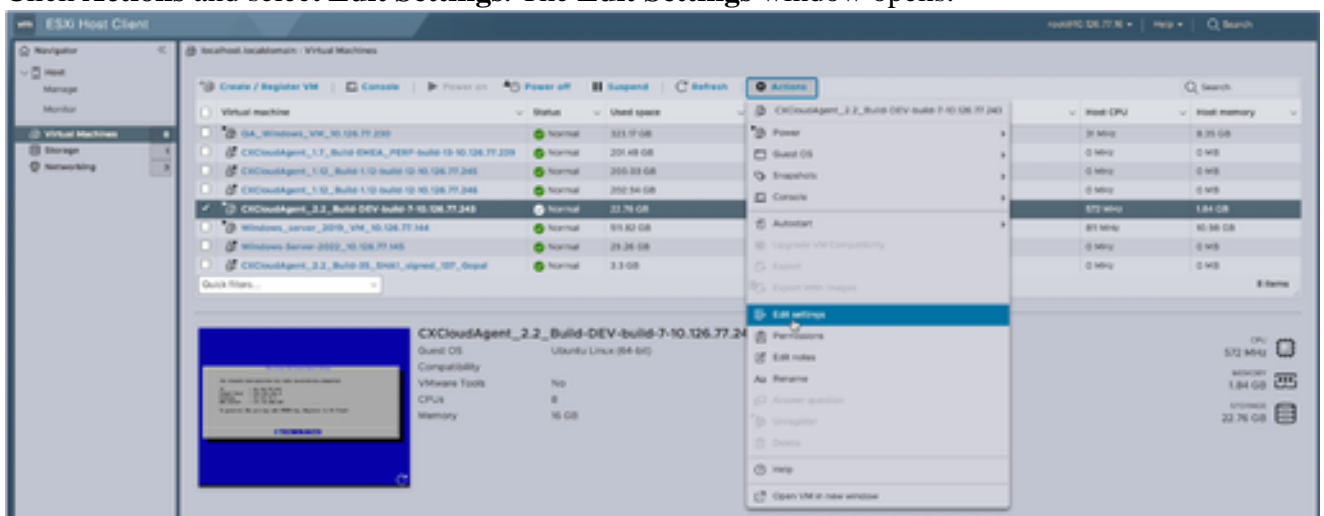
List of VMs

3. Select the target VM.

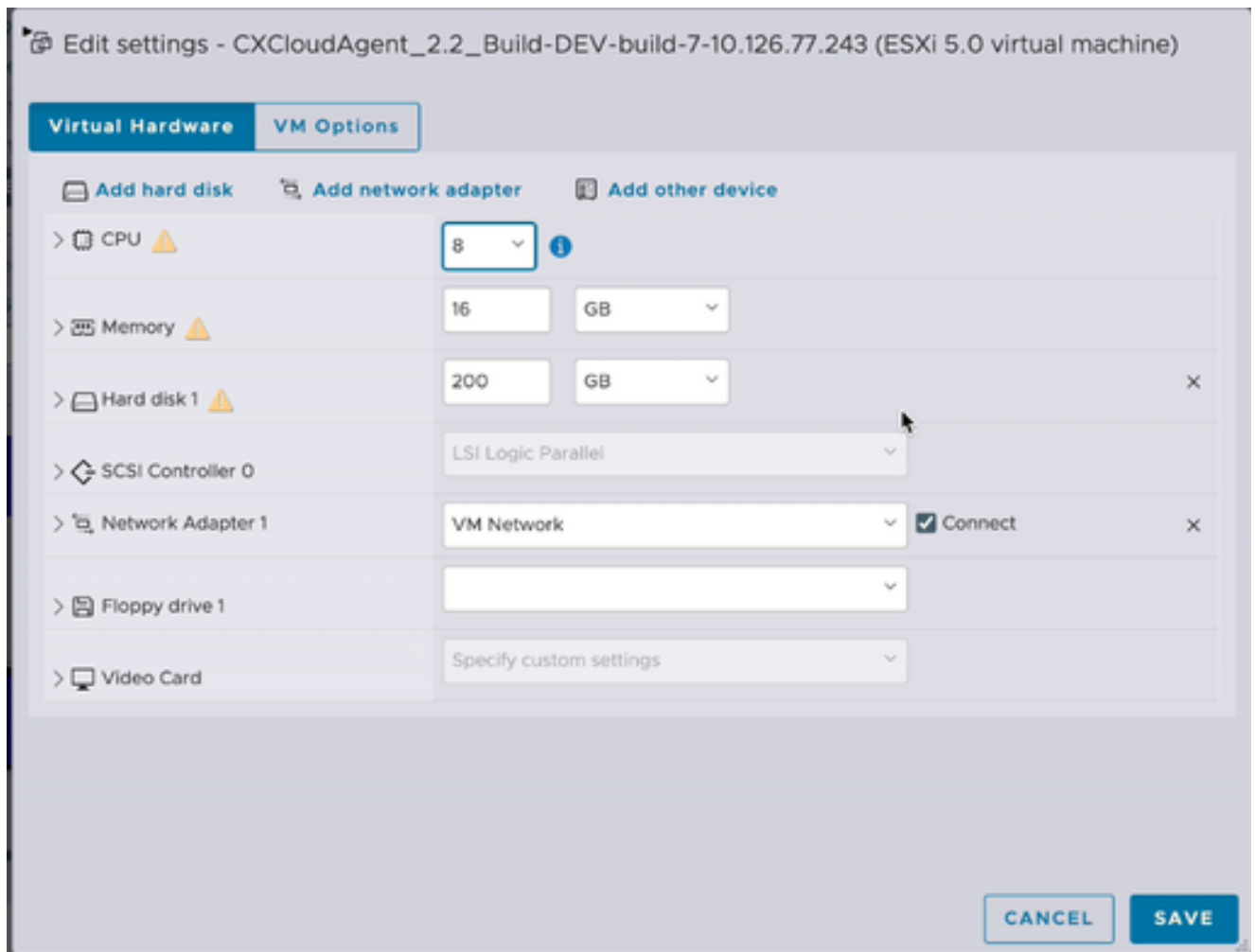


Target VM

4. Click **Actions** and select **Edit Settings**. The **Edit Settings** window opens.

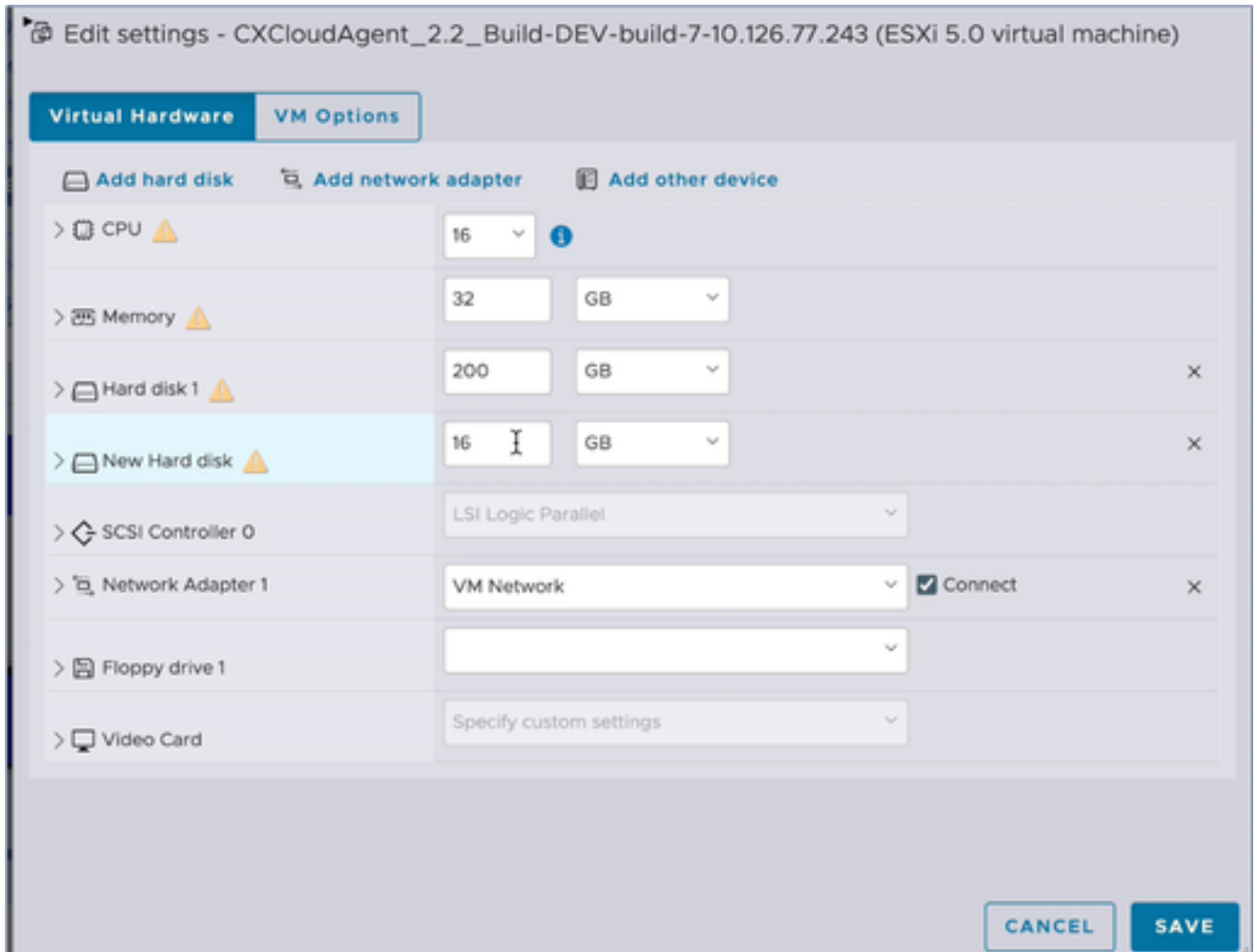


Actions



*Edit Settings*

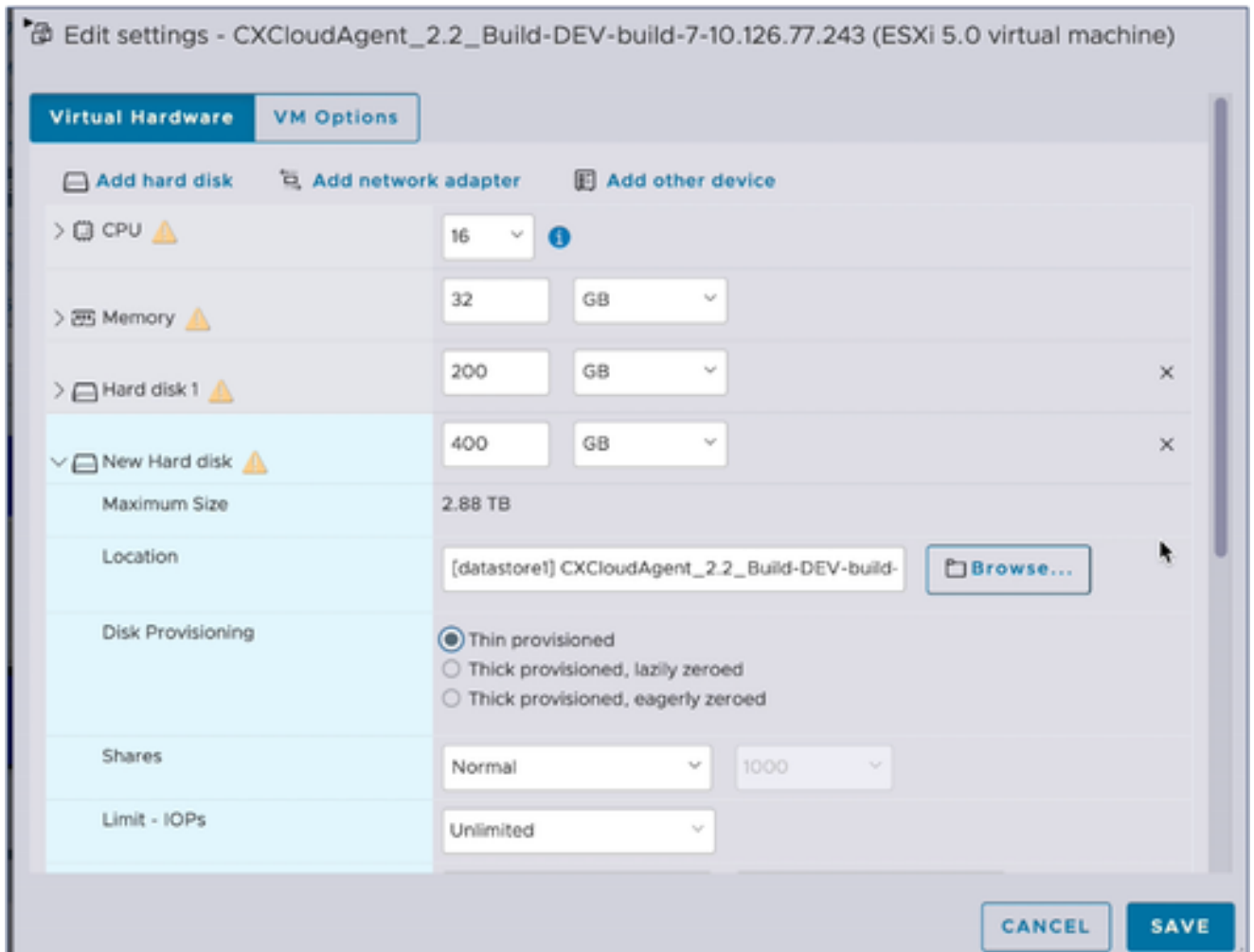
5. Update the **CPU** value as specified:  
Medium: 16 core (8 sockets \*2 core/socket)  
Large: 32 core (16 sockets \*2 core/socket)
6. Update the **Memory** value as specified:  
Medium: 32 GB  
Large: 64 GB
7. Click **Add hard disk** > **New standard hard disk**. The new hard disk entry displays in the **Edit settings** window.



*Edit Settings*

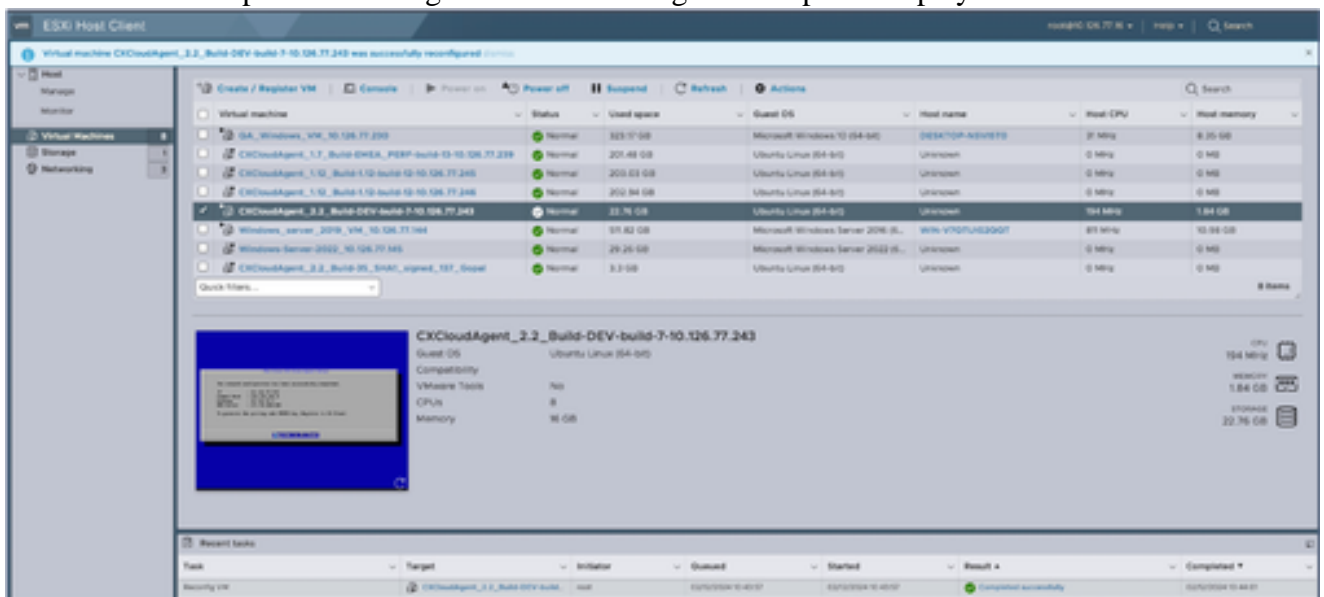
- Update **New Hard disk** values as specified:
  - Small to Medium: 400 GB, (Initial size 200 GB, increasing total space to 600 GB)
  - Small to Large: 1000 GB, (Initial size 200 GB, increasing total space to 1200 GB)
- Click the arrow to expand **New Hard disk**. The properties display.





*Edit Settings*

10. Select the **Thin provisioned** radio button.
11. Click **Save** to complete the configuration. The configuration update displays in the **Recent tasks**.



*Recent Tasks*

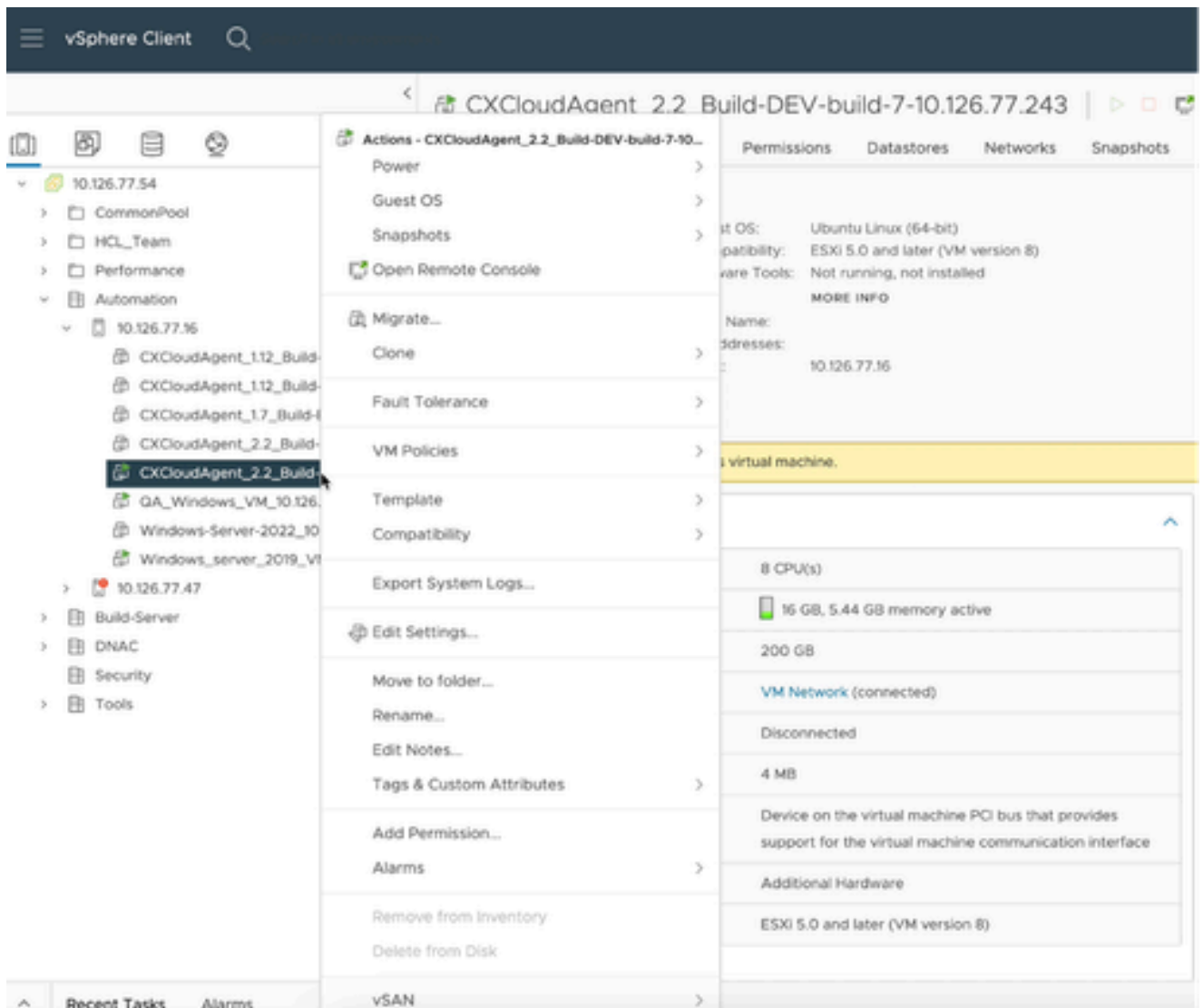
## Reconfiguring Using Web Client vCenter

To update the VM configurations using the Web Client vCenter:





*vCenter*

1. Log in to vCenter. The **Home** page displays.



List of VMs

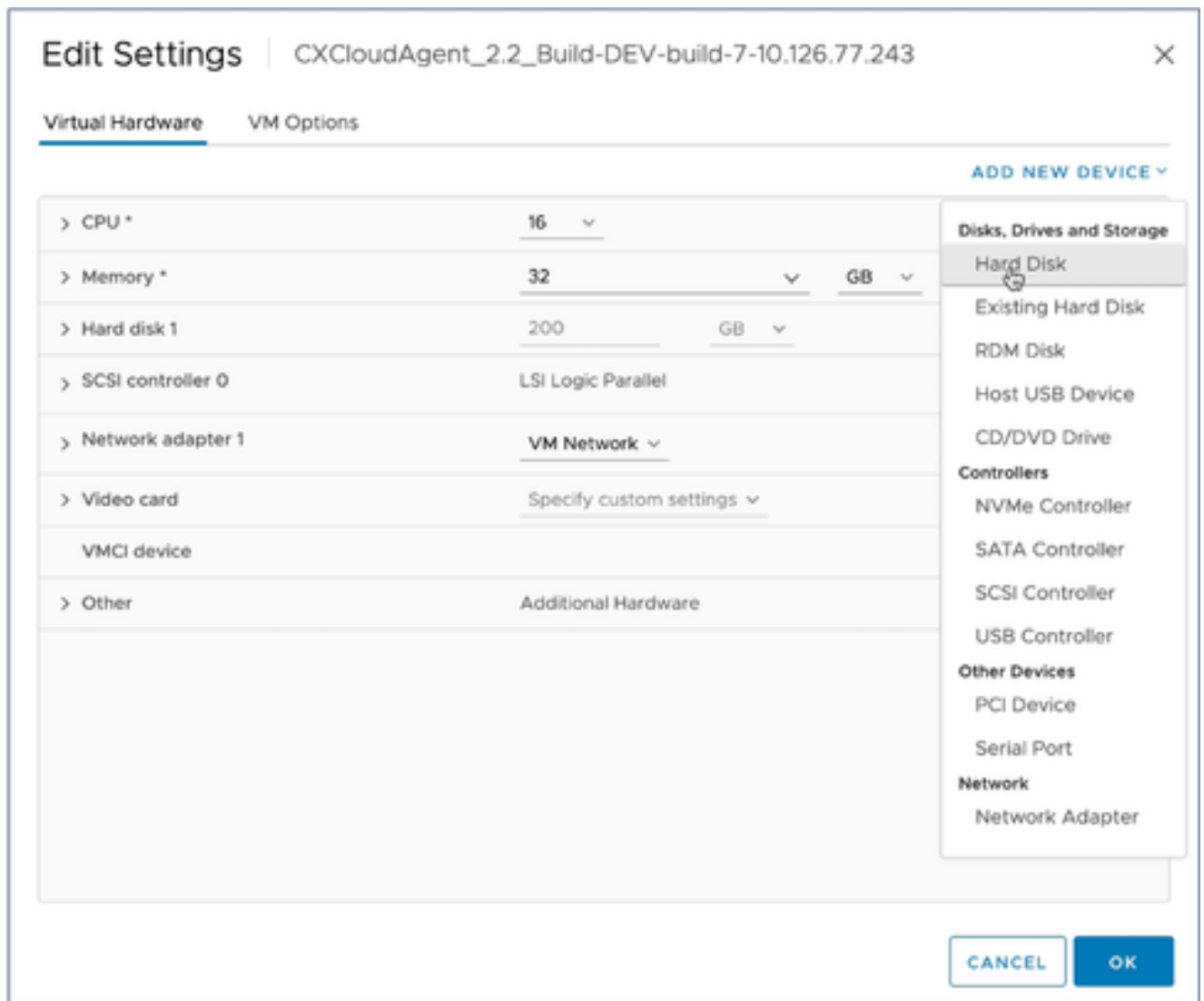
2. Right-click the target VM and select **Edit Settings** from the menu. The **Edit Settings** window opens.

> CPU	8 ▾	
> Memory	16 ▾	GB ▾
> Hard disk 1 	200	GB ▾
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	VM Network ▾	<input checked="" type="checkbox"/> Connected
> Video card	Specify custom settings ▾	
VMCI device		
> Other	Additional Hardware	

CANCEL OK

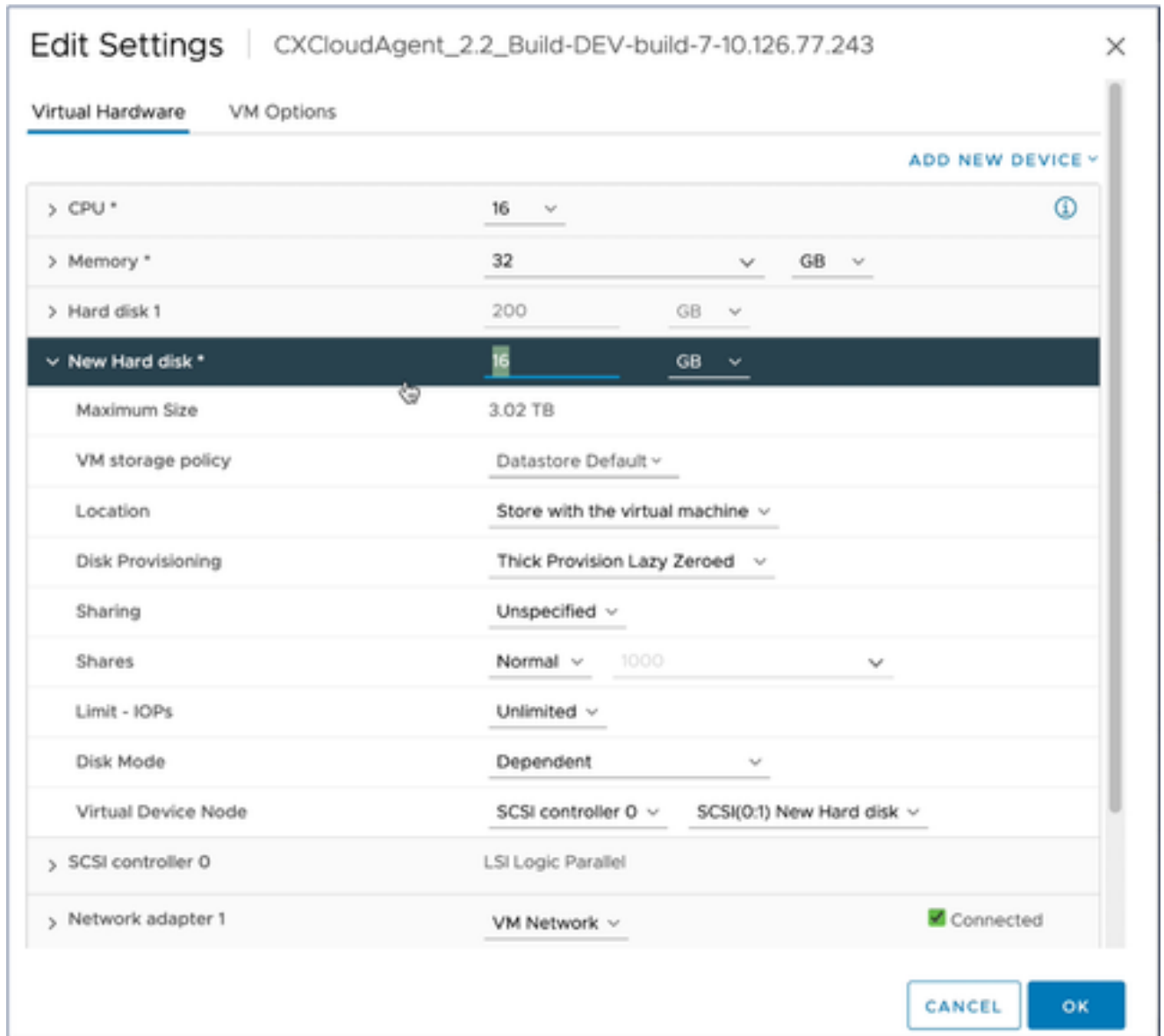
*Edit Settings*

3. Update the **CPU** values as specified:  
 Medium: 16 core (8 sockets \*2 core/socket)  
 Large: 32 core (16 sockets \*2 core/socket)
4. Update the **Memory** values as specified:  
 Medium: 32 GB  
 Large: 64 GB



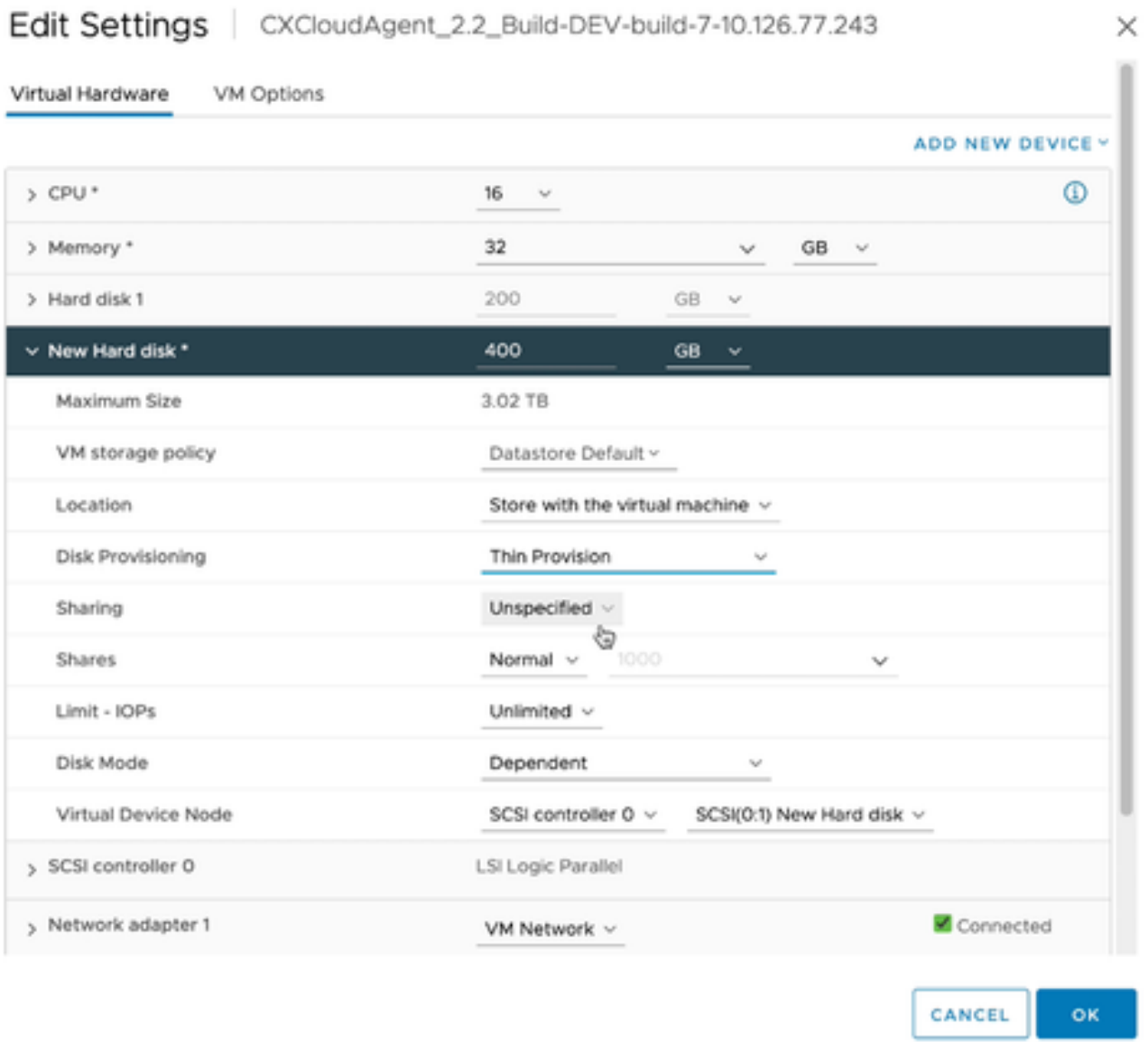
*Edit Settings*

5. Click **Add New Device** and select **Hard Disk**. The **New Hard disk** entry is added.



*Edit Settings*

6. Update **New Hard disk** memory as specified:  
Small to Medium: 400 GB, (Initial size 200 GB, increasing total space to 600 GB)  
Small to Large: 1000 GB, (Initial size 200 GB, increasing total space to 1200 GB)



*Edit Settings*

7. Select **Thin Provision** from the **Disk Provisioning** drop-down list.
8. Click **OK** to complete the upgrade.

## Deployment and Network Configuration

Select any of these options to deploy the CX Cloud Agent:

- [VMware vSphere/vCenter Thick Client ESXi 5.5/6.0](#)
- [VMware vSphere/vCenter Web Client ESXi 6.0](#) or [Web Client vCenter Installation](#)
- [Oracle Virtual Box 7.0.12](#)
- [Microsoft Hyper-V Installation](#)

### OVA Deployment

#### Thick Client ESXi 5.5/6.0 Installation

This client allows deployment of CX Cloud Agent OVA by use of the vSphere thick client.

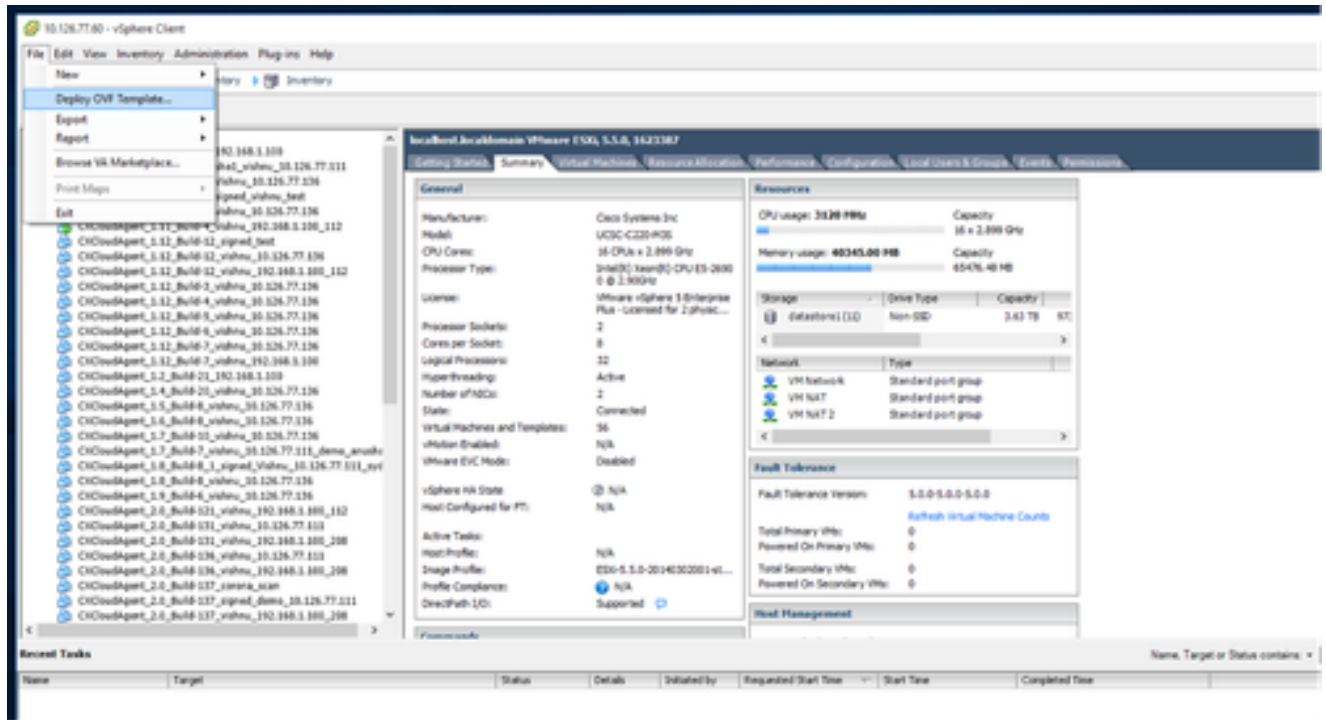
1. After downloading the image, launch the **VMware vSphere Client** and log in.



*Login*

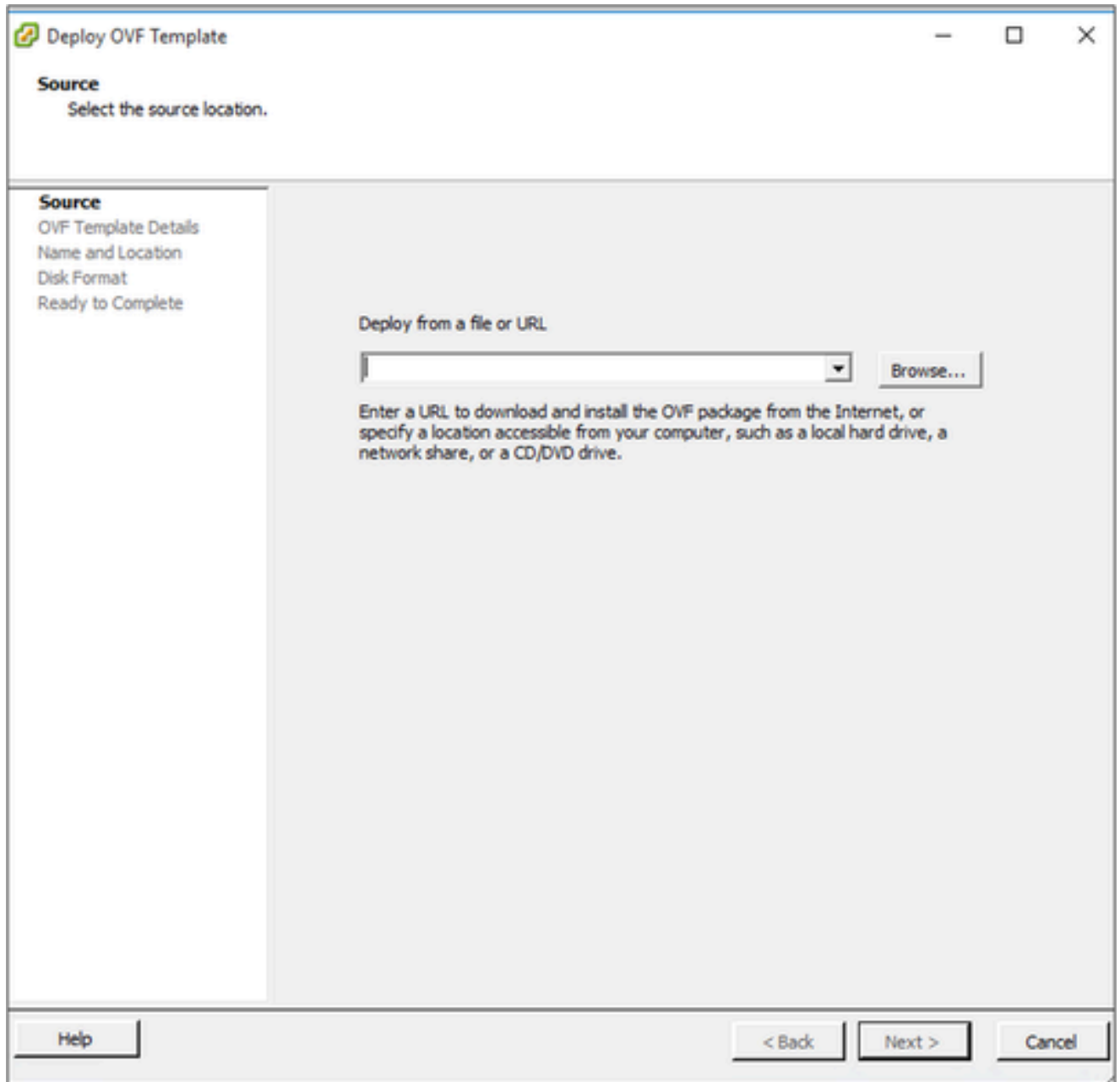
2. From the menu, select **File > Deploy OVF Template**.





vSphere Client

3. Browse to select the **OVA file** and click **Next**.



*OVA Path*

4. Verify the **OVF Details** and click **Next**.

### OVF Template Details

Verify OVF template details.

<b>SOURCE</b> <b>OVF Template Details</b> Name and Location Disk Format Network Mapping Ready to Complete	Product:	CXCloudAgent_2.0_Build-144
	Version:	2.0
	Vendor:	Cisco Systems, Inc
	Publisher:	<input checked="" type="checkbox"/> CISCO SYSTEMS, INC.
	Download size:	1.1 GB
	Size on disk:	3.1 GB (thin provisioned) 200.0 GB (thick provisioned)
	Description:	CXCloudAgent_2.0_Build-144

Help < Back Next > Cancel

Template Details

5. Enter a **Unique Name** and click **Next**.

**Name and Location**

Specify a name and location for the deployed template

[Source](#)  
[OVF Template Details](#)  
**Name and Location**  
Disk Format  
Network Mapping  
Ready to Complete

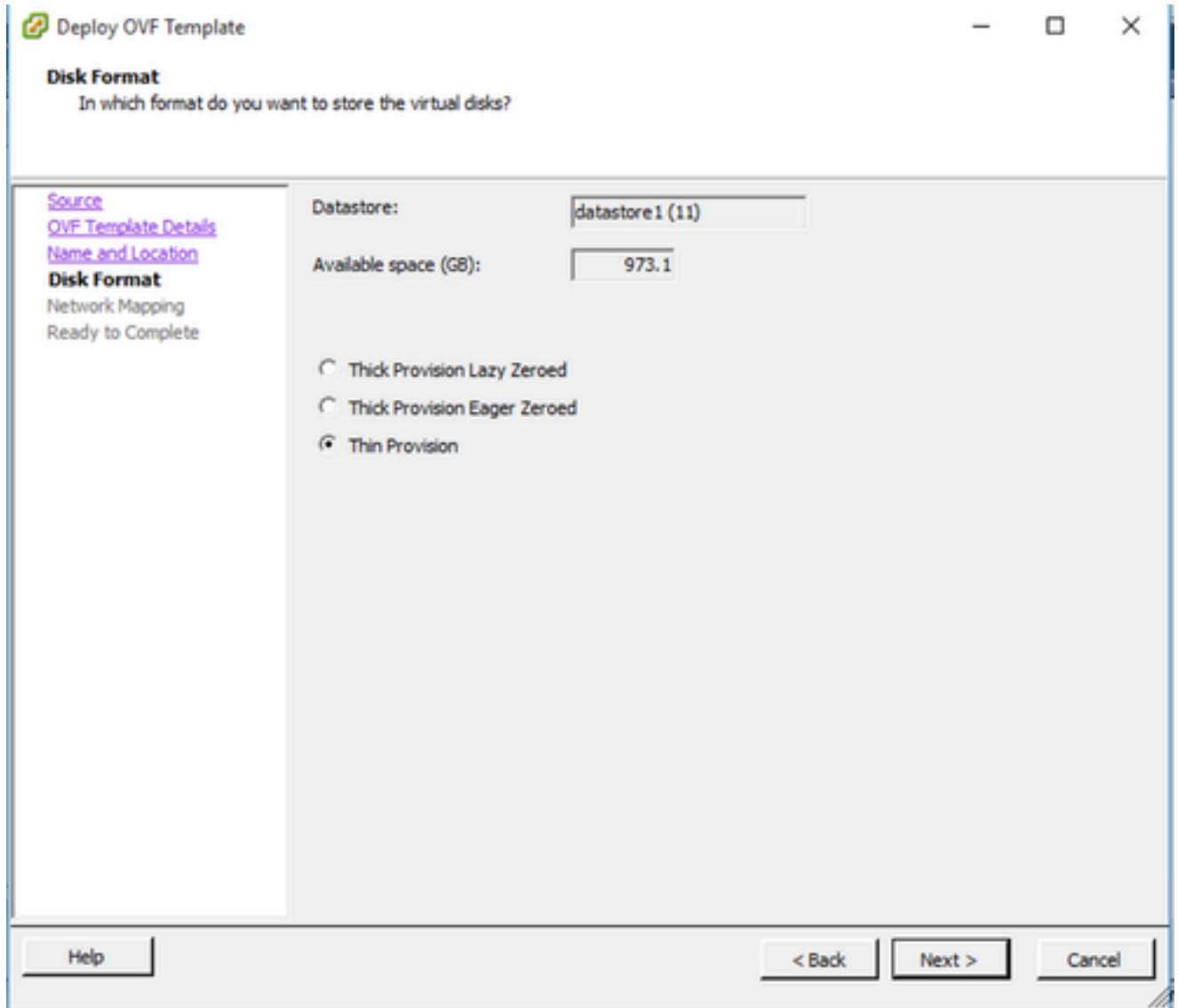
Name:

The name can contain up to 80 characters and it must be unique within the inventory folder.

Help < Back Next > Cancel

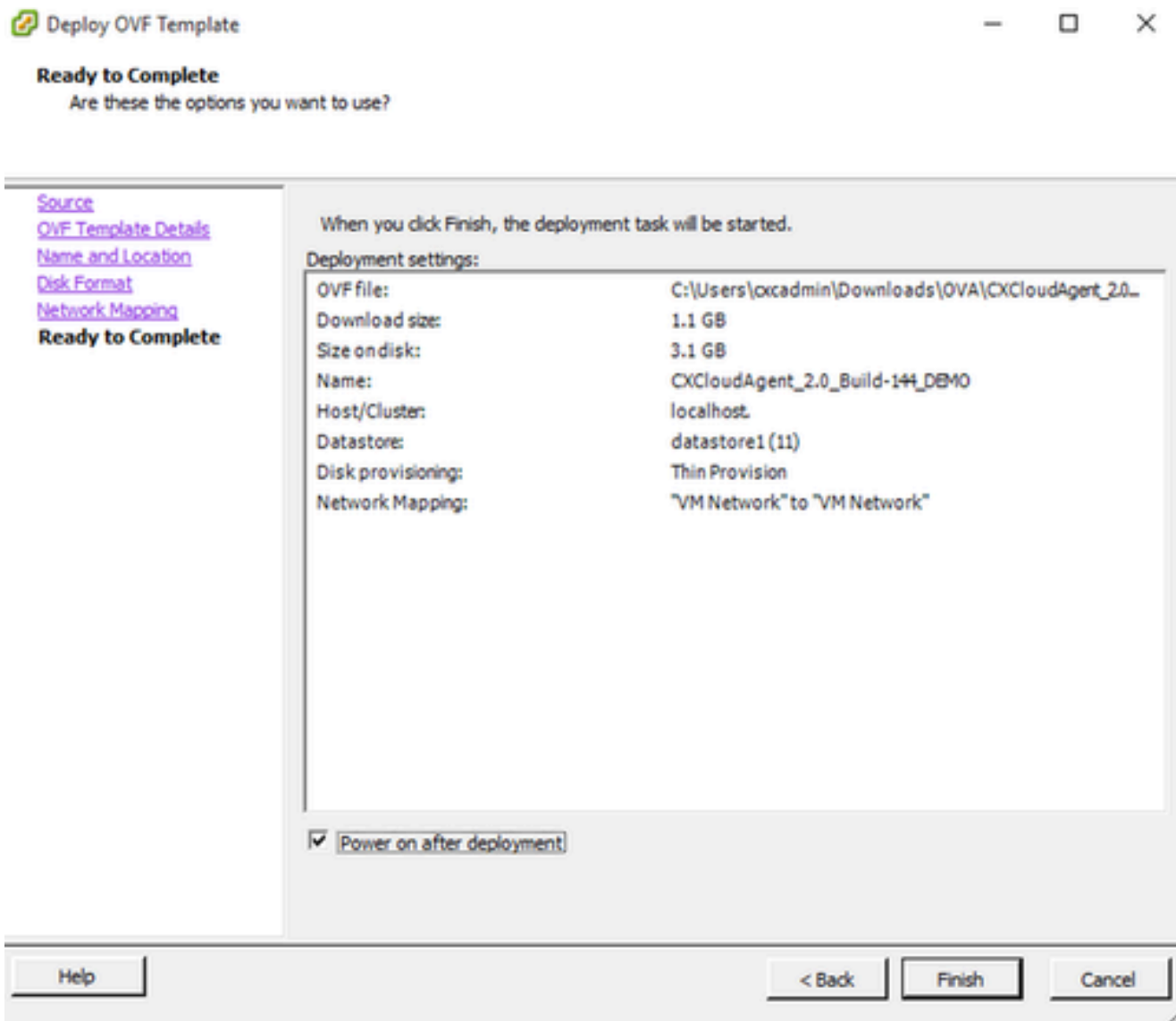
*Name and Location*

6. Select a **Disk Format** and click **Next** (Thin Provision is recommended).



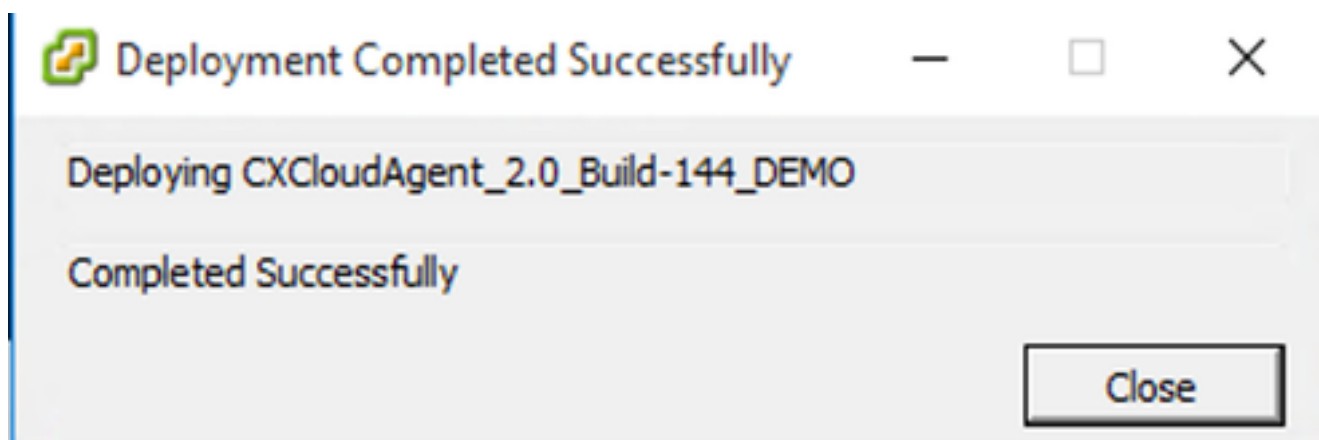
*Disk Format*

7. Select the **Power on after deployment** check box and click **Close**.



Ready to Complete

Deployment can take several minutes. Confirmation displays upon successful deployment.



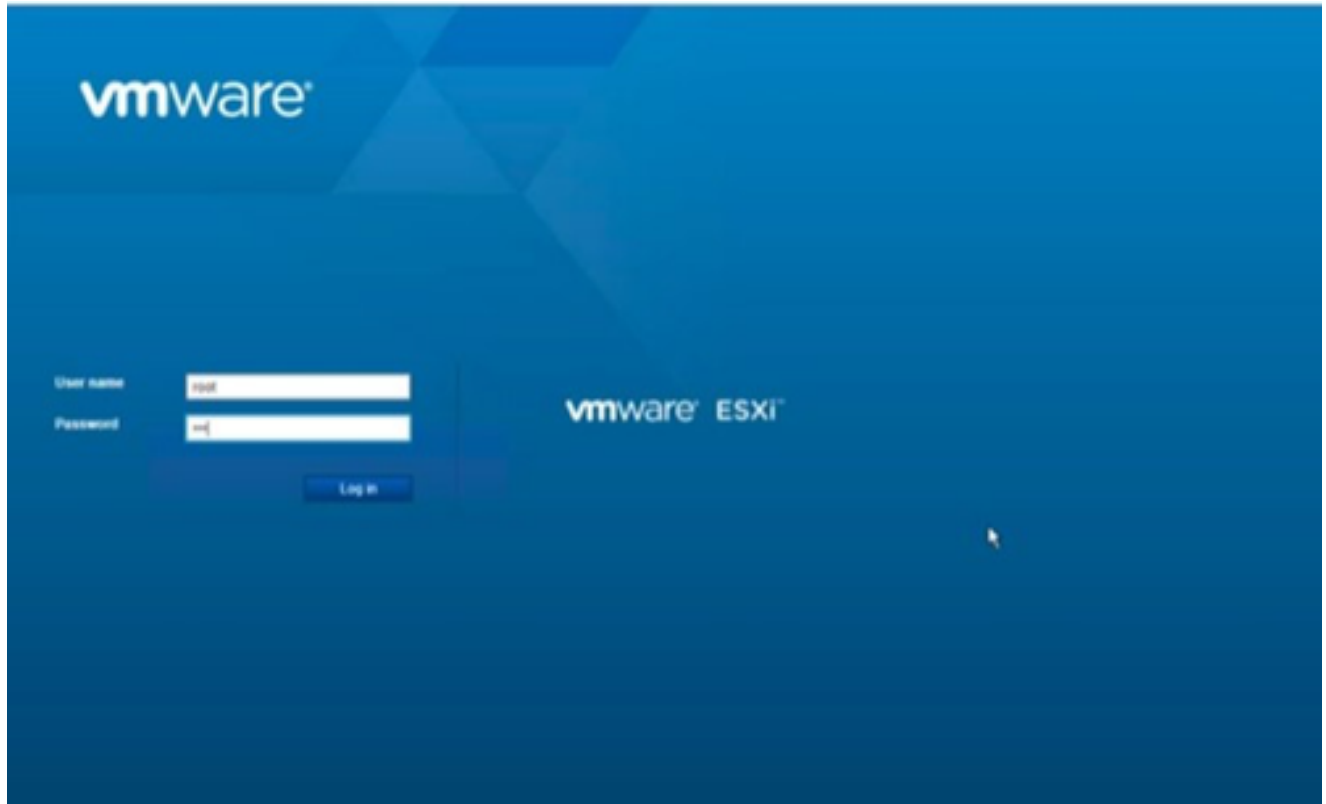
Deployment Complete

8. Select the deployed VM, open the console, and go to [Network Configuration](#) to proceed with the next steps.

## Web Client ESXi 6.0 Installation

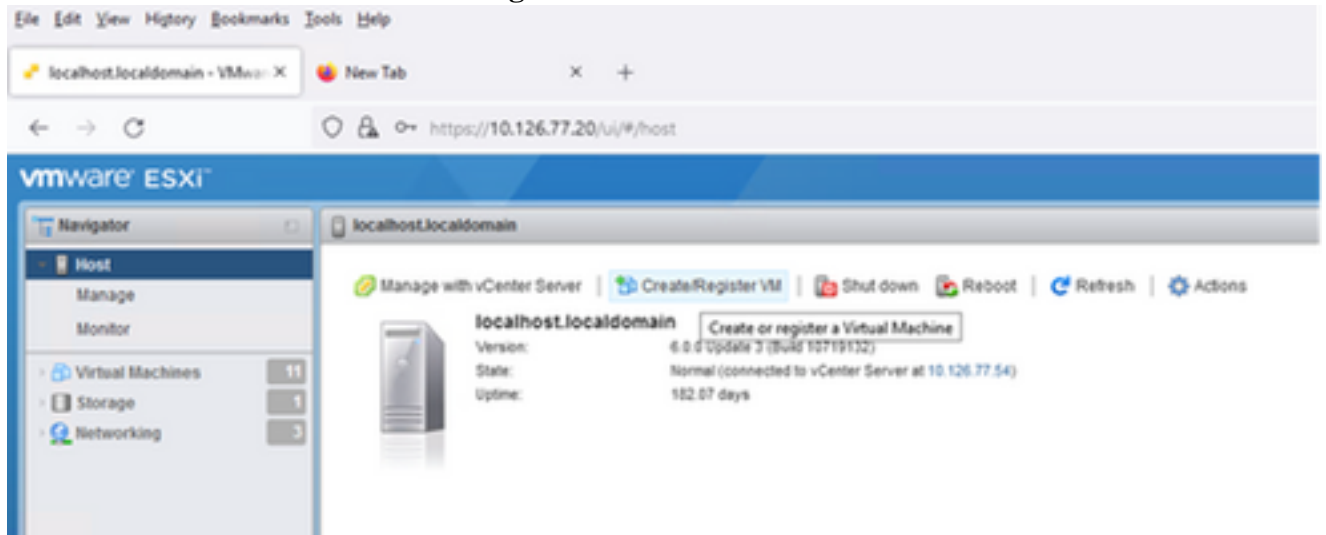
This client deploys CX Cloud Agent OVA by use of the vSphere web.

1. Log in to the VMWare UI with the ESXi/hypervisor credentials used for deploying VM.



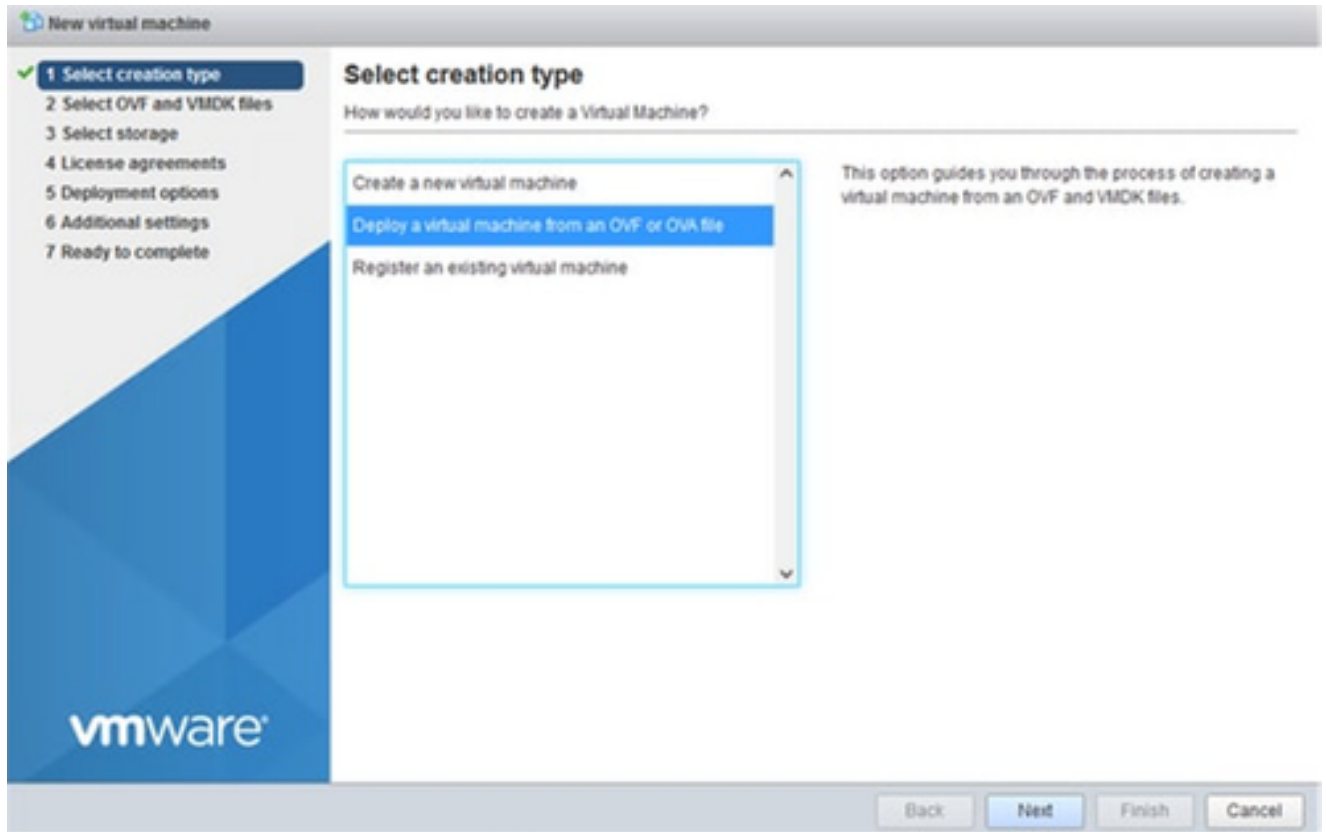
*VMWare ESXi Login*

2. Select **Virtual Machine > Create / Register VM.**



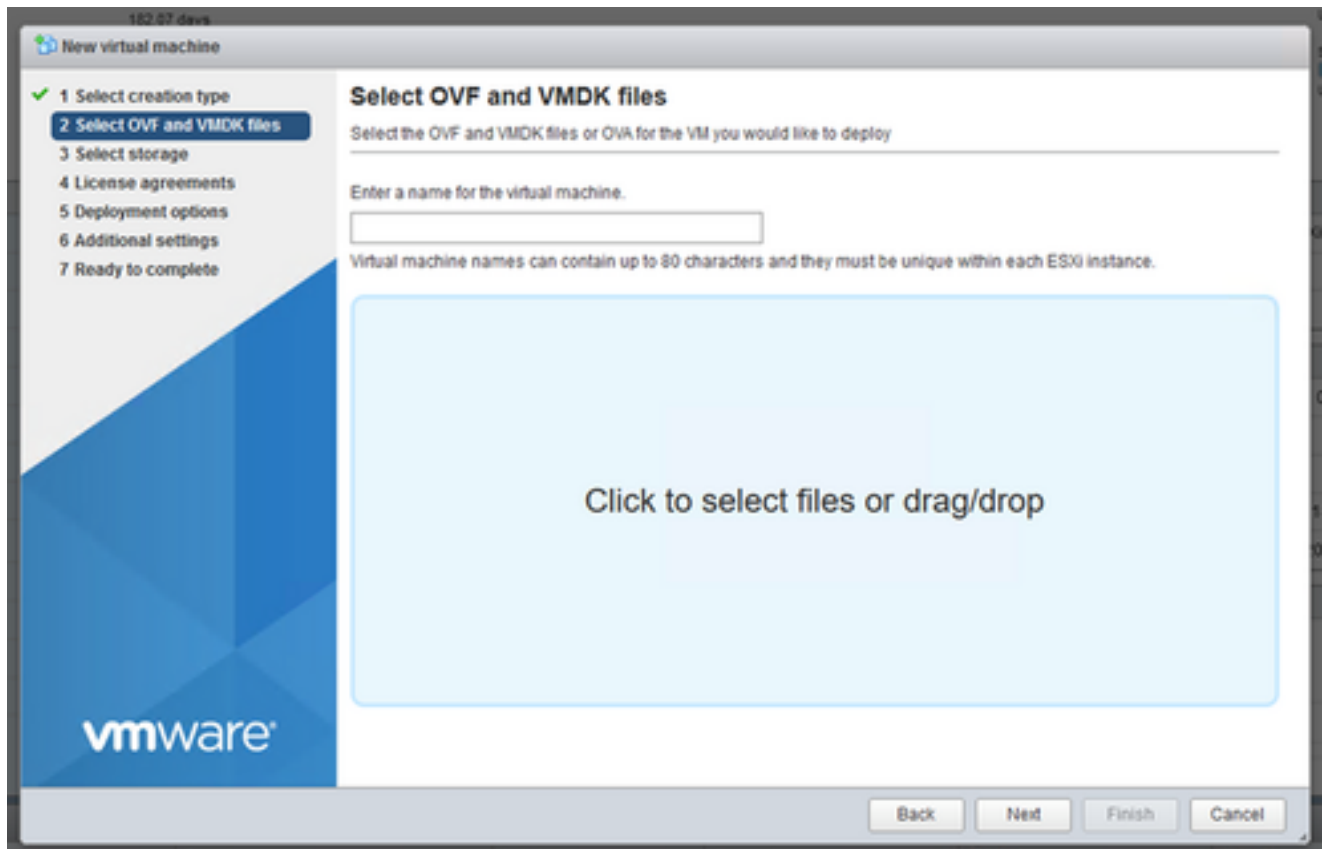
*Create VM*

3. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



*Select Creation Type*

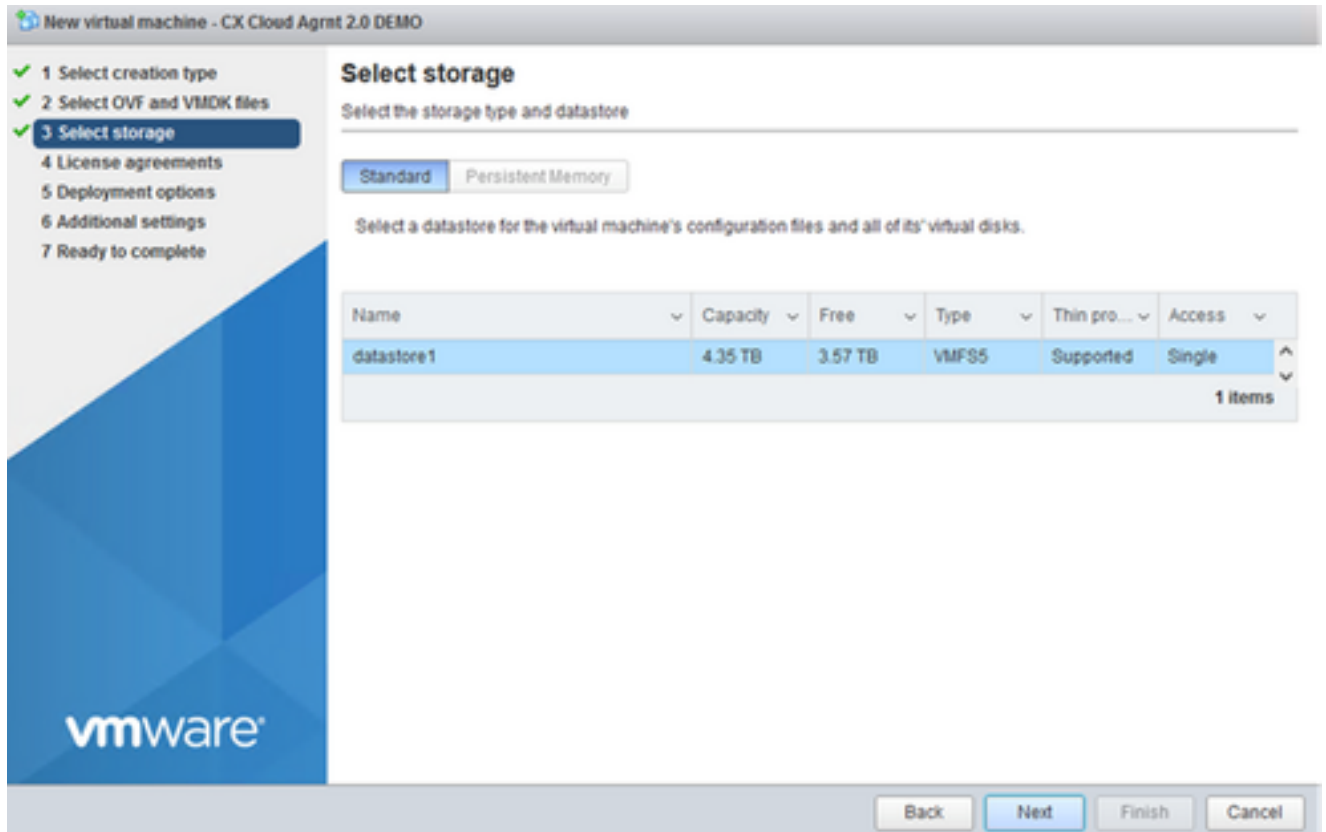
4. Enter the name of the VM, browse to select the file, or drag-and-drop the downloaded OVA file.
5. Click **Next**.



*OVA Selection*

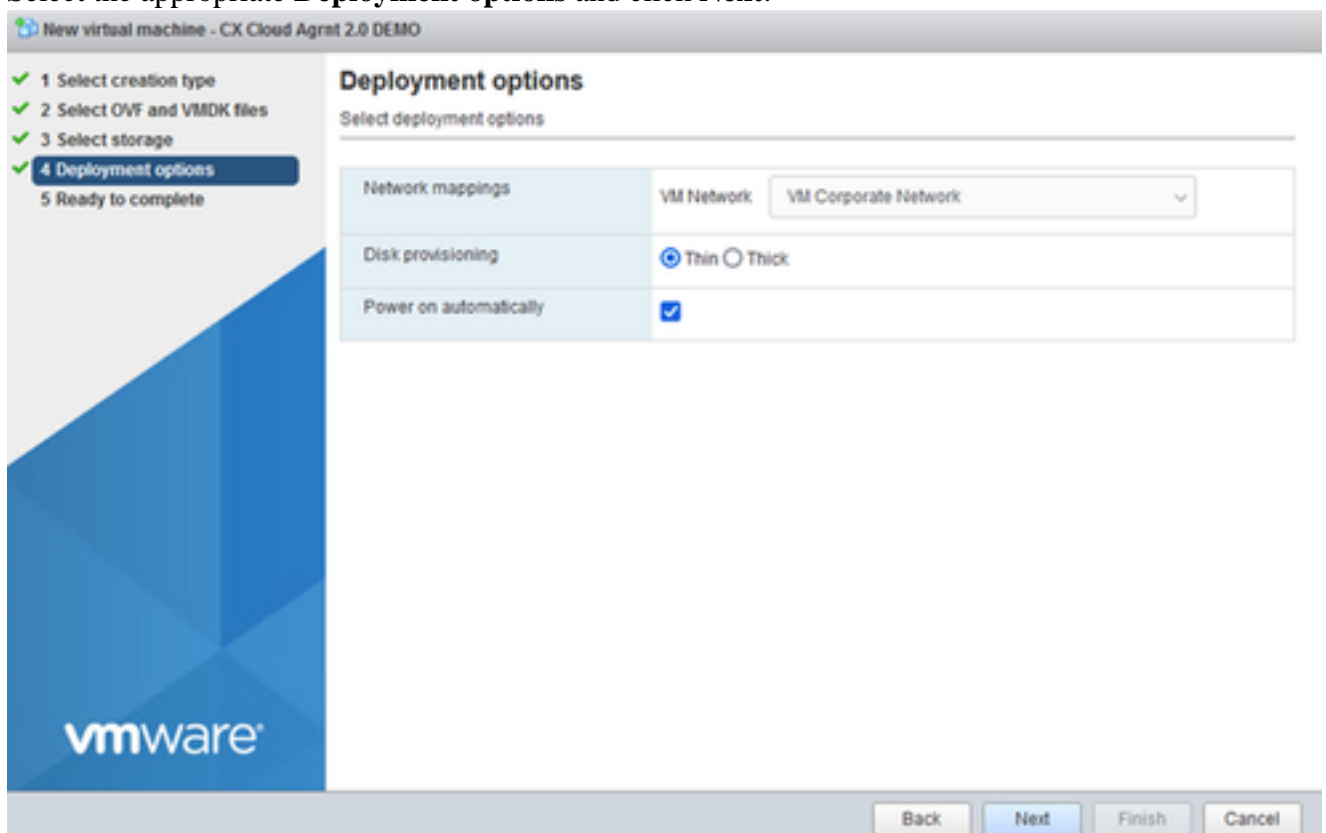
6. Select **Standard** storage and click **Next**.





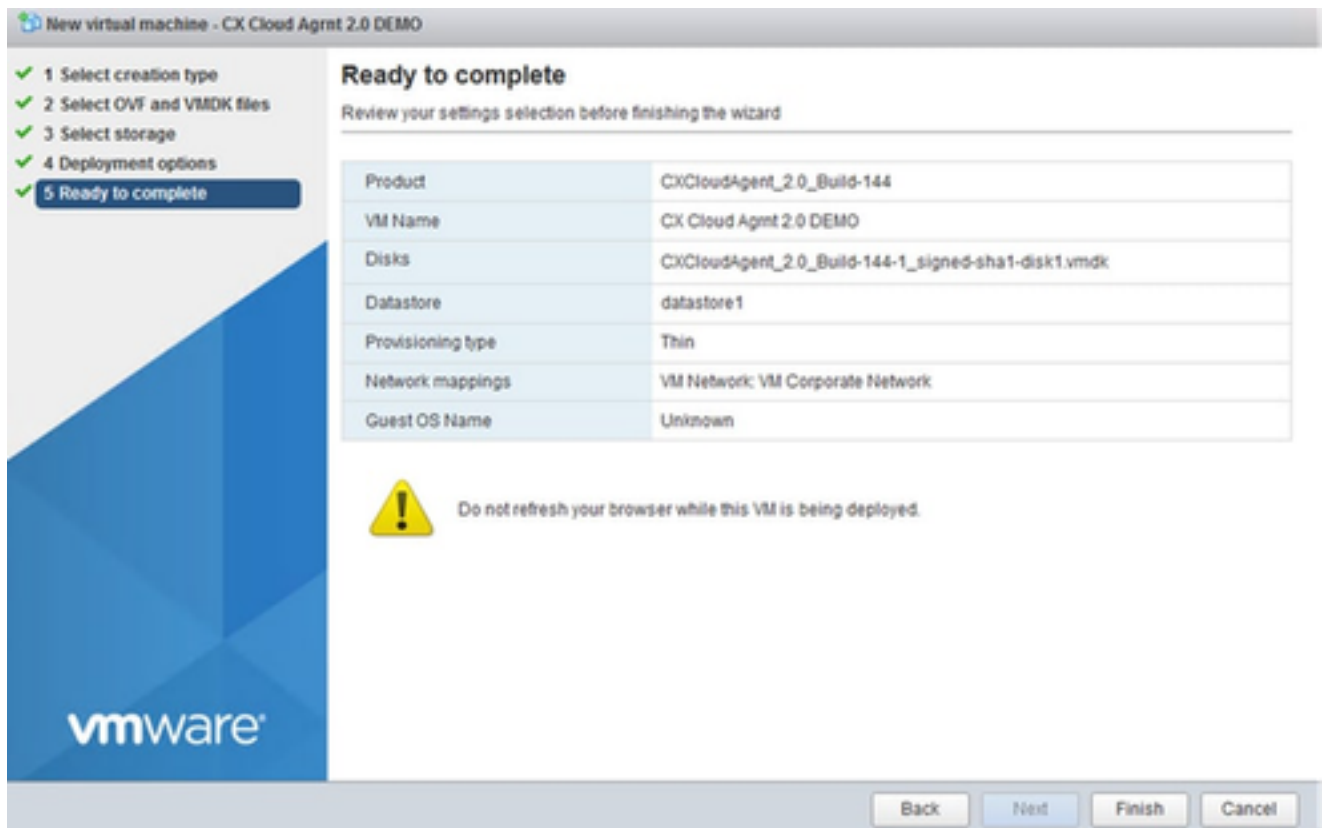
Select Storage

7. Select the appropriate **Deployment options** and click **Next**.

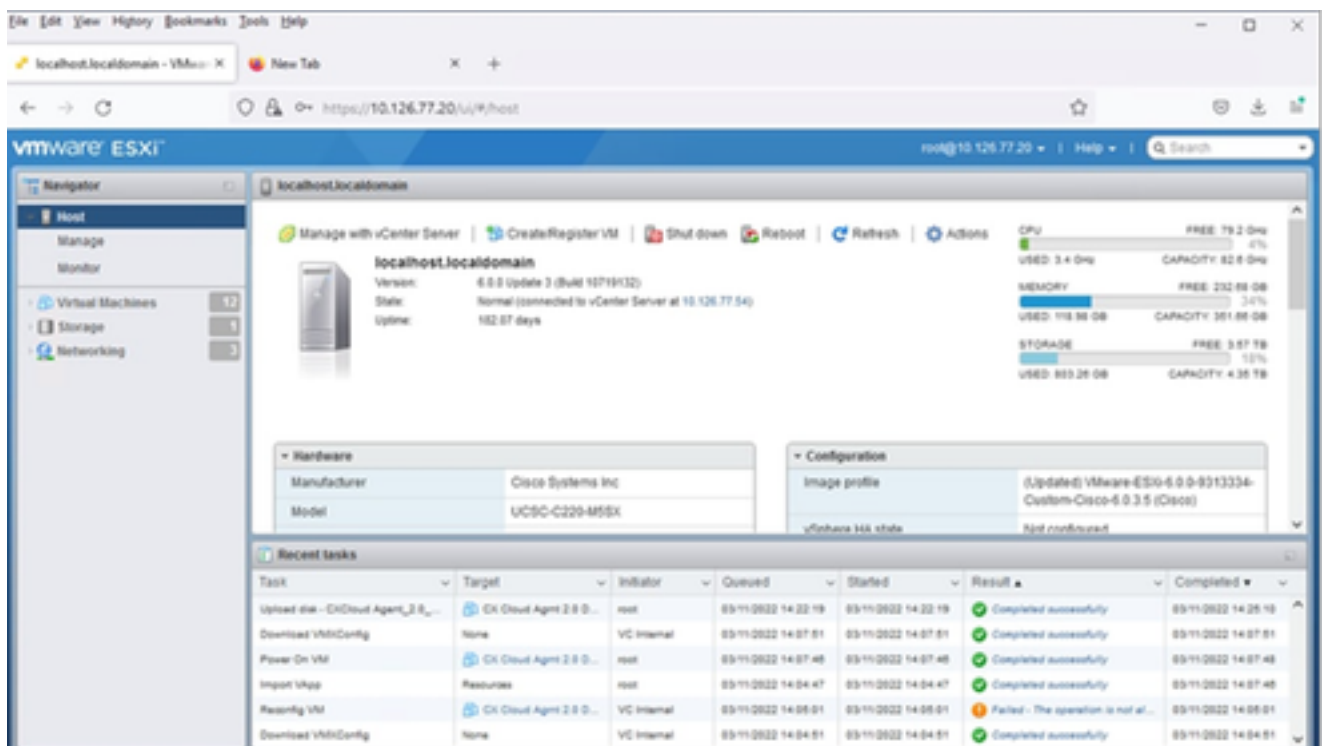


Deployment Options

8. Review the settings and click **Finish**.

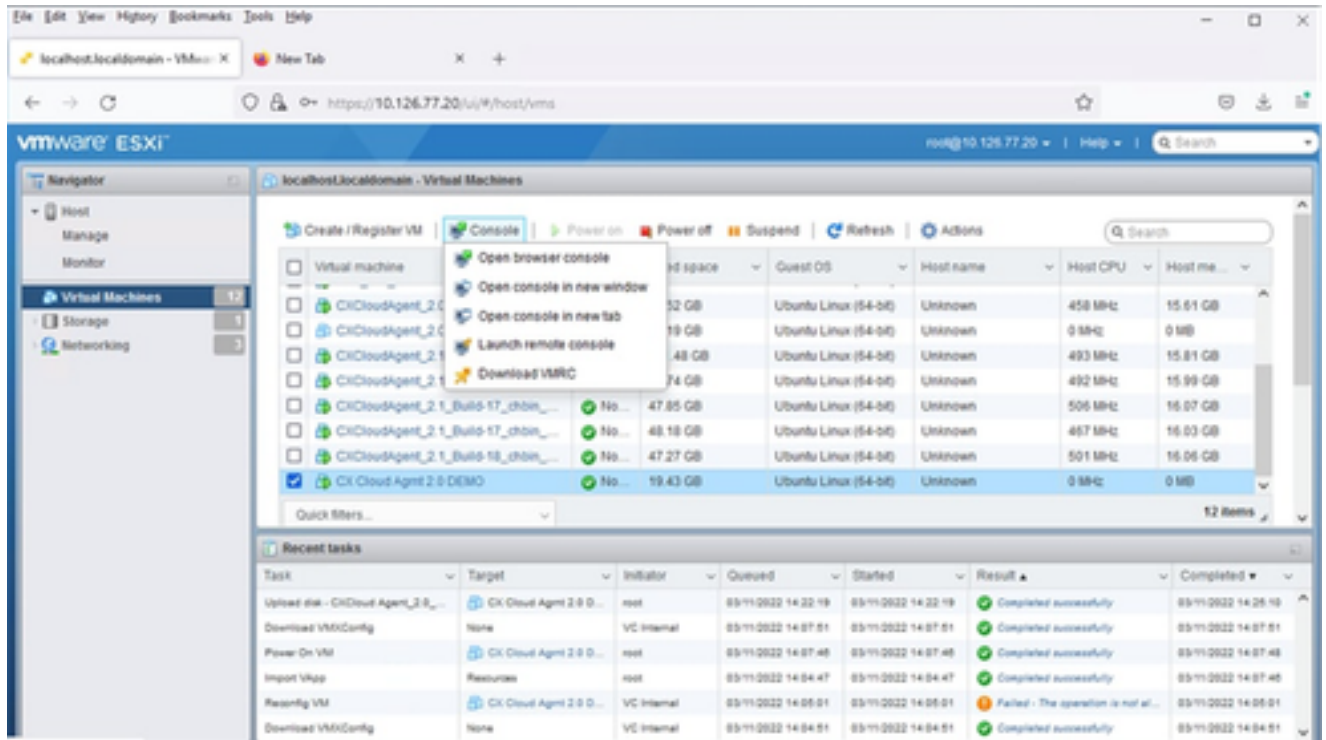


Ready to Complete



Successful Completion

9. Select the VM just deployed and select **Console > Open browser console**.



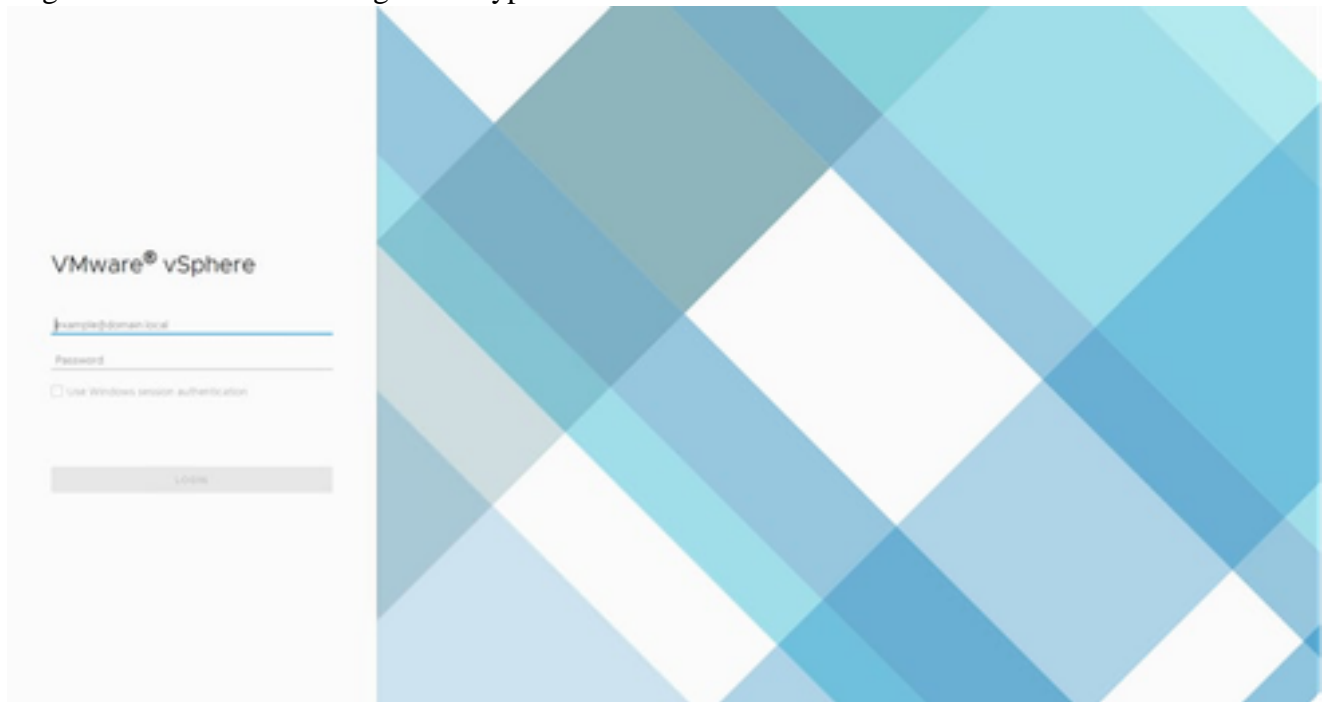
Console

10. Navigate to [Network Configuration](#) to proceed with the next steps.

## Web Client vCenter Installation

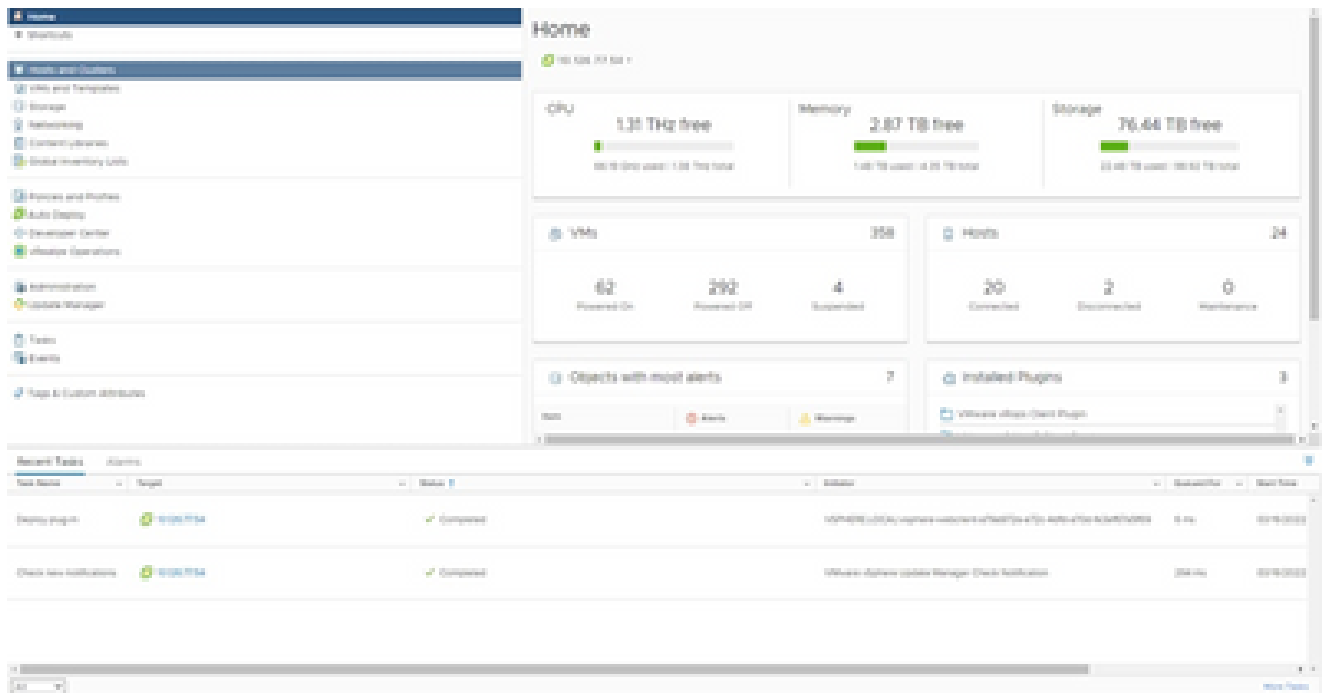
Perform these steps:

1. Log into vCenter Client using ESXi/hypervisor credentials.



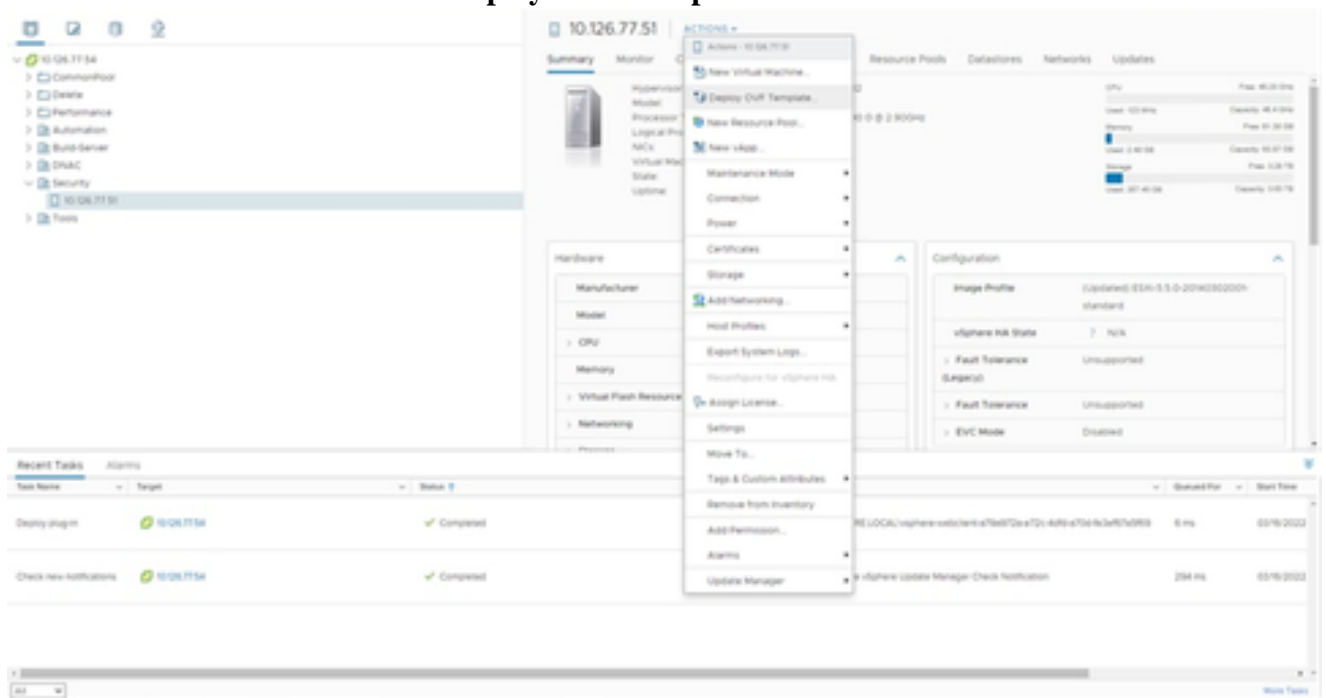
Log In

2. From the **Home** page, click **Hosts and Clusters**.



Home Page

3. Select the VM and click **Action > Deploy OVF Template**.



Actions

## 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 Ready to complete

### Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

No file chosen

 Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

*Select Template*

4. Add the URL directly or browse to select the OVA file and click **Next**.
5. Enter a unique name and browse to the location if required.
6. Click **Next**.

# 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

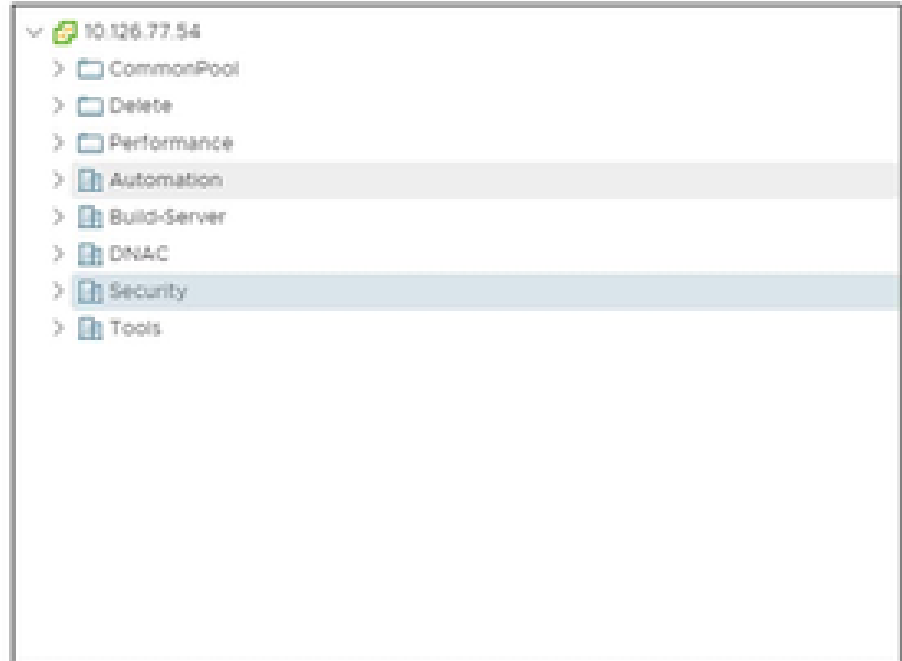
6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: CXCloudAgent\_2.0\_Build-144-demo

Select a location for the virtual machine.



CANCEL

BACK

NEXT

*Name and Folder*


7. Select a compute resource and click **Next**.


## 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 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

▼  Security

>  10.126.77.51

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

*Select Computer Resource*

8. Review the details and click **Next**.

## 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 Ready to complete

### Review details

Verify the template details.

Publisher	DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate)
Product	CxCloudAgent_3.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CxCloudAgent_3.0_Build-144
Download size	1.1 GB
Size on disk	3.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

CANCEL

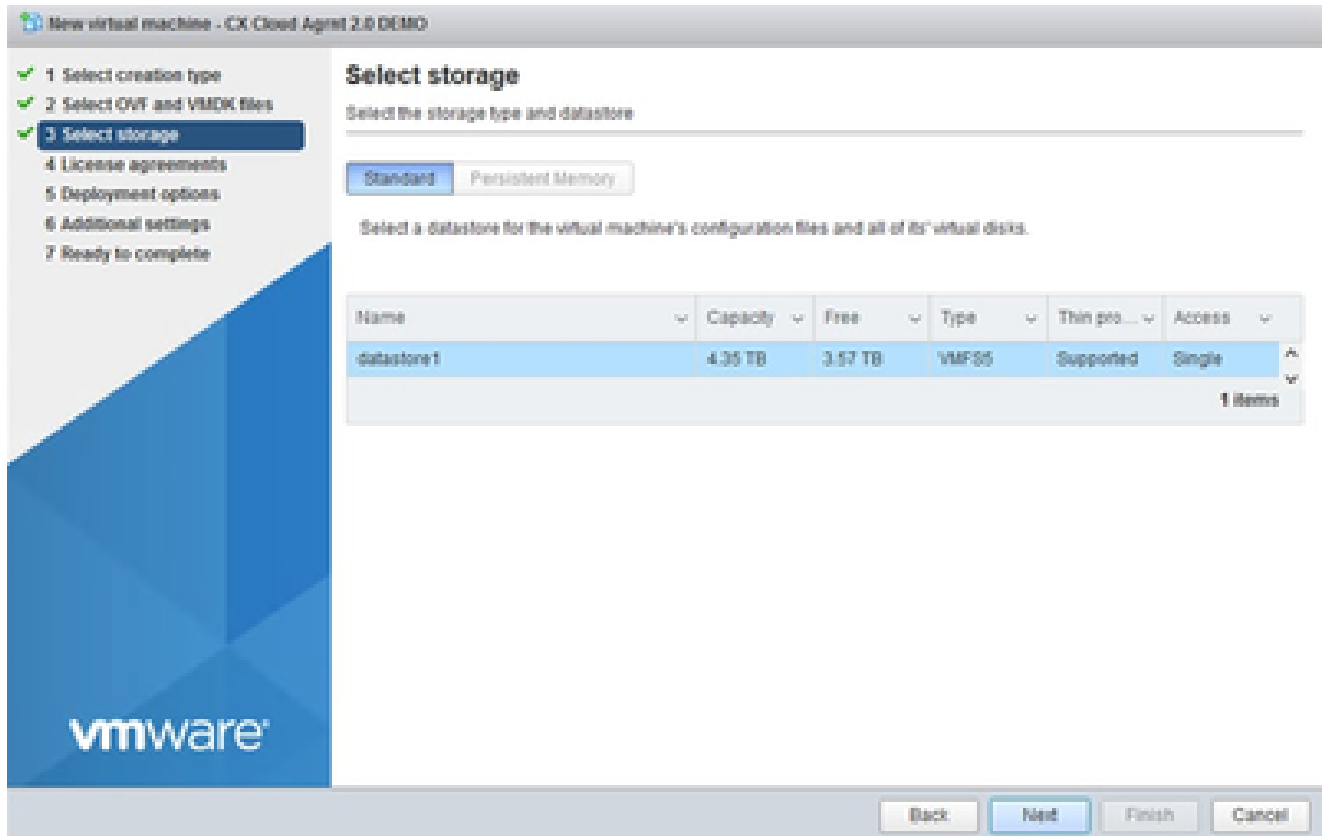
BACK

NEXT

*Review Details*

9. Select the **virtual disk format** and click **Next**.





*Select Storage*

10. Click **Next**.

## 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 Ready to complete

### Review details

Verify the template details.

Publisher	DigiCert SHA2 Assured ID Code Signing CA (Trusted certificate)
Product	CxCloudAgent_3.0_Build-144
Version	2.0
Vendor	Cisco Systems, Inc
Description	CxCloudAgent_3.0_Build-144
Download size	1.1 GB
Size on disk	3.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

CANCEL

BACK

NEXT

*Select Network*

11. Click **Finish**.

# 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 Ready to complete**

Ready to complete  
Click Finish to start creation.

Provisioning type	Deploy from template
Name	CxCloudAgent_2.0_Build-144-demo
Template name	CxCloudAgent_2.0_Build-144-1_signed-sha1
Download size	11 GB
Size on disk	3.1 GB
Folder	Security
Resource	10.126.77.51
Storage mapping	1
All disks	Datastore: datastore1 (23); Format: Thin provision
Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

CANCEL BACK FINISH

Ready to Complete

12. Click the name of the newly added VM to view the status.

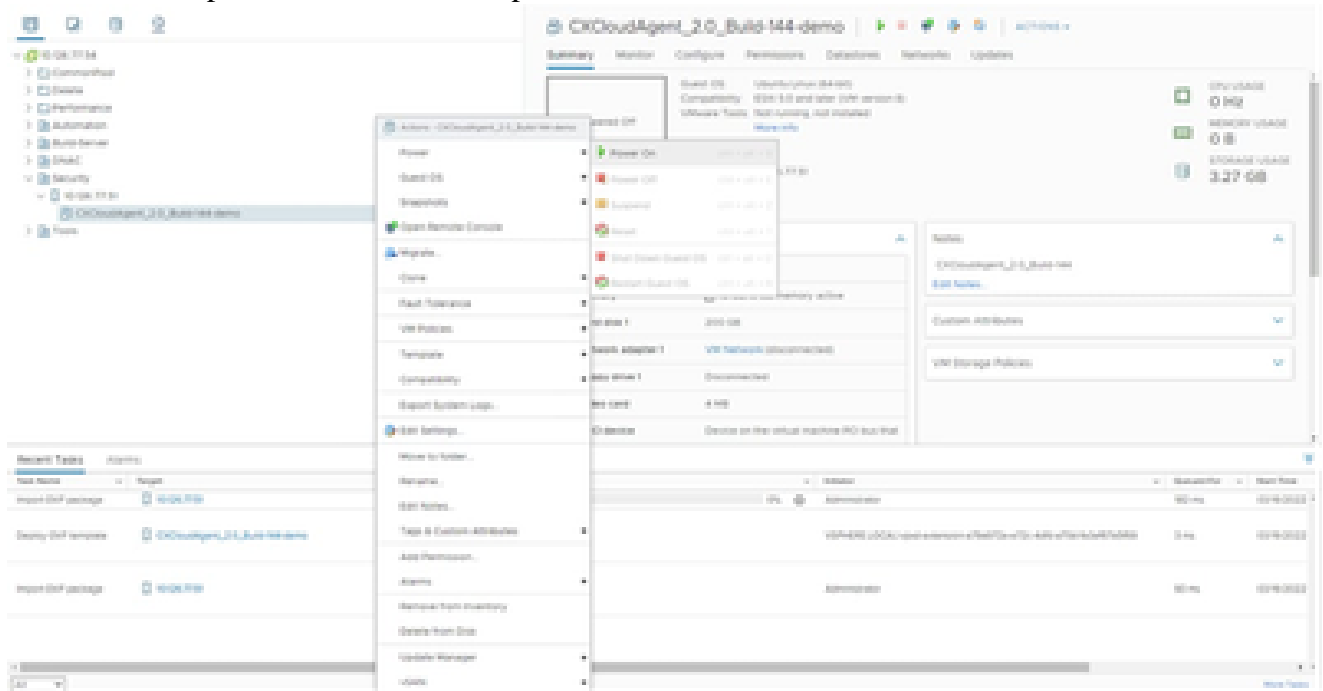
The screenshot displays the vSphere interface for a newly created VM named 'CxCloudAgent\_2.0\_Build-144-demo'. The VM is currently in a 'Powered Off' state. The main content area provides detailed information about the VM's hardware, including CPU (0 CPUs), Memory (0 MB, 0 MB memory active), Hard disk 1 (200 GB), Network adapter 1 (VM Network (disconnected)), Floppy disk 1 (Disconnected), Video card (4 MB), and VMX space (Device on the virtual machine (0) on the host).

At the bottom of the interface, the 'Recent Tasks' table shows the following entries:

Task Name	Host	Status	Message	Start Time	End Time
Import OVF package	10.126.77.51	Completed	Administration	00 ms	12/9/2022
Deploy OVF template	CxCloudAgent_2.0_Build-144-demo	Completed	VMX: VMX: user extension of Path: /usr/lib/vmtoolsd/patches	0 ms	12/9/2022
Import OVF package	10.126.77.51	Completed	Administration	00 ms	12/9/2022

VM Added

13. Once installed, power on the VM and open the console.



Open Console

14. Navigate to [Network Configuration](#) to proceed with the next steps.

## Oracle Virtual Box 5.2.30 Installation

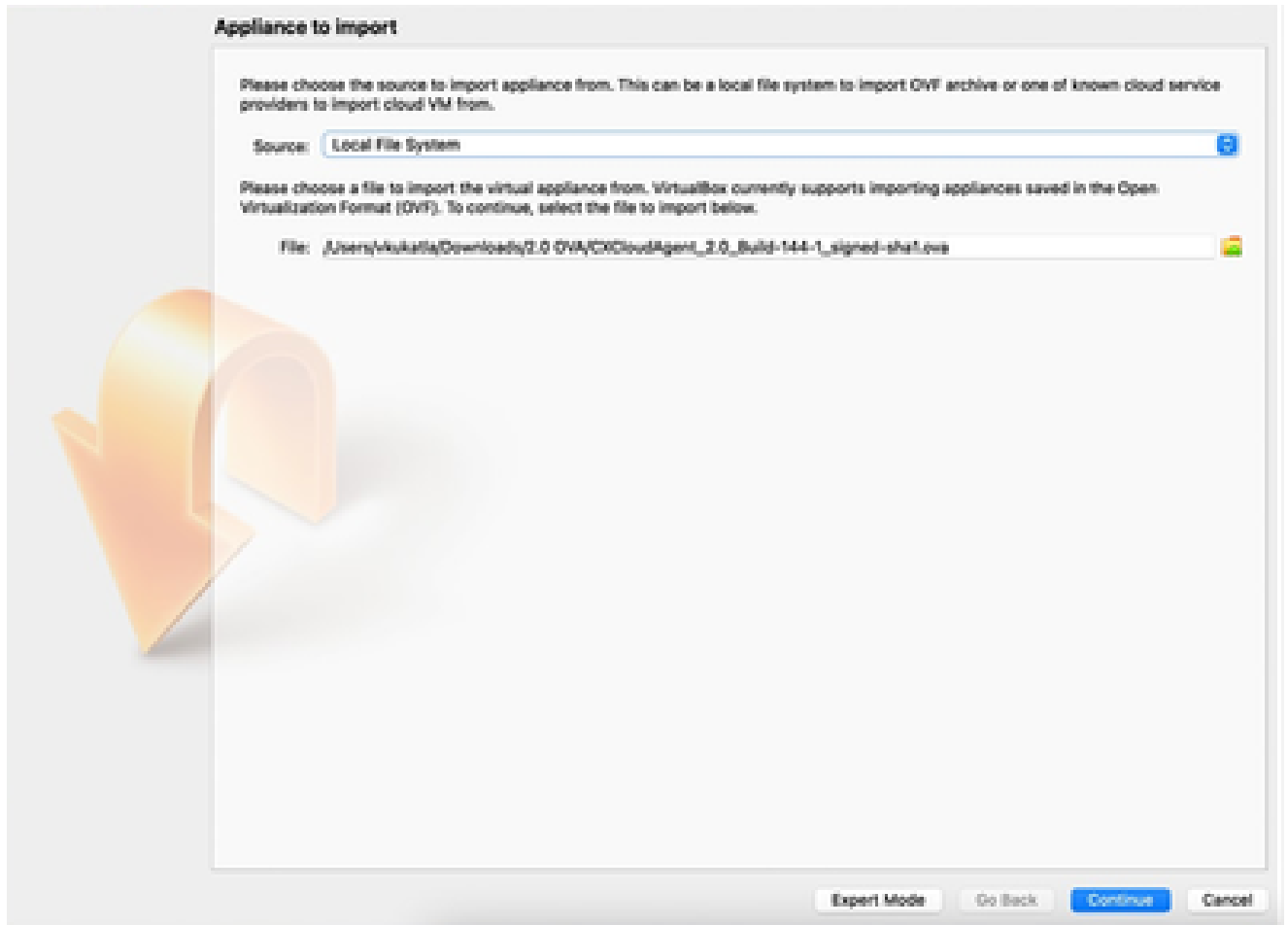
This client deploys CX Cloud Agent OVA though the Oracle Virtual Box.

1. Open the Oracle VM UI and select **File> Import Appliance**.



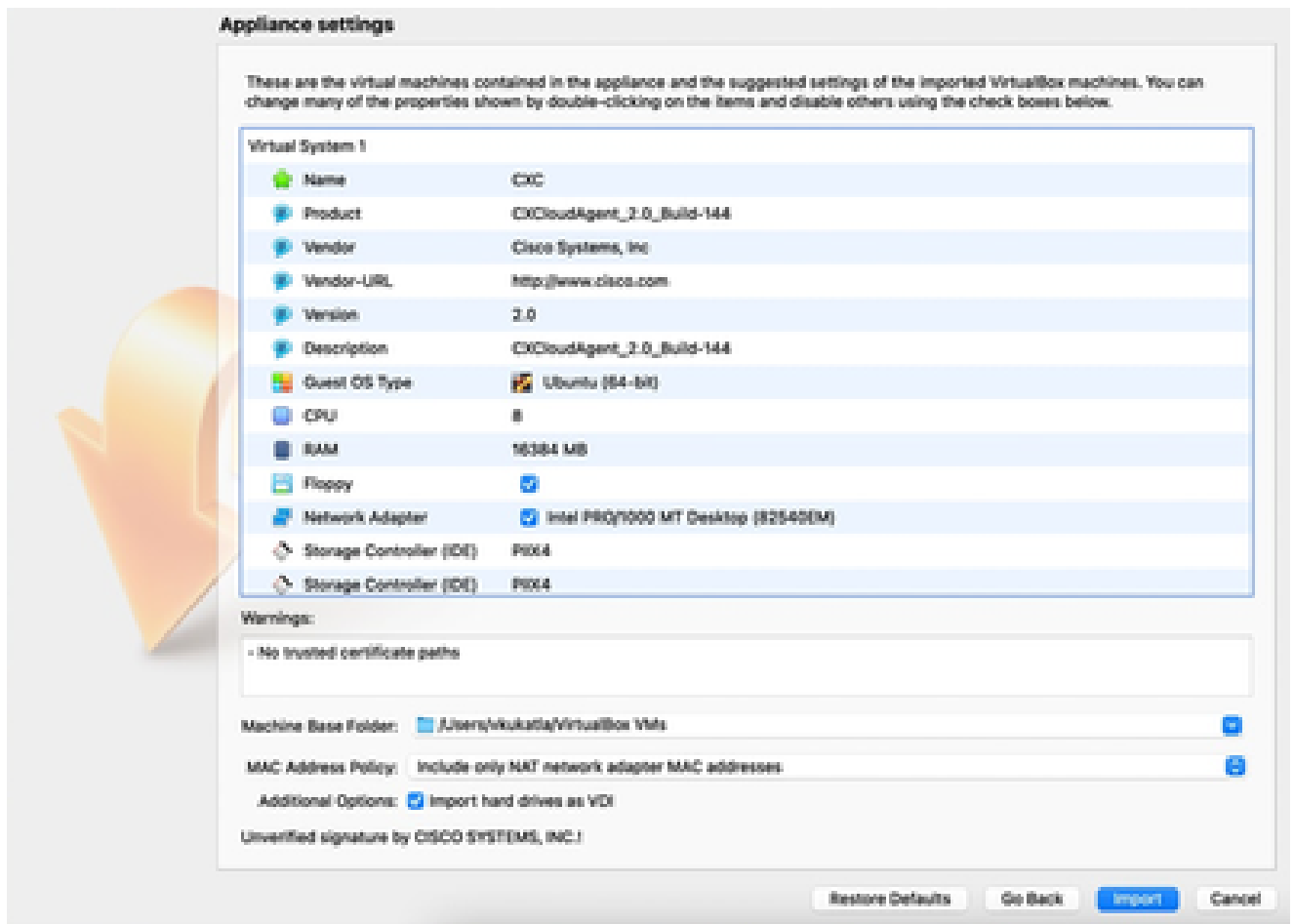
Oracle VM

2. Browse to import the OVA file.



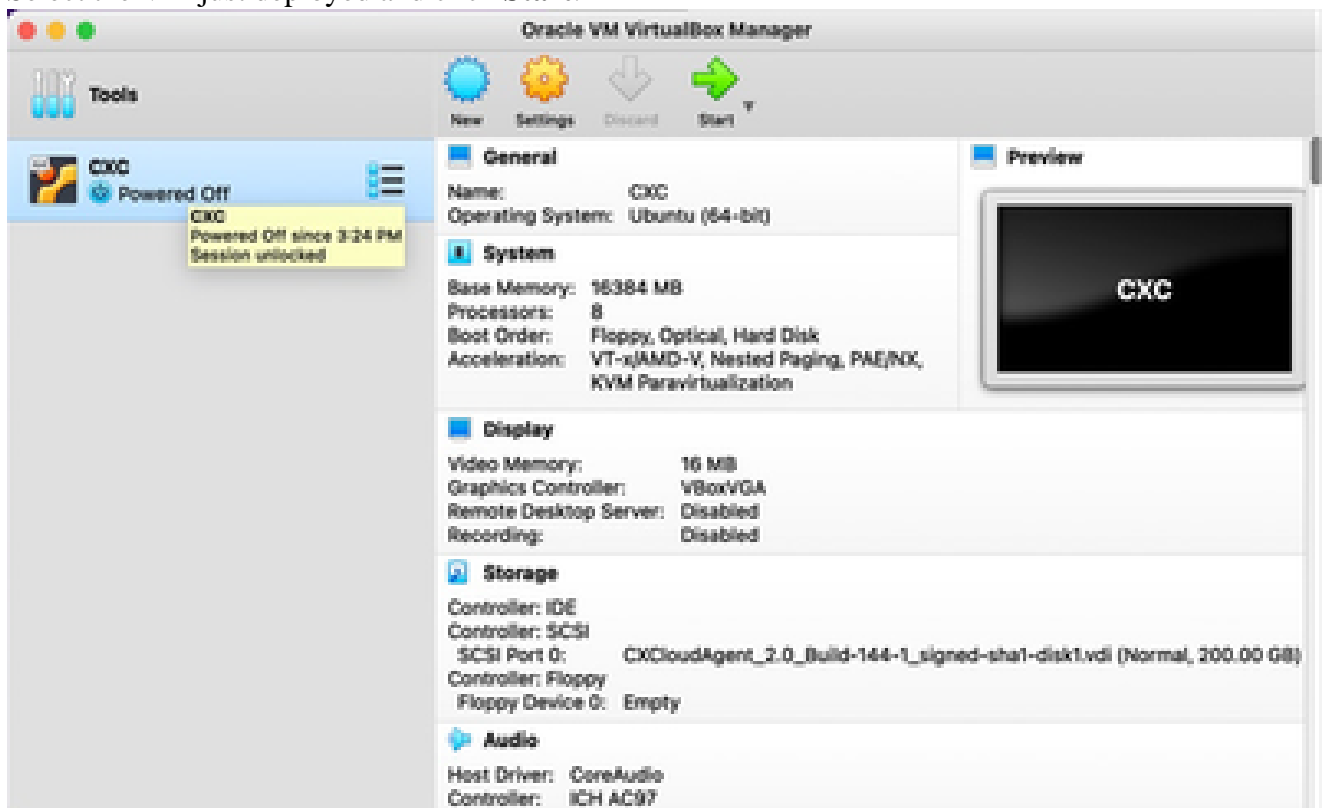
*Select File*

3. Click **Import**.

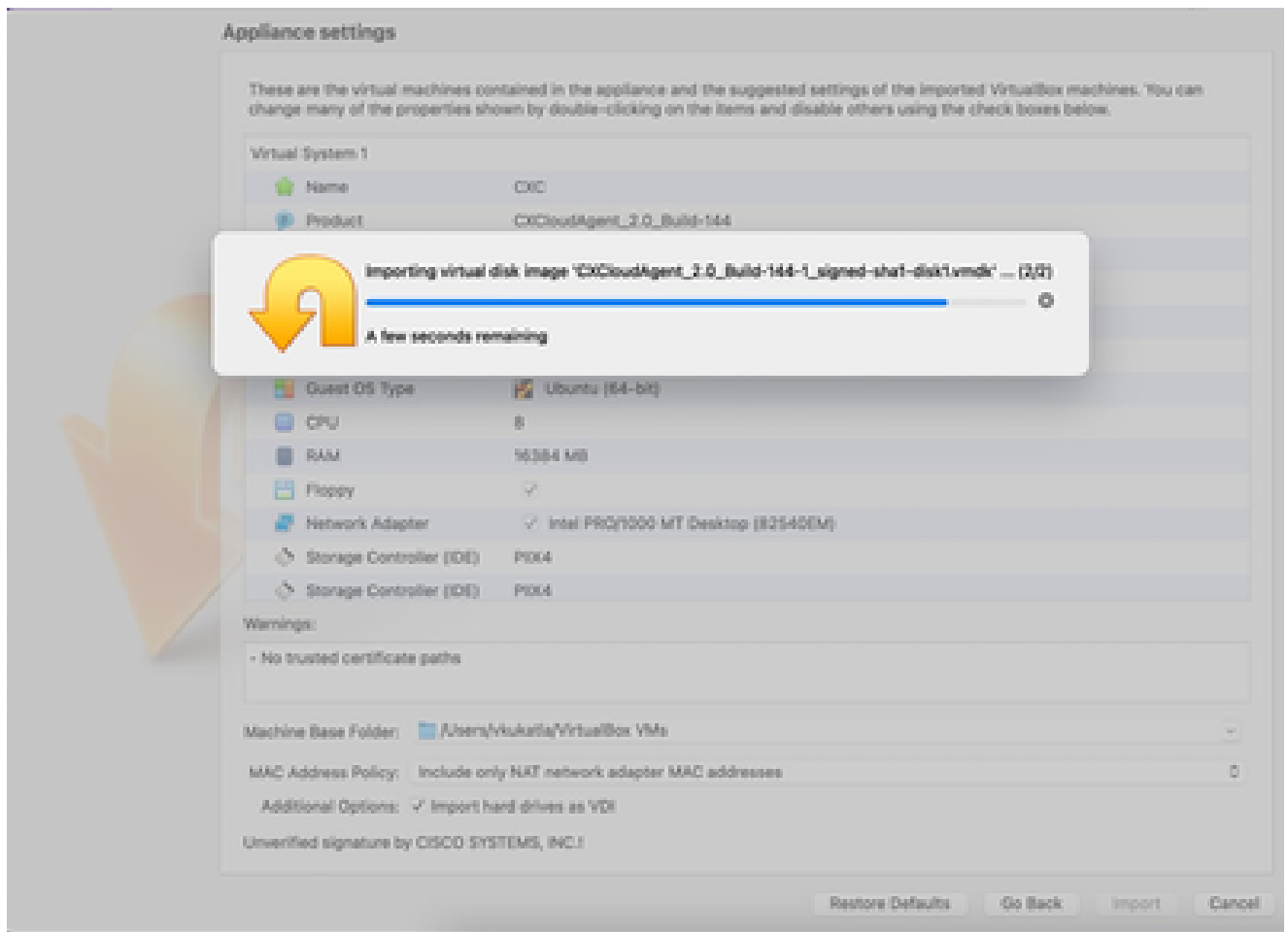


*Import File*

4. Select the VM just deployed and click **Start**.



*VM Console Startup*



*Import in Progress*

5. Power on the VM. The console displays.



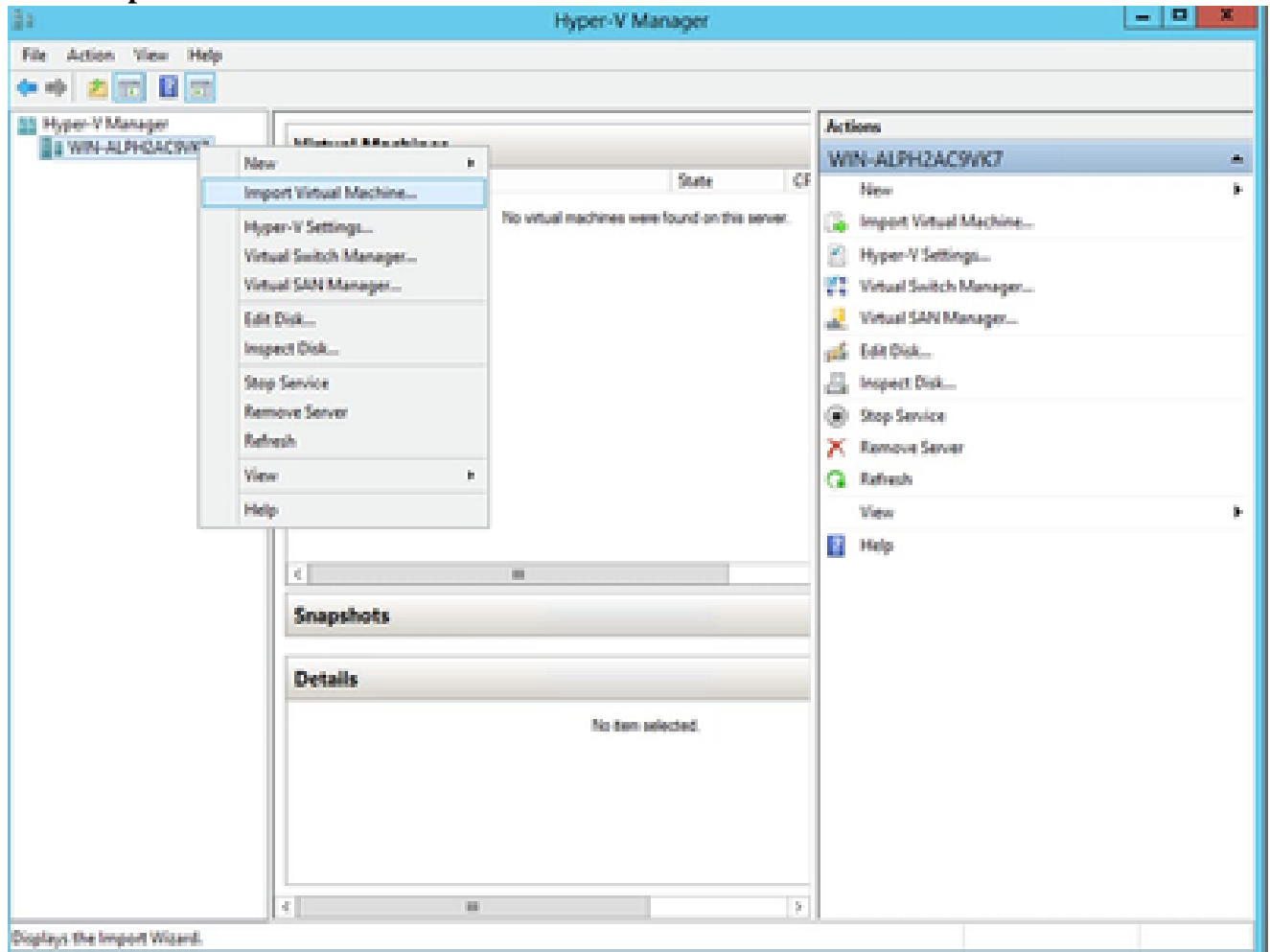
*Open Console*

6. Navigate to [Network Configuration](#) to proceed with the next steps.

## Microsoft Hyper-V Installation

Perform these steps:

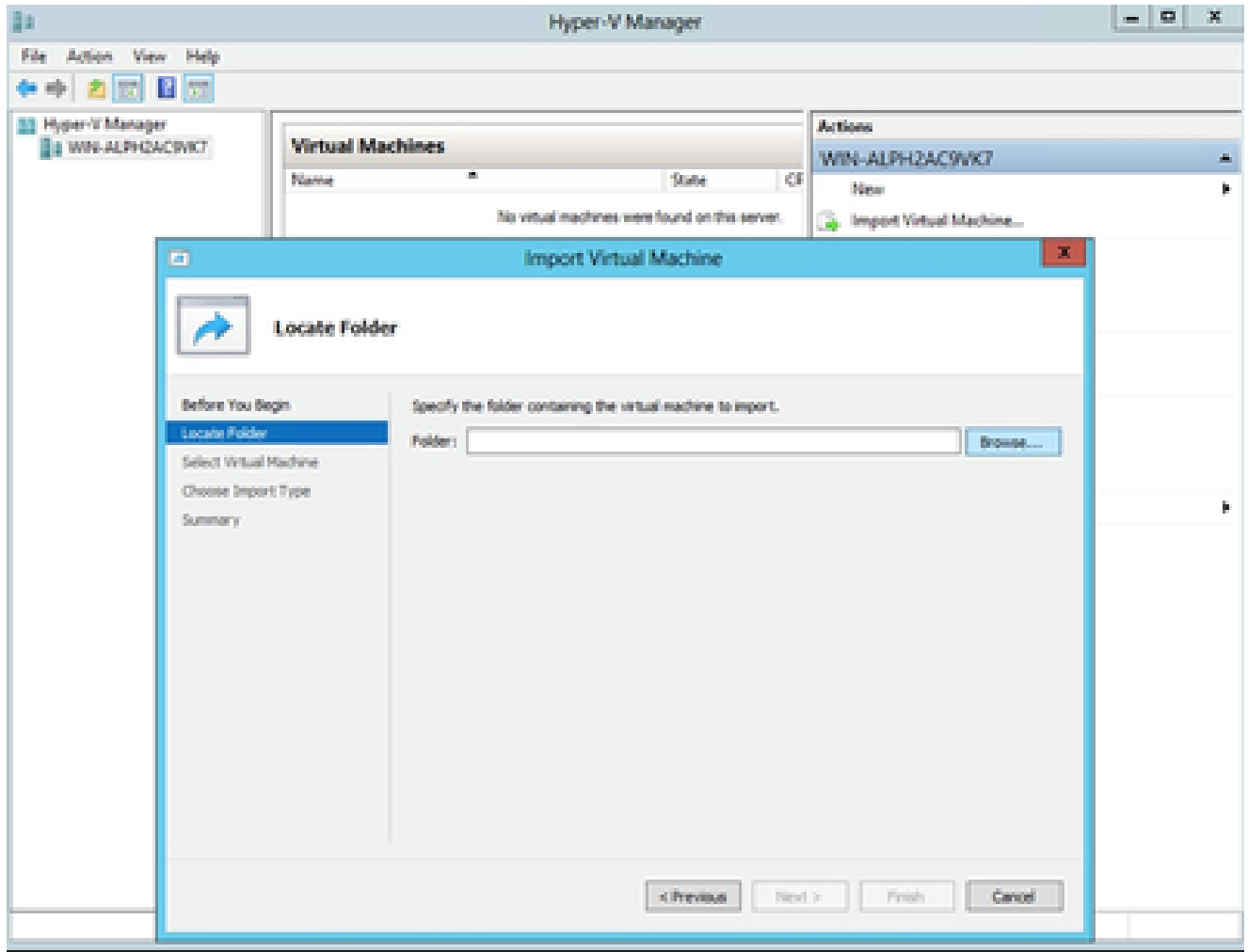
1. Select **Import Virtual Machine**.



*Hyper V Manager*

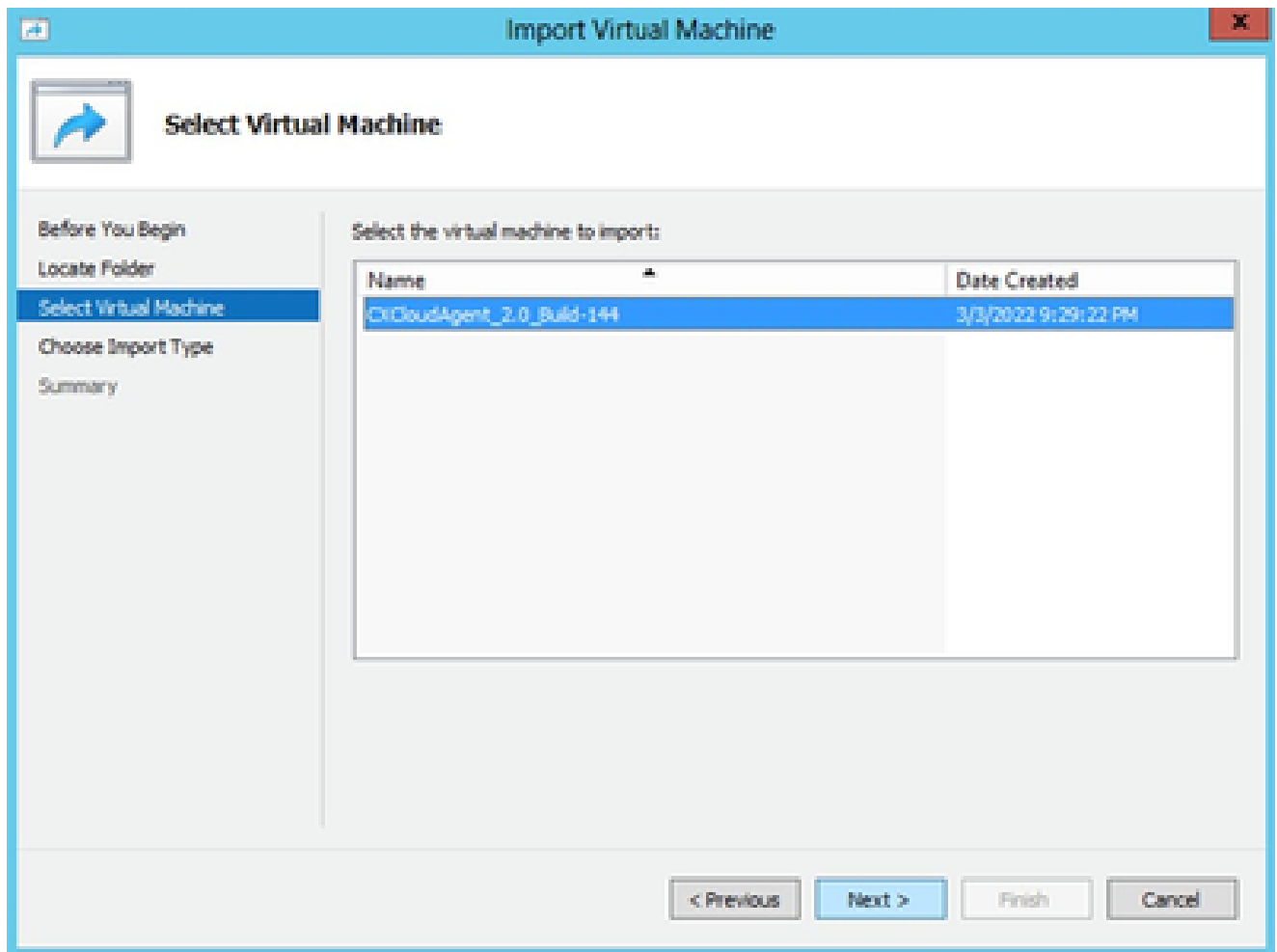
2. Browse and select the **download folder**.
3. Click **Next**.





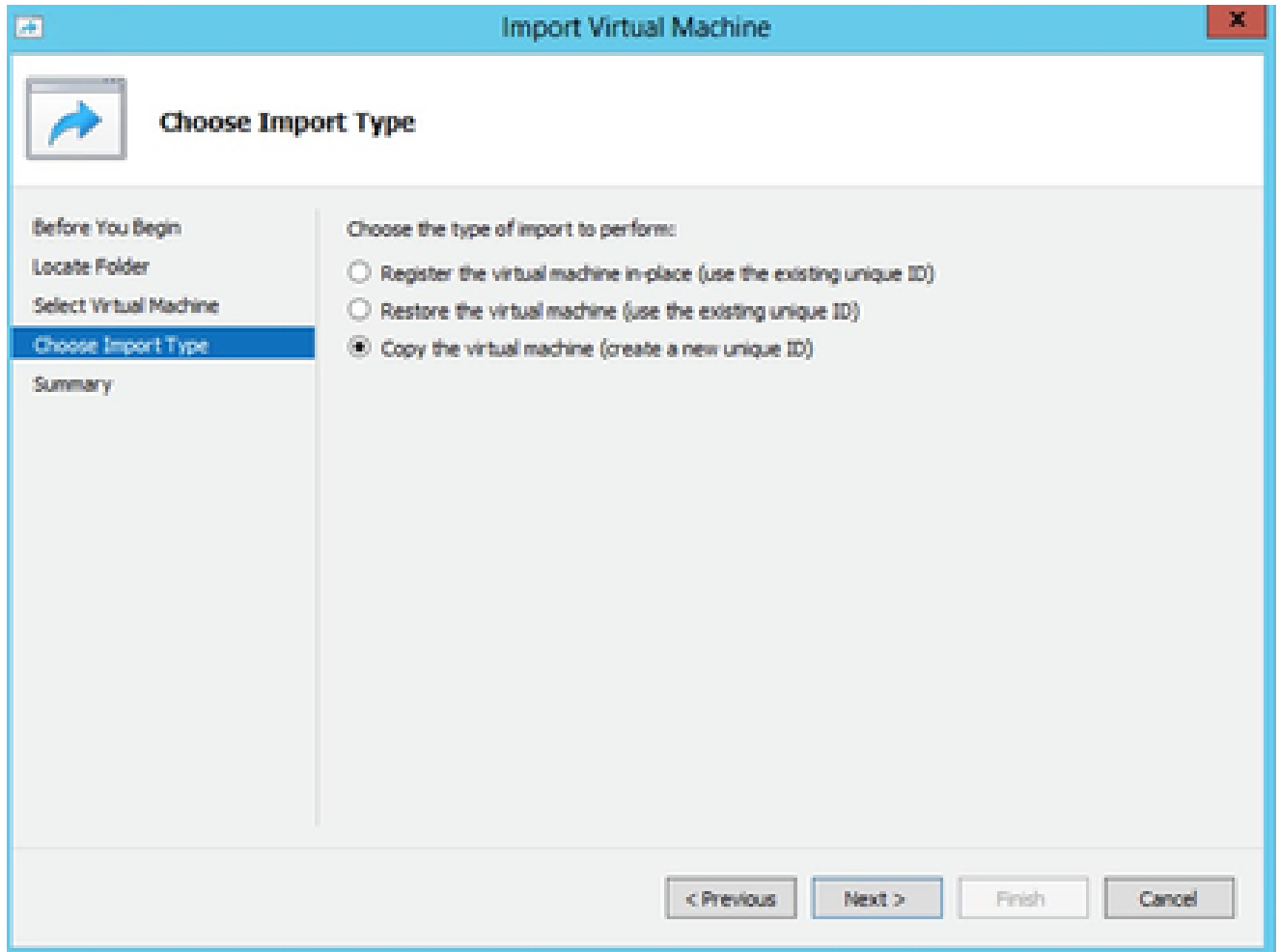
*Folder to Import*

4. Select the **VM** and click **Next**.



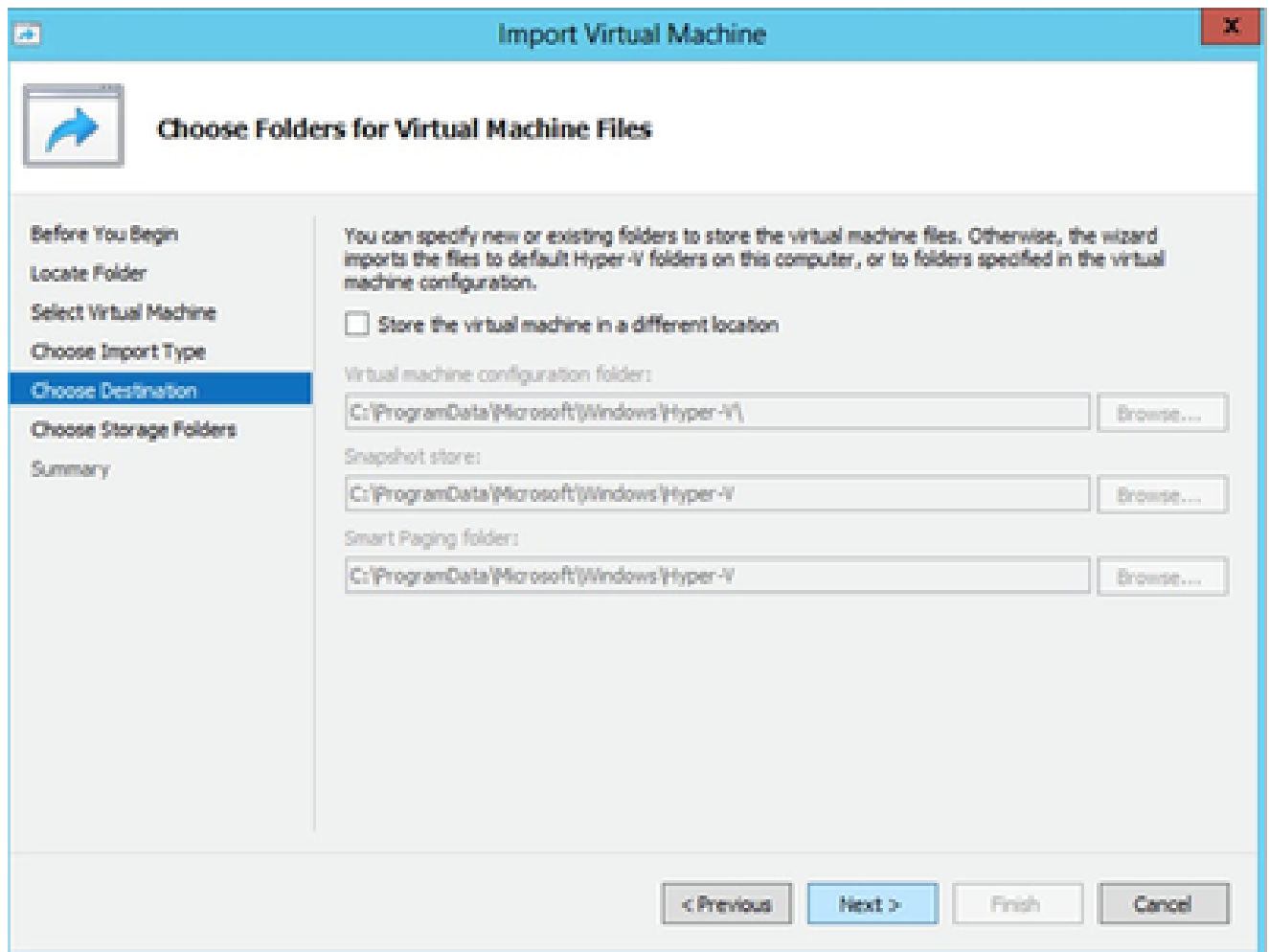
*Select VM*

5. Select the **Copy the virtual machine (create a new unique ID)** radio button and click **Next**.



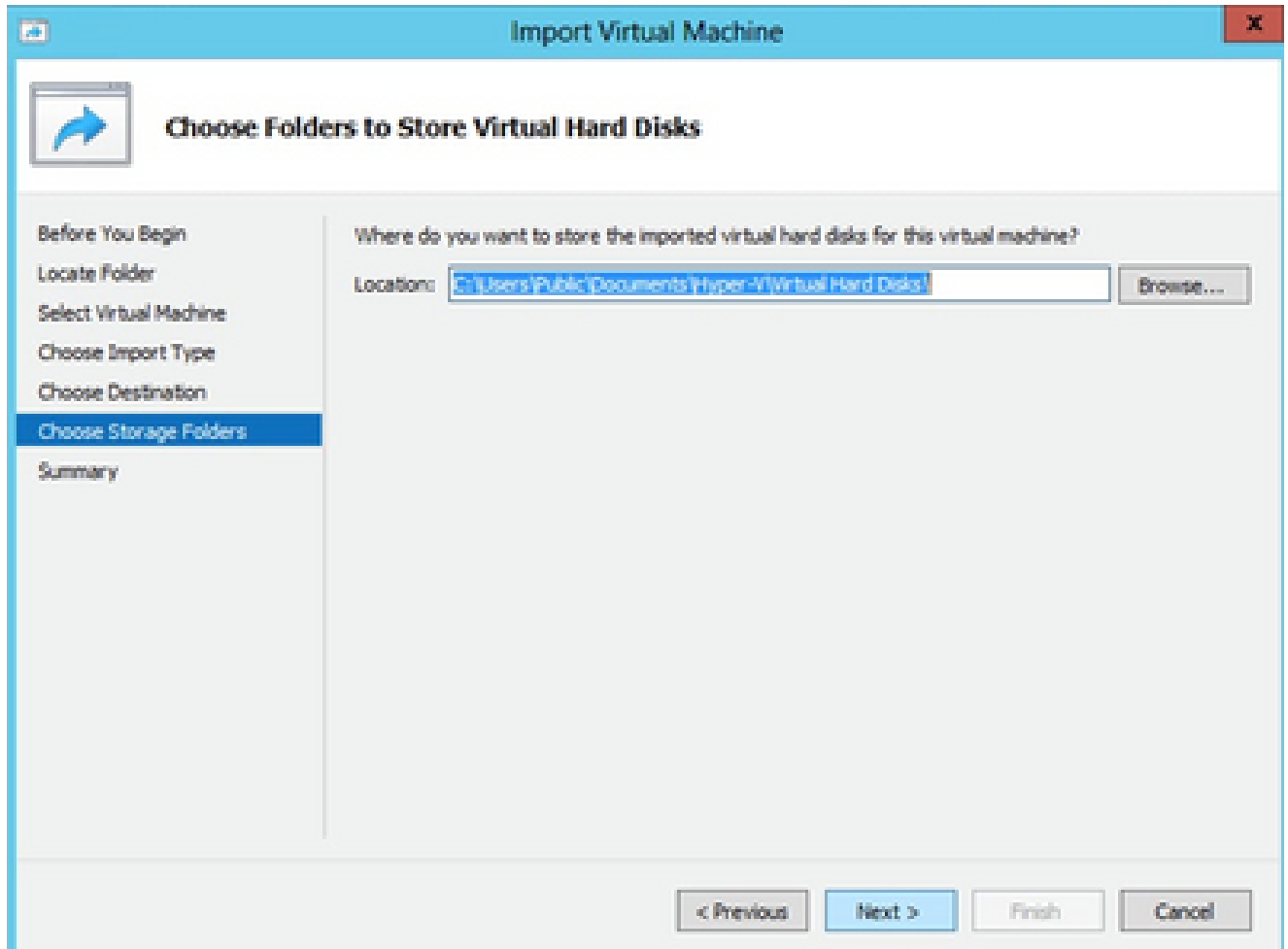
*Import Type*

6. Browse to select the folder for VM files. It is recommended to use the default paths.
7. Click **Next**.



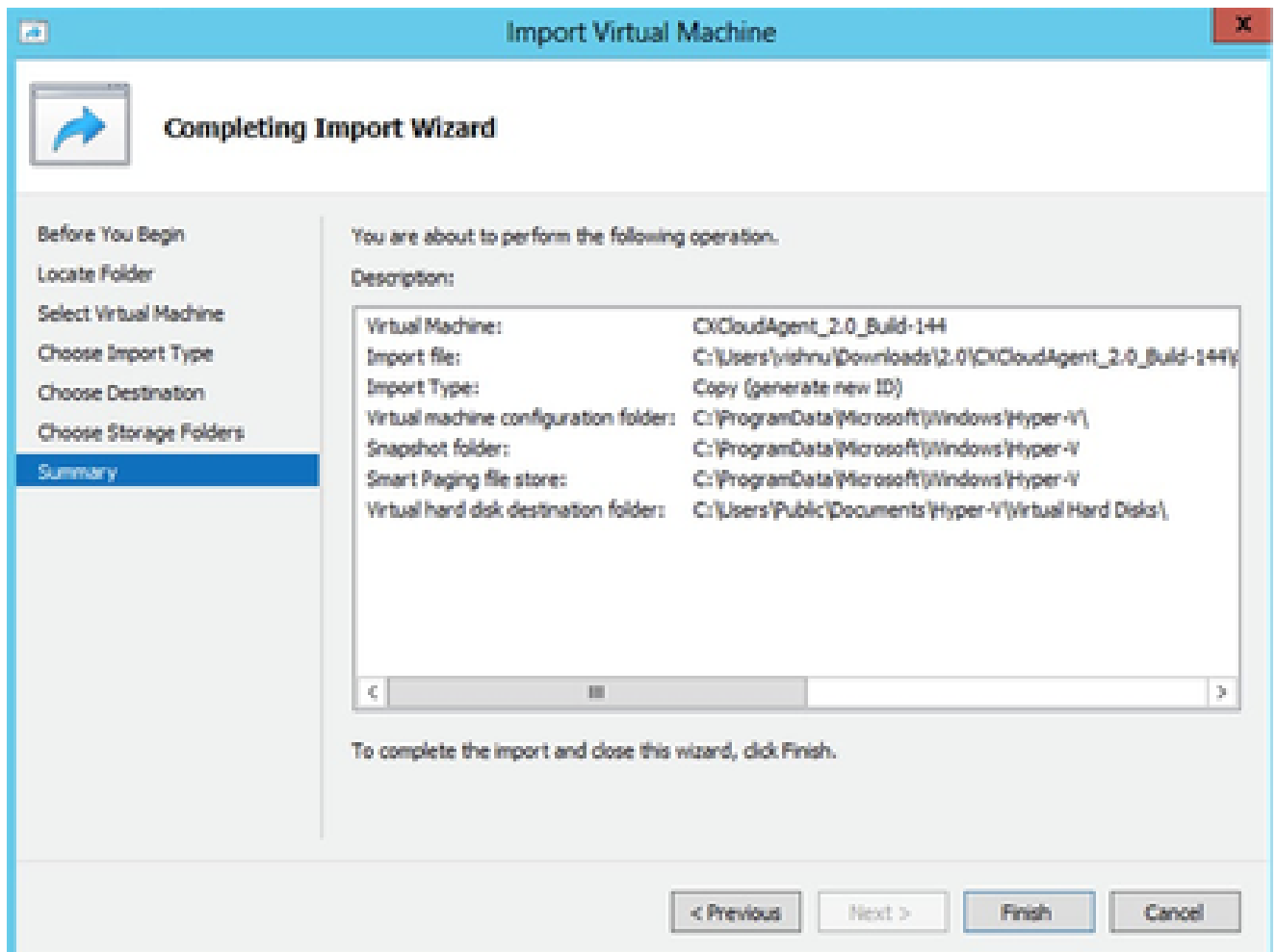
*Choose Folders for Virtual Machine Files*

8. Browse and select the folder to store the VM hard disk. It is recommended to use default paths.
9. Click **Next**.



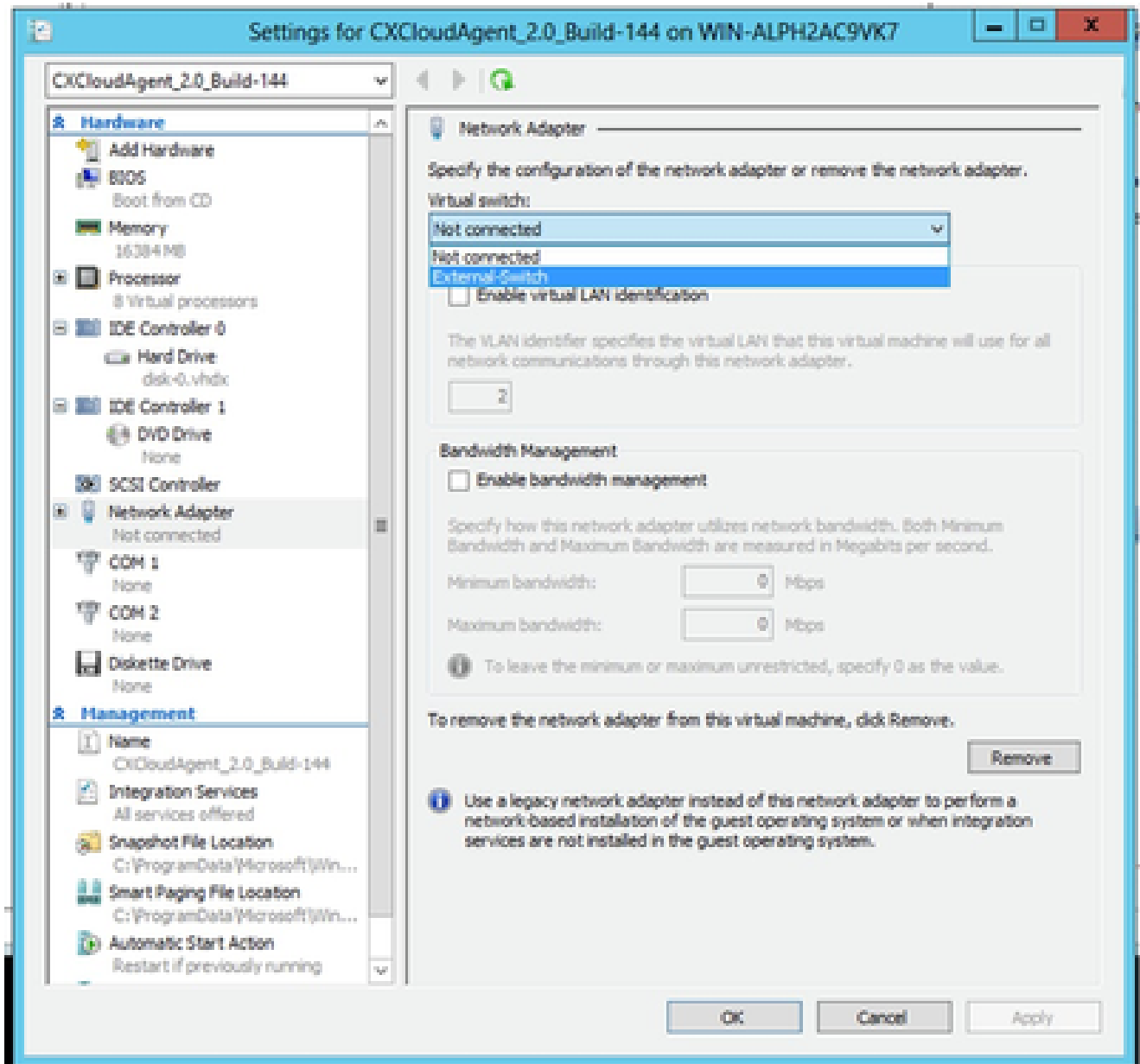
*Folder to Store the Virtual Hard Disks*

10. The VM summary displays. Verify all inputs and click **Finish**.



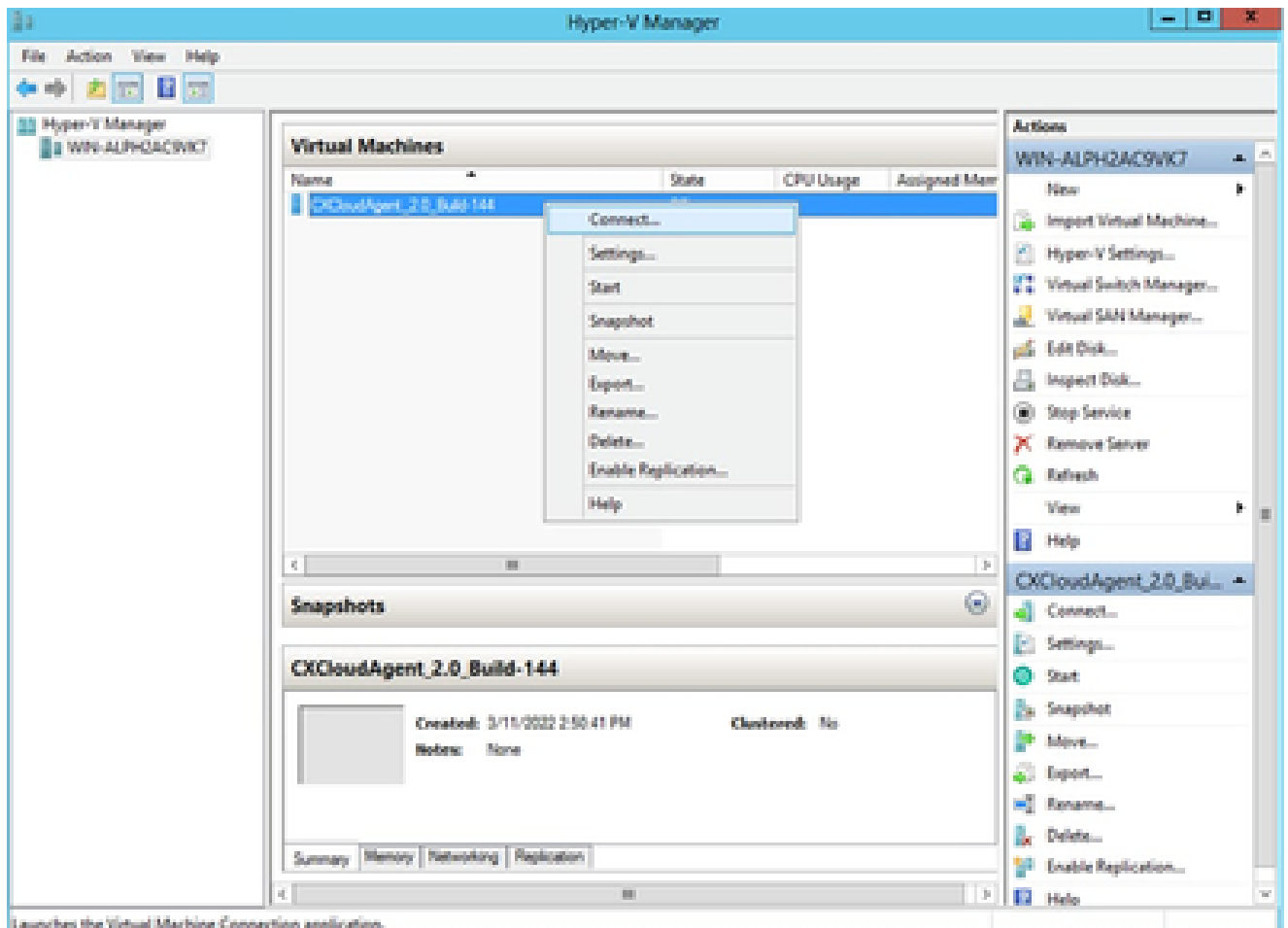
#### Summary

11. Once the import is completed successfully, a new VM is created on Hyper-V. Open the VM setting.
12. Select the **network adaptor** on the left pane and choose the available **Virtual Switch** from the drop-down.



*Virtual Switch*

13. Select **Connect** to start the VM.

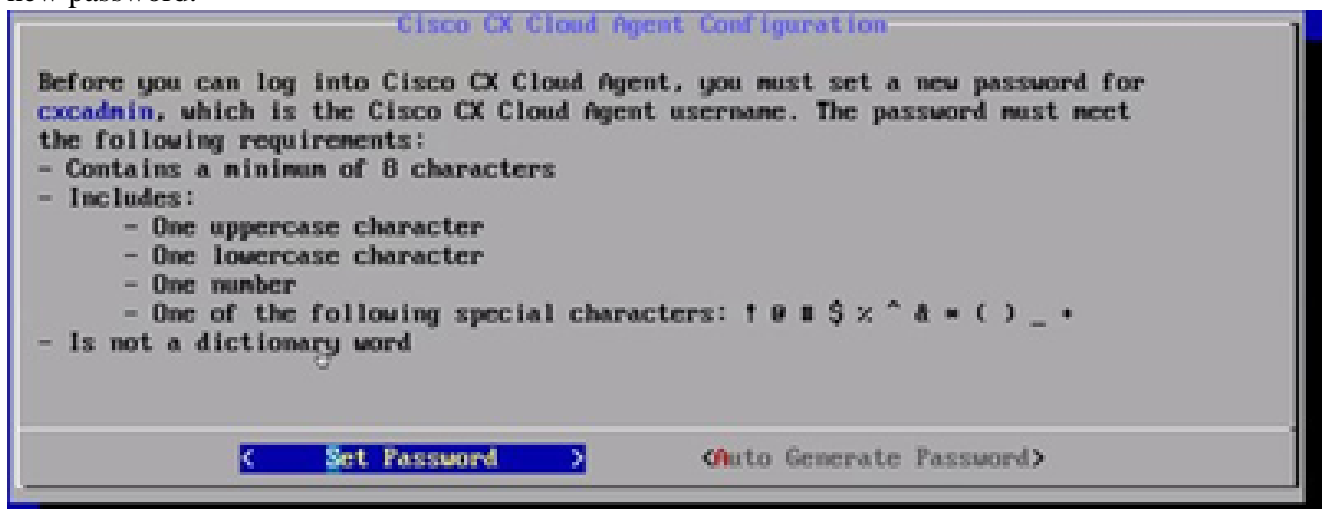


Starting VM

14. Navigate to [Network Configuration](#) to proceed with the next steps.

## Network Configuration

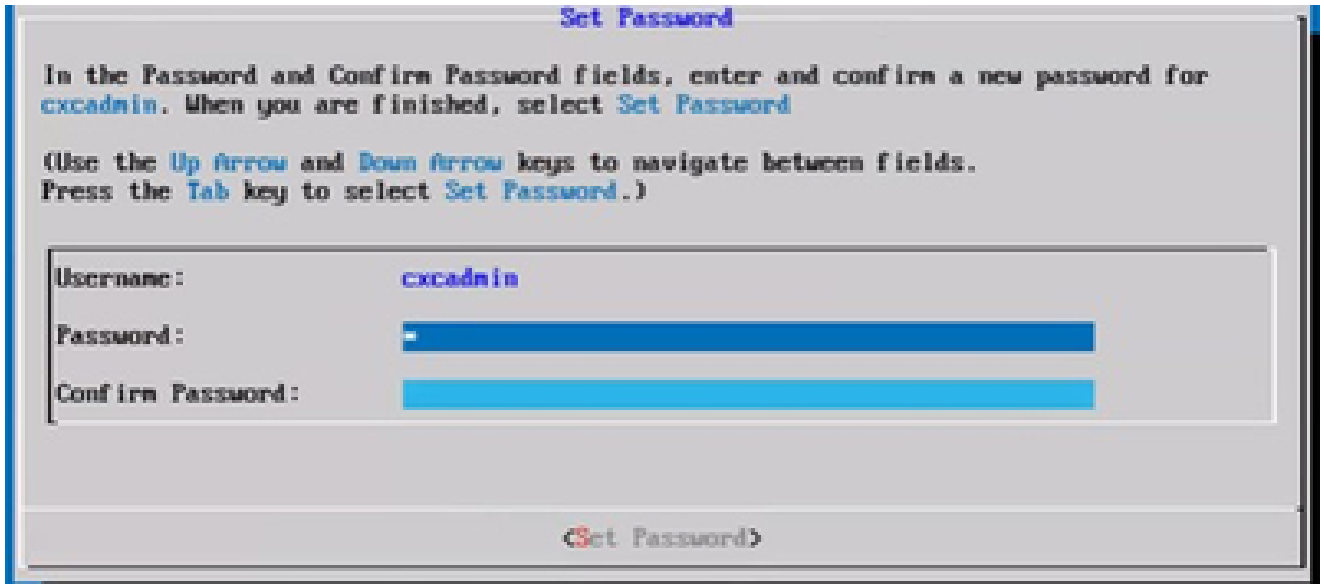
1. Click **Set Password** to add a new password for cxcadmin OR click **Auto Generate Password** to get a new password.



Set Password

2. If **Set Password** is selected, enter the password for cxcadmin and confirm it. Click **Set Password** and go to Step 3.





*New Password*

OR

If **Auto Generate Password** is selected, copy the password generated and store it for future use. Click **Save Password** and go to Step 4.



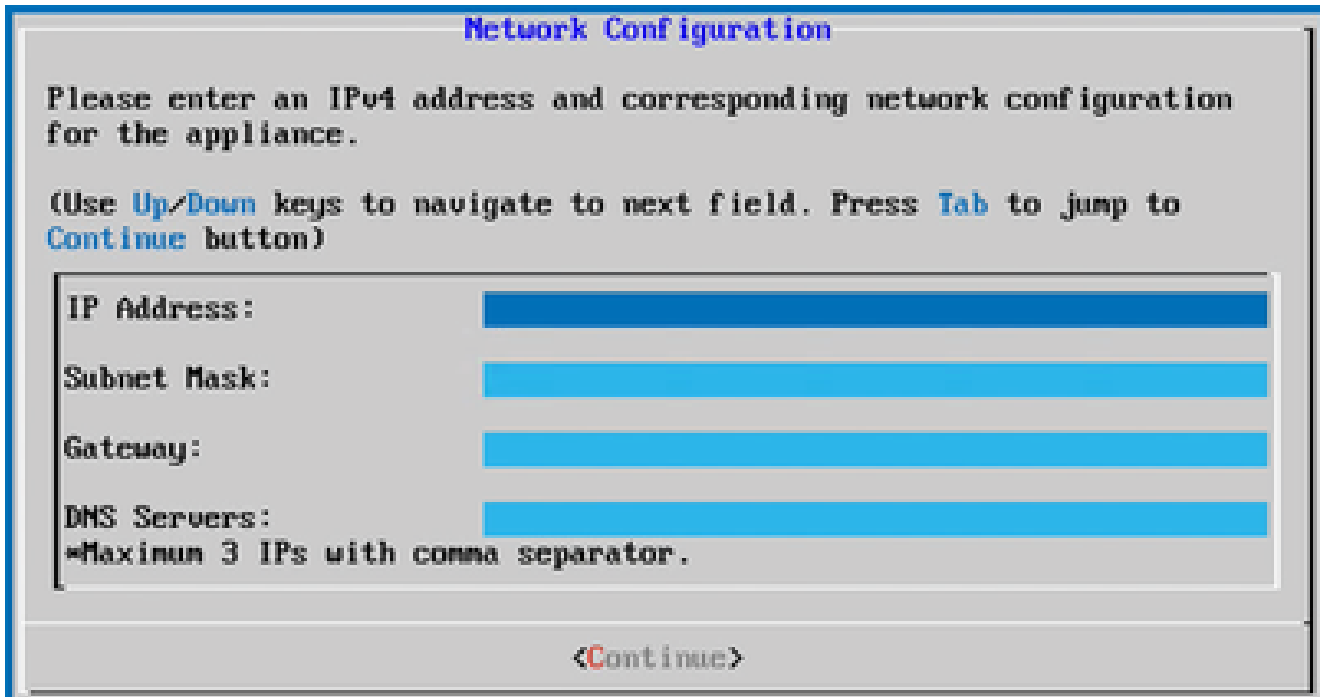
*Auto Generated Password*

3. Click **Save Password** to use it for authentication.



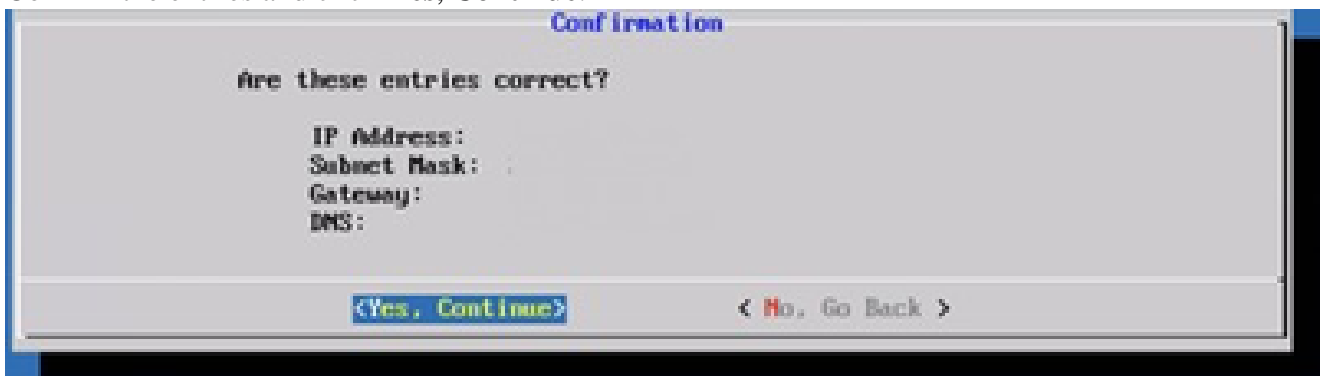
*Save Password*

4. Enter the **IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server** and click **Continue**.



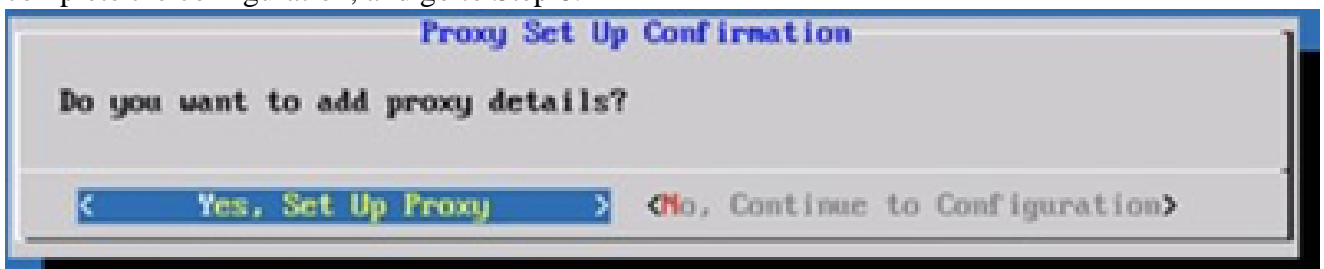
Network Configuration

5. Confirm the entries and click **Yes, Continue**.



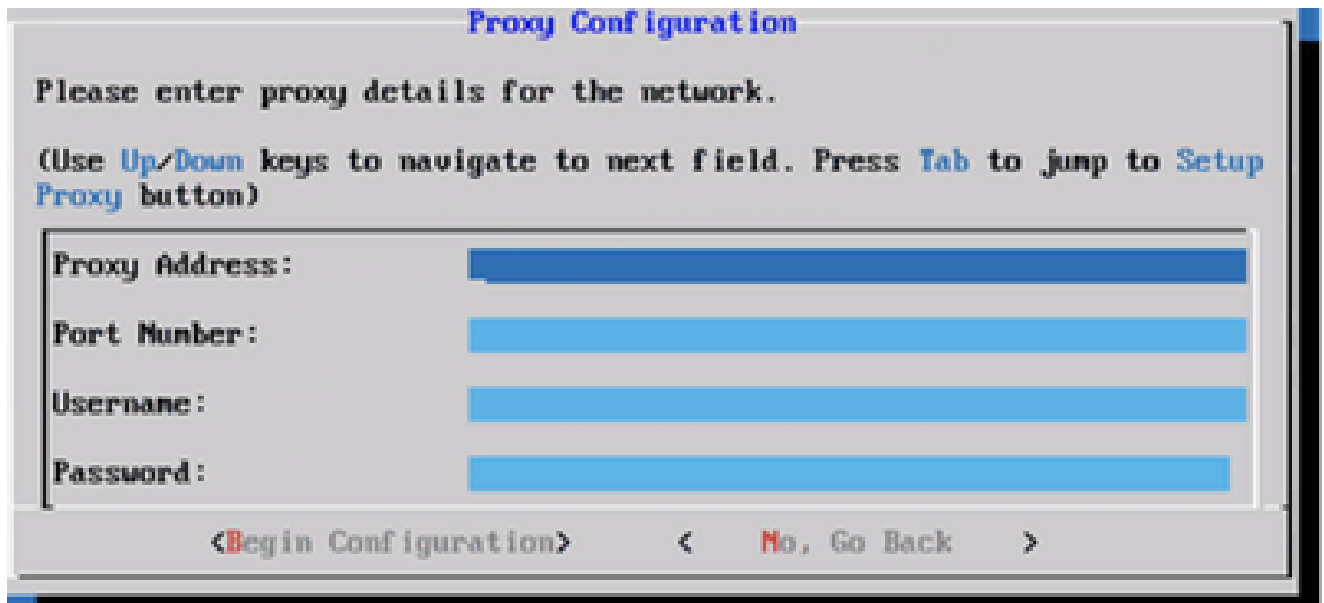
Configuration

6. To set the proxy details, click **Yes, Set Up Proxy** or click **No, Continue to Configuration** to complete the configuration, and go to Step 8.



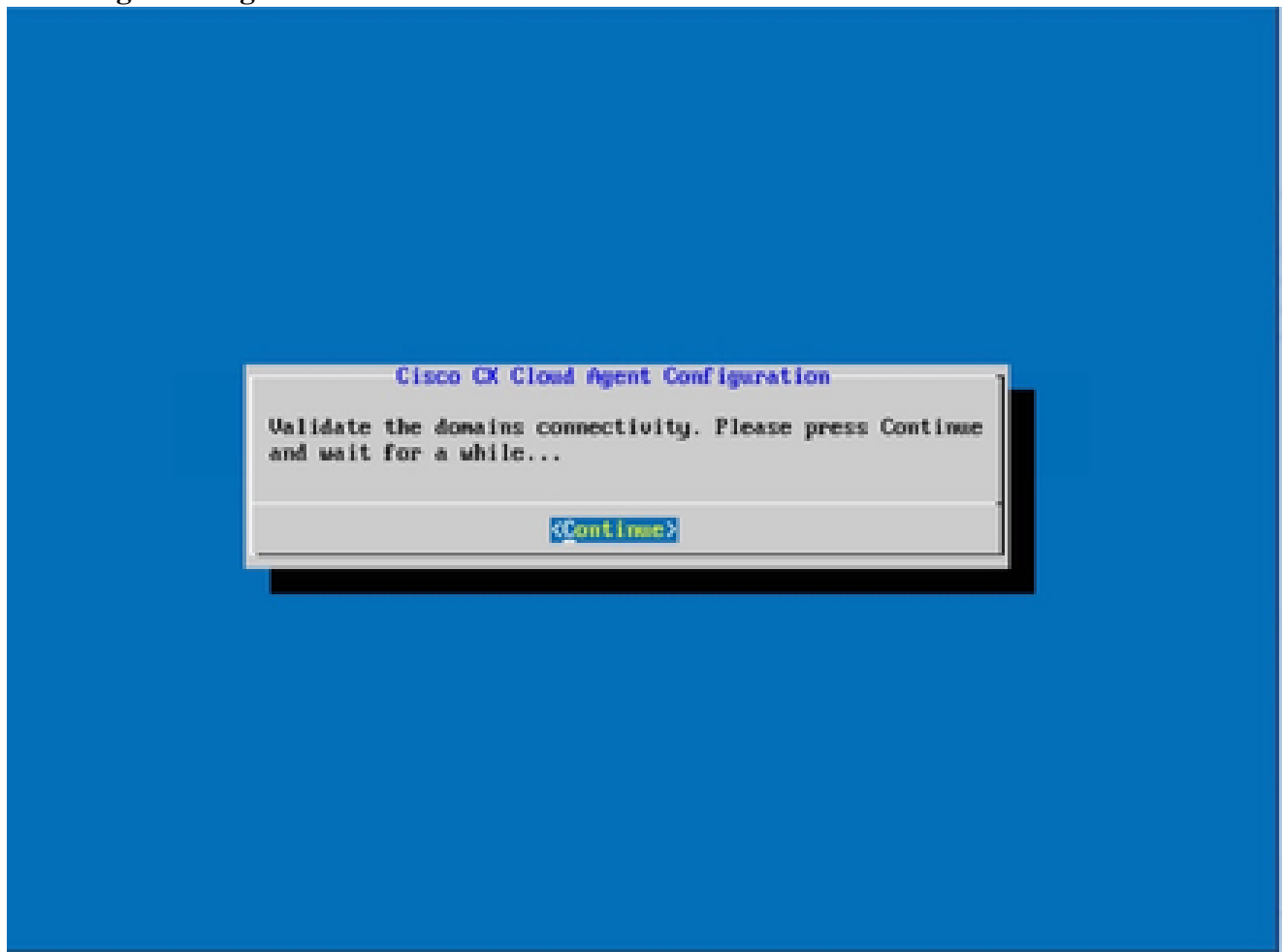
Proxy Setup

7. Enter the **Proxy Address, Port Number, Username, and Password**.



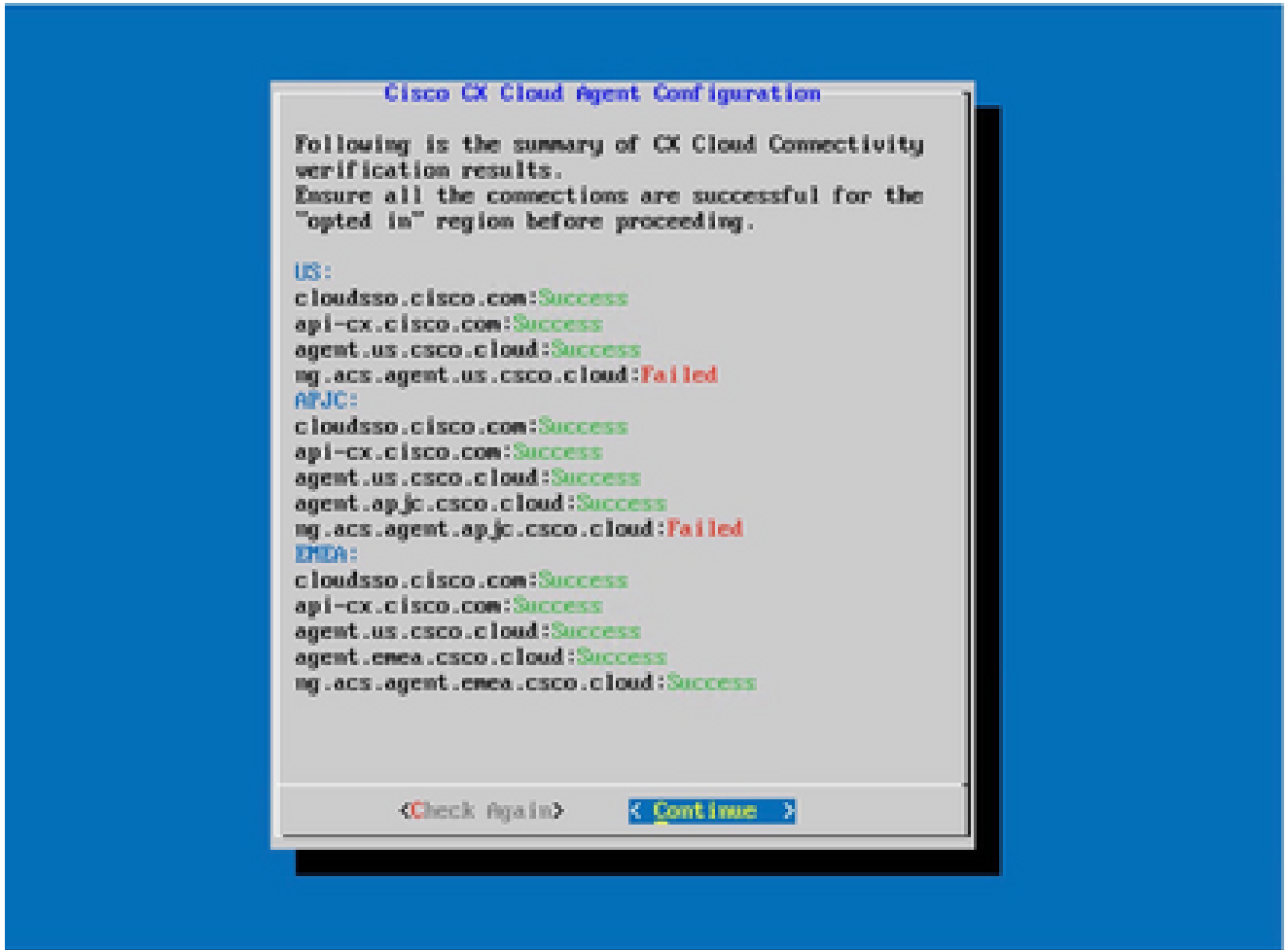
*Proxy Configuration*

8. Click **Begin Configuration**.




*Begin Configuration*

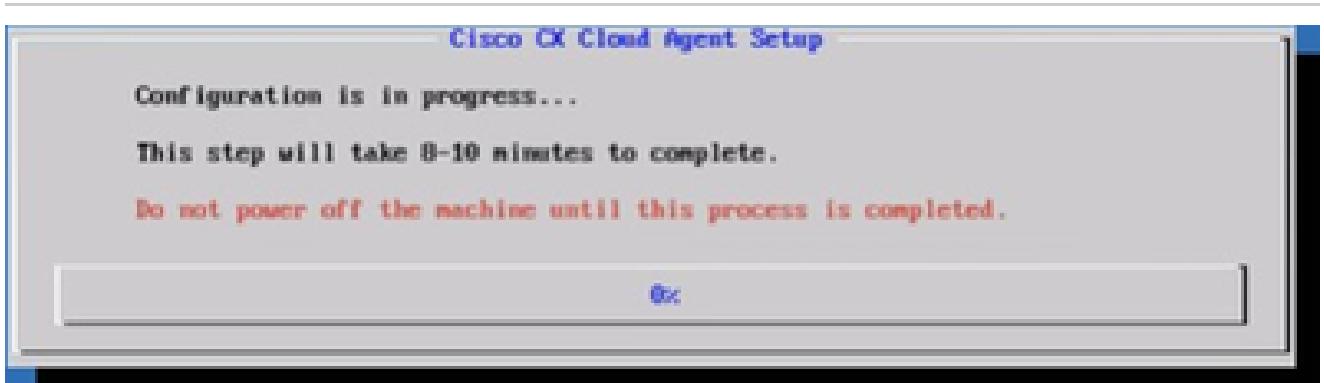
9. Click **Continue**.



Configuration Continues

10. Click **Continue** to proceed with the configuration for successful domain reach. The configuration can take several minutes to complete.

 **Note:** If the domains cannot be reached successfully, the customer must fix domain reachability by making changes in their firewall to ensure that domains are reachable. Click **Check Again** once the domains reachability issue is resolved.



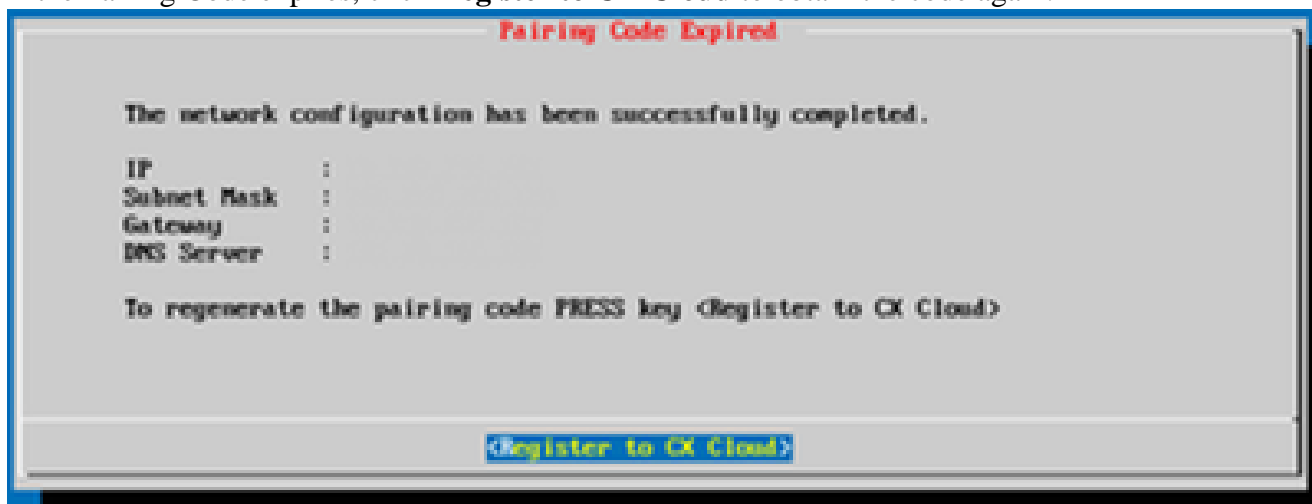
Configuration in Progress

11. Copy the **Pairing Code** and return to CX Cloud to continue the setup.



*Pairing Code*

12. If the Pairing Code expires, click **Register to CX Cloud** to obtain the code again.



*Code Expired*

13. Click **OK**.



*Registration Successful*

## Alternative Approach to Generate Pairing Code Using CLI

Users can also generate a pairing code by using CLI options.

To generate a pairing code using CLI:

1. Log in to the Cloud Agent via SSH using the cxcadmin user credential.
2. Generate the pairing code using the command `cxcli agent generatePairingCode`.

```

cxcadmin@cxcloudagent:~$ cxcli agent generatePairingCode

Pairing Code : xJ7I0P
Expires in: 5 minutes
Please use the Pairing Code in the CX Cloud to proceed with CX Cloud Agent registration.

cxcadmin@cxcloudagent:~$

```

Generate Pairing Code CLI

3. Copy the Pairing Code and return to CX Cloud to continue the setup.

## Configure Cisco Catalyst Center To Forward Syslog to CX Cloud Agent

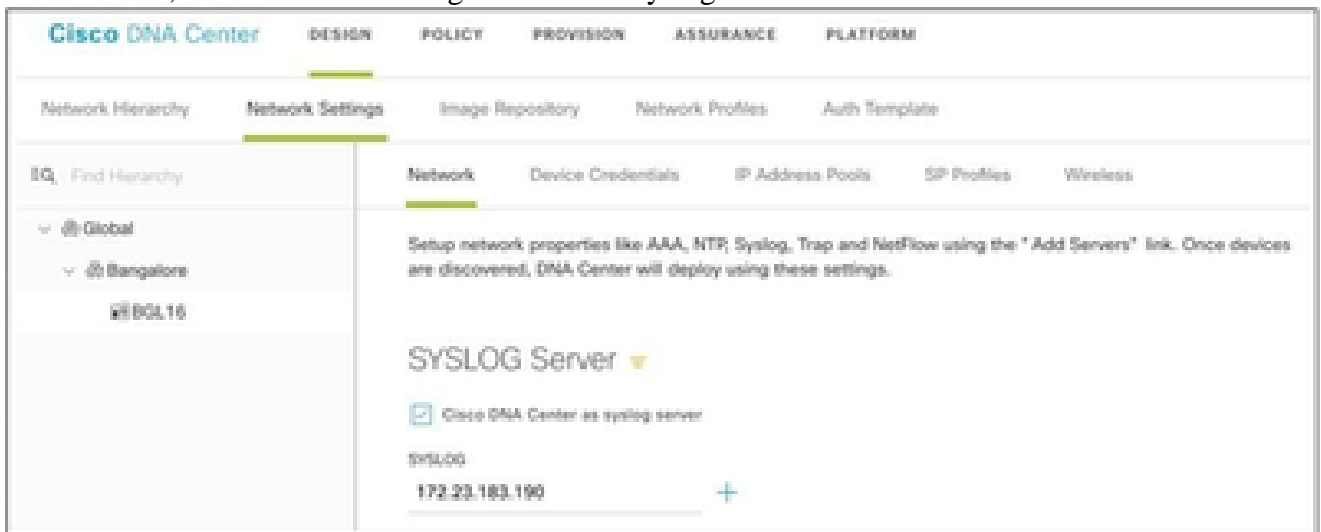
### Prerequisites

Supported Cisco Catalyst Center versions are 2.1.2.0 to 2.2.3.5, 2.3.3.4 to 2.3.3.6, 2.3.5.0, and Cisco Catalyst Center Virtual Appliance

### Configure Syslog Forward Setting

To configure Syslog Forwarding to CX Cloud Agent in the Cisco Catalyst Center, perform these steps:

1. Launch Cisco Catalyst Center.
2. Go to **Design > Network Settings > Network**.
3. For each site, add the CX Cloud Agent IP as the Syslog Server.




Syslog Server

**Note:** Once configured, all devices associated with that site are configured to send syslog with level critical to CX Cloud Agent. Devices must be associated to a site for enabling the syslog forwarding from the device to CX Cloud Agent. When a syslog server setting is updated, all devices associated with that site are automatically set to default critical level.

## Configure Other Assets to Forward Syslog to CX Cloud Agent

Devices must be configured to send Syslog messages to the CX Cloud Agent to use the Fault Management feature of CX Cloud.

---


 **Note:** Only Campus Success Track Level 2 devices are eligible to configure other assets to forward syslog.

---

### Existing Syslog Servers with Forward Capability

Perform the configuration instructions for the syslog server software and add the CX Cloud Agent IP Address as a new destination.

---

 **Note:** When forwarding syslogs, ensure that the source IP address of the original syslog message is preserved.

---

### Existing Syslog Servers without Forward Capability OR without Syslog Server

Configure each device to send syslogs directly to the CX Cloud Agent IP Address. Refer to this documentation for specific configuration steps.

[Cisco IOS® XE Configuration Guide](#)

[AireOS Wireless Controller Configuration Guide](#)

### Enable Information Level Syslog Settings

To make Syslog Information level visible, perform these steps:

1. Navigate to **Tools>Telemetry**.



## TOOLS

**Discovery**

**Inventory**

**Topology**

**Image Repository**

**Command Runner**

**License Manager**

**Template Editor**

**Telemetry**

**Data and Reports**



2. Select and expand the **Site View** and select a **site** from site hierarchy.



Site View

3. Select the required site and select all devices using the **Device name** check box.

4. Select **Optimal Visibility** from the **Actions** drop-down.



Actions

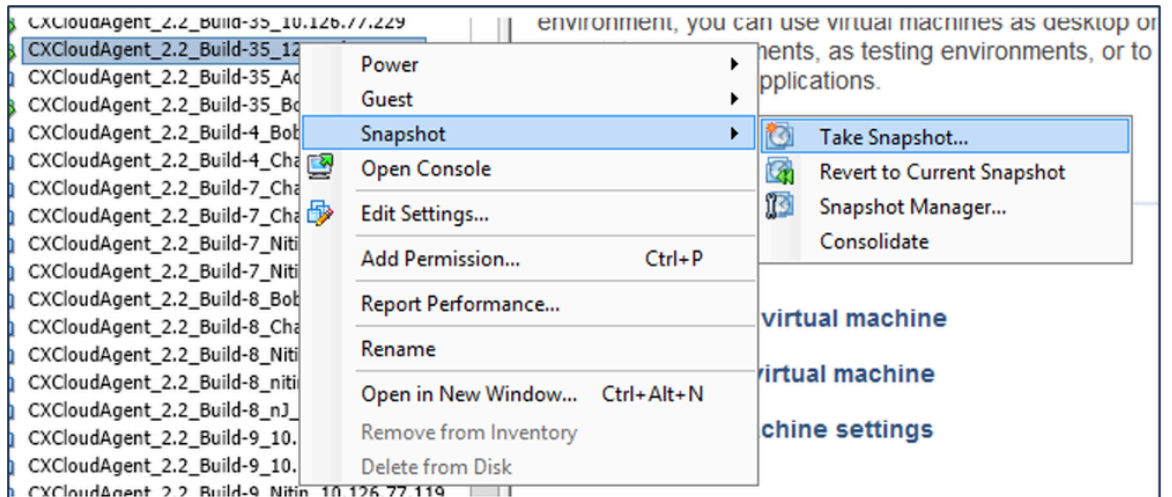
## Back Up and Restore the CX Cloud VM

It is recommended to preserve the state and data of a CX Cloud Agent VM at a specific point in time using the snapshot feature. This feature facilitates CX Cloud VM restoration to the specific time that the snapshot is taken.

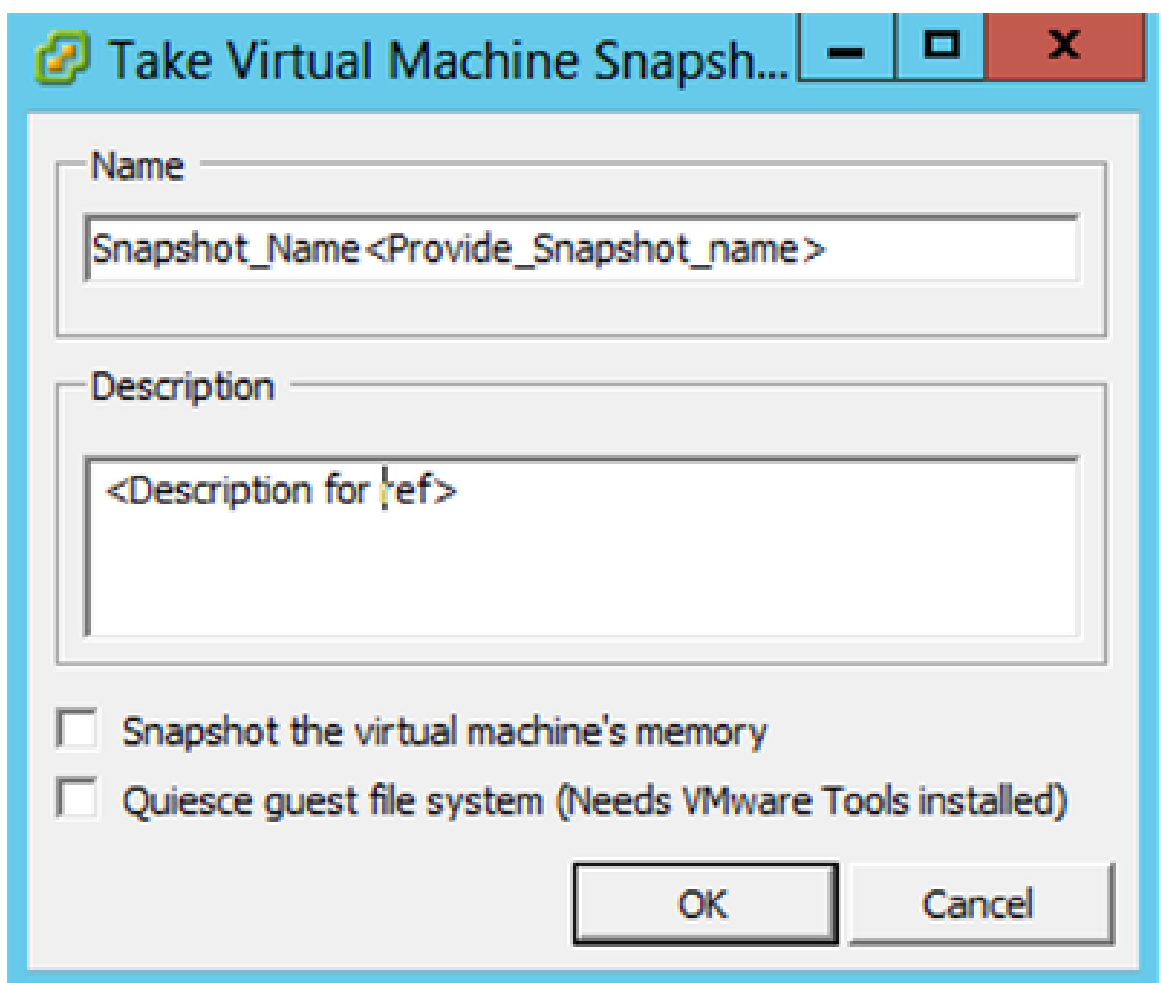
### Back Up

To back up the CX Cloud VM:

1. Right-click the **VM** and select **Snapshot > Take Snapshot**. The **Take Virtual Machine Snapshot** window opens.




Select VM



Take Virtual Machine Snapshot

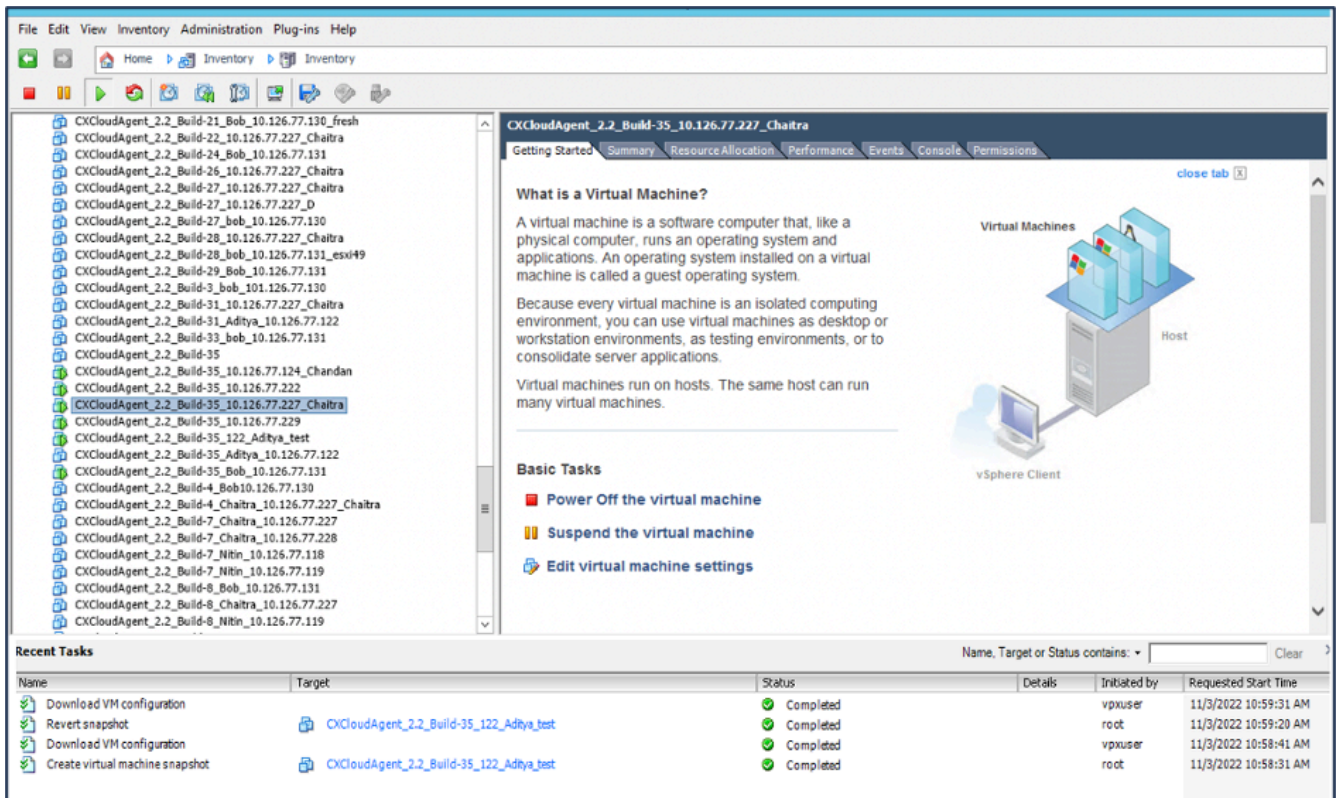
2. Enter **Name** and **Description**.

---

 **Note:** Verify that the Snapshot the virtual machine's memory check box is cleared.

---

3. Click **OK**. The **Create virtual machine snapshot** status displays as **Completed** in the Recent Tasks list.

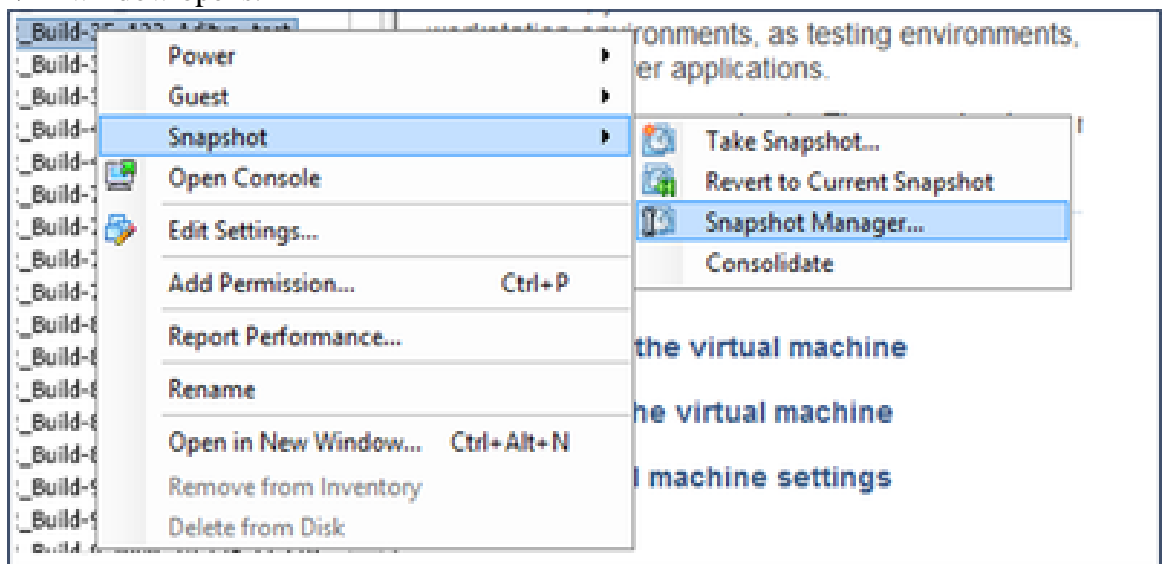


Recent Tasks

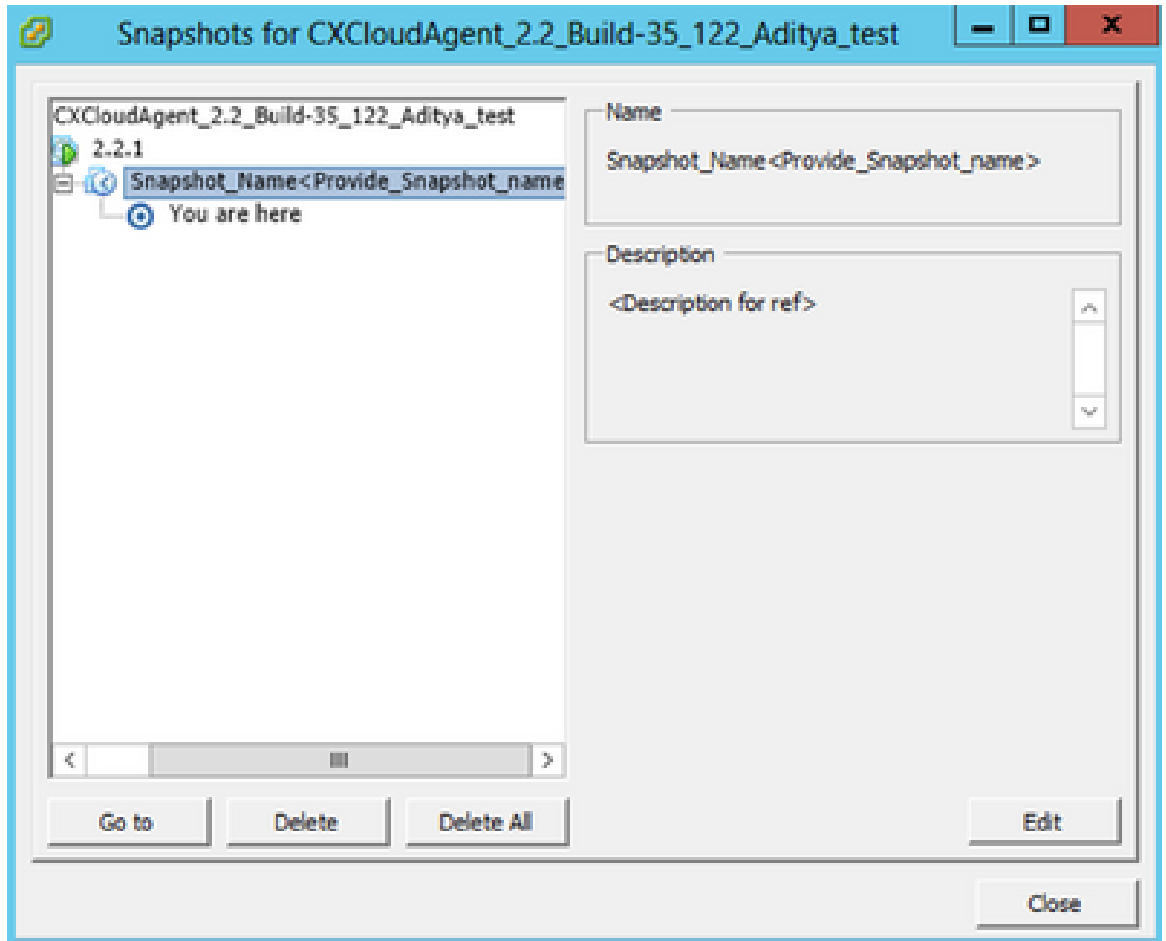
## Restore

To restore the CX Cloud VM:

1. Right-click the VM and select **Snapshot > Snapshot Manager**. The Snapshots of the VM window opens.

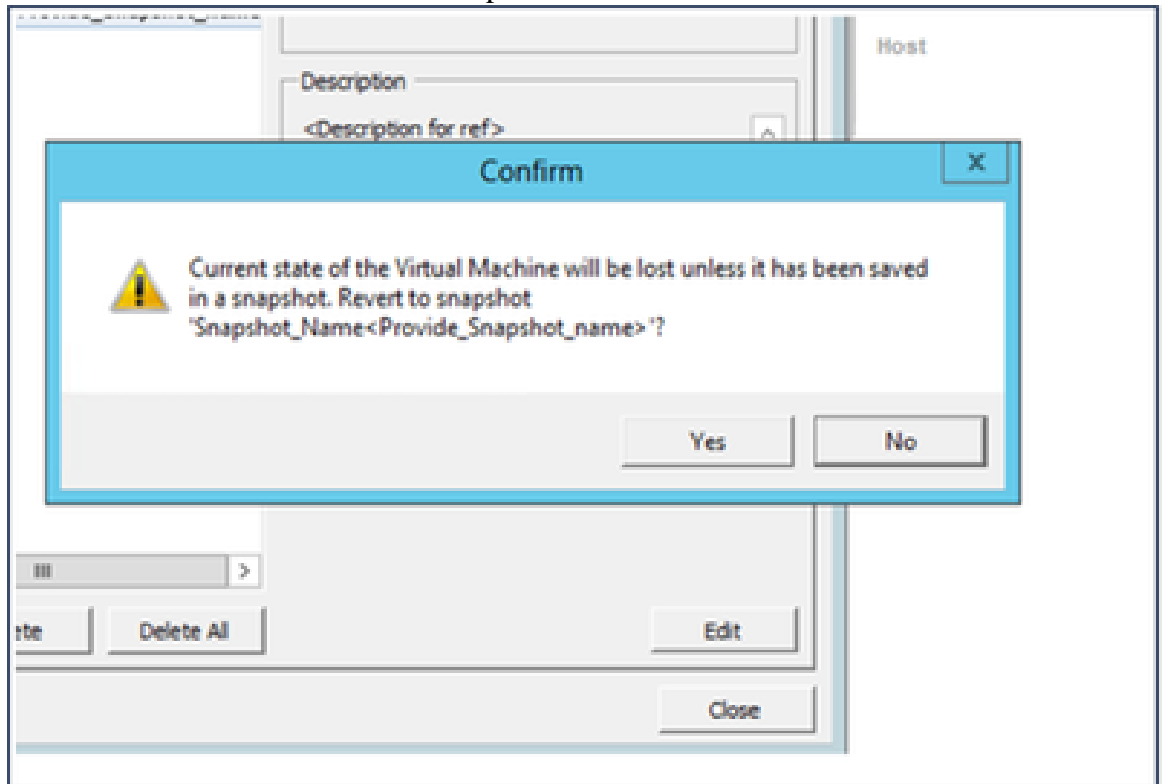


Select VM window



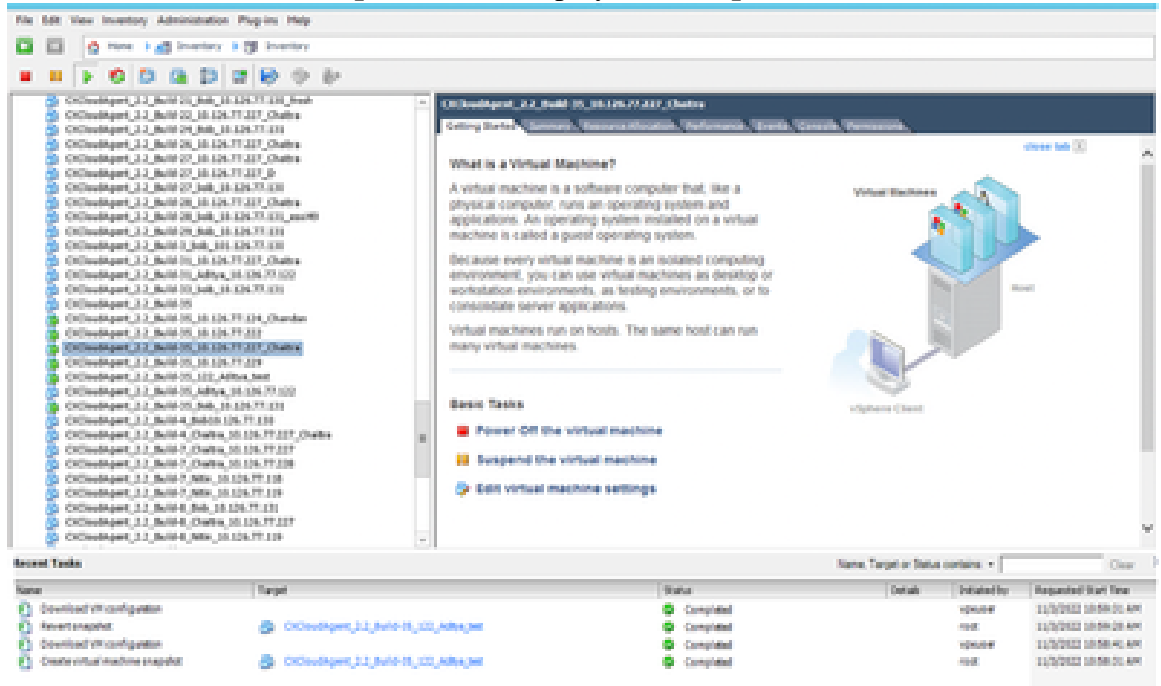
*Snapshots Window*

2. Click **Go to**. The **Confirm** window opens.



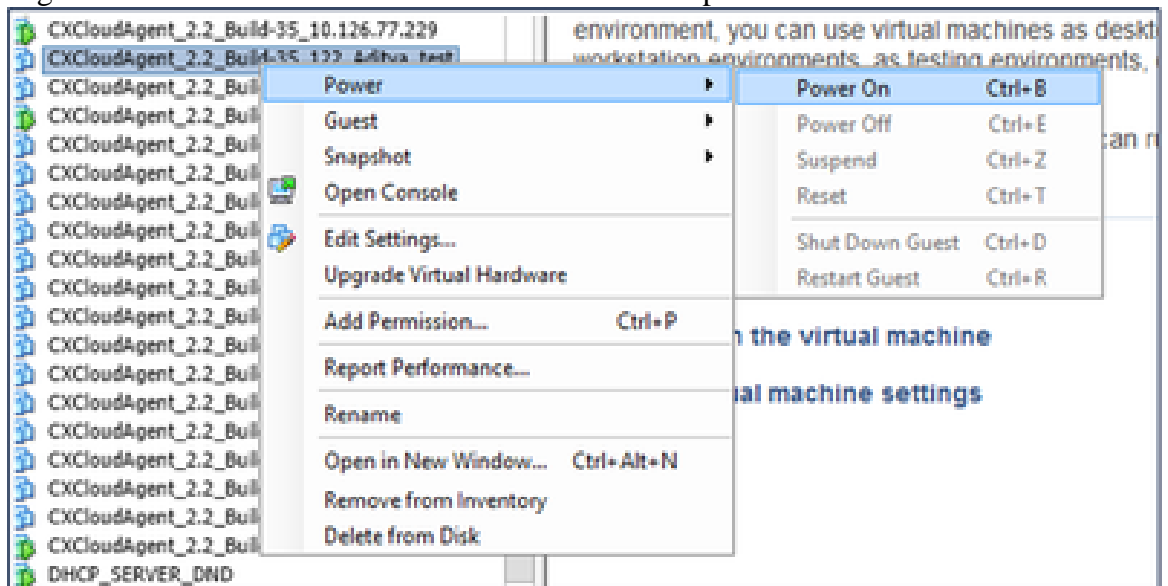
*Confirm Window*

3. Click **Yes**. The **Revert snapshot** status displays as **Completed** in the Recent Tasks list.



Recent Tasks

4. Right-click the VM and select **Power > Power On** to power on the VM.



## Security

CX Cloud Agent assures the customer of end-to-end security. The connection between CX Cloud and CX Cloud Agent is TLS secured. Cloud Agent's default SSH user is limited to perform only basic operations.

## Physical Security

Deploy CX Cloud Agent OVA image in a secured VMware server firm. The OVA is shared securely through Cisco software download center. Bootloader (single user mode) password is set with a randomly unique password. Users must refer to this [FAQ](#) to set this bootloader (single-user mode) password.

## Account Security

During deployment, the cxcadmin user account is created. Users are forced to set a password during the initial configuration. cxcadmin user/credentials are used to access both the CX Cloud Agent APIs and to connect to the appliance over SSH.

cxcadmin users have restricted access with the least privileges. The cxcadmin password follows the security policy and is one-way hashed with an expiry period of 90 days. cxcadmin users can create a cxcroot user using the utility called remoteaccount. cxcroot users can gain root privileges.

## Network Security

The CX Cloud Agent VM can be accessed using SSH with cxcadmin user credentials. Incoming ports are restricted to 22 (SSH), 514(Syslog).

## Authentication

Password based authentication: Appliance maintains a single user (cxcadmin) which enables the user to authenticate and communicate with the CX Cloud Agent.

- Root privileged actions on the appliance using SSH.

cxcadmin users can create cxcroot user using a utility called remoteaccount. This utility displays an RSA/ECB/PKCS1v1\_5 encrypted password which can be decrypted only from the SWIM portal ([DECRYPT Request Form](#)). Only authorized personnel have access to this portal. cxcroot users can gain root privileges using this decrypted password. Passphrase is valid only for two days. cxcadmin users must recreate the account and obtain the password from the SWIM portal post password expiry.

## Hardening

CX Cloud Agent appliance follows Center of Internet Security hardening standards.

## Data Security

CX Cloud Agent appliance does not store any customer personal information. Device credential application (running as one of the pods) stores encrypted server credentials inside secured database. The collected data is not stored in any form inside the appliance except temporarily when it is being processed. Telemetry data is uploaded to CX Cloud as soon as possible after the collection is complete and is promptly deleted from local storage after it is confirmed that the upload was successful.

## Data Transmission

The registration package contains the required unique [X.509](#) device certificate and keys to establish secure connection with Iot Core. Using that agent establishes a secure connection using Message Queuing Telemetry Transport (MQTT) over Transport Layer Security (TLS) v1.2

## Logs and Monitoring

Logs do not contain any form of Personal Identifiable Information (PII) data. Audit logs capture all security-sensitive actions performed on the CX Cloud Agent appliance.

## Cisco Telemetry Commands

CX Cloud retrieves asset telemetry using the APIs and commands listed in the [Cisco Telemetry Commands](#). This document categorizes commands based on their applicability to the Cisco Catalyst Center inventory,

Diagnostic Bridge, Intersight, Compliance Insights, Faults, and all other sources of telemetry collected by the CX Cloud Agent.

Sensitive information within asset telemetry is masked before being transmitted to the cloud. The CX Cloud Agent masks sensitive data for all the collected assets that send telemetry directly to the CX Cloud Agent. This includes passwords, keys, community strings, usernames, and so on. Controllers provide data masking for all controller-managed assets before transferring this information to the CX Cloud Agent. In some instances, controller-managed assets telemetry can be anonymized further. Refer to the corresponding [product support documentation](#) to learn more about anonymizing the telemetry (for example, the [Anonymize Data](#) section of the Cisco Catalyst Center Administrator Guide).

While the list of telemetry commands cannot be customized and the data masking rules cannot be modified, customers can control which assets' telemetry CX Cloud accesses by specifying data sources as discussed in the [product support documentation](#) for controller-managed devices or the Connecting Data Sources section of this document (for Other assets collected by CX Cloud Agent).

## Security Summary

Security Features	Description
Bootloader Password	Bootloader (Single user mode) password is set with a randomly unique password. Users must refer to <a href="#">FAQ</a> to set his bootloader (single user mode) password.
User Access	SSH: <ul style="list-style-type: none"> <li>Access to appliance using excadmin user requires credentials created during installation.</li> <li>Access to appliance using excroot user requires credentials to be decrypted using SWIM portal by authorized personnel.</li> </ul>
User Accounts	<ul style="list-style-type: none"> <li>excadmin: default user account created; User can execute CX Cloud Agent application commands using excli and has least privileges on the appliance; excroot user and its encrypted password is generated using excadmin user.</li> <li>excroot: excadmin can create this user using the utility remoteaccount; User can gain root privileges with this account.</li> </ul>
excadmin password policy	<ul style="list-style-type: none"> <li>Password is one-way hashed using SHA-256 and stored securely.</li> <li>Minimum eight (8) characters, containing three of these categories: uppercase, lowercase, numbers, and special characters.</li> </ul>
excroot password policy	<ul style="list-style-type: none"> <li>excroot password is RSA/ECB/PKCS1v1_5 encrypted</li> <li>The passphrase generated needs to be decrypted in SWIM portal.</li> <li>The excroot user and password is valid for two days and can be regenerated using excadmin user.</li> </ul>

ssh login password policy	<ul style="list-style-type: none"><li>· Minimum of eight characters that contains three of these categories: uppercase, lowercase, numbers, and special characters.</li><li>· Five failed log in attempts lock the box for 30 minutes; Password expires in 90 days.</li></ul>
Ports	Open Incoming Ports – 514(Syslog) and 22 (SSH)
Data Security	<ul style="list-style-type: none"><li>· No Customer information stored.</li><li>· No Device data stored.</li><li>· Cisco Catalyst Center server credentials encrypted and stored in the database.</li></ul>