

CX Cloud Agent Overview v2.2

Contents

[Introduction](#)

[Prerequisites](#)

[Critical Domains Access](#)

[Cisco DNA Center Supported Version](#)

[Supported Browsers](#)

[Supported Product List](#)

[Connecting Data Sources](#)

[Setting Up CX Cloud Agent](#)

[Connecting CX Cloud Agent to CX Cloud](#)

[Adding Cisco DNA Center as a Data Source](#)

[Adding Other Assets as Data Sources](#)

[Overview](#)

[Discovery Protocols](#)

[Connectivity Protocols](#)

[Add Devices Using a Seed File](#)

[TelemetryProcessing Limitations for Devices](#)

[Add Devices Using a New Seed File](#)

[Add Devices Using a Modified Seed File](#)

[Add Devices Using IP Ranges](#)

[Editing IP Ranges](#)

[Scheduling Diagnostics Scans](#)

[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](#)

[ConfigureCisco DNA 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](#)

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

[EnableInformation 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](#)

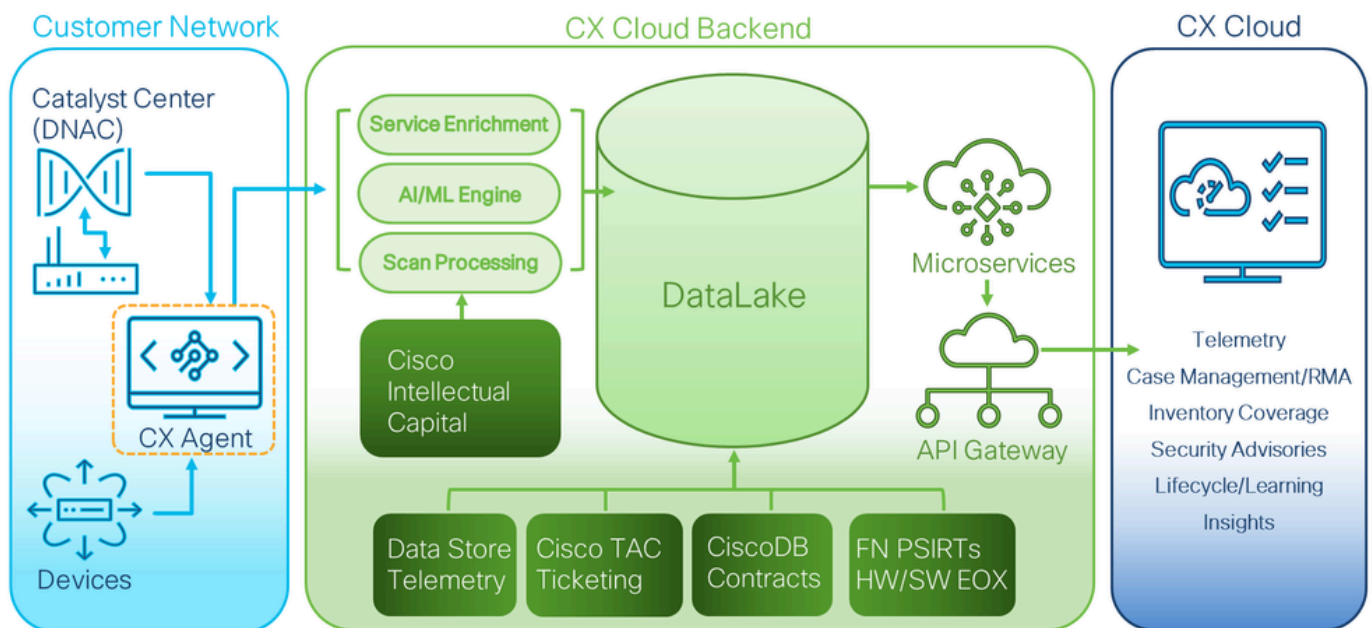
[Security Summary](#)

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.

This guide is specific to CX Cloud Agent v2.2 and onwards. Refer to the [Cisco CX Cloud Agent](#) page to access prior versions.

CX Cloud Architecture



CX Cloud Architecture

 **Note:** Images (and the content within) in this guide are for reference purpose 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).

Requirements to deploy:

- Any of these hypervisors:
 - VMware ESXi version 5.5 or later
 - Oracle Virtual Box 5.2.30 or later
 - Windows Hypervisor version 2012 to 2022
- The hypervisor can host a VM which requires:
 - 8 Core CPU
 - 16 GB Memory/RAM
 - 200GB Disk Space
- 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:

Source		Destination		Protocol	Port	Purpose	Type
IP Address		Hostname					
CX Cloud Agent Traffic							
Data Collection and Transfer							
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.cisco.cloud DNAC Servers Additionally, For Americas region, FQDN: ng.acs.agent.us.cisco.cloud For EMEA region, FQDN: agent.emea.cisco.cloud, and FQDN: ng.acs.agent.emea.cisco.cloud For APJC region, FQDN: agent.apjc.cisco.cloud, and FQDN: ng.acs.agent.apjc.cisco.cloud		HTTPS	TCP/ 443	Data collection via DNAC servers, Data transfer to CX Cloud, including upgrade functionality	Outbound connection to DNAC servers + Outbound to Cisco AWS regional data centers
Agent IP		Customer Device		SNMP	UDP/161	Collect OIDs and MIBs for other assets collected by CX Cloud Agent	Outbound to LAN
Devices		Agent IP		SYSLOG	UDP/514	Stream Syslog messages from Device to Agent	Inbound from LAN
Agent IP		Customer Device		SSH	TCP/22	Collect CLI commands	Outbound to LAN
Agent IP		Customer Device		Echo	TCP/7	Check the device reachability	Outbound to LAN
Agent IP		Customer Device		Telnet	TCP/23	Collect CLI commands	Outbound to LAN
Agent Administration Access							
Support VM		Agent IP		SSH	TCP/22	Agent Maintenance	Inbound from LAN

Other Notes:

- 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 Cisco DNA Center versions are 2.1.2.x to 2.2.3.x, 2.3.3.x, 2.3.5.x and Cisco Catalyst Center Virtual Appliance and Cisco DNA 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 should not be used

Critical Domains Access

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.com	mixpanel.com
cisco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

Domains Specific to CX Cloud Agent OVA

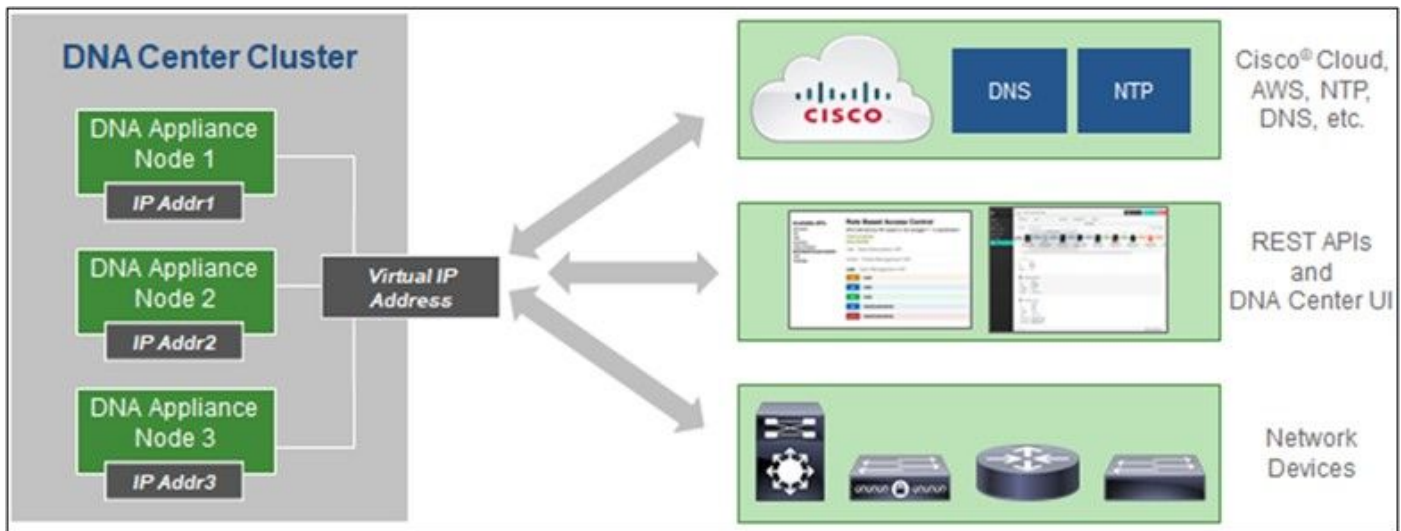
AMERICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.cisco.cloud	agent.us.cisco.cloud	agent.us.cisco.cloud

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.

Cisco DNA Center Supported Version

Supported single node and HA Cluster Cisco DNA Center versions are 2.1.2.x to 2.2.3.x, 2.3.3.x, 2.3.5.x and Cisco Catalyst Center Virtual Appliance and Cisco DNA 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](#).

Connecting Data Sources

To connect data sources:

1. Click cx.cisco.com to log in to CX Cloud.

CX Cloud Home page

2. Select **Admin Settings** icon. The **Data Sources** window opens.








Name	Type	Data Last Updated	Status
Contract	Covered Assets	82 days ago	● Last collection succeeded
Cloud Network	Intersight	-	● First collection pending ⓘ
Data Center Compute	Intersight	-	● First collection pending ⓘ
Meraki	Meraki	33 days ago	● Collection completed
Collaboration	Webex	2 days ago	● Last collection succeeded

Data Sources

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

Add Data Source

Search data sources Q

-  **Cisco DNA Center**
Uses CX Cloud Agent to support the Success Tracks for Campus Network and WAN (supported asset types) Add Data Source
-  **Contracts**
Supports all Success Tracks and offers Add Data Source
-  **Intersight**
Supports the Data Center Compute and Cloud Network Success Tracks Add Data Source
-  **Other Assets**
Uses CX Cloud Agent to support Success Tracks Add Data Source
-  **Smart Accounts**
Supports licensing Add Data Source
-  **Webex**
Supports the Success Track for Collaboration Add Data Source
-  **Cisco Catalyst SD-WAN Manager**
Supports the Success Track for WAN Add Data Source


Add Data Source

4. Click **Add Data Source** to select the applicable data source. If the CX Cloud Agent was not previously set up, the [Setting Up CX Cloud Agent](#) window opens where set up must be completed. If set up is complete, connection continues. Refer to one of the following sections to continue:

[Setting up CX Cloud Agent](#)

[Adding Cisco DNA Center as Data Source](#)

[Adding Other Assets as Data Sources](#)

 **Note:** The **Other Assets** option is only available if direct-device connectivity has not previously been configured.

Setting Up CX Cloud Agent

CX Cloud Agent set up is prompted when connecting data sources if it has not previously been completed.

To set up CX Cloud Agent:

Set Up CX Cloud Agent

Help



SET UP CX CLOUD AGENT

0%

- Review Deployment Requirements
- Accept Strong Encryption Agreement
- Download Image File
- Deploy and Pair with Virtual Machine



Add Cloud Agent to your CX Cloud pit crew

CX Cloud Agent gathers telemetry data from the devices on your network, allowing you to take advantage of all the hyper-relevant insights and trusted expertise that CX Cloud has to offer.

Review deployment requirements

Prepare your network for CX Cloud Agent

CX Cloud Agent runs as a virtual machine (VM), so you'll need a hypervisor to host it.

Before you download and install the image file, make sure CX Cloud Agent is able to connect to the designated server(s) via HTTPS on port 443 using both the FQDN and the IP address:

For **AWS US** data centers:

- FQDN: agent.us.cisco.cloud
- FQDN: ng.acs.agent.us.cisco.cloud
- FQDN: cloudssso.cisco.com
- FQDN: api-cx.cisco.com



Review the [CX Cloud Agent Overview](#) for complete hardware and software prerequisites.



CX Cloud takes security seriously. Review the [Security](#) section of the [CX Cloud Agent Overview](#) to learn how CX Cloud Agent handles and stores your data.

I set up this configuration on port 443

Continue

Review Deployment Requirements


1. Review the **Review deployment requirements** and select the **I set up this configuration on port 443** check box.
2. Click **Continue**. The Set Up CX Cloud Agent - **Accept the strong encryption agreement** window opens.

Set Up CX Cloud Agent
Help

SET UP CX CLOUD AGENT

25%

- Review Deployment Requirements
- Accept Strong Encryption Agreement**
- Download Image File
- Deploy and Pair with Virtual Machine



Accept the strong encryption agreement

Then you can download the image file for the CX Cloud Agent virtual machine.

Instructions

To apply for eligibility to download strong encryption software images:

1. Ensure the address listed in your [Cisco.com User Profile](#) is correct and complete.
2. Read each of the conditions below carefully prior to selecting your answer.

First Name Samuel	Last Name Deckard
Email tadeckar@cisco.com	Cisco User Id CXSuperAdmin38333

Business Division's Function:

Commercial/Civilian entity

Government entity, a Military entity or Defense Contractor

If Government entity, a Military entity or Defense Contractor, Are you in

Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom or the United States.

Yes No

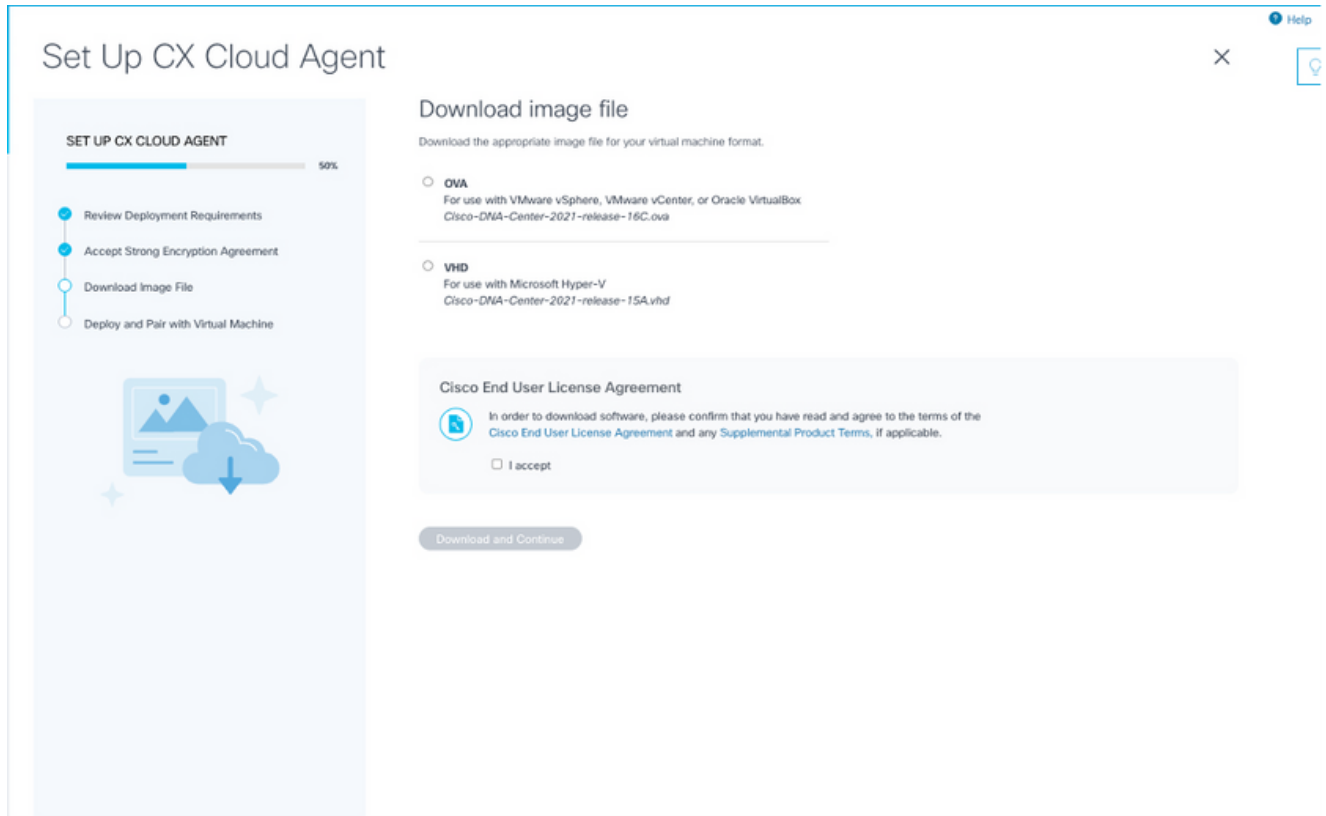
Confirmation

By checking this field, I hereby certify that I, as a duly authorized representative of the organization, understand and agree to abide by the conditions set forth above regarding the usage of Cisco Systems, Inc. hardware and/or software.

[Continue](#)

Encryption Agreement

3. Verify the pre-populated information in the **First Name**, **Last Name**, **E-mail**, and **Cisco User Id** fields.
4. Select the appropriate **Business Division's Function**.
5. Select the **Confirmation** check box to agree to the usage conditions.
6. Click **Continue**. The Set Up CX Cloud Agent - **Download image file** window opens.



Download Image

7. Select the appropriate file format to download the image file required for installation.
8. Select the **I accept** check box to agree to the Cisco End User License Agreement.
9. Click **Download and Continue**. The Set Up CX Cloud Agent - **Deploy and pair with your virtual machine** window opens.
10. Refer to [Network Configuration](#) to obtain the pairing code required in the next section.

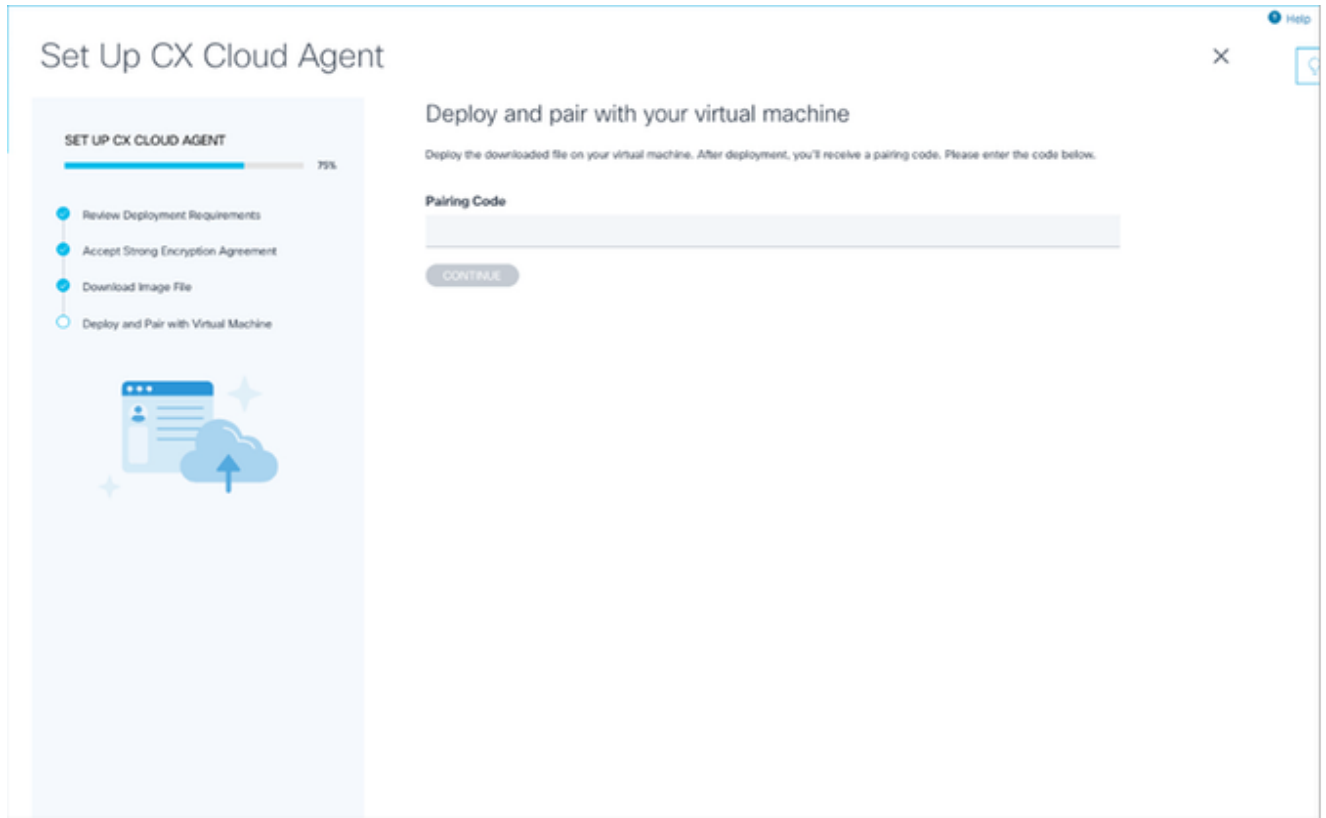
Connecting CX Cloud Agent to CX Cloud

Connecting CX Cloud Agent to CX Cloud is required for telemetry collection to begin so information in the UI can be updated to display the current assets and insights. This section provides details to complete the connection and troubleshooting guidelines.

To connect CX Cloud Agent to CX Cloud:

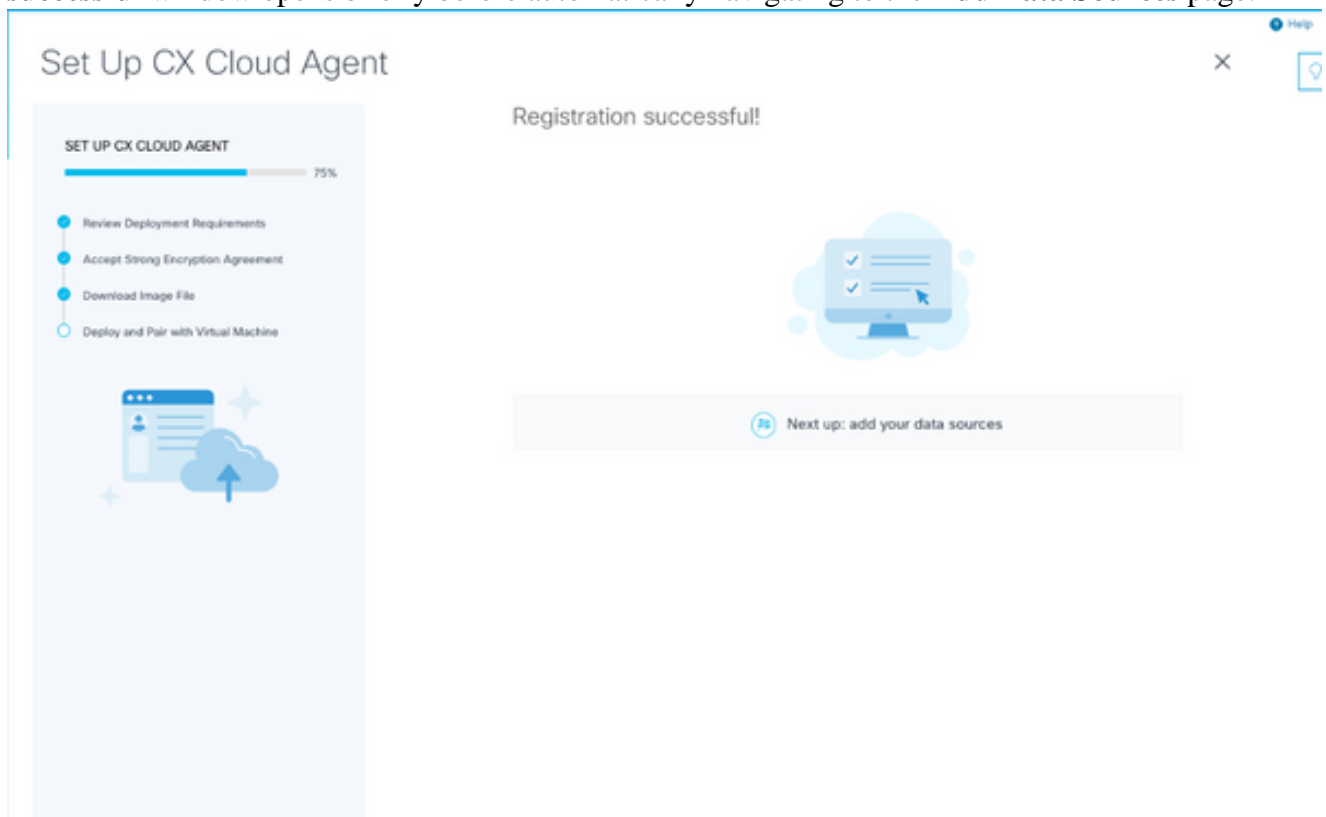
1. Enter the **Pairing Code** provided in the console dialog or Command Line Interface (CLI) of the Virtual Machine connected via Agent.

 **Note:** The pairing code is received after deployment of downloaded OVA file.



Pairing Code

2. Click **Continue** to register the CX Cloud Agent. The **Set Up CX Cloud Agent - Registration successful** window opens briefly before automatically navigating to the **Add Data Sources** page.



Registration Successful

Adding Cisco DNA Center as a Data Source


When **Cisco DNA Center** is selected from the data sources connection window (refer to **Connect Data Sources** image in Connecting Data Sources section), the following window opens:

The screenshot shows the 'Connect to CX Cloud' interface. At the top left, there is a 'Back To Data Sources' link. The main heading is 'Connect to CX Cloud'. Below it, the sub-heading is 'Connect a Cisco DNA Center'. There are four input fields: 'IP Address or FQDN', 'City', 'Username', and 'Password'. Below these fields is the 'Schedule inventory collection' section, which includes three dropdown menus for 'Frequency', 'Time', and 'IST'. A checkbox labeled 'Run the first collection now (this may take up to 75 minutes)' is checked. At the bottom of the form is a 'Connect' button.

Connect to CX Cloud

To add Cisco DNA Center as data source:

1. Enter the Cisco DNA Center IP Address or virtual **IP Address or FQDN**, **City** (location of Cisco DNA Center), **Username** and **Password**.

 **Note:** Do not use an individual cluster node IP.

2. Schedule an inventory collection by entering a **Frequency and Time** to indicate how often the CX Cloud Agent should perform network scans and update information on connected devices.

 **Note:** The first inventory collection may take up to 75 minutes.

3. Click **Connect**. A confirmation displays with the Cisco DNA Center IP address.

Connect to CX Cloud

Connected

**Cisco DNA Center 10.122.58.165**
Inventory collection runs every day At 02:00 AM IST
First collection will run immediately after data sources are added!

Connect another data source to CX Cloud Agent?

+ Add Another Cisco DNA Center

Done

Successfully Connected


4. Click **Add Another Cisco DNA Center**, **Done** or **Back to Data Sources** to navigate back to the **Data Sources** window.


Adding Other Assets as Data Sources

Overview

Telemetry collection has been extended to devices not managed by the Cisco DNA 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 Cisco DNA Centers within the infrastructure monitored by CX Cloud. Users can also connect CX Cloud Agent directly to other hardware assets in their environment, up to 10,000 directly connected devices.

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 should 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.

 **Note:**
Either the seed file or IP range can be used. It is not possible to change this selection after the initial set-up.

 **Note:**
An initial seed file can be replaced with another seed file while an initial IP range can be edited to a new IP range.

When **Other Assets** is selected from the data sources connection window, the following window opens:



Connect to CX Cloud

How would you like to connect these assets?

Upload a seed file (recommended)

Add your devices to a [Seed File Template](#). You can reupload this file later if you need to make changes.

Provide an IP Address range

Select any connection method(s). At least one SNMP and SSH are required.

SNMP v3

SNMP v2c

SSH v2

[More](#)

These options support legacy products

SSH v1

Telnet

[Continue](#)



Configure connection to CX Cloud

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 below 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 will, 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 should 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.

Add Devices Using a Seed File


About Seed File

A seed file is a comma-separated values (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 should 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 will attempt to connect to the devices but may not 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.

The following 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	SNMPv3 protocol permits Authentication via either

Seed File Column	Column Header / Identifier	Purpose of the Column
	can be MD5 or SHA	the MD5 or SHA Algorithm. If the device is configured with secure Authentication, then the respective Auth Algorithm must be provided. Note: MD5 is considered insecure, and SHA should be used on all devices that 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	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. Note: 56-bit keys used by DES are considered too short to provide cryptographic security, and that 3DES should be used on all devices that support it.
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.
J	cliProtocol: values can be 'telnet', 'sshv1', 'sshv2'. If empty will 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.

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

Telemetry Processing Limitations 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 device telemetry.
- Telemetry attributes may be inaccurate or missing in the CX Cloud **Assets** page for devices that are not part of the Campus Success Track.
- If a device from the seed file or IP range collections is also part of the Cisco DNA Center inventory,

the device is reported only once for the Cisco DNA Center entry. The seed file/ IP range entry is not collected or processed to avoid duplication.

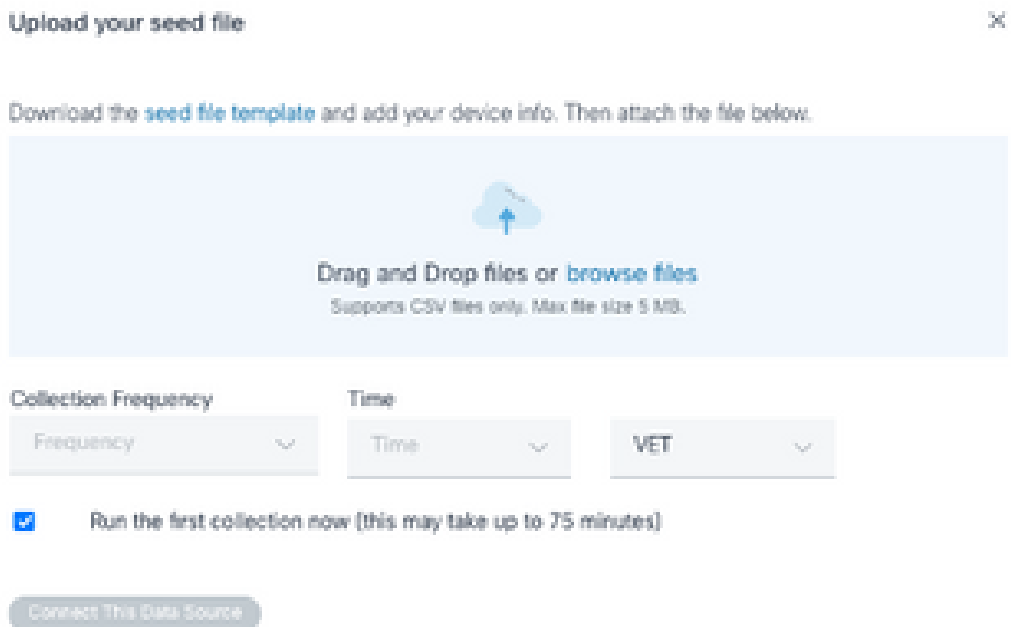
Add Devices Using a New Seed File

To add devices using a new seed file:

1. Download the seed file template (PDF) using the embedded link in this document (refer to **About the Seed File**) or through a link in the **Configure Connection to CX Cloud** window.

 **Note:** The link in the **Configure Connection to CX Cloud** window is no longer available once the initial seed file has been downloaded.

Configure connection to CX Cloud




Configure connect to CX Cloud window


2. Open an Excel spreadsheet (or any preferred spreadsheet) and enter the headings as shown in the template.
3. Enter data manually or import data into the file.
4. Once complete, save the template as a .csv file to import the file into CX Cloud Agent.

Configure connection to CX Cloud

Upload your seed file ✕



You've reached your file limit.
To upload a new file, please remove an existing file.

	nextgen_seedfile.csv Completed.	Delete
---	------------------------------------	------------------------

Schedule Inventory Collection

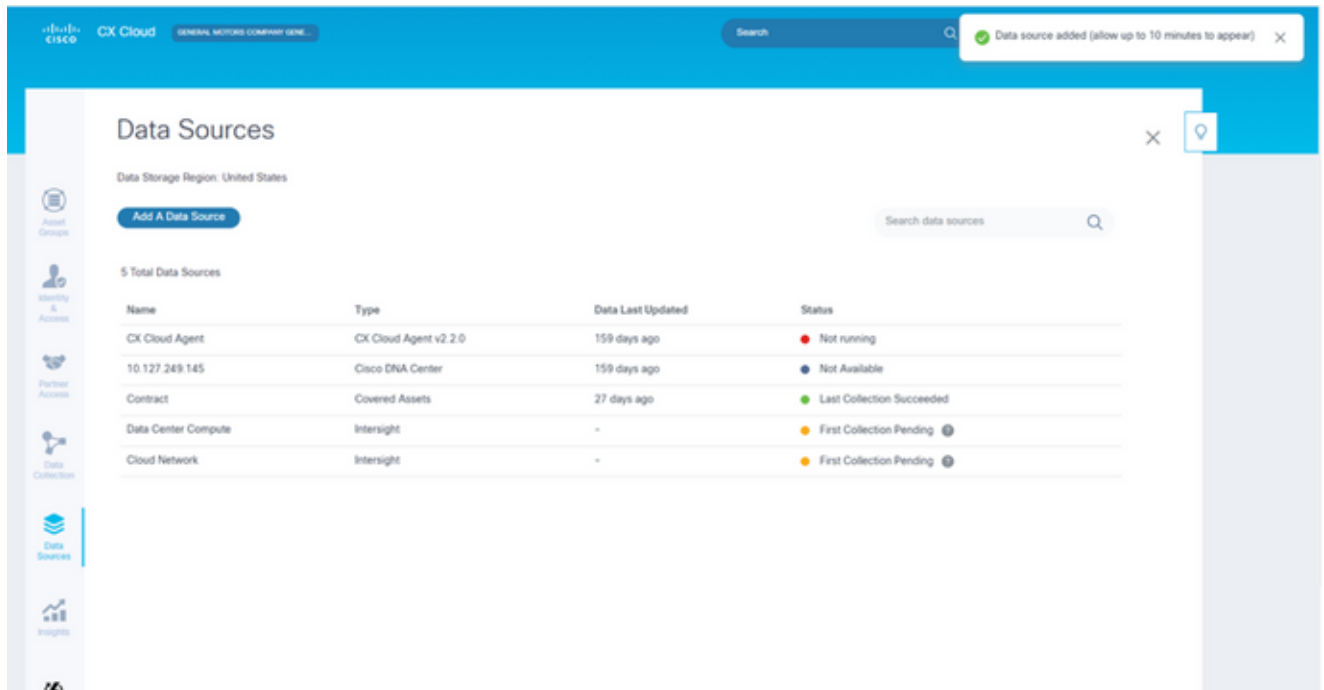
Collection Frequency	Time	Day	
Weekly ▼	12:00am ▼	VET ▼	Sunday ▼

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

[Connect](#)

Upload seed file window

5. In the **Upload your seed file** window, drag-and-drop the newly created .csv file or click **browse files** and navigate to the .csv file.
6. Complete the **Schedule Inventory Collection** section and click **Connect**. The **Data Sources** window opens, displaying a confirmation message.
7. 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.




Confirmation message

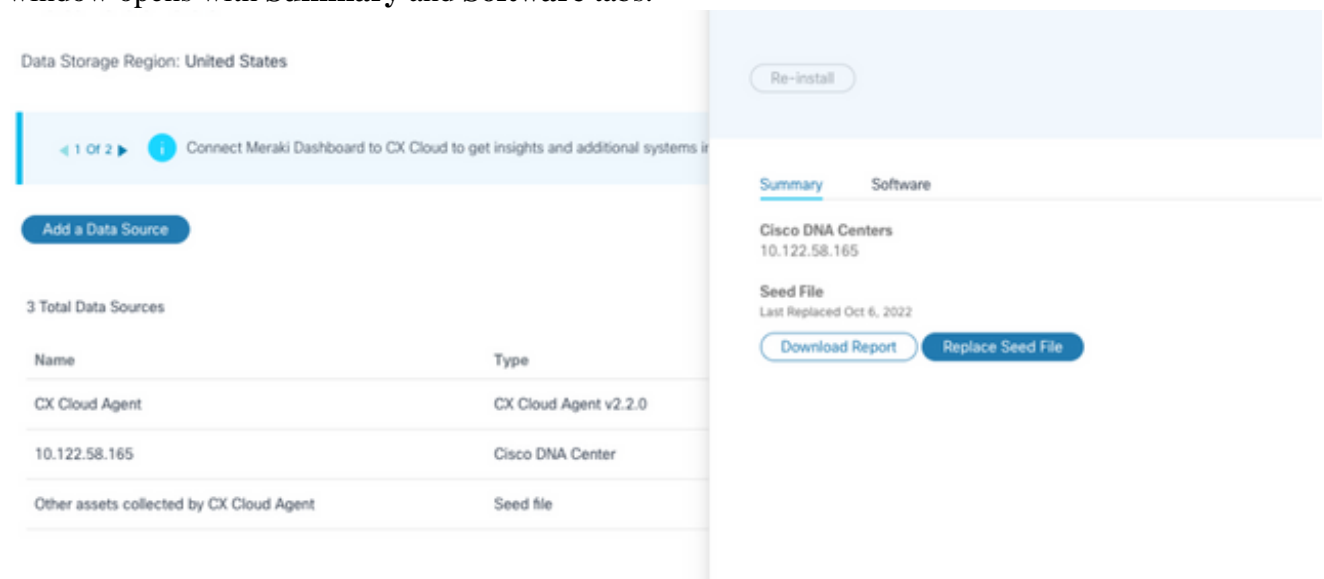
Add Devices Using a Modified Seed File

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.

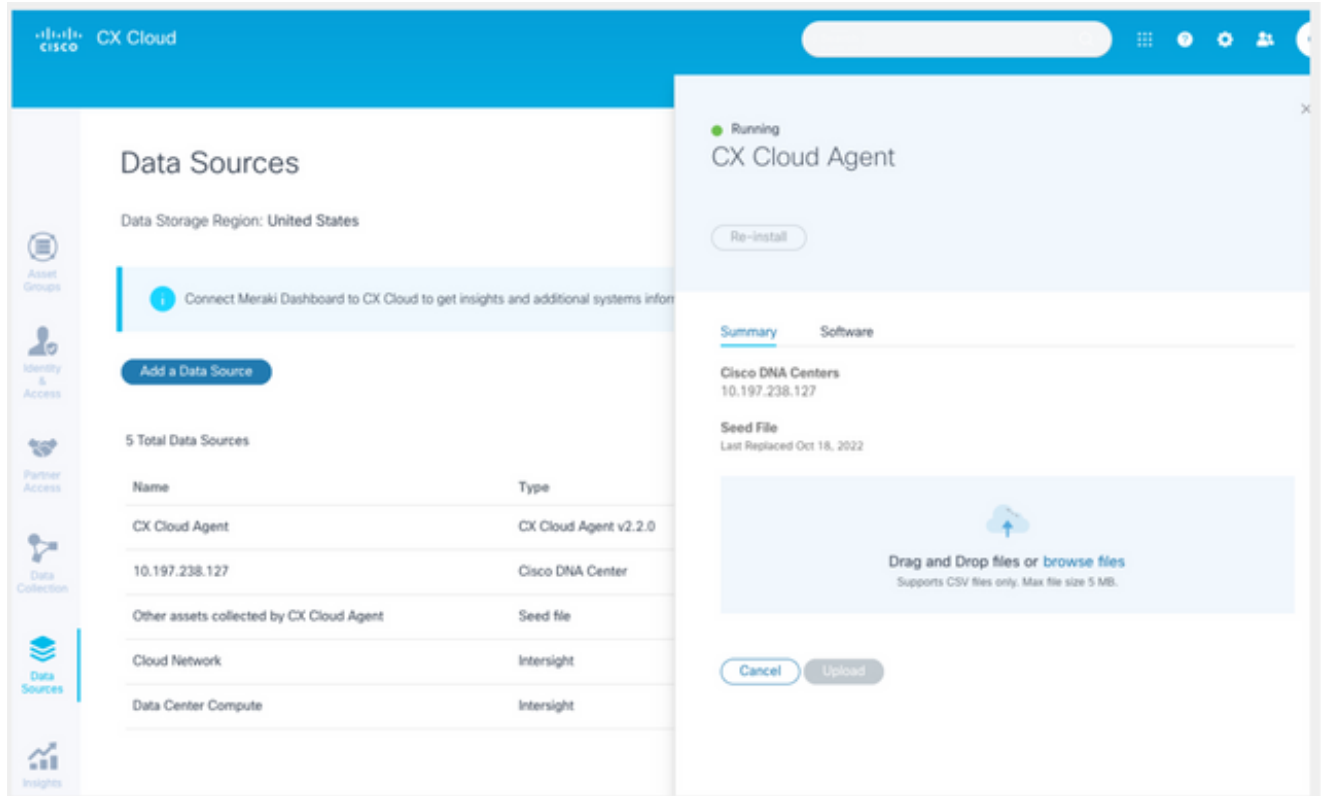
 **Note:** To add assets to the seed file, append those assets to the previously created seed file and reload the file. This is necessary since uploading a new seed file replaces the current seed file. Only the latest uploaded seed file is used for discovery and collection.

2. From the **Data Sources** page, select a data source that has a **Type** of CX Cloud Agent. A details window opens with **Summary** and **Software** tabs.



Details Window

3. Click **Download Report** to generate a report on all assets for the selected data source. The report provides information on the device IP Address, Serial Number, Reachability, Command Type, Command Status, and Command Error, if applicable.
4. Click **Replace Seed File**. The **CX Cloud Agent window** opens.



CX Cloud Agent Window

5. Drag and drop the modified seed file into the window or browse to the file and add it in the window.
6. Click **Upload**.


Add Devices Using IP Ranges

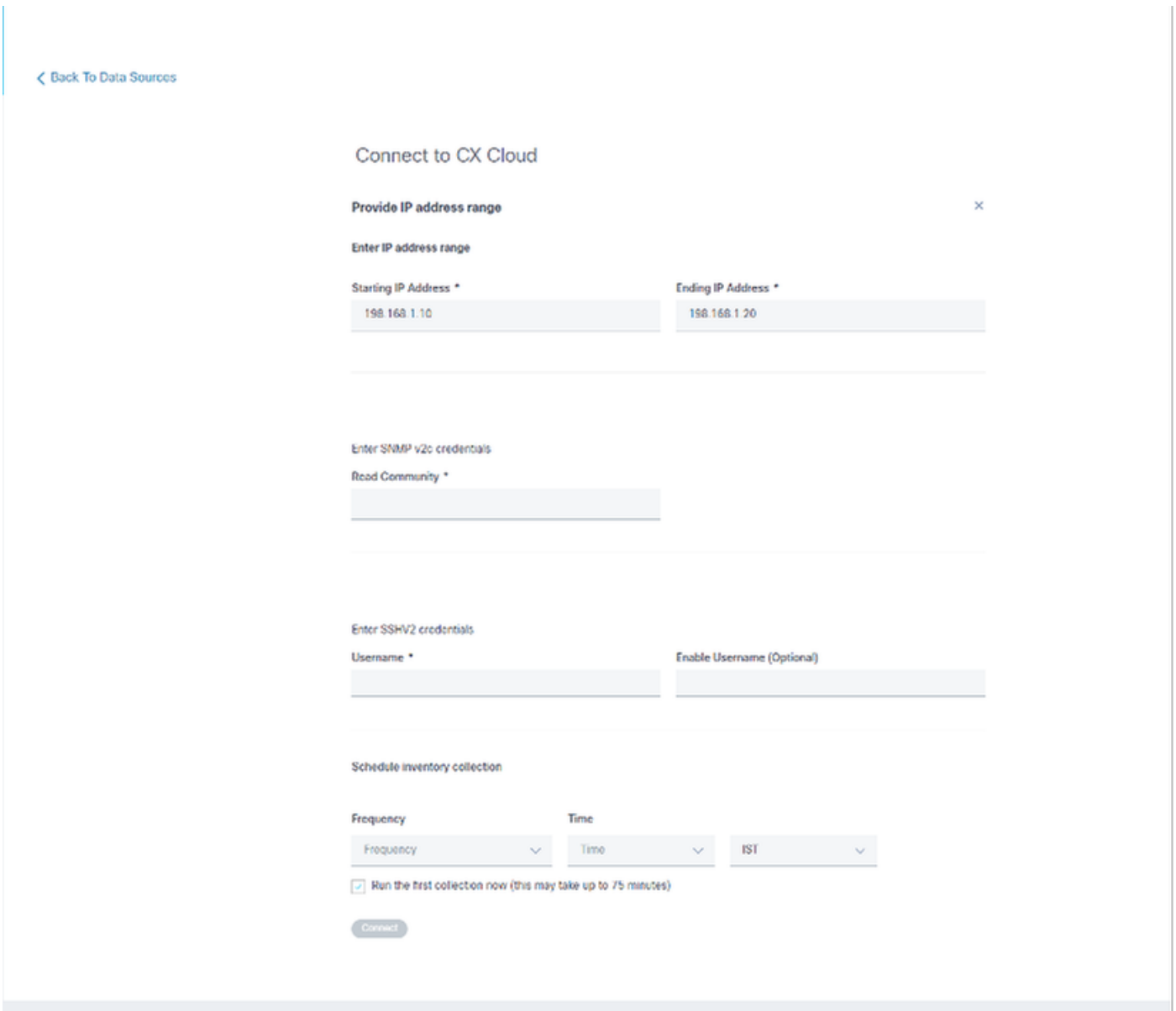
IP ranges allow users to identify hardware assets and, subsequently, collect telemetry from those devices based on IP addresses. The devices for telemetry collection can be uniquely identified by specifying a single network-level IP range, which should be scanned by CX Cloud Agent using the SNMP protocol.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



Initial IP address range window

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.

To add devices using the IP range:

1. In the **Configure connection to CX Cloud** window, select the **Provide an IP Address range** option.

Configure connection to CX Cloud

Provide IP address range

✕

Enter IP address range

Starting IP Address *

Ending IP Address *

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

Add devices using IP addresses form

2. Complete the form with the relevant information.
3. Several connection options can be selected. The following screens display the configuration credentials for the options. Refer to [About the Seed File](#) for a description of the credential fields for each connection option.

Configure connection to CX Cloud

Provide IP address range

×

Enter IP address range

Starting IP Address *

Ending IP Address *

Enter SNMP v3 credentials

Username

Engine ID

Authorization Algorithm

Authorization Password

Privacy Algorithm

Privacy Password

SNMP v3 Credentials

Enter SNMP v2c credentials

Read Community *

Enter SSHV2 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

Enter SSHV1 credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

SNMP v2, SSHV2, and SSHV1 Credentials

Enter Telnet credentials

Username

Enable Username (Optional)

Password

Enable Password (Optional)

Schedule Inventory Collection

Collection Frequency

Time

IST

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

Connect

Telnet credentials and network scan scheduling

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

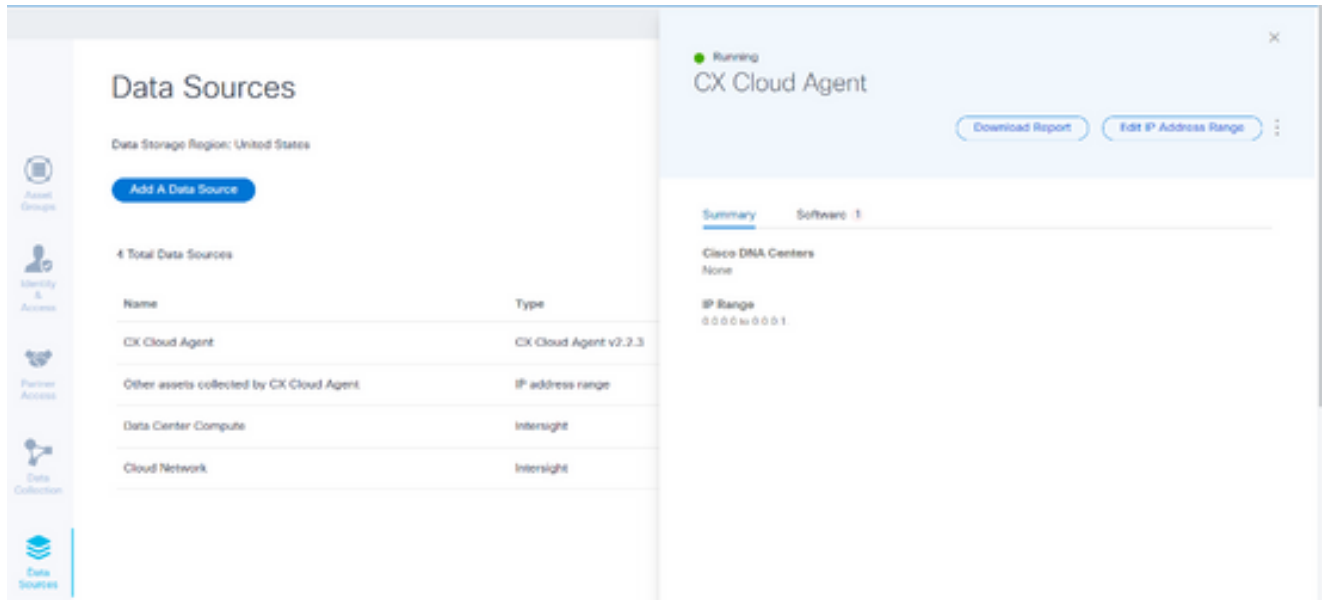
Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.2.0	159 days ago	Not running
10.127.249.145	Cisco DNA Center	159 days ago	Not Available
Contract	Covered Assets	27 days ago	Last Collection Succeeded
Data Center Compute	Interight	-	First Collection Pending
Cloud Network	Interight	-	First Collection Pending

Confirmation

Editing IP Ranges

To edit an IP range;

1. Navigate to the **Data Sources** window.



Data Sources

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.

[← Back To Data Sources](#)

Connect to CX Cloud

Provide an IP address range

[Edit The Protocols](#)

Enter IP address range

Starting IP address *

0.0.0.0

Ending IP address *

0.0.0.1

Cancel

Continue

Provide an IP Range

4. Update the new IPs in the **Starting IP address** and **Ending IP address** fields.
5. Click the **Edit the Protocols** link. The **Connect to CX Cloud – Select a protocol** window opens.

[← Back To Data Sources](#)

Connect to CX Cloud

Select a protocol

At least one discovery and collection method are required.

Discovery options

- SNMP v3 (recommended)
- SNMP v2c

Collection options

- SSH v2 (recommended)
- SSH v1
- Telnet

Cancel

Continue

Select a Protocol

6. Select the applicable protocols by clicking the appropriate check boxes.
7. Click **Continue**. The **Provide an IP address range** window opens.

Provide an IP address range

[Edit The Protocols](#)

Enter IP address range

Starting IP address *

0.0.0.0

Ending IP address *

0.0.0.2

Enter SNMP v2c credentials

Read community *

Enter SSH v1 credentials

Username *

Enable Username (Optional)

Password *

Enable Password (Optional)

Cancel


Connect

Enter Credentials

8. Enter configuration credentials.
9. Click **Connect**. The **Data Sources** window opens, displaying a confirmation message.

The screenshot shows the Cisco CX Cloud interface. At the top, there is a blue header with the Cisco logo, 'CX Cloud', and 'FBI/UNITED STATES'. A search bar is visible. A notification banner at the top right states 'IP address range updated'. The main content area is titled 'Data Sources' and includes a search bar and a table of data sources. The table has columns for Name, Type, Data Last Updated, and Status.

Name	Type	Data Last Updated	Status
CX Cloud Agent	CX Cloud Agent v2.2.3	3 minutes ago	Running
Other assets collected by CX Cloud Agent	IP address range	3 minutes ago	1 unreachable
Data Center Compute	Intersight	-	First Collection Pending
Cloud Network	Intersight	-	First Collection Pending

 **Note:** The confirmation message does not ensure that the devices in the edited range are reachable, and credentials have been accepted.

About Devices Discovered from Multiple Controllers

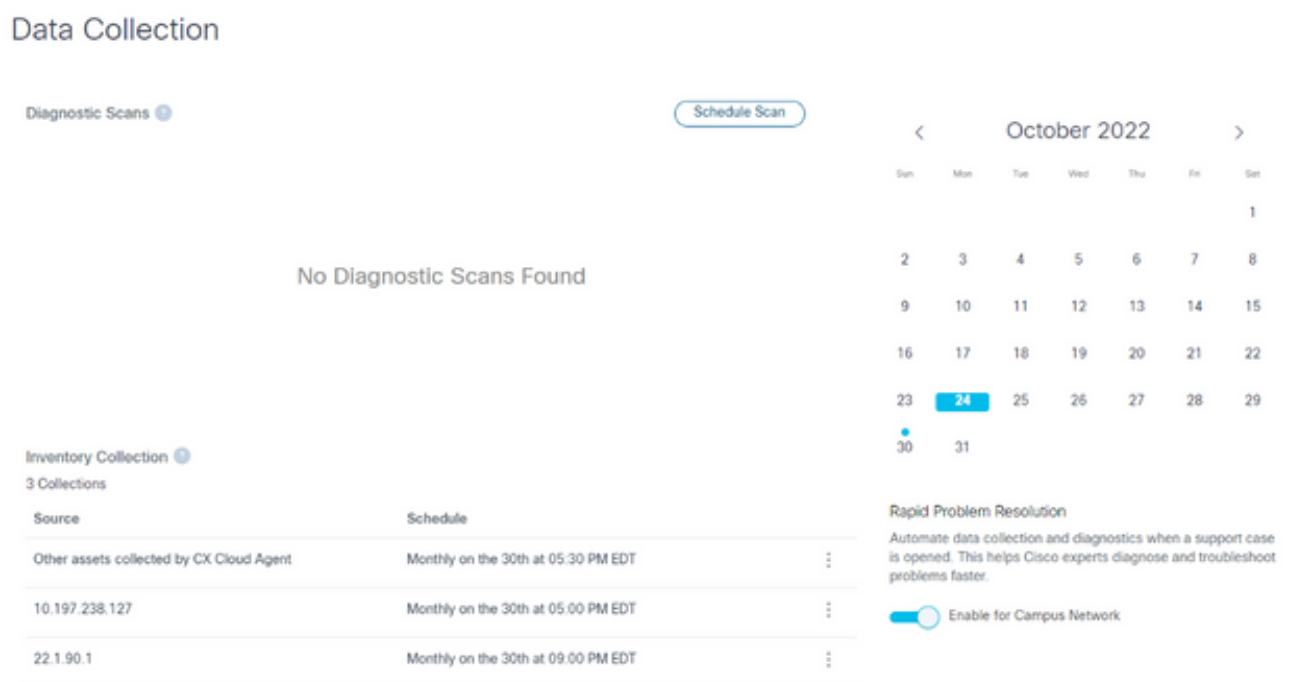
It is possible that some devices could be discovered by both the Cisco DNA Center and direct device connection to CX Cloud Agent causing duplicate data to be collected from those devices. To avoid collecting duplicate data and having only one controller manage the devices, a precedence for which CX Cloud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

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

Scheduling Diagnostics Scans

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**.



The screenshot shows the 'Data Collection' interface. At the top, there is a 'Diagnostic Scans' section with a 'Schedule Scan' button. Below this, a message states 'No Diagnostic Scans Found'. To the right, a calendar for October 2022 is visible, with the 24th highlighted. Below the calendar, there is a section for 'Inventory Collection' with 3 collections. A table lists these collections with their sources and schedules.

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

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

Schedule: Frequency at Time EST Save Changes

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

Add >

< Remove

<input type="checkbox"/>	Device	Source IP	IP Address
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.

Data Collection

Diagnostic Scans 2 Scans Schedule Scan

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

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

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 Interstage. Enable or disable tech support bundle collection in Interstage for these Success Tracks.

[View detailed instructions](#)

Data Collection with Edit and Delete Schedule options

Deployment and Network Configuration

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

- To select VMware vSphere/vCenter Thick Client ESXi 5.5/6.0 go to [Thick Client](#)
- To select VMware vSphere/vCenter Web Client ESXi 6.0 go to [Web Client](#) or [vSphere Center](#)
- To select Oracle Virtual Box 5.2.30 go to [Oracle VM](#)
- To select Microsoft Hyper-V go to [Hyper-V](#)

OVA Deployment

Thick Client ESXi 5.5/6.0 Installation

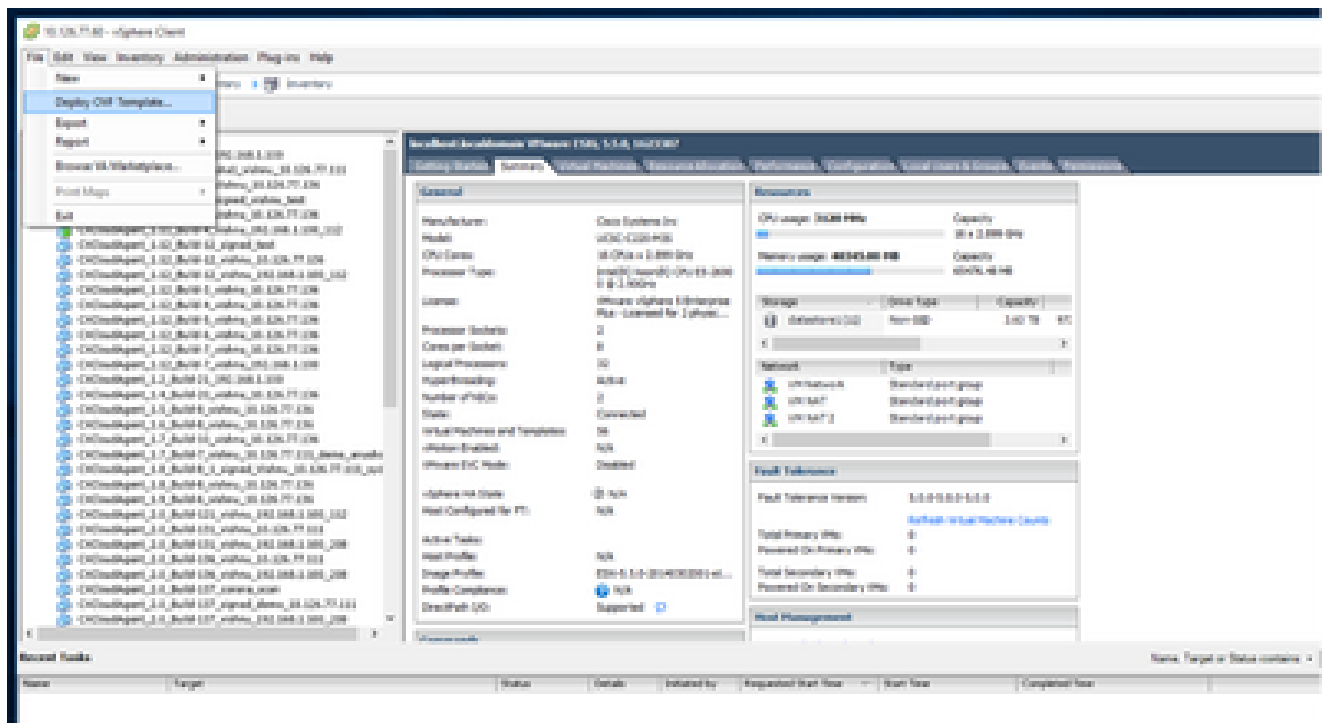
This client allows deployment of CX Cloud Agent OVA by use of the vSphere thick client.

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



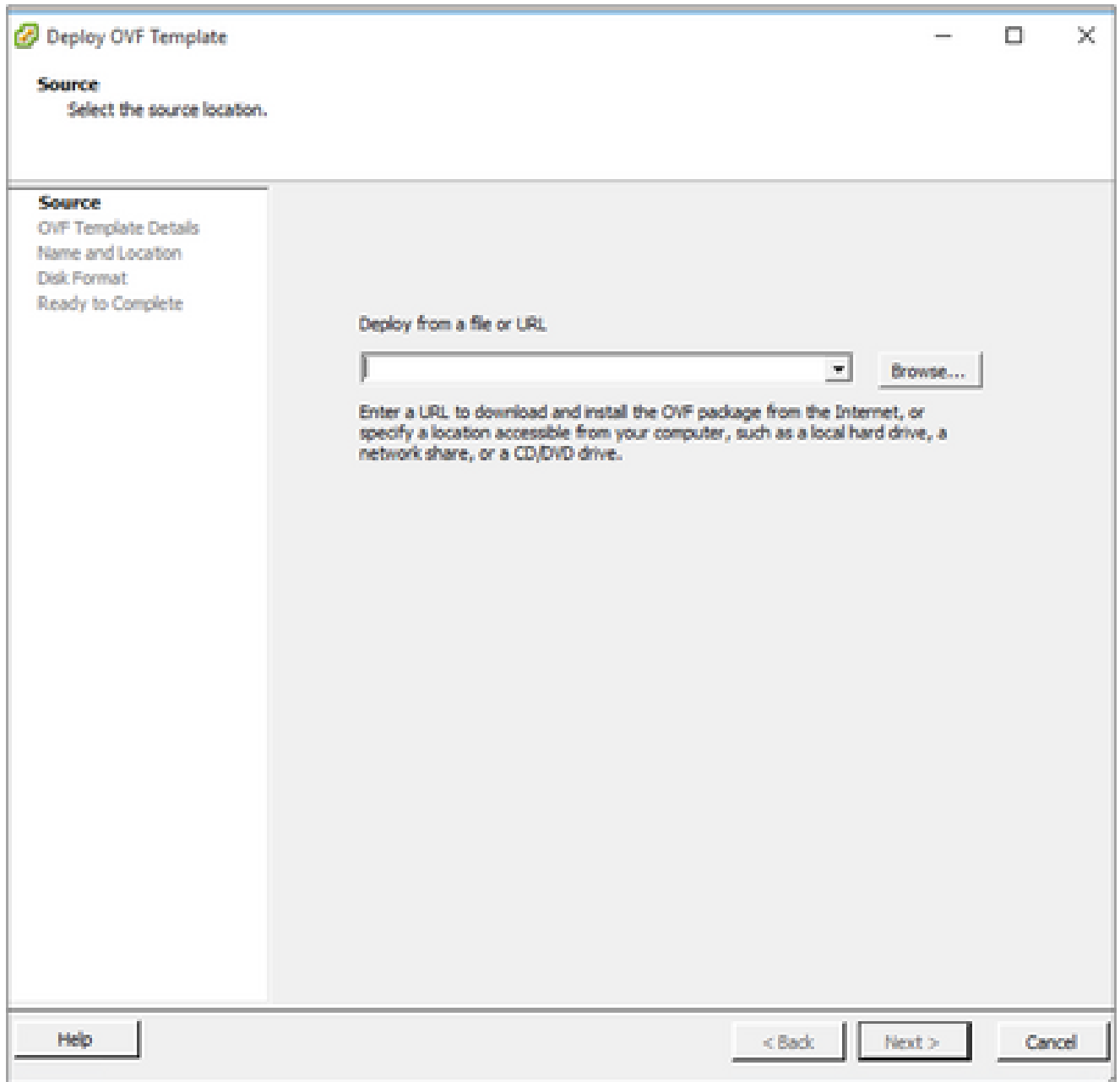
Login

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.

SOURCE

OVF Template Details

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

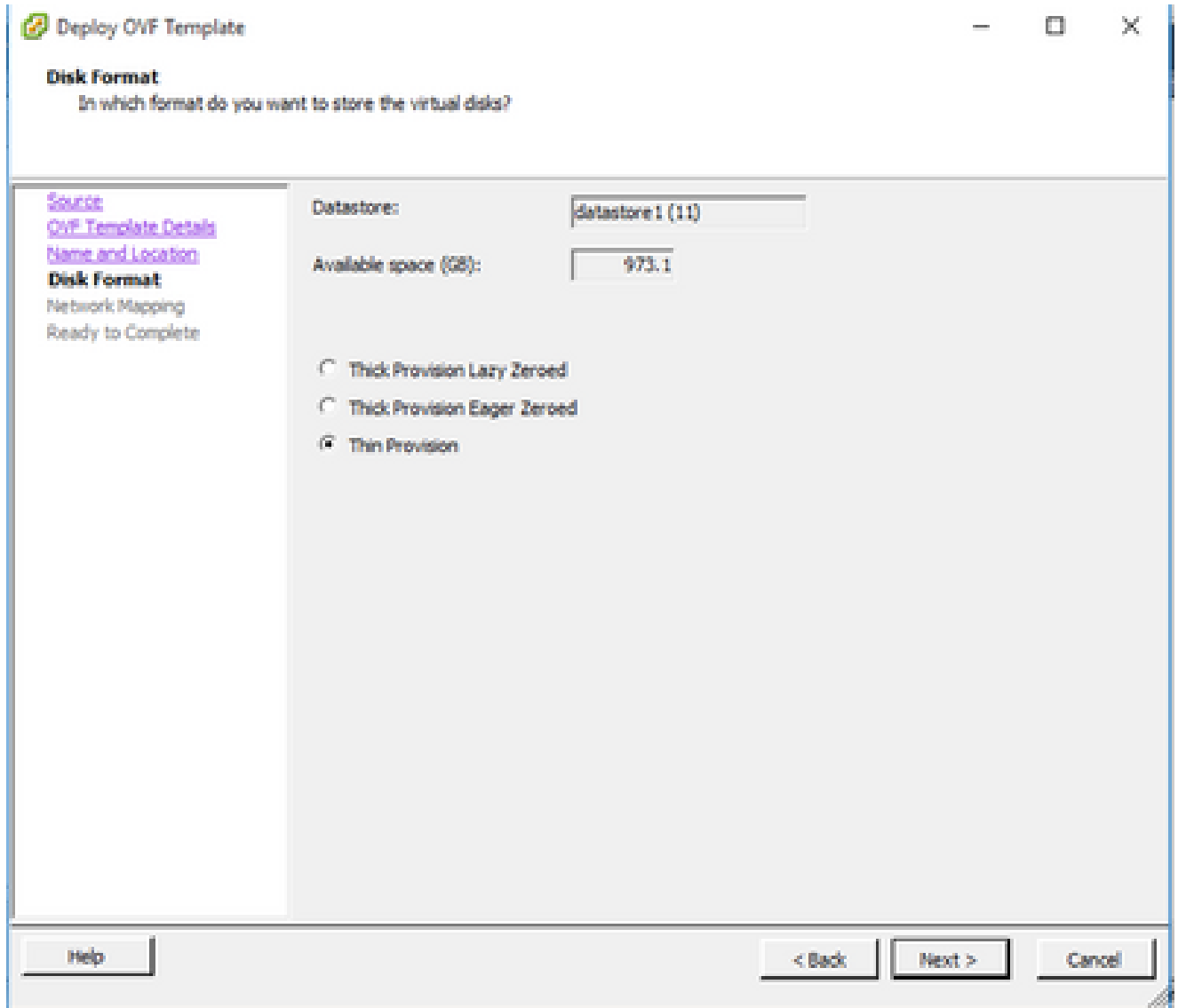
Name:
C:\CloudAgent_2.0_Build-144_0000

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

Help < Back Next > Cancel

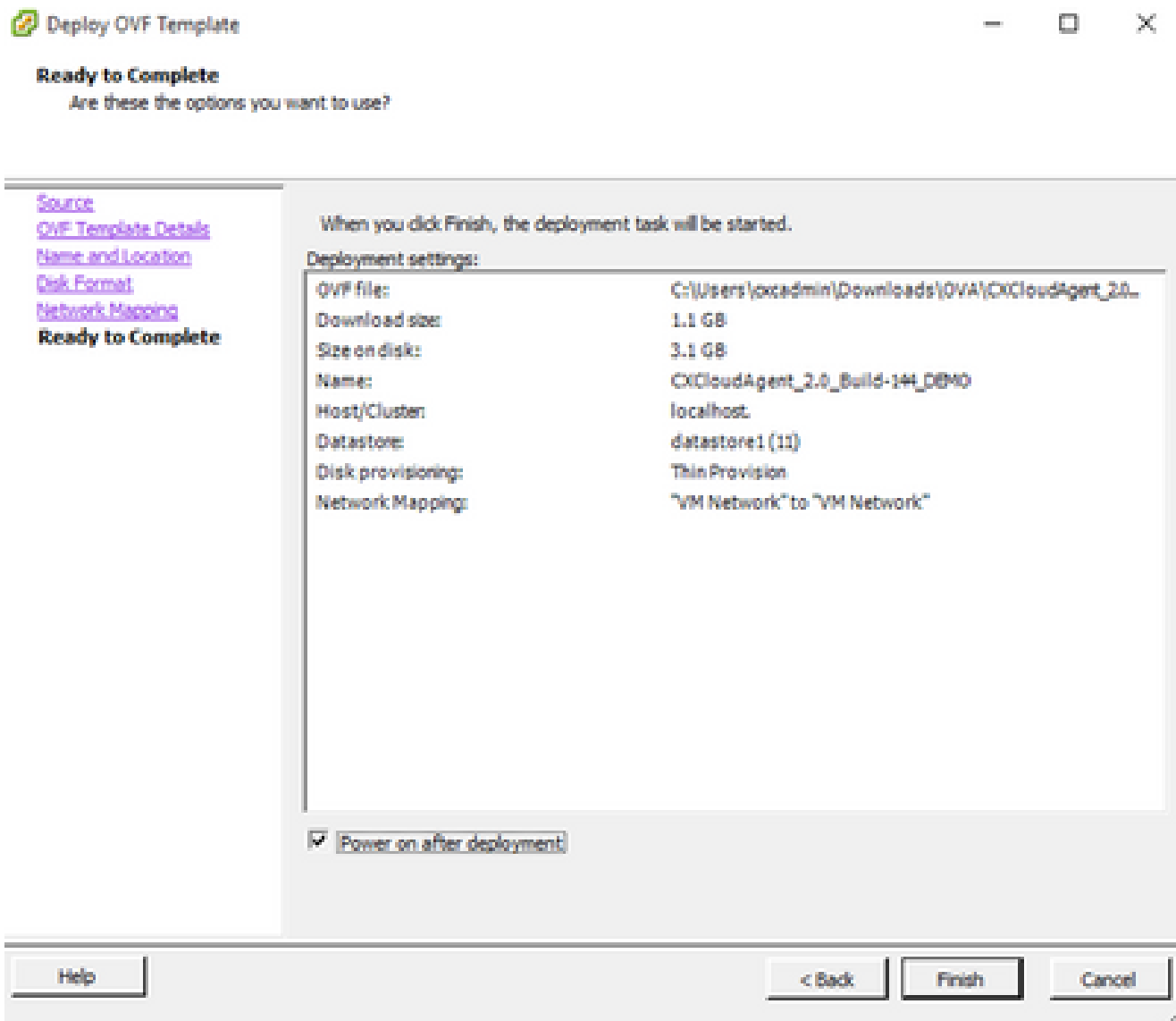
Name and Location

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



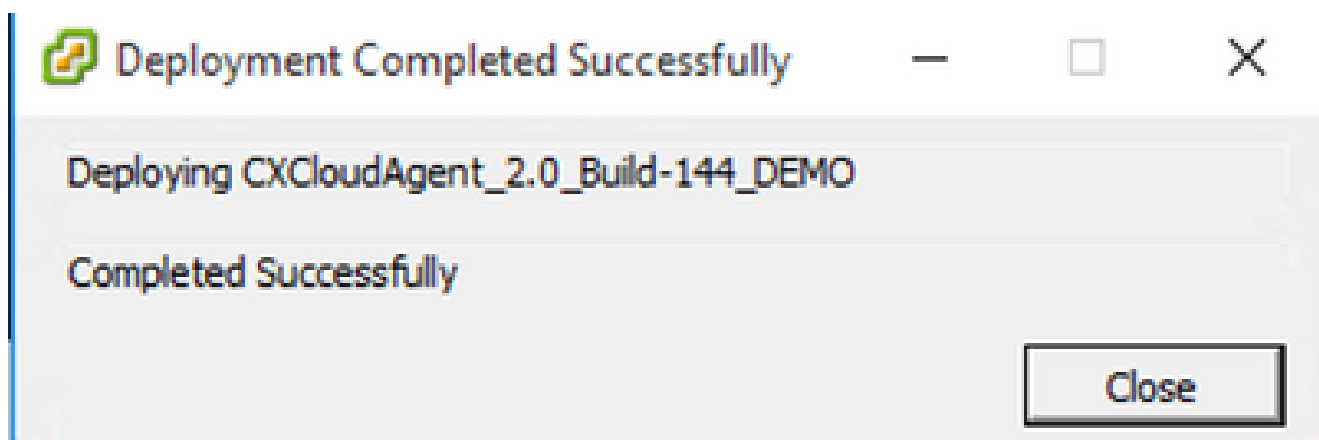
Disk Format

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



Ready to Complete

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



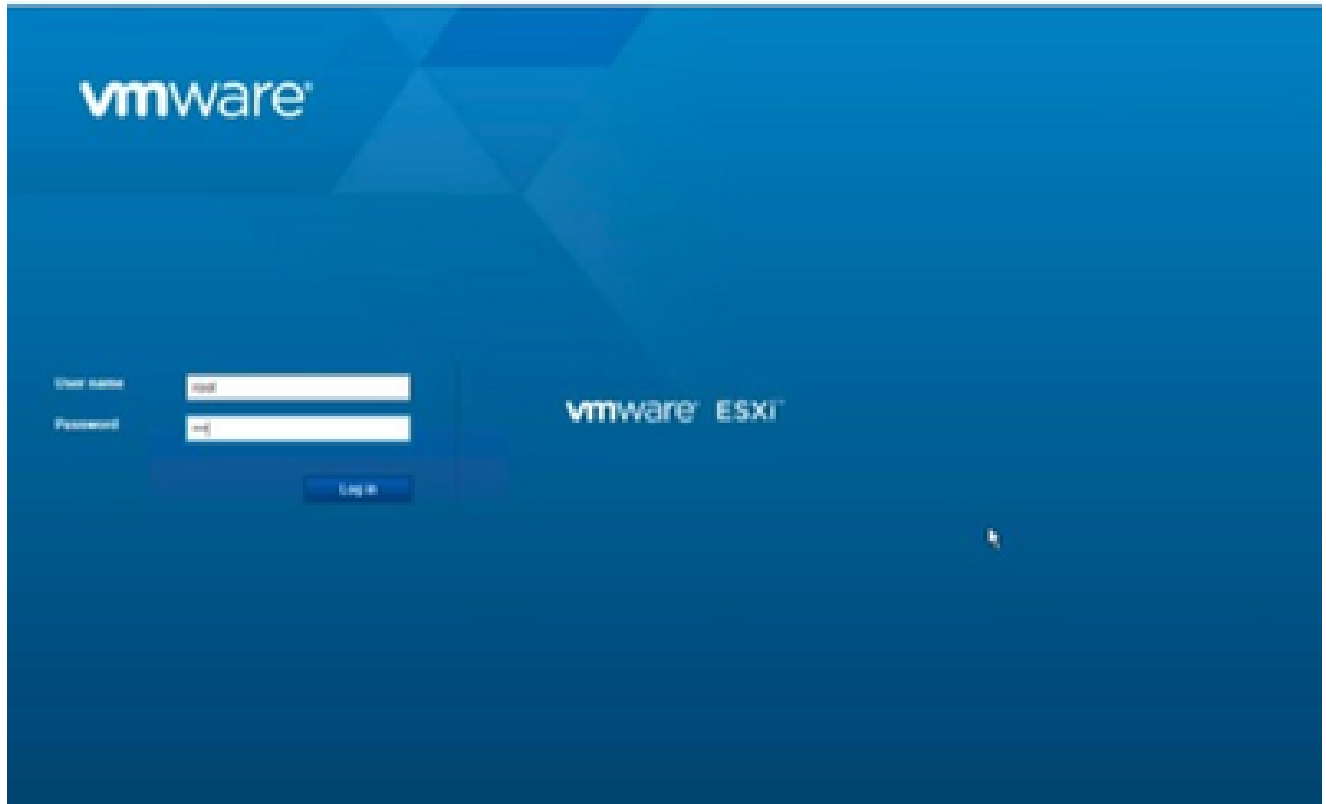
Deployment Complete

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

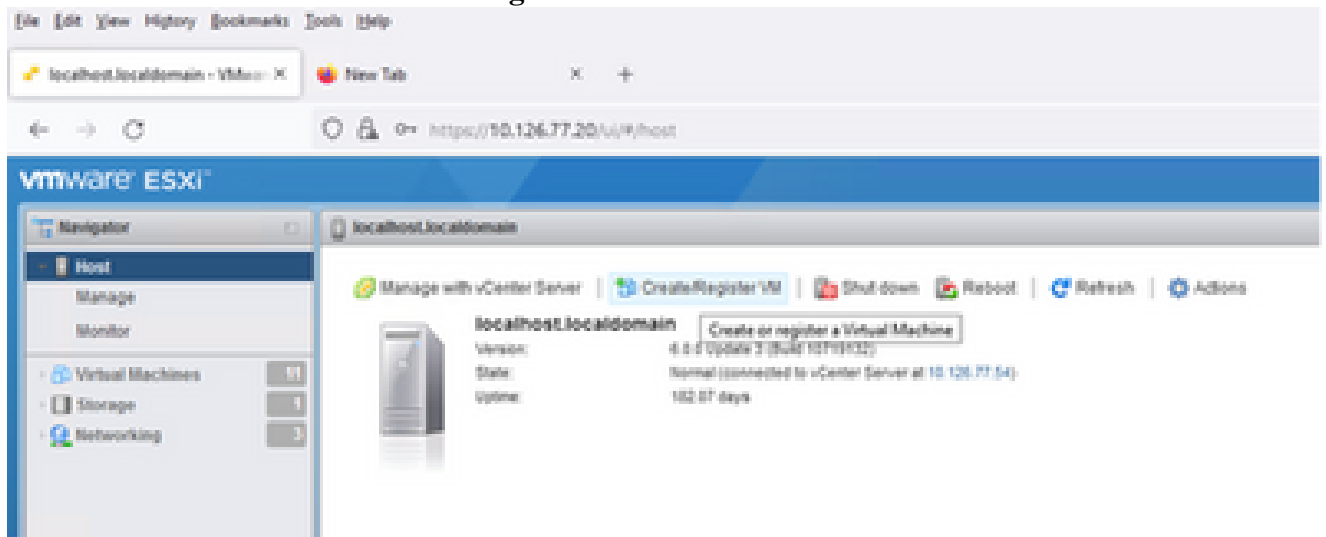
This client deploys CX Cloud Agent OVA by use of the vSphere web.

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



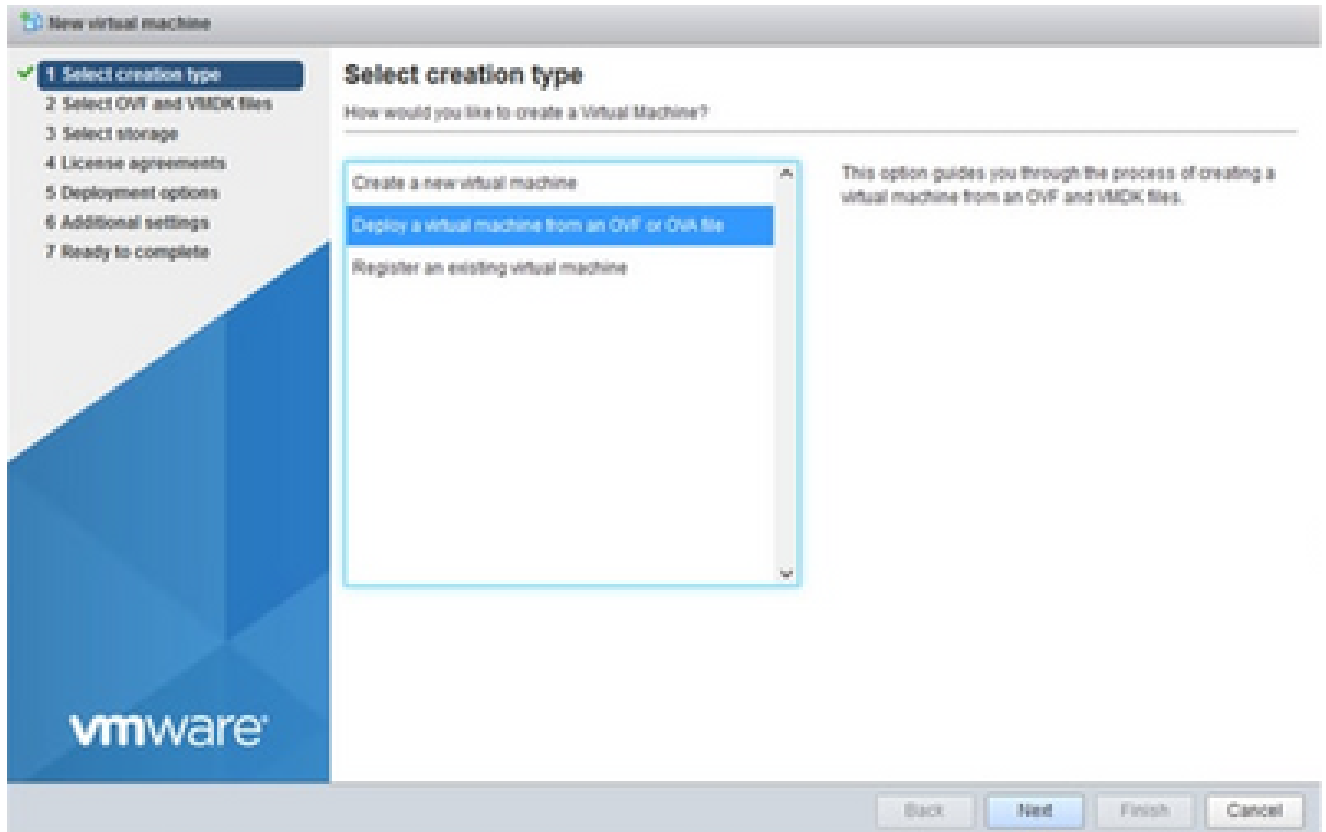
VMWare ESXi Login

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



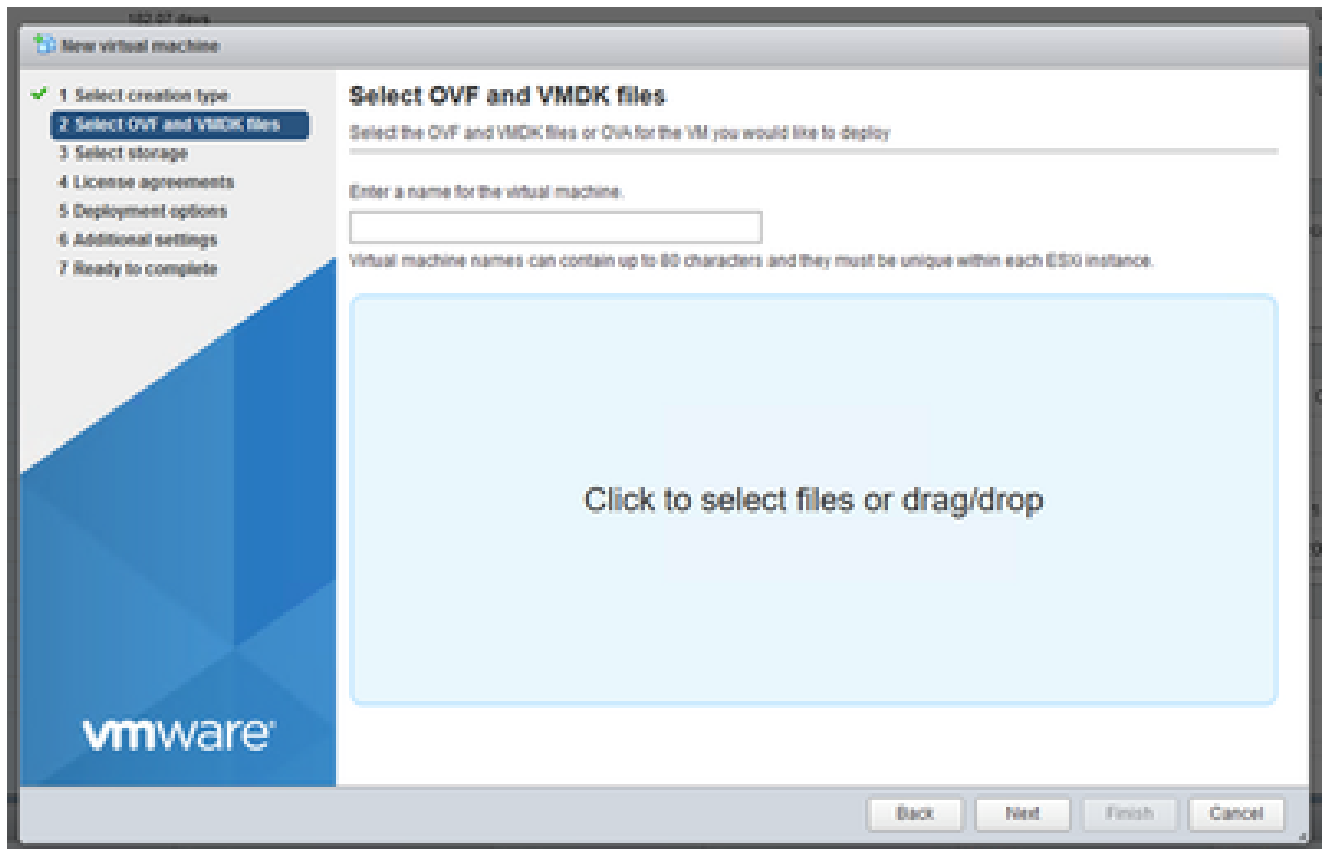
Create VM

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



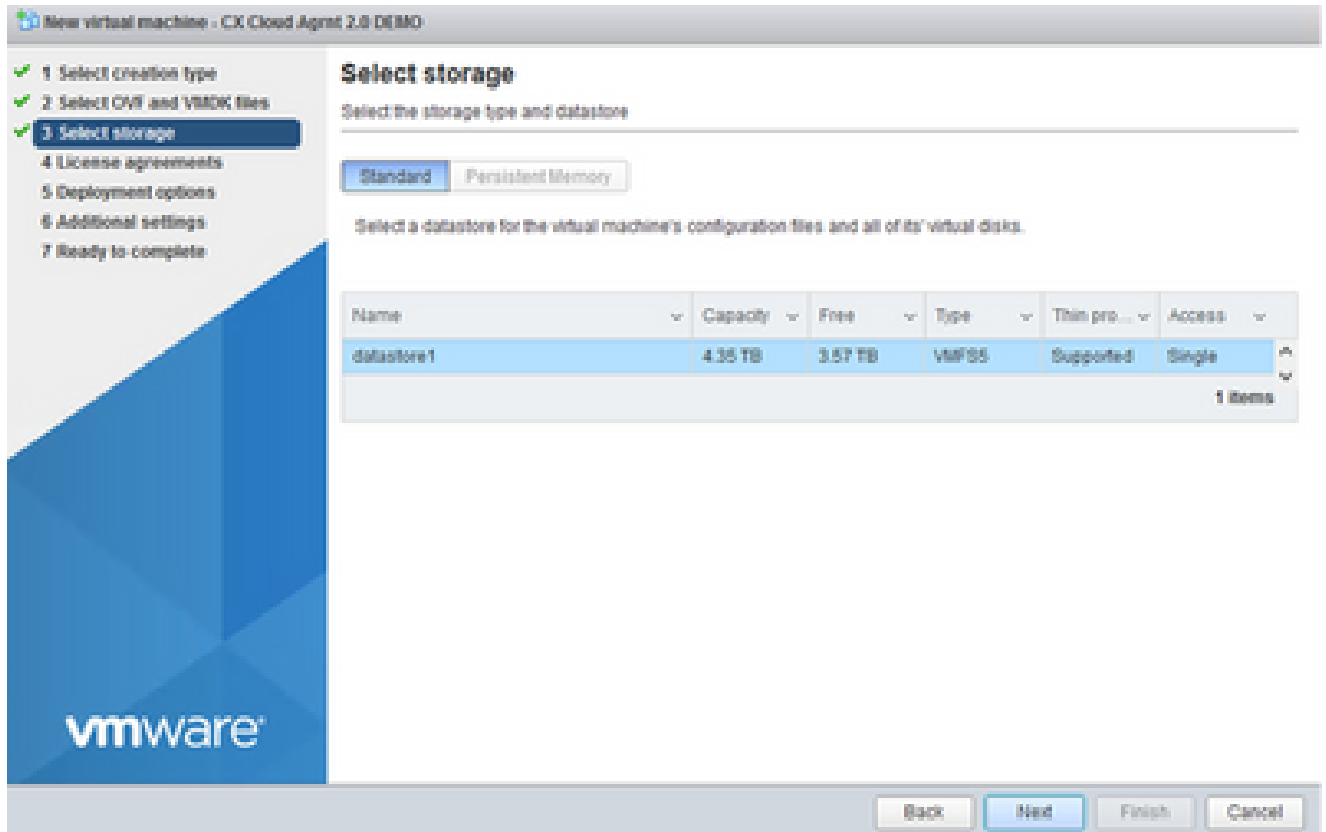
Select Creation Type

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



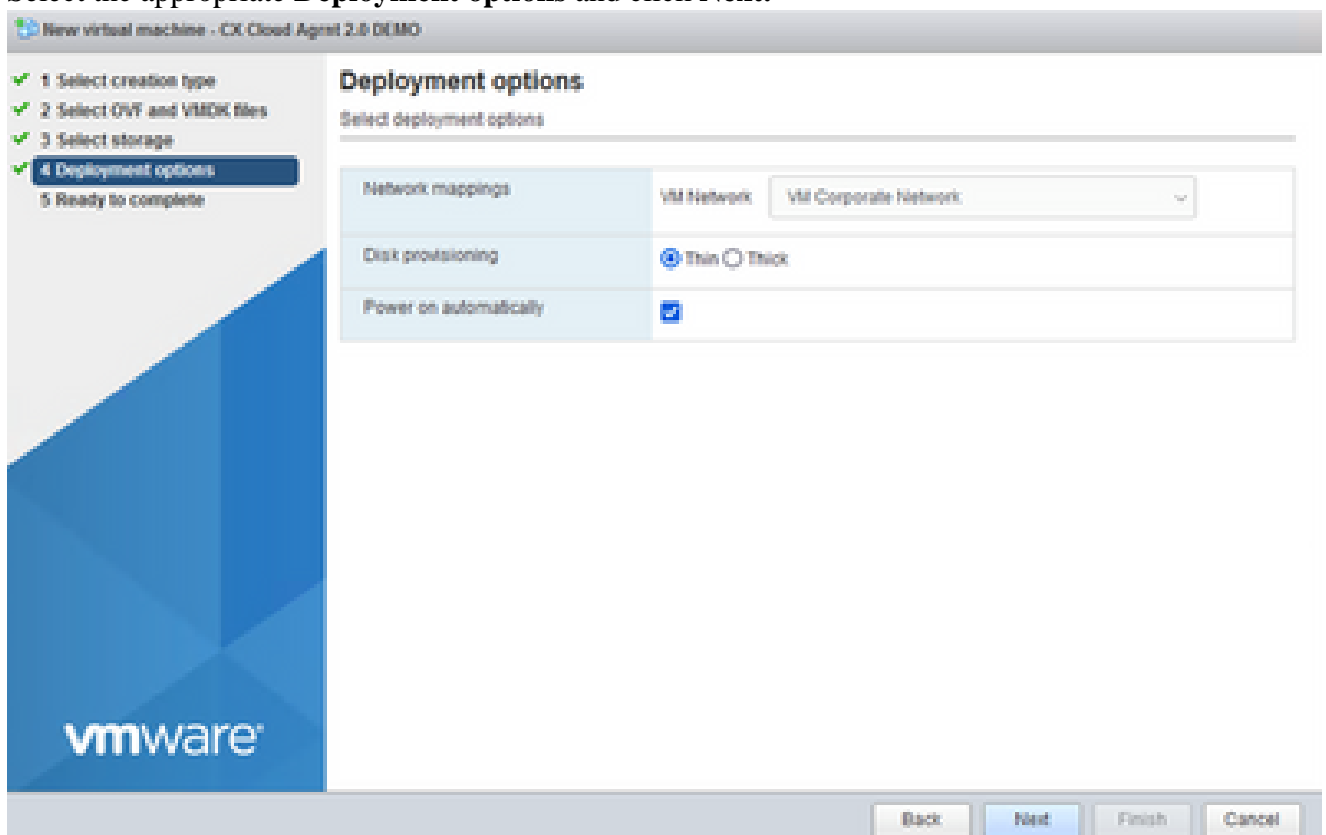
OVA Selection

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



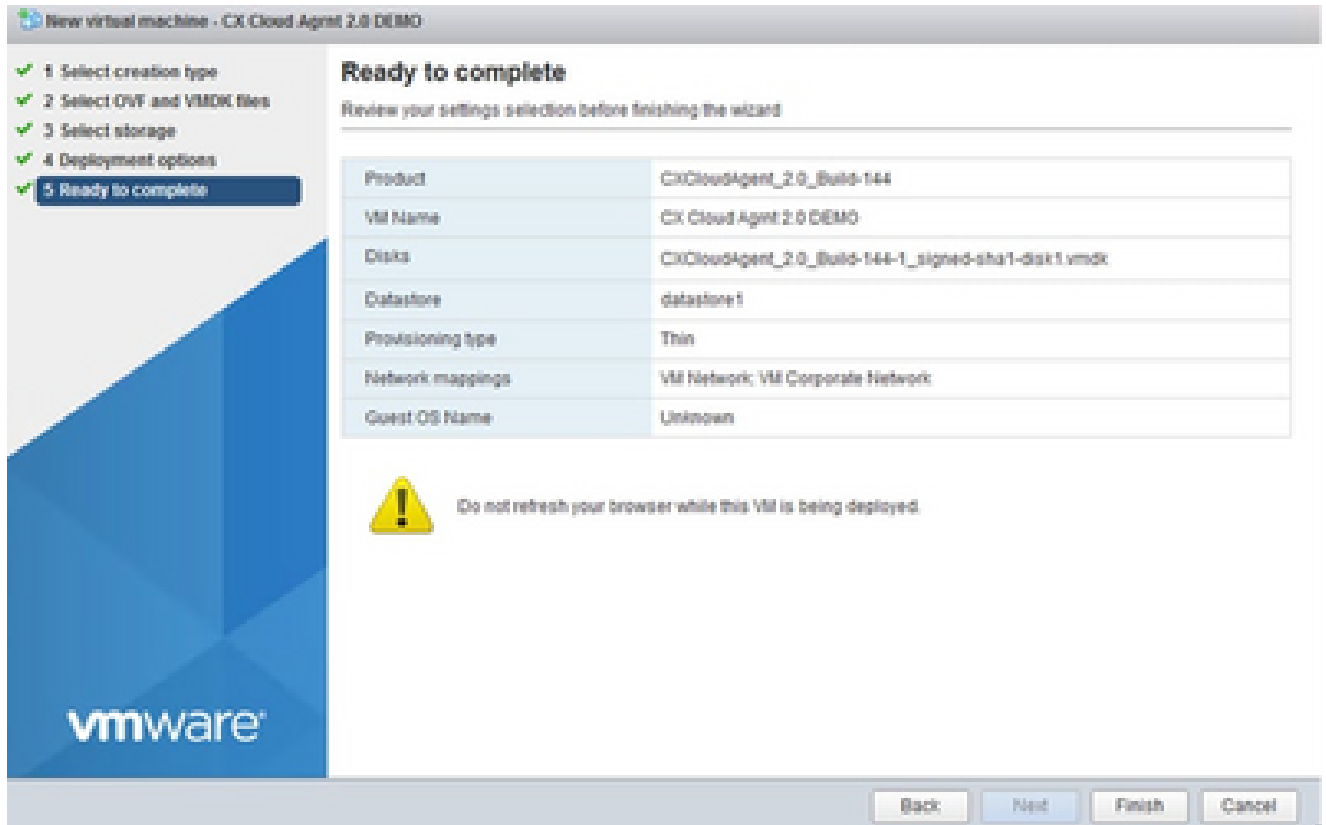
Select Storage

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

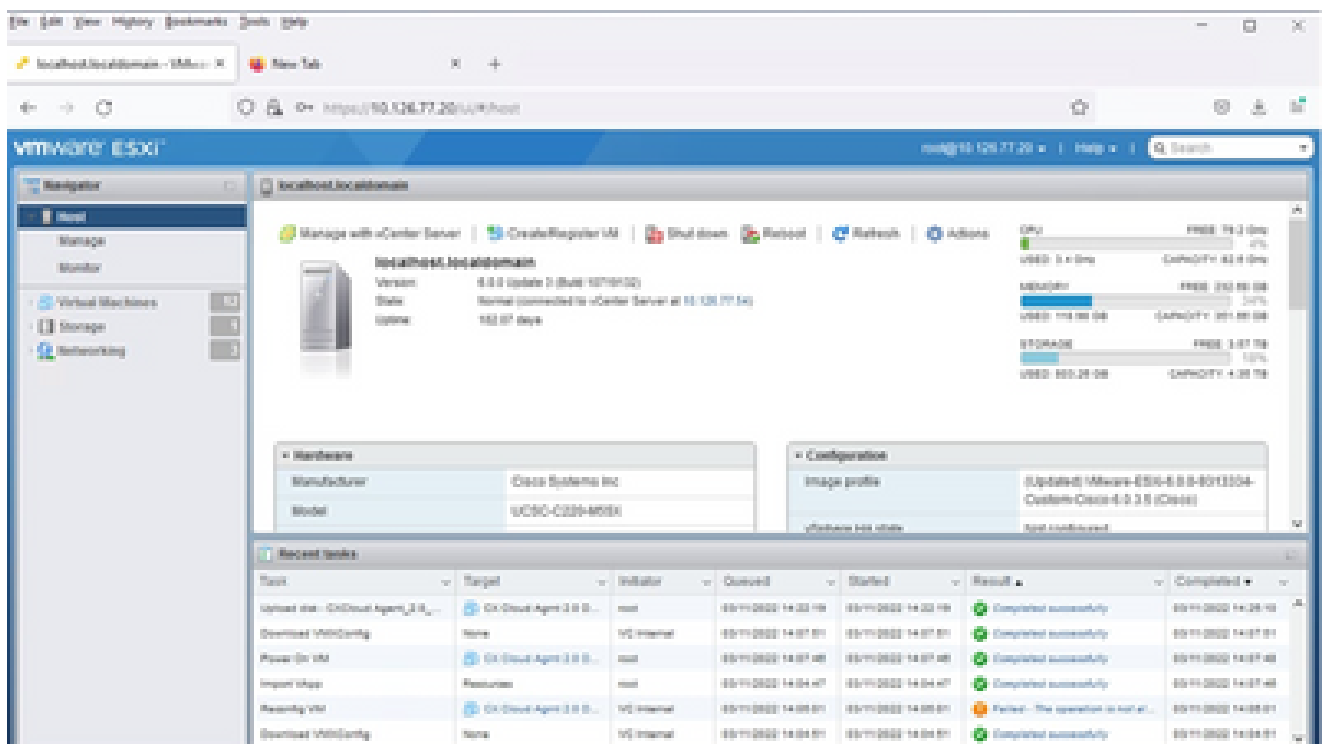


Deployment Options

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

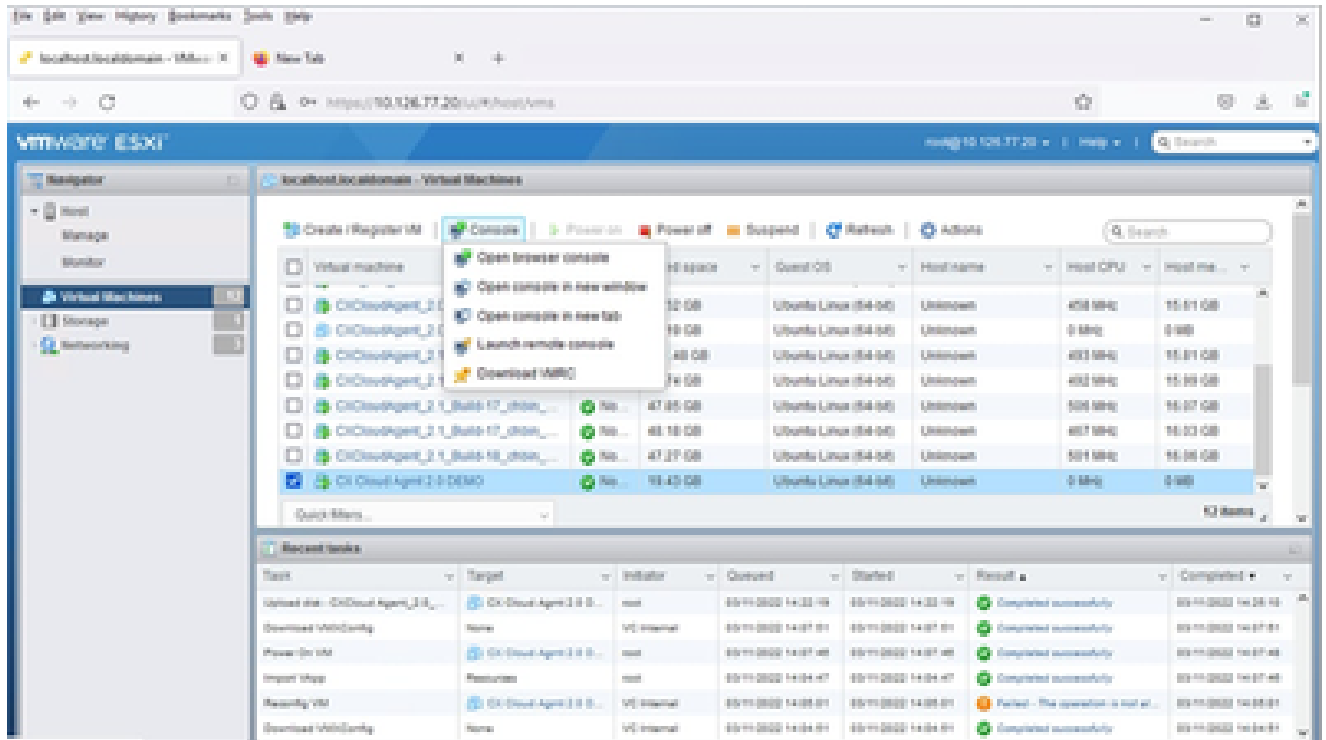


Ready to Complete



Successful Completion

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



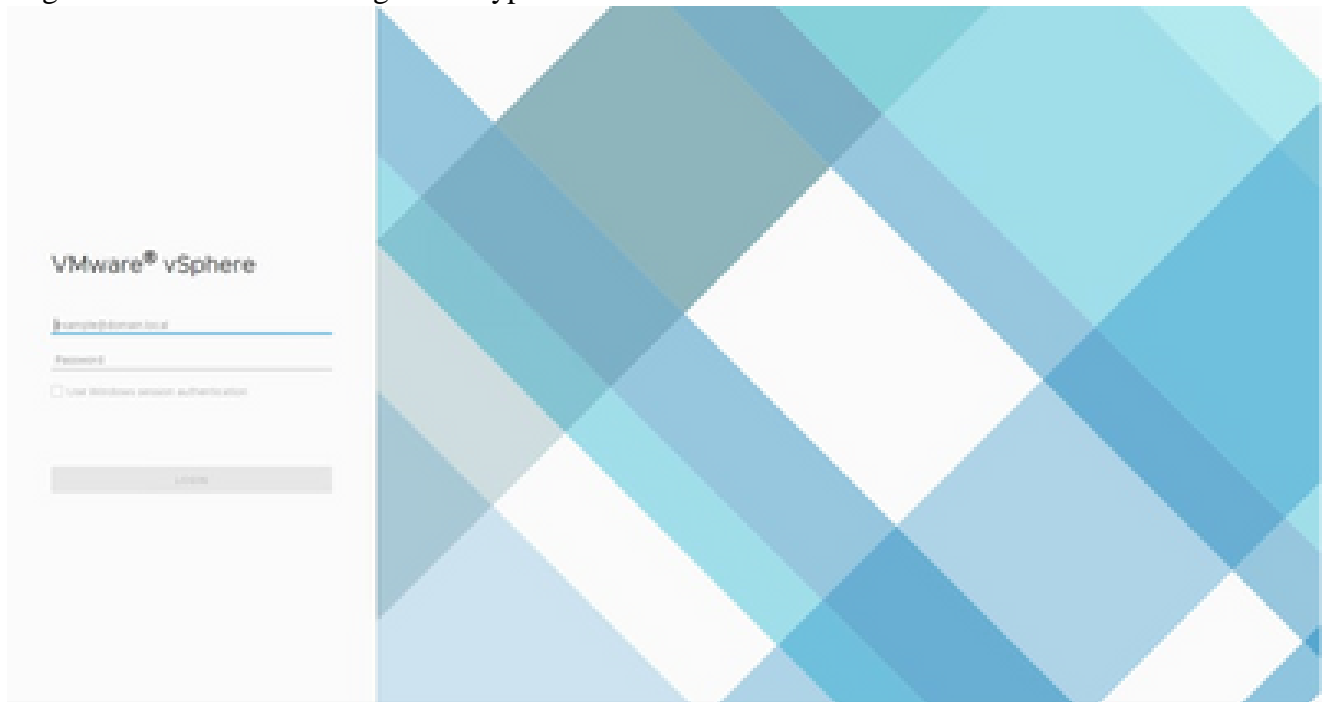
Console

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

Web Client vCenter Installation

Perform the following:

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



Log In

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

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.

10.126.77.54

- > CommonPool
- > Delete
- > Performance
- > Automation
- > Build-Server
- > DNAC
- > Security
- > Tools

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)

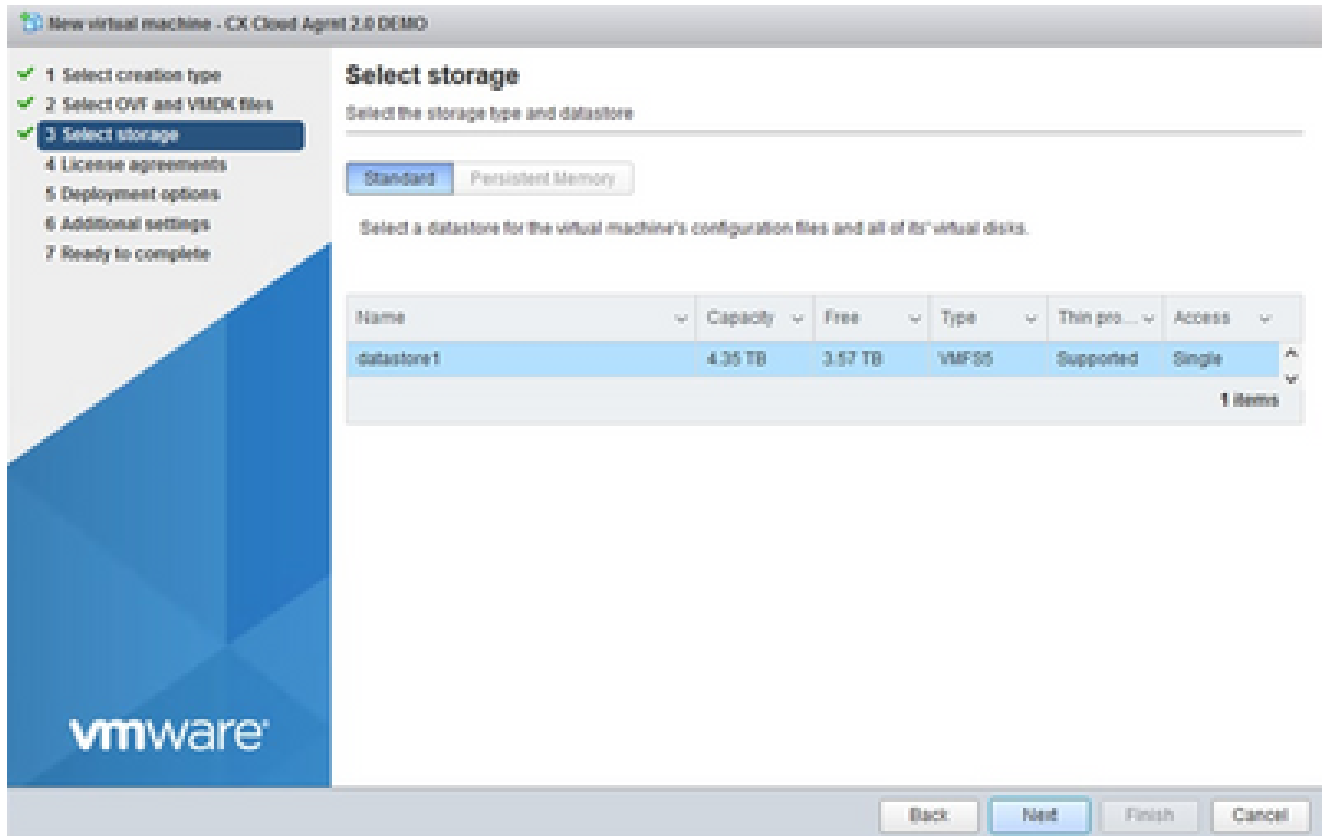
CANCEL

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 shows the vSphere interface with the VM 'CxCloudAgent_2.0_Build-144-demo' selected. The main panel displays the VM's status as 'Powered Off' and provides details on its hardware configuration:

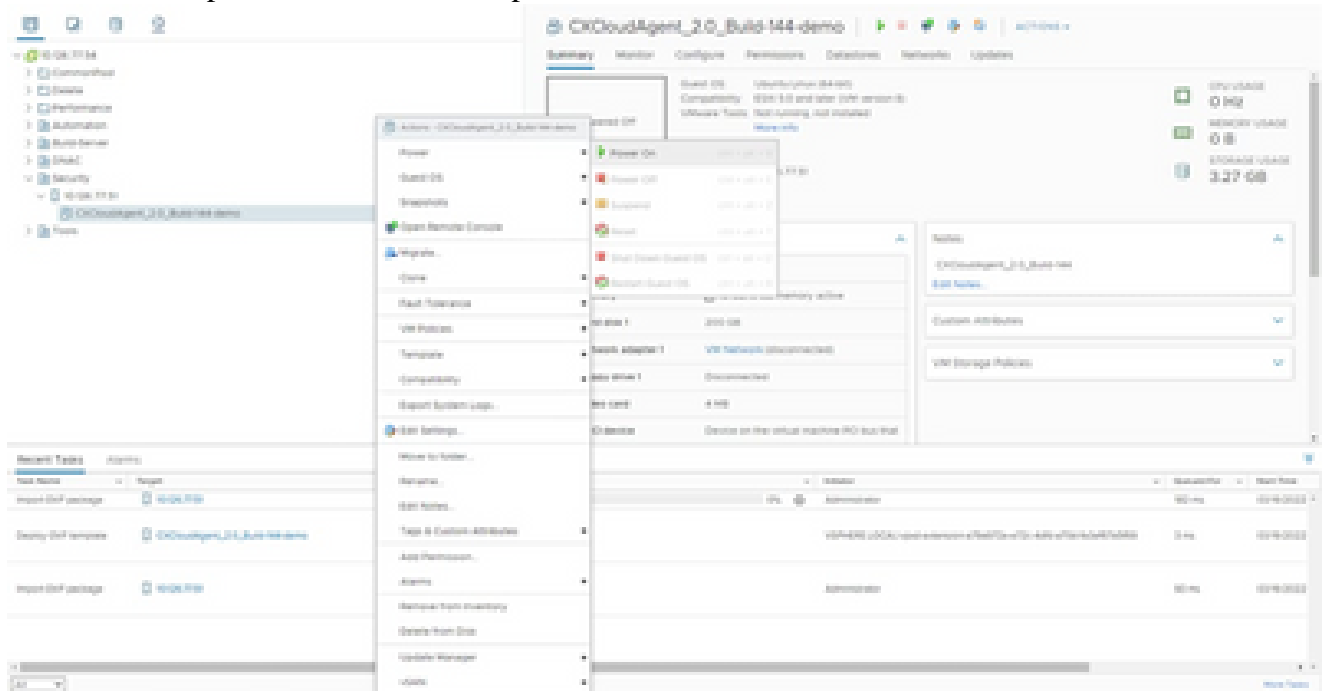
- Summary:** Shows 'Powered Off' status, OS (Ubuntu (64-bit)), and various system details.
- VM Hardware:**
 - CPU: 0 CPUs
 - Memory: 4 GB, 0 GB memory active
 - Hard disk 1: 200 GB
 - Network adapter 1: VM Network (disconnected)
 - Floppy disk 1: Disconnected
 - Video card: 4 MB
 - VMX device: Device on the virtual machine (0) on the host
- Notes:** A note is present with the title 'CxCloudAgent_2.0_Build-144'.

At the bottom, the 'Recent Tasks' table shows the completion of the VM creation process:

Task Name	State	Message	Success/Fail	Start Time
Import OVF package	Completed		Success	12/19/2023
Deploy OVF template	Completed		Success	12/19/2023
Import OVF package	Completed		Success	12/19/2023

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

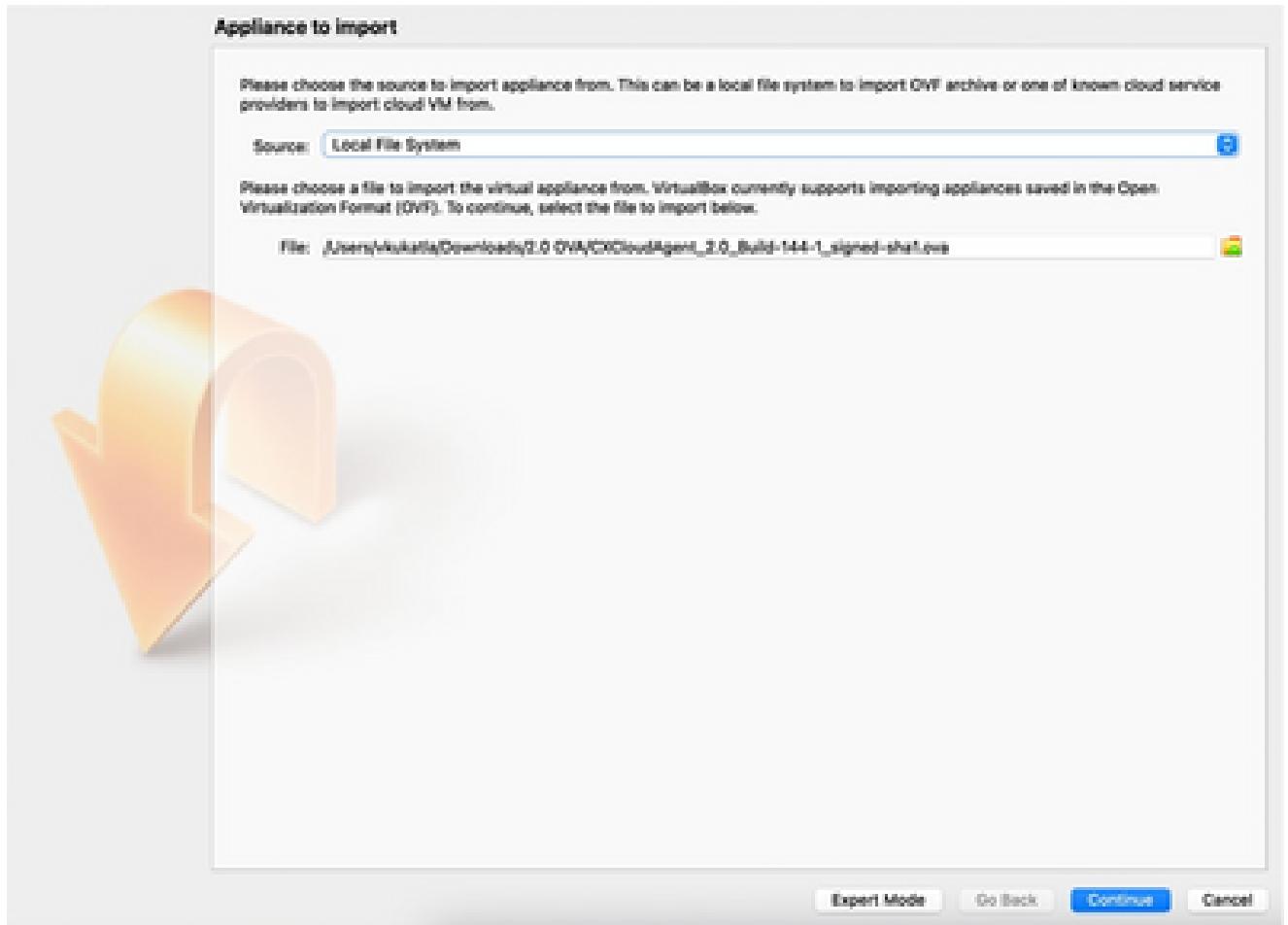
This client deploys CX Cloud Agent OVA though the Oracle Virtual Box.

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



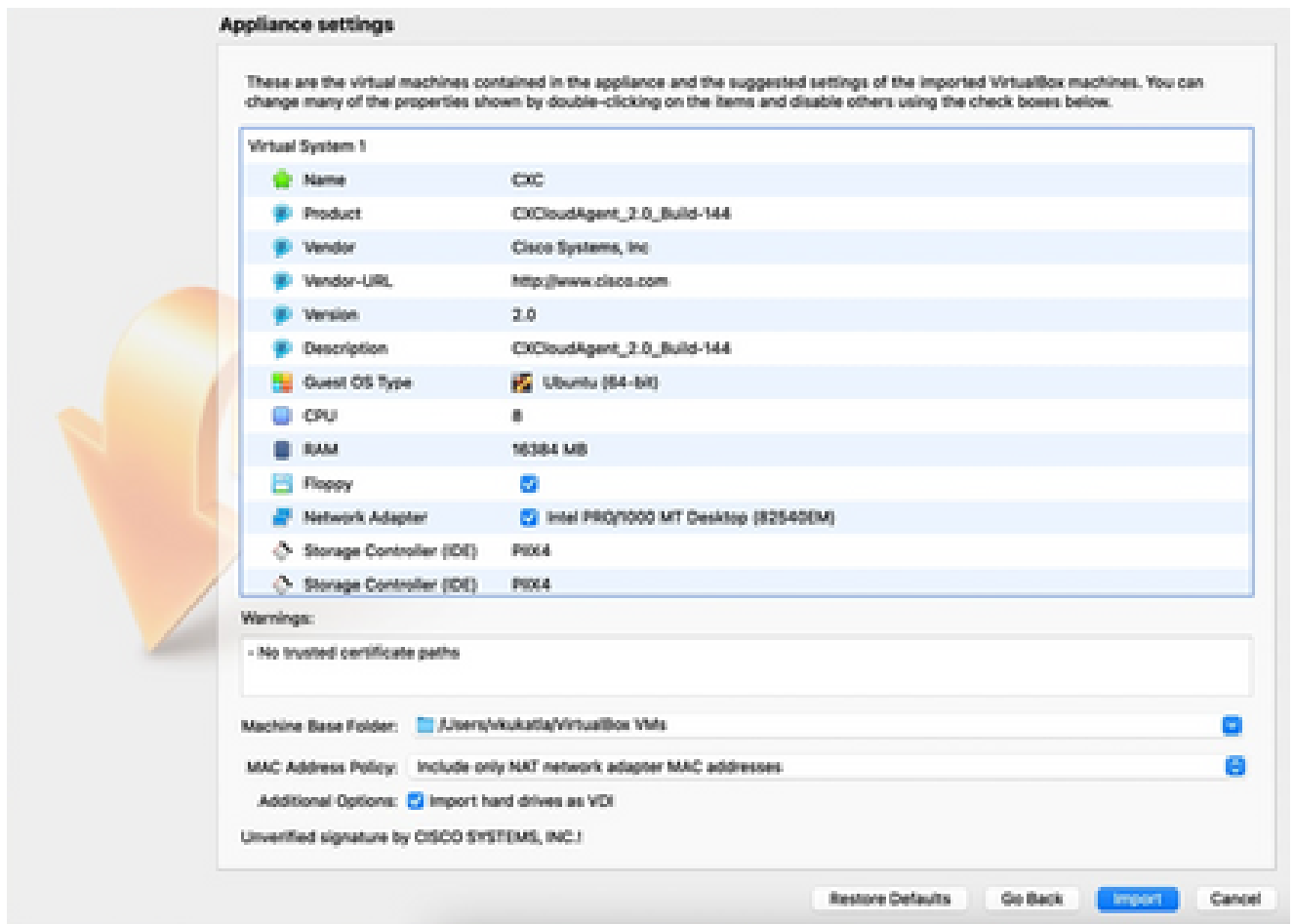
Oracle VM

2. Browse to import the OVA file.



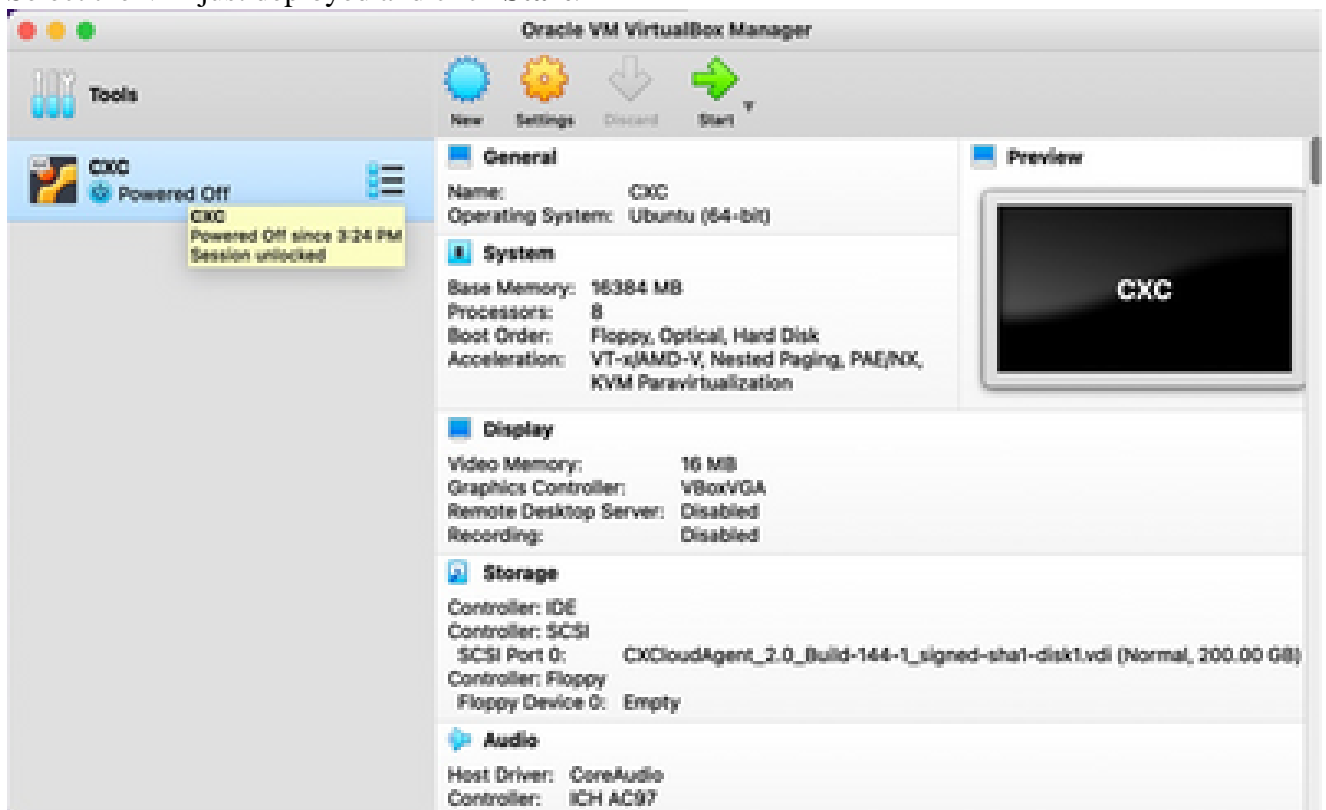
Select File

3. Click **Import**.

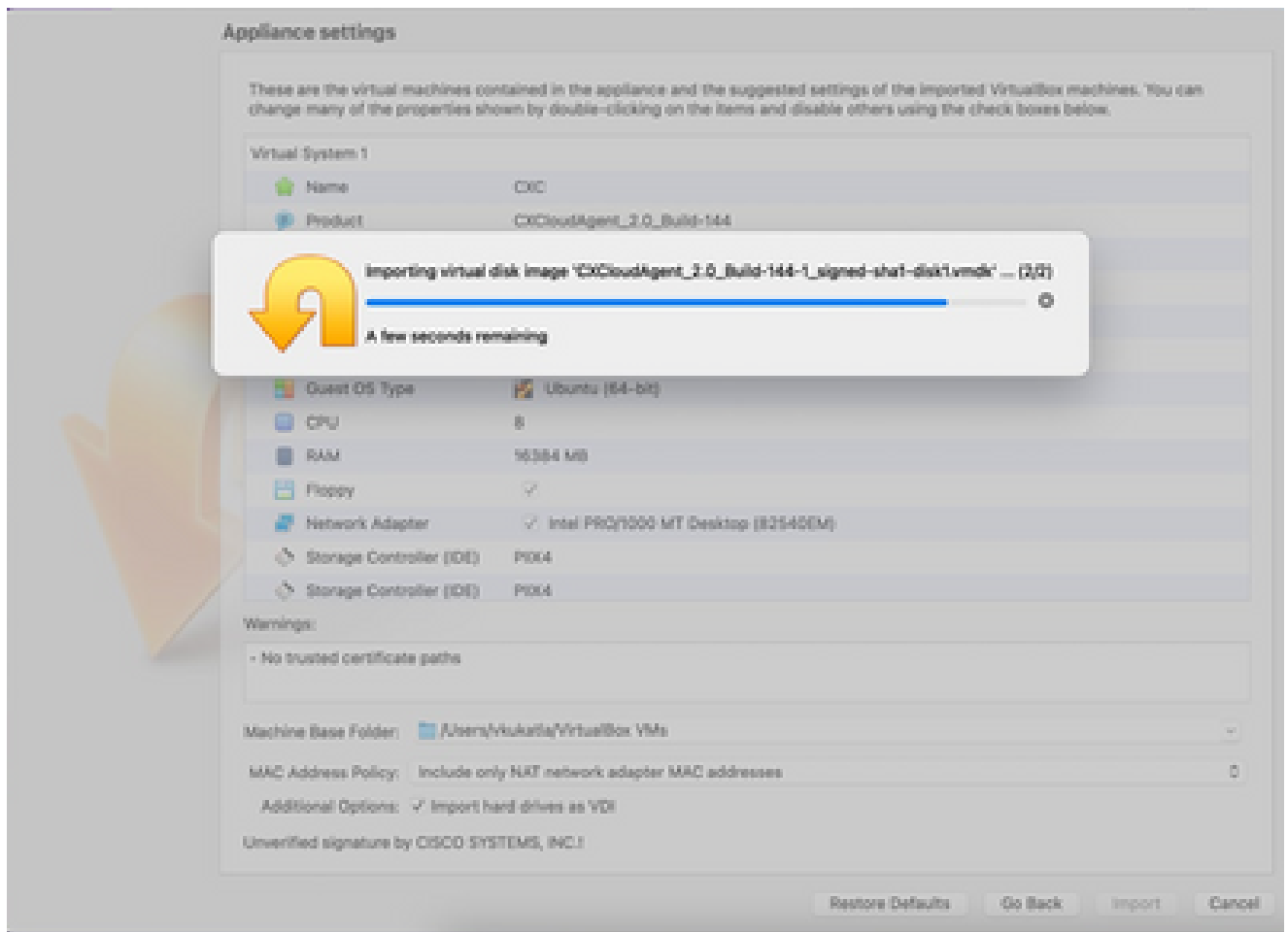


Import File

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



VM Console Startup



Import in Progress

5. Power on the VM. The console displays.



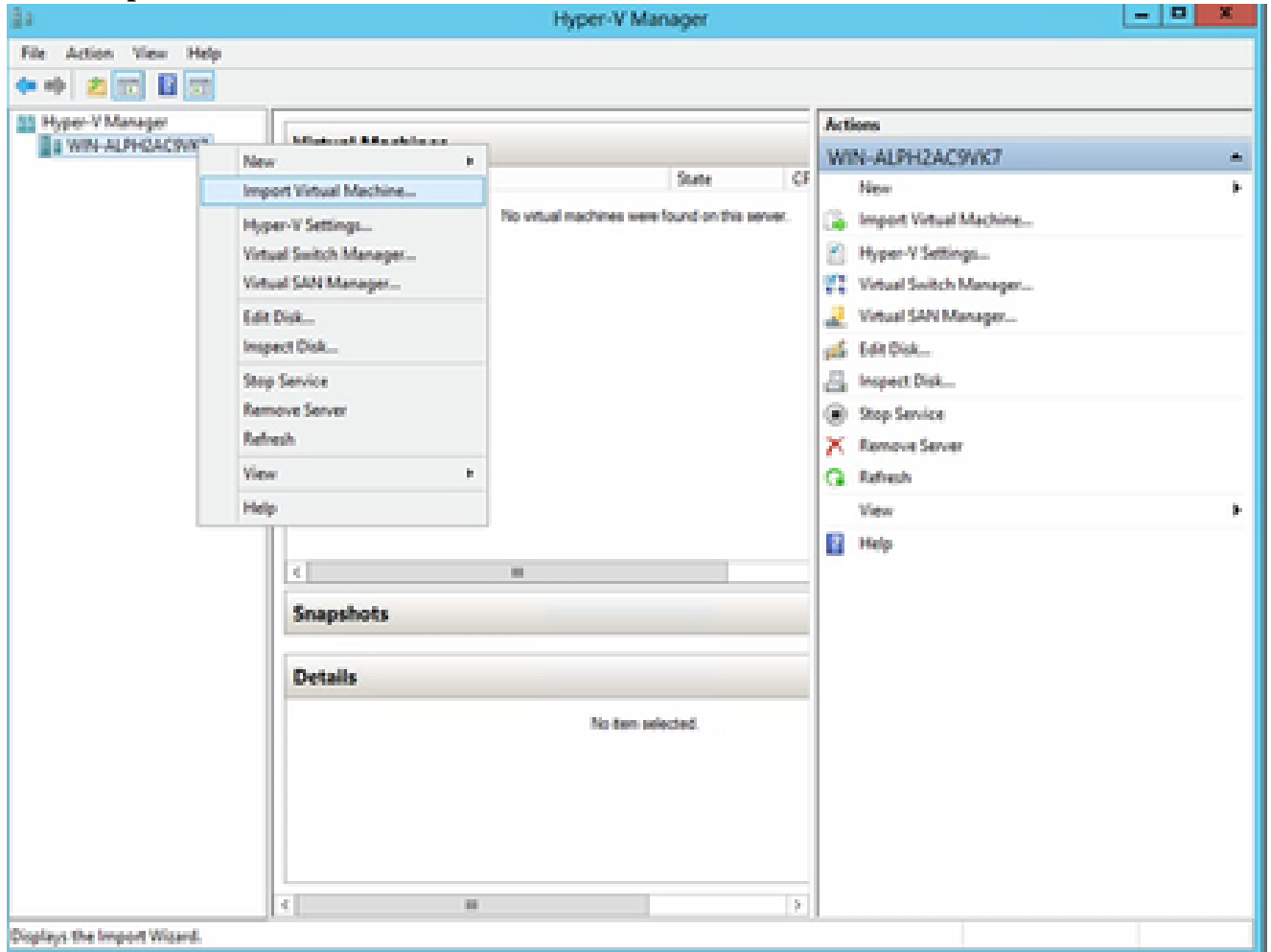
Open Console

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

Microsoft Hyper-V Installation

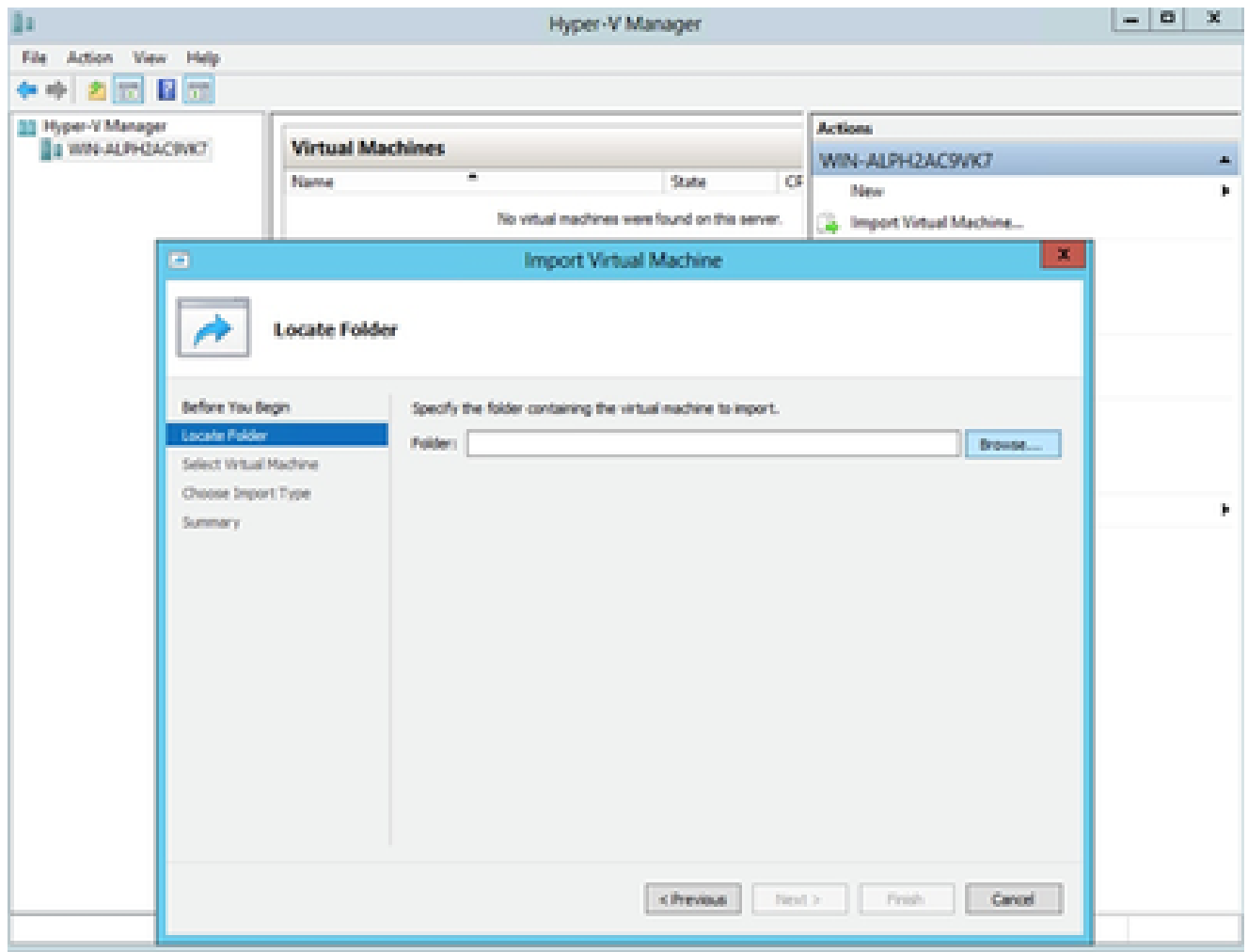
Perform the following:

1. Select **Import Virtual Machine**.



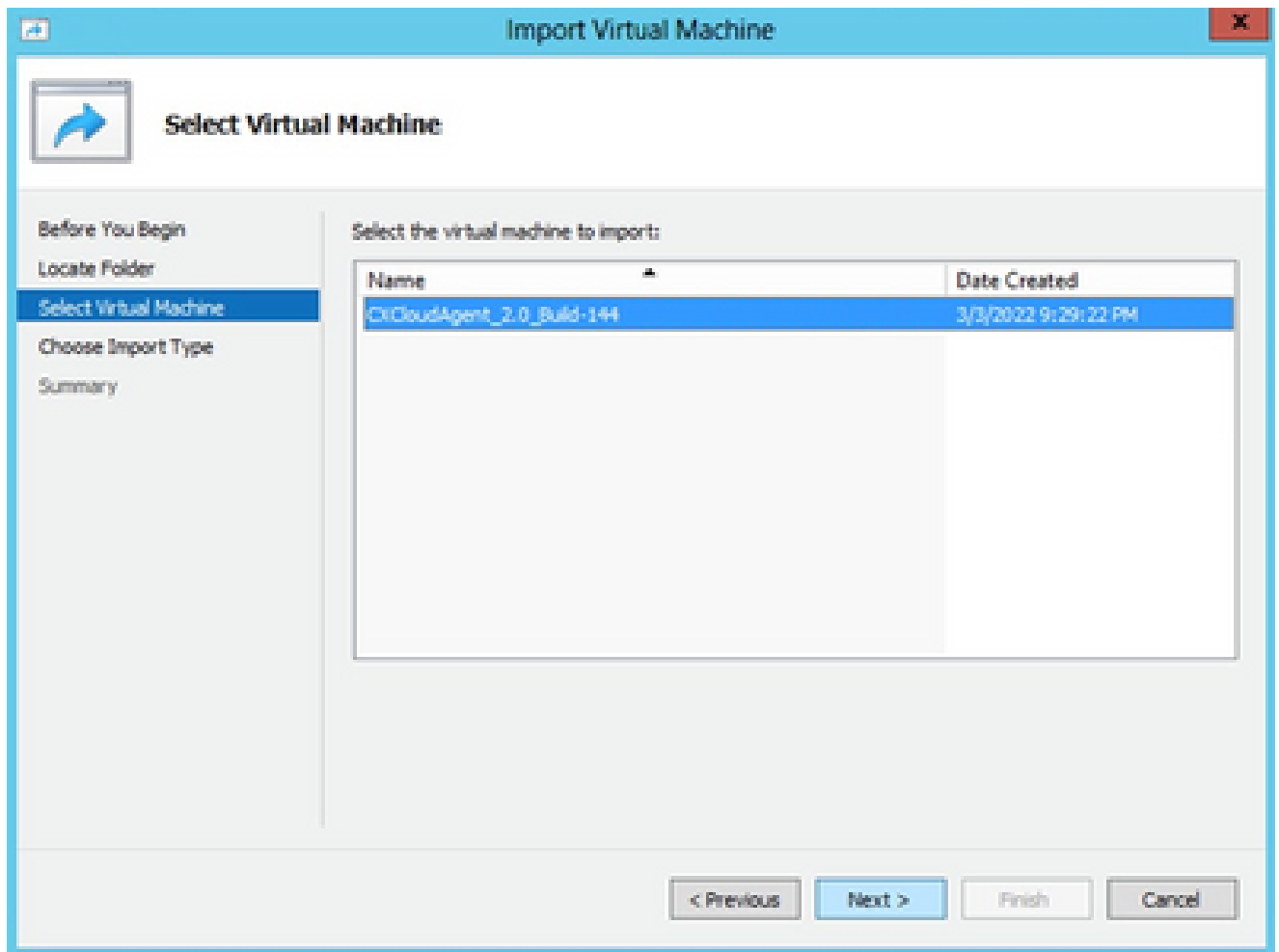
Hyper V Manager

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



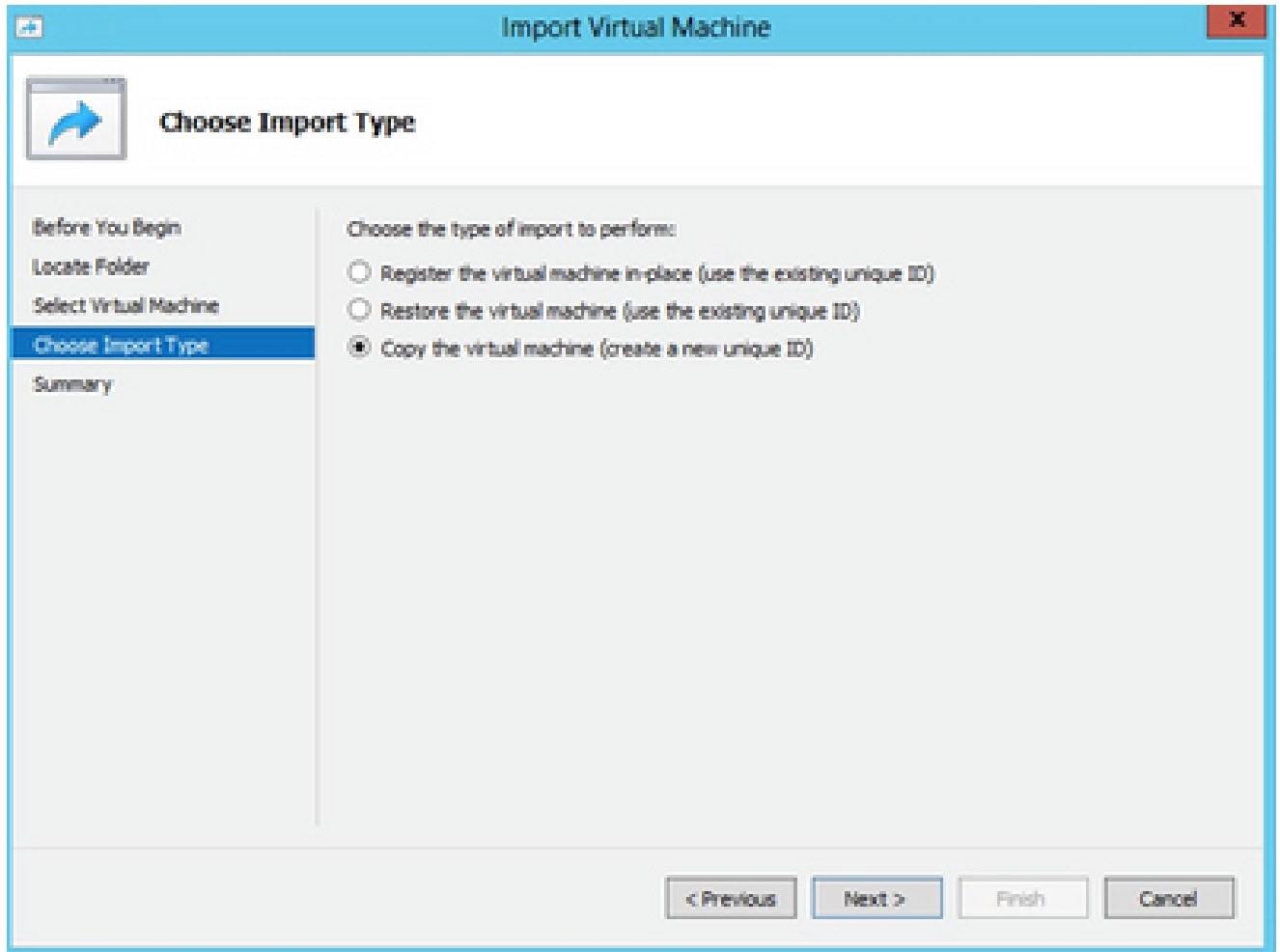
Folder to Import

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



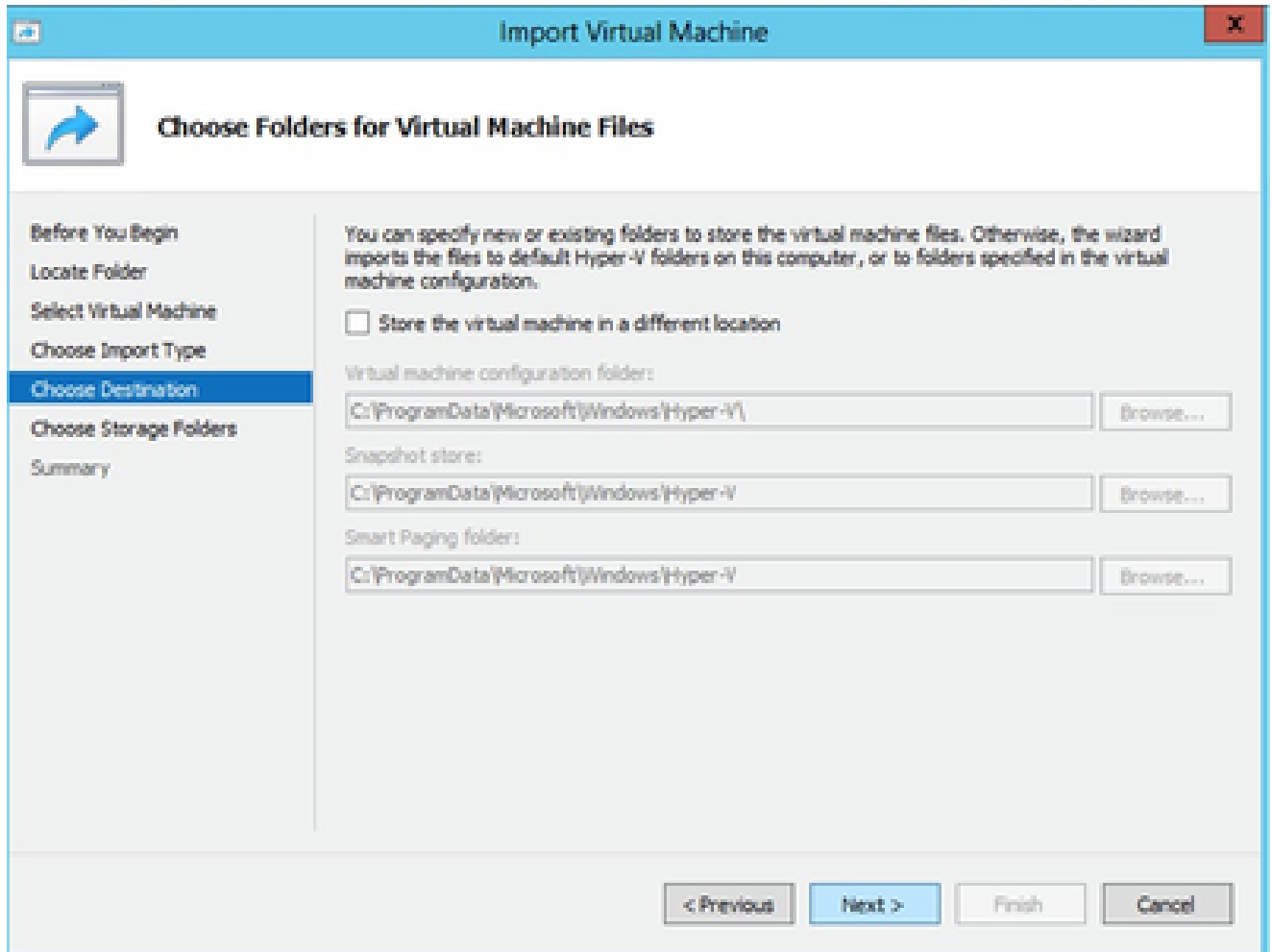
Select VM

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



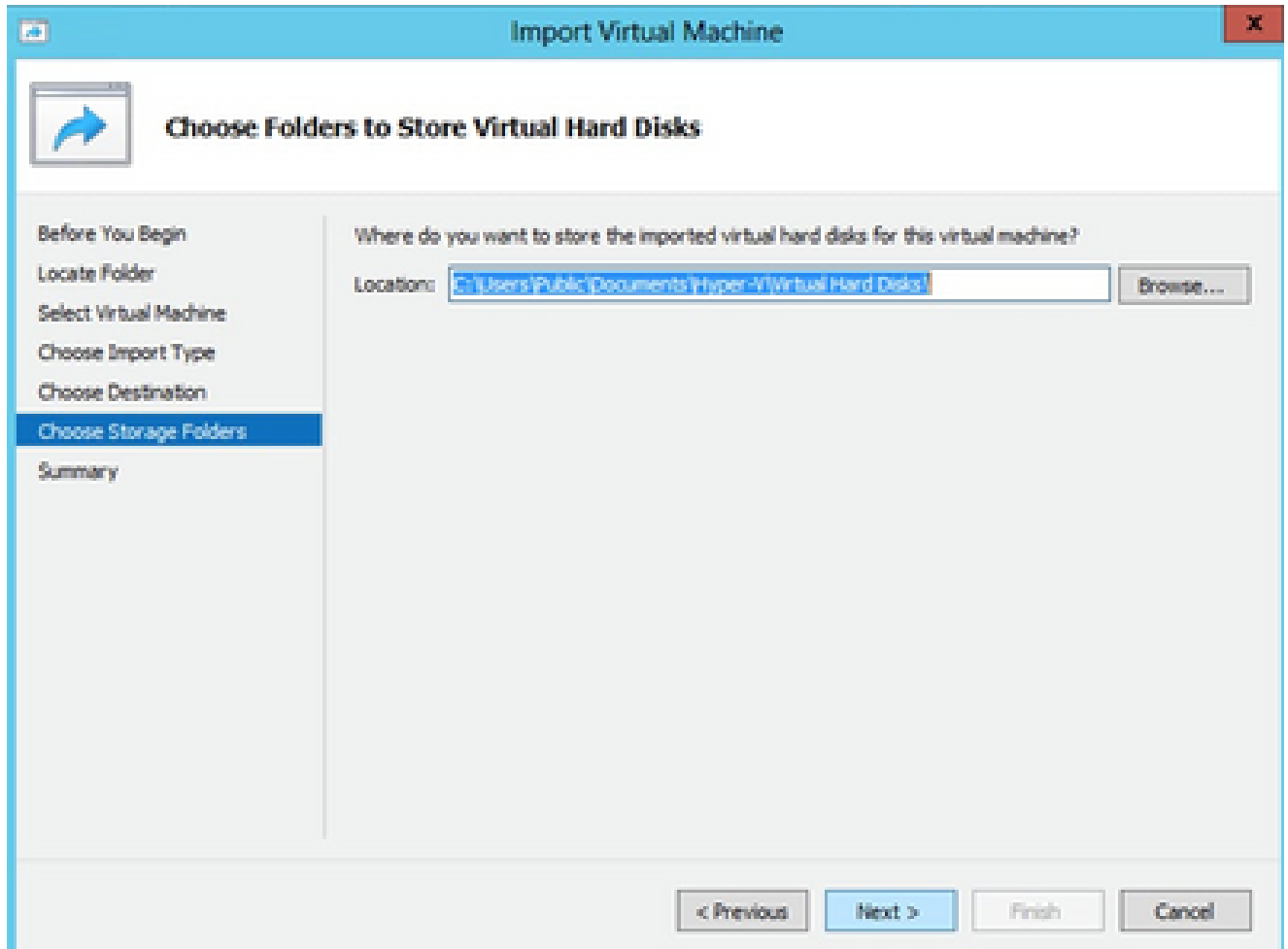
Import Type

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



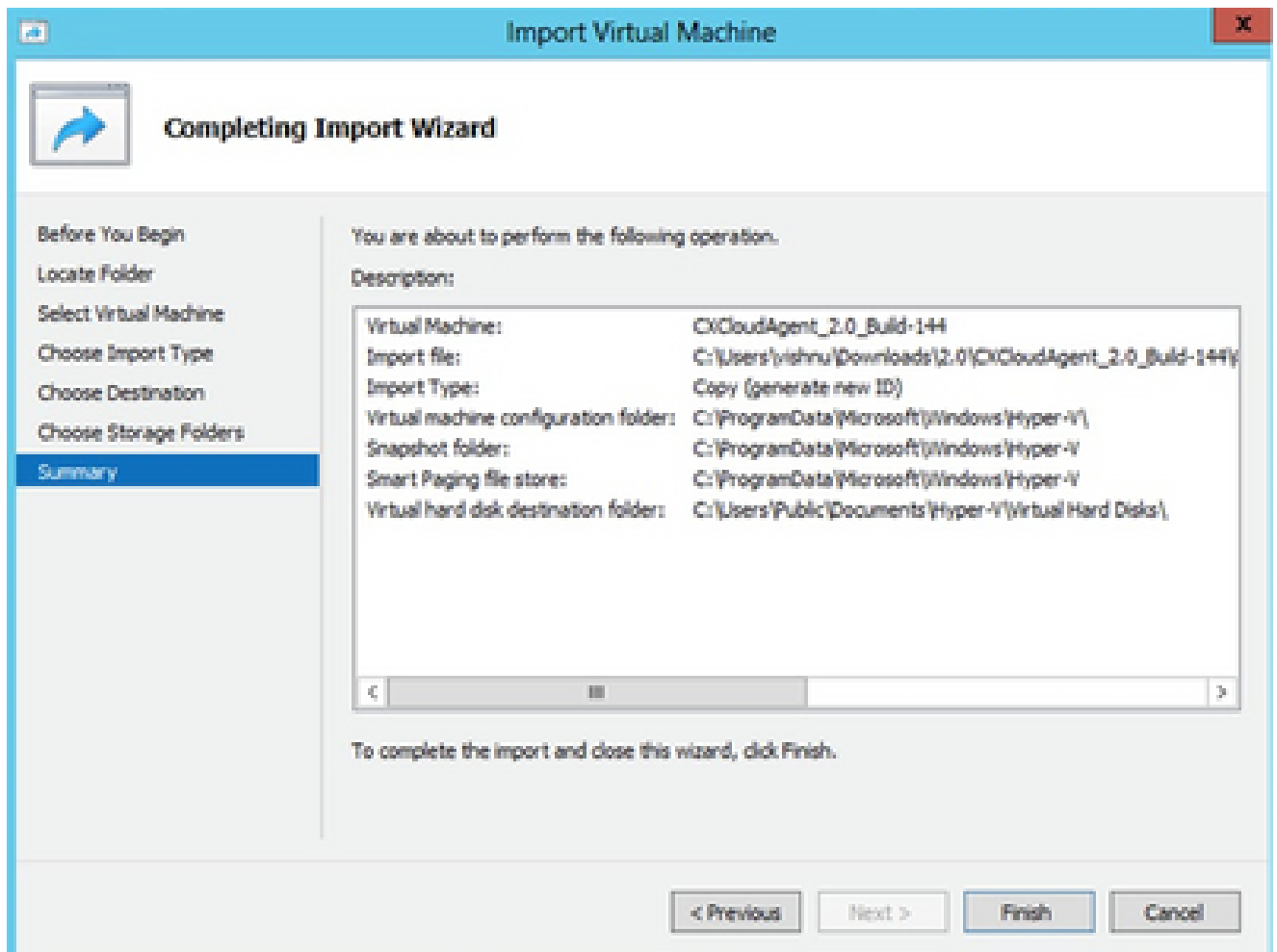
Choose Folders for Virtual Machine Files

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



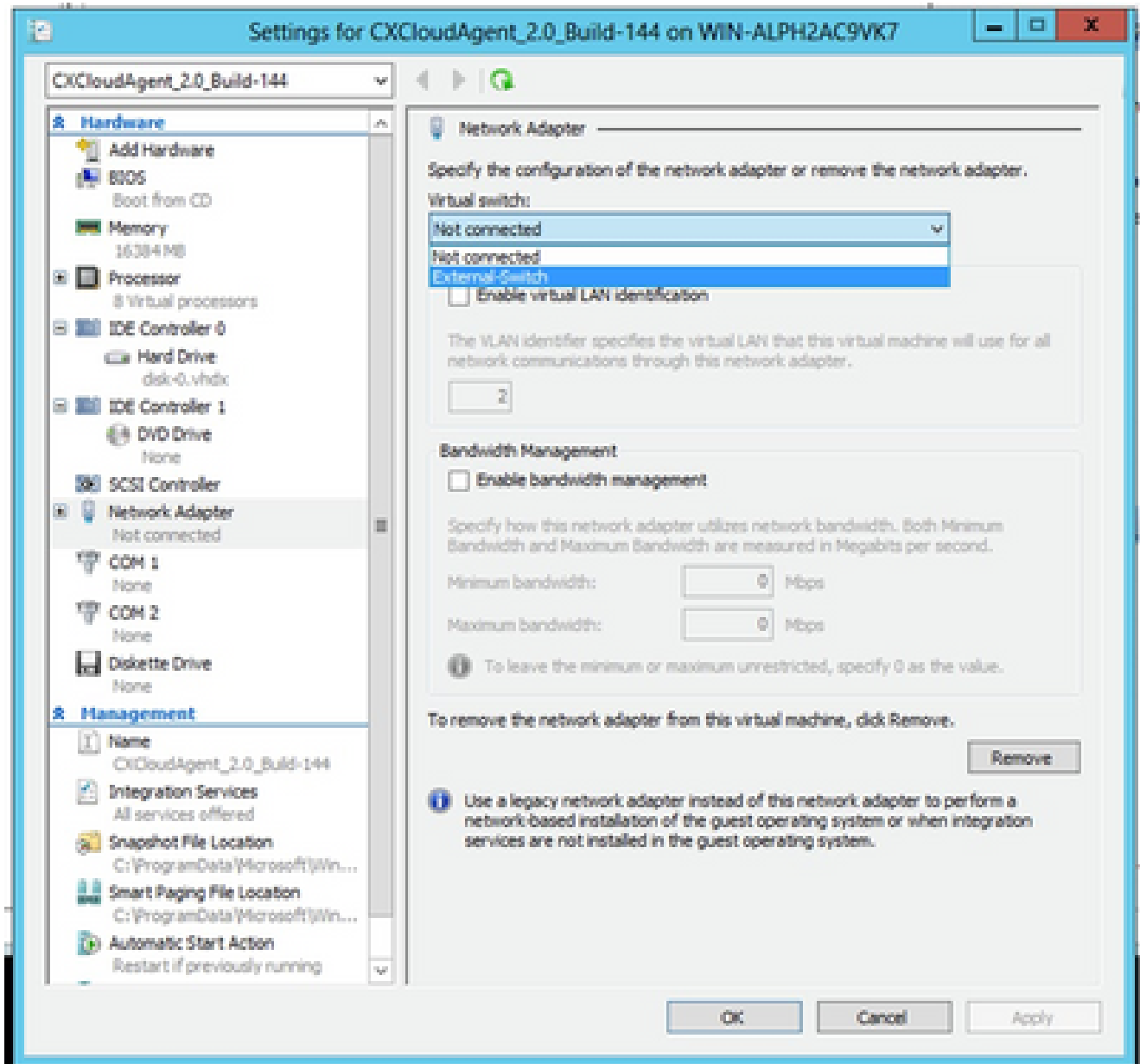
Folder to store the virtual hard disks

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



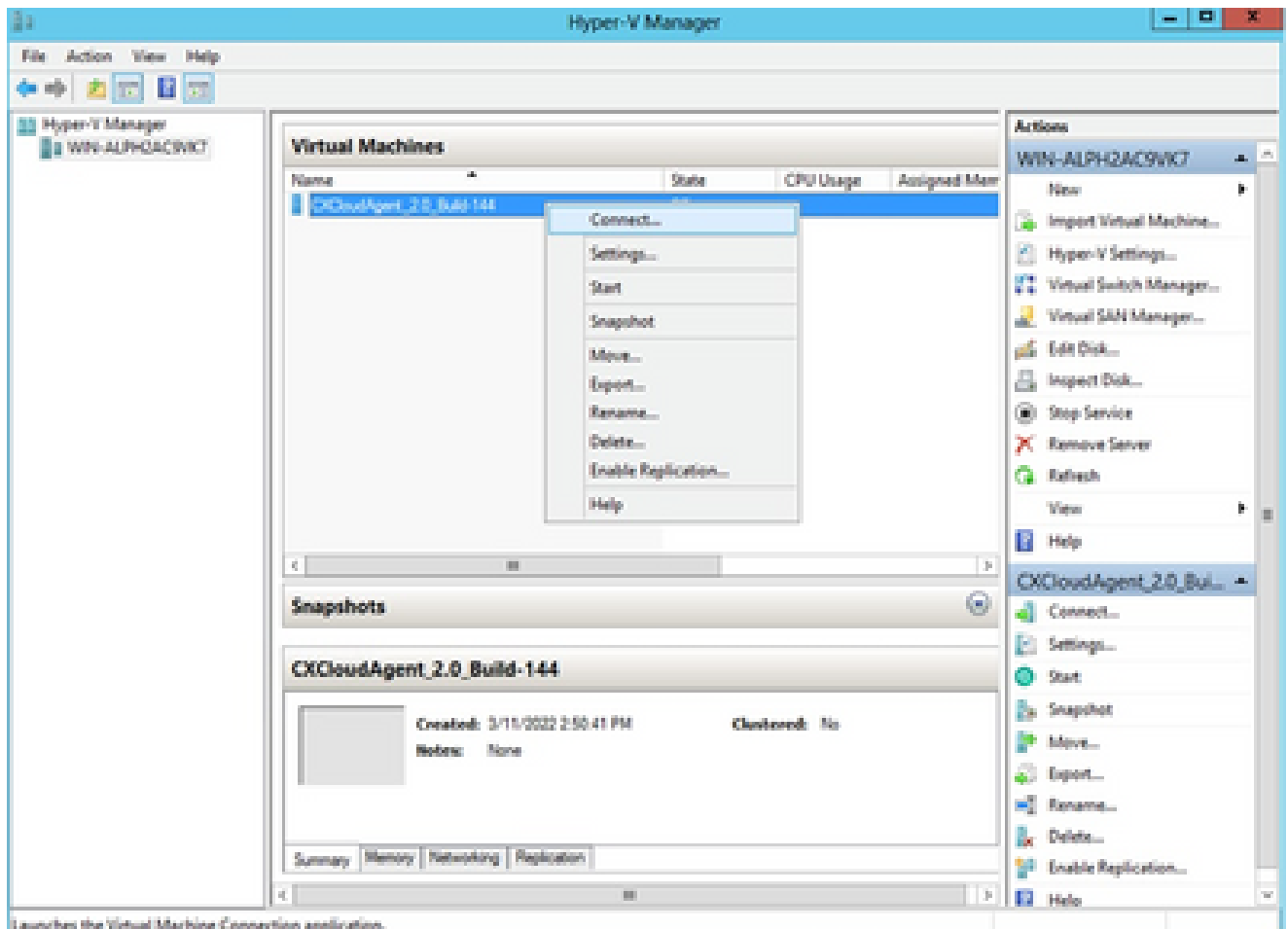
Summary

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.

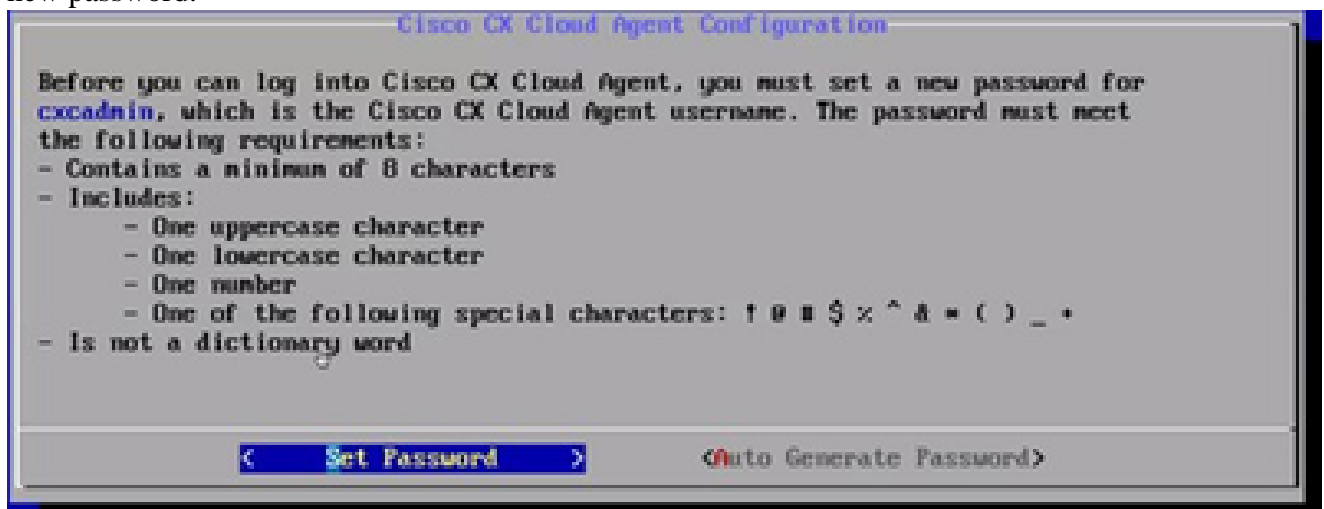


Starting VM

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

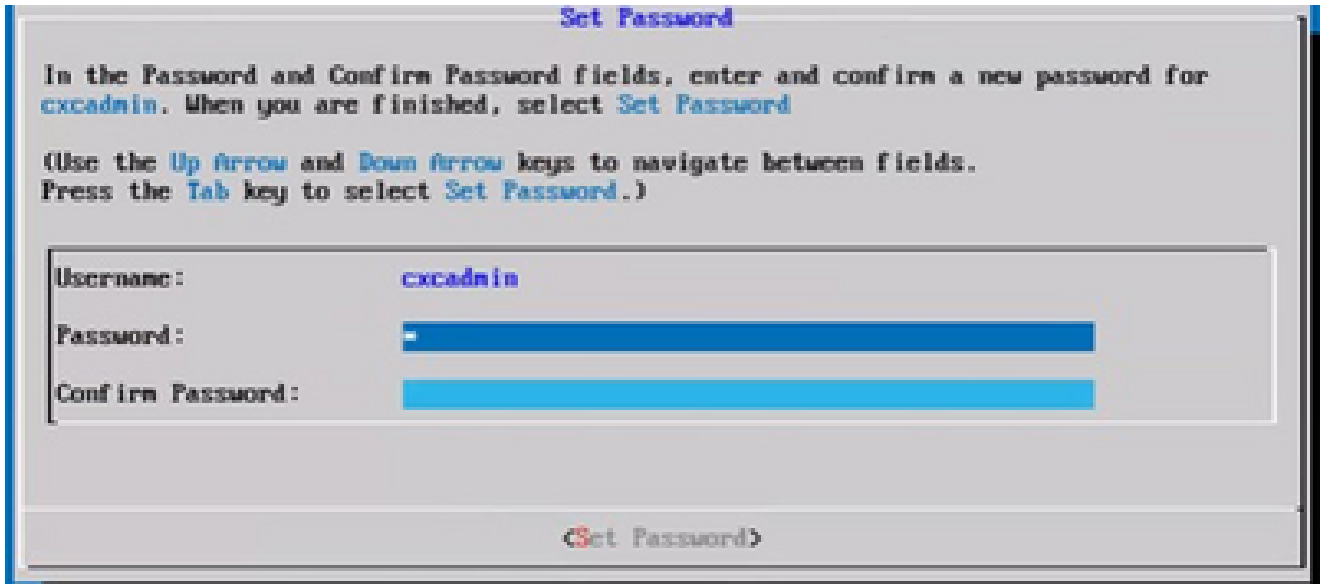
Network Configuration

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

Please enter an IPv4 address and corresponding network configuration for the appliance.

(Use **Up/Down** keys to navigate to next field. Press **Tab** to jump to **Continue** button)

IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Gateway:	<input type="text"/>
DNS Servers:	<input type="text"/>

•Maximum 3 IPs with comma separator.

<Continue>

Network Configuration

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

Confirmation

Are these entries correct?

IP Address:
Subnet Mask: :
Gateway:
DNS:

<Yes, Continue> **<No, Go Back >**

Configuration

- 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.

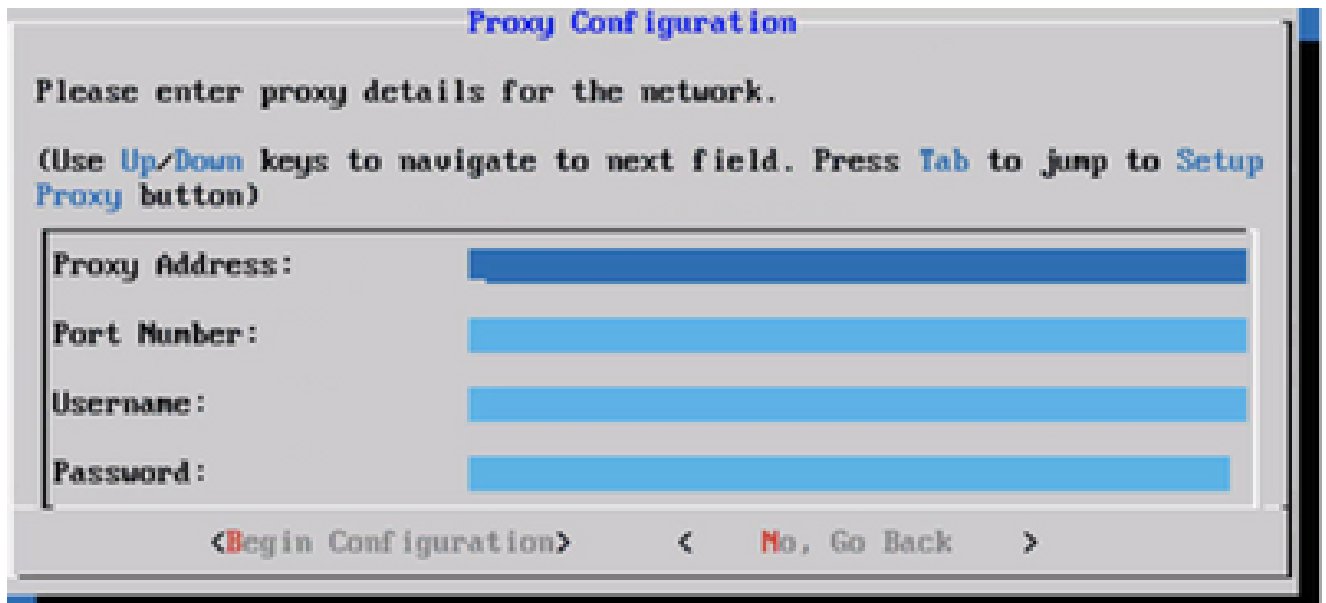
Proxy Set Up Confirmation

Do you want to add proxy details?

< Yes, Set Up Proxy > **<No, Continue to Configuration>**

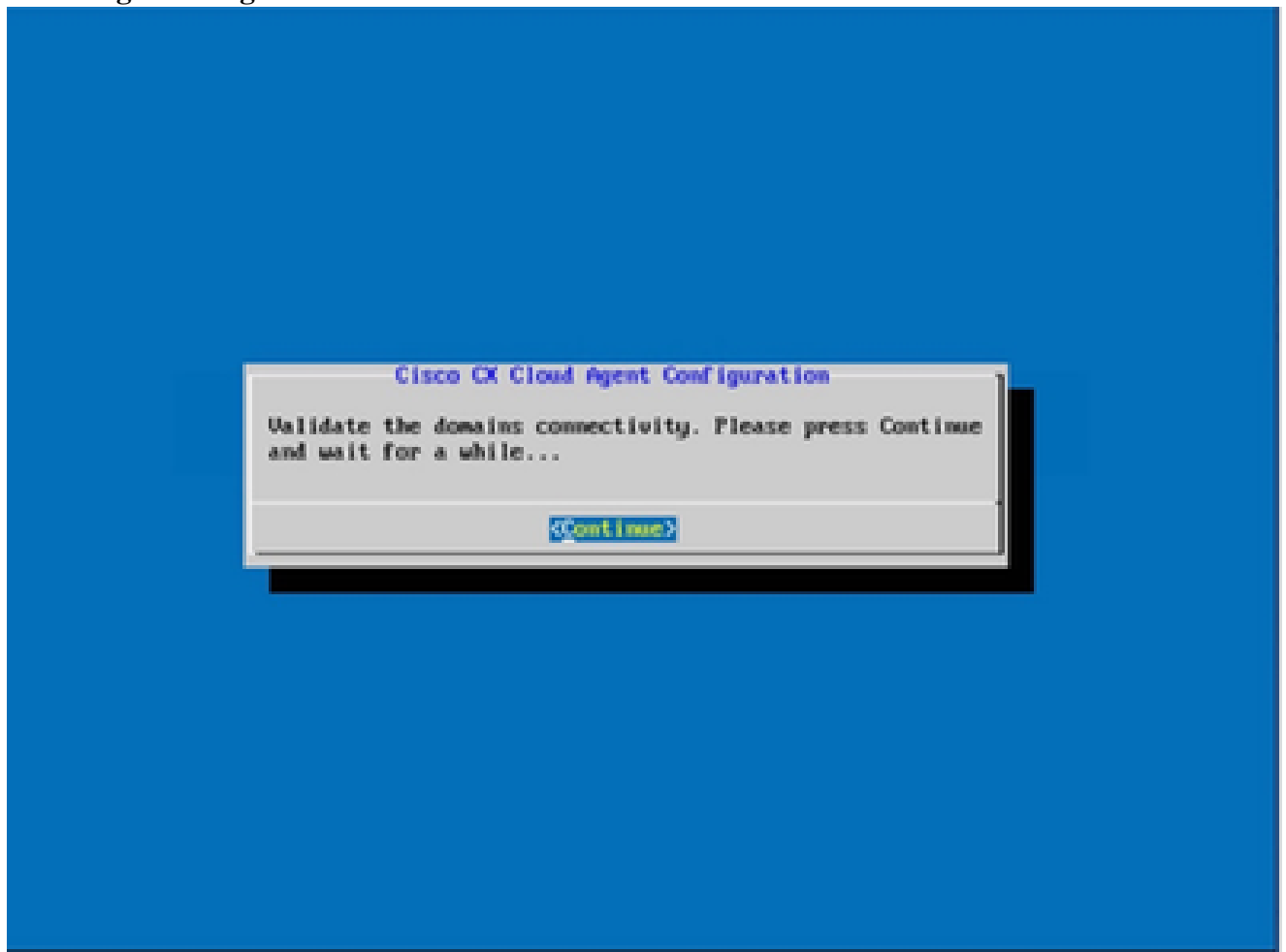
Proxy Setup

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



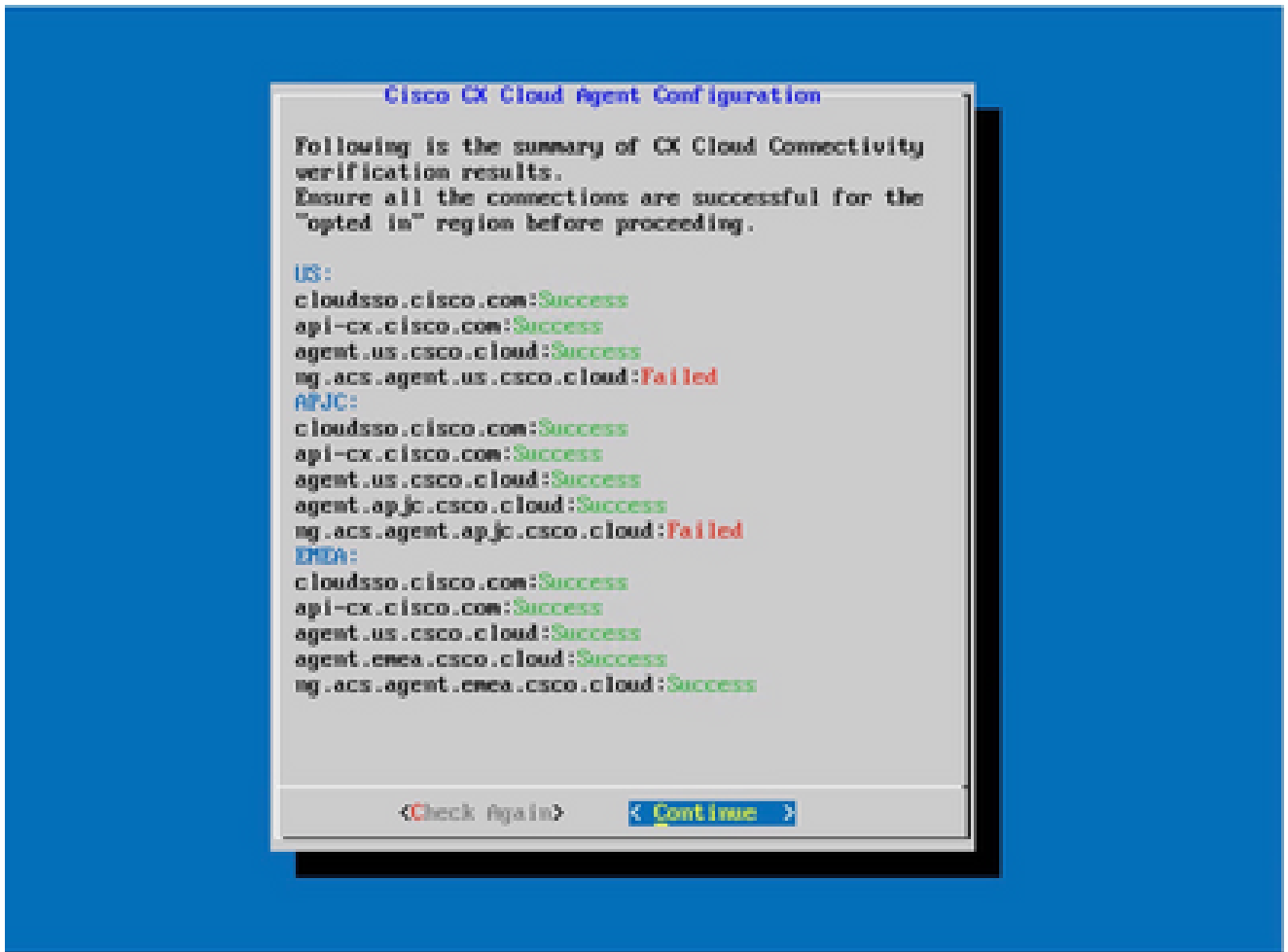
Proxy Configuration

8. Click **Begin Configuration**.




Begin Configuration

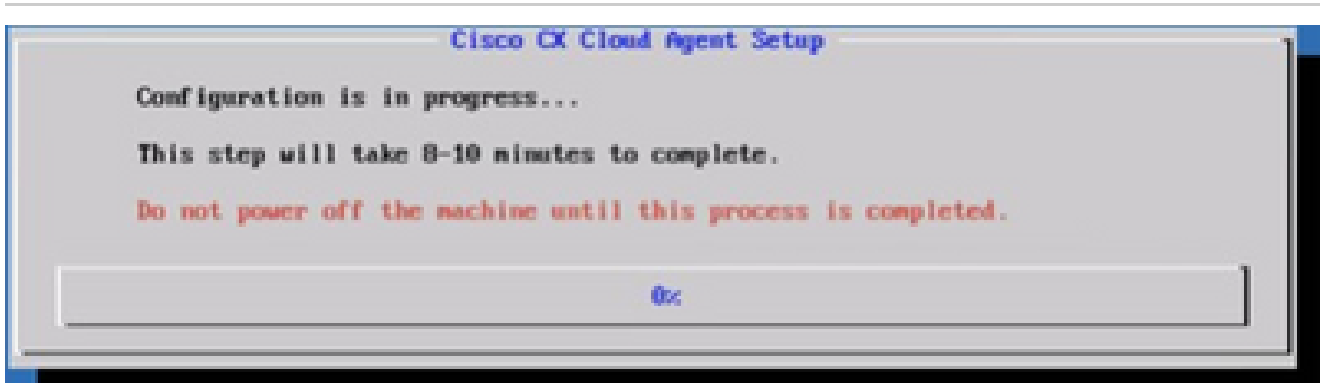
9. Click **Continue**.



Configuration continues

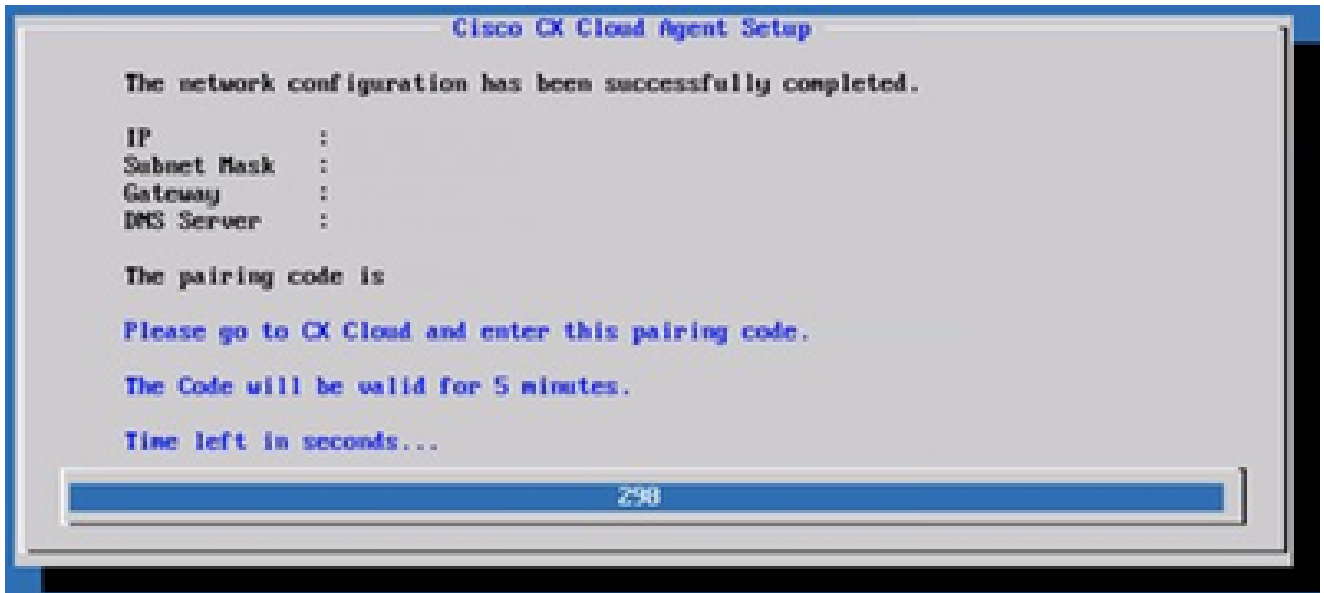
10. Click **Continue** to proceed with the configuration for successful domain reach. The configuration can take several minutes to complete.

 **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.



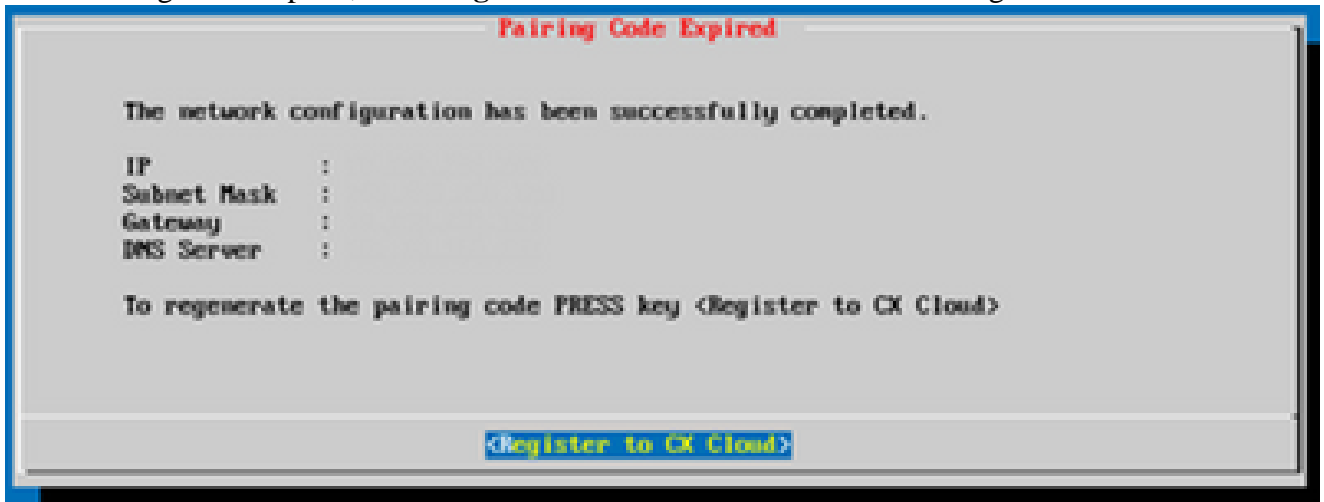
Configuration in Progress

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



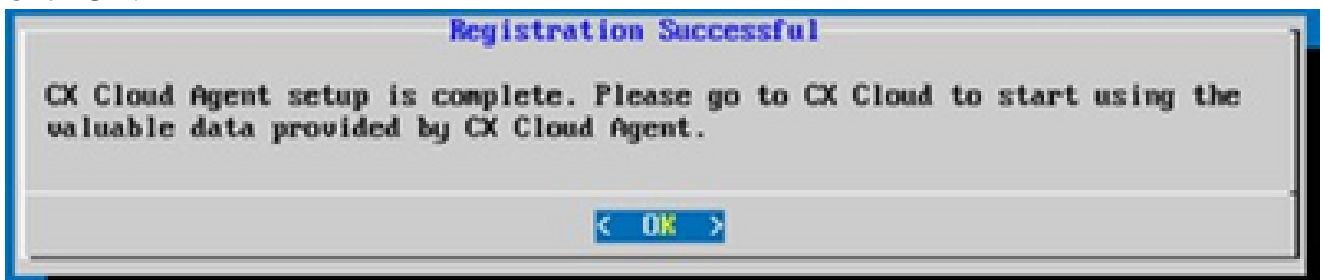
Pairing Code

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: 3 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 DNA Center To Forward Syslog to CX Cloud Agent

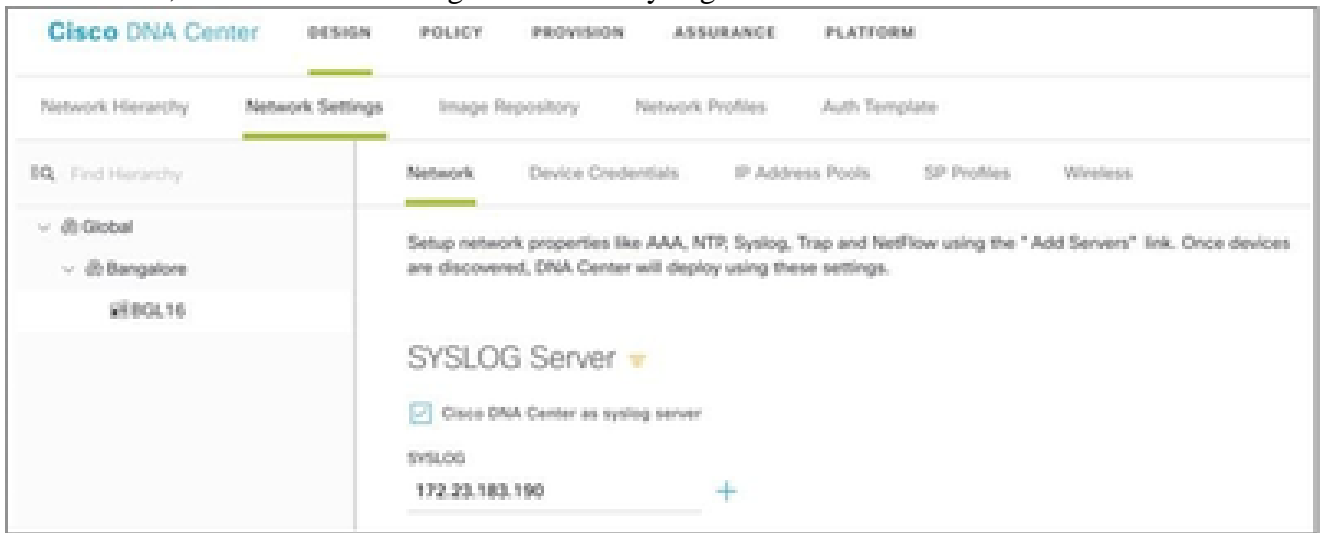
Prerequisites

Supported Cisco DNA 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 DNA Center Virtual Appliance

Configure Syslog Forward Setting


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

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




Syslog Server

-
- Notes:**
- 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 the following documentation for specific configuration steps.

[IOS-XE Configuration Guide](#)

[AireOS Wireless Controller Configuration Guide](#)

Enable Information Level Syslog Settings

To make Syslog Information level visible, perform the following 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

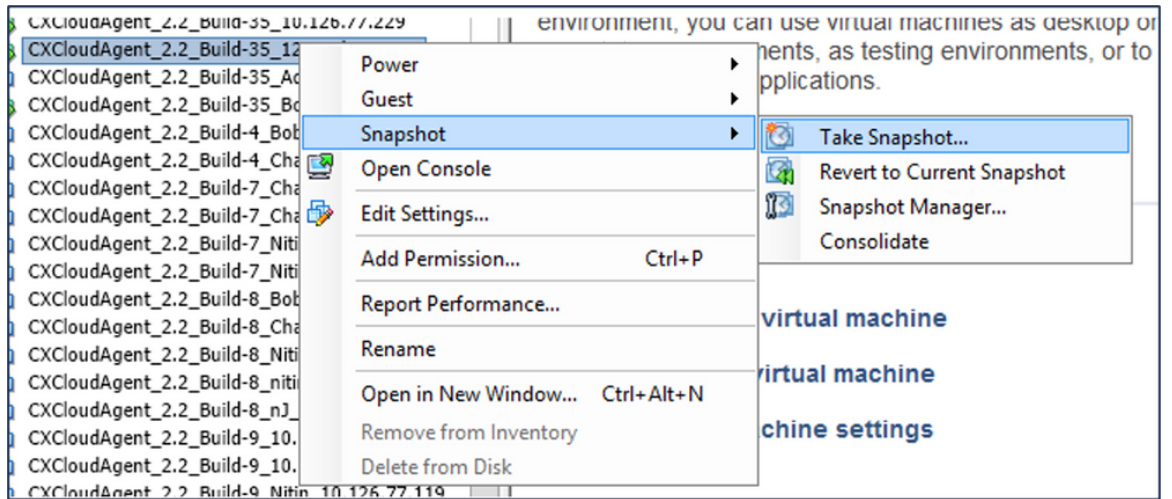
Back up and Restore the CX Cloud VM

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.

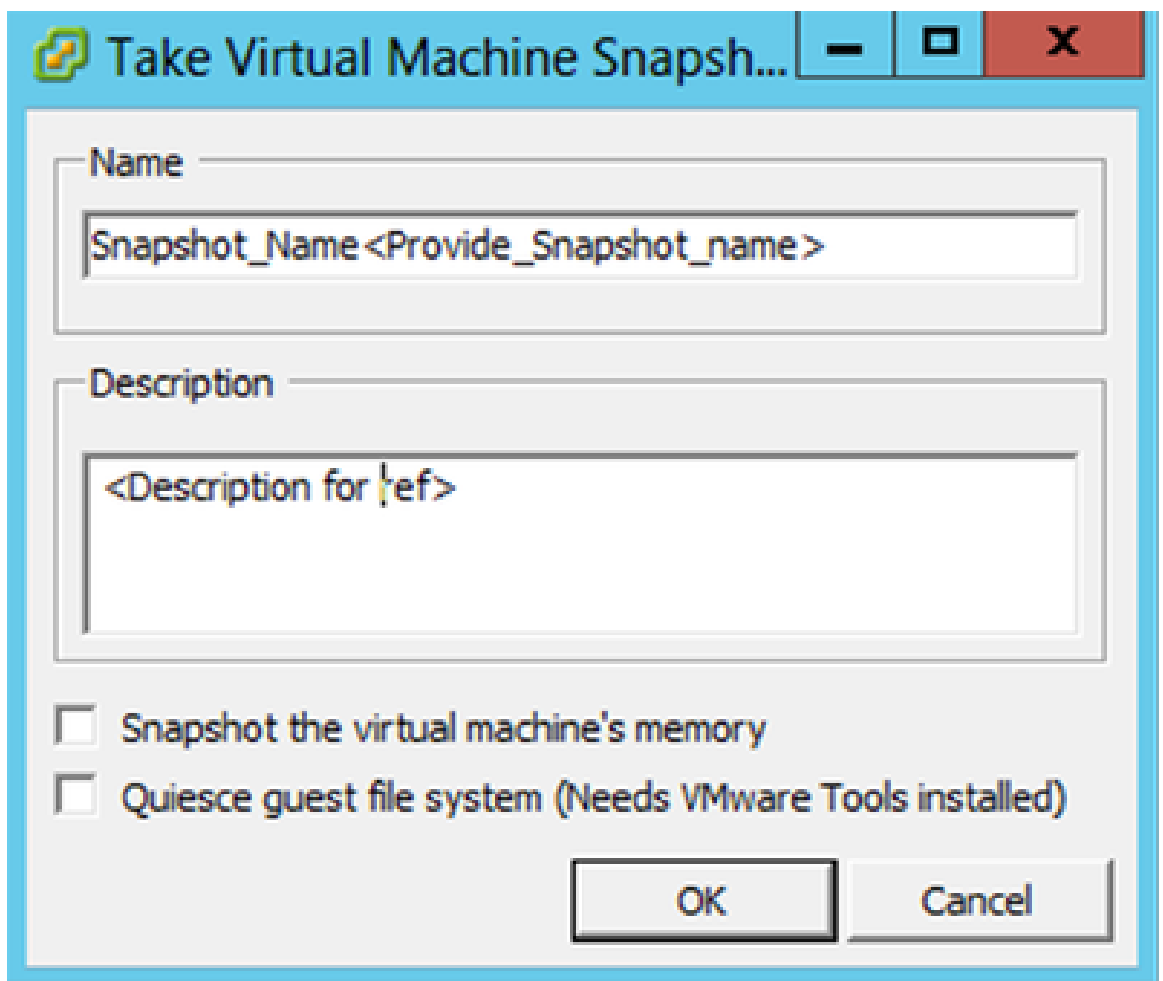
Back Up

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

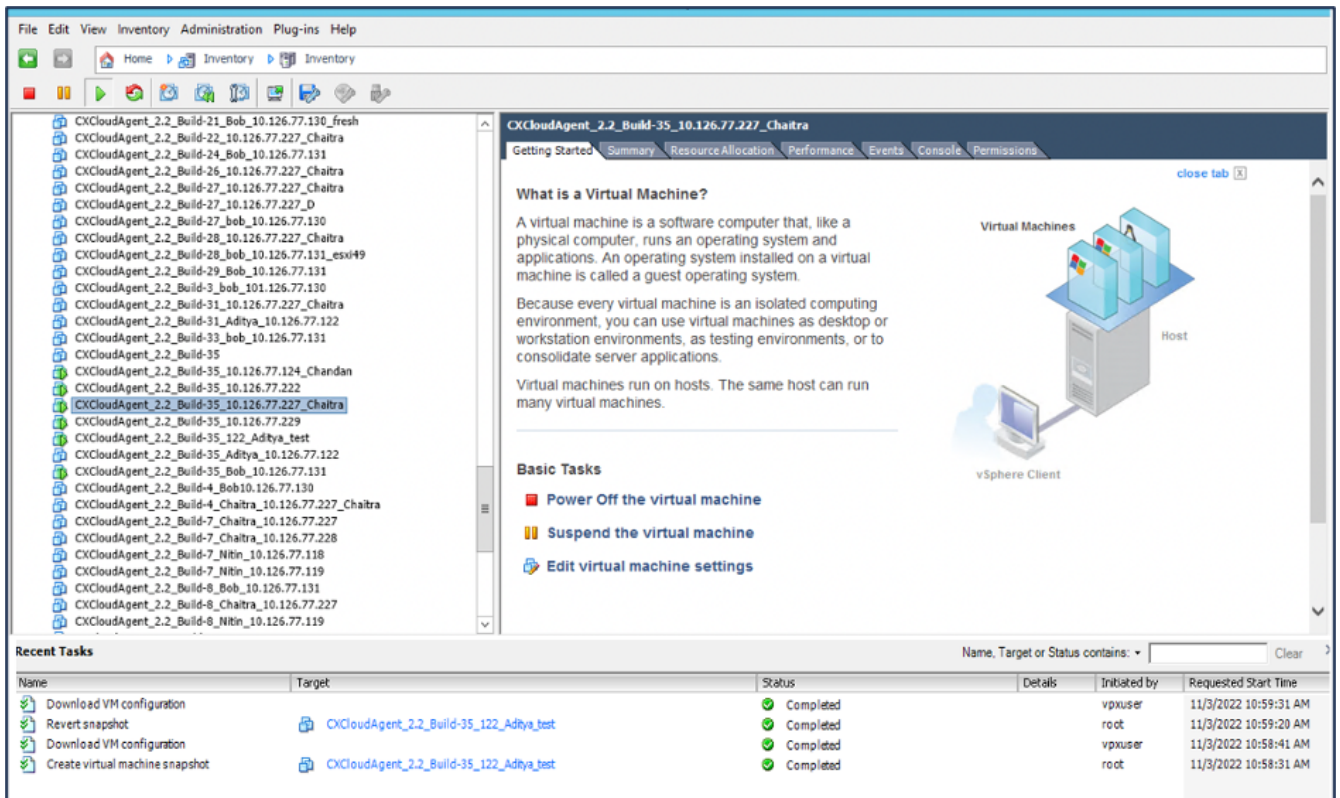


Take Virtual Machine Snapshot

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.

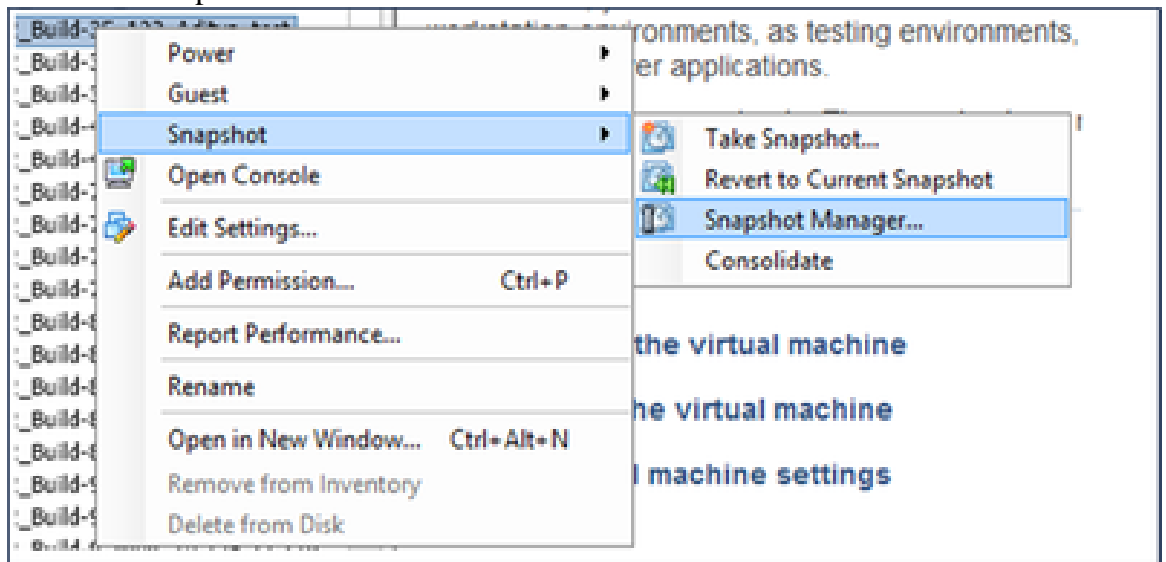


Recent Tasks

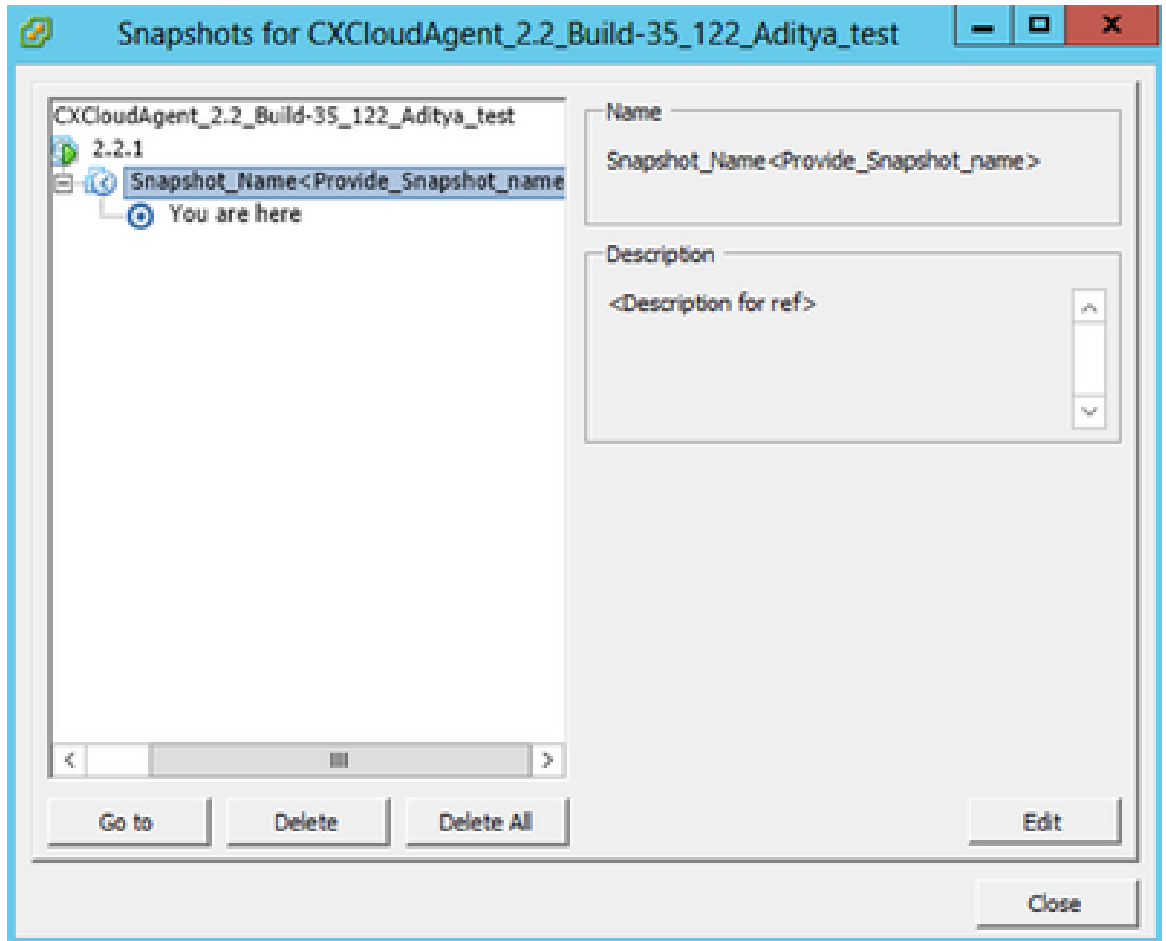
Restore

To restore the CX Cloud VM:

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

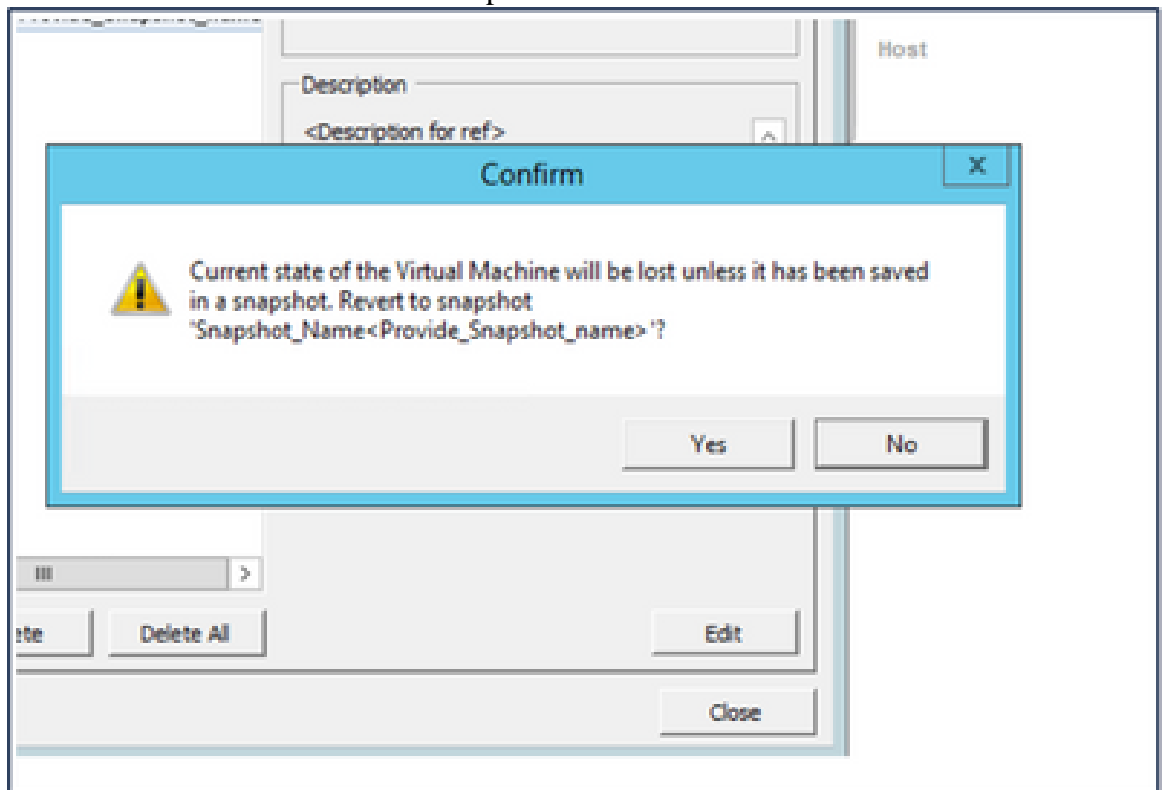


Select VM window



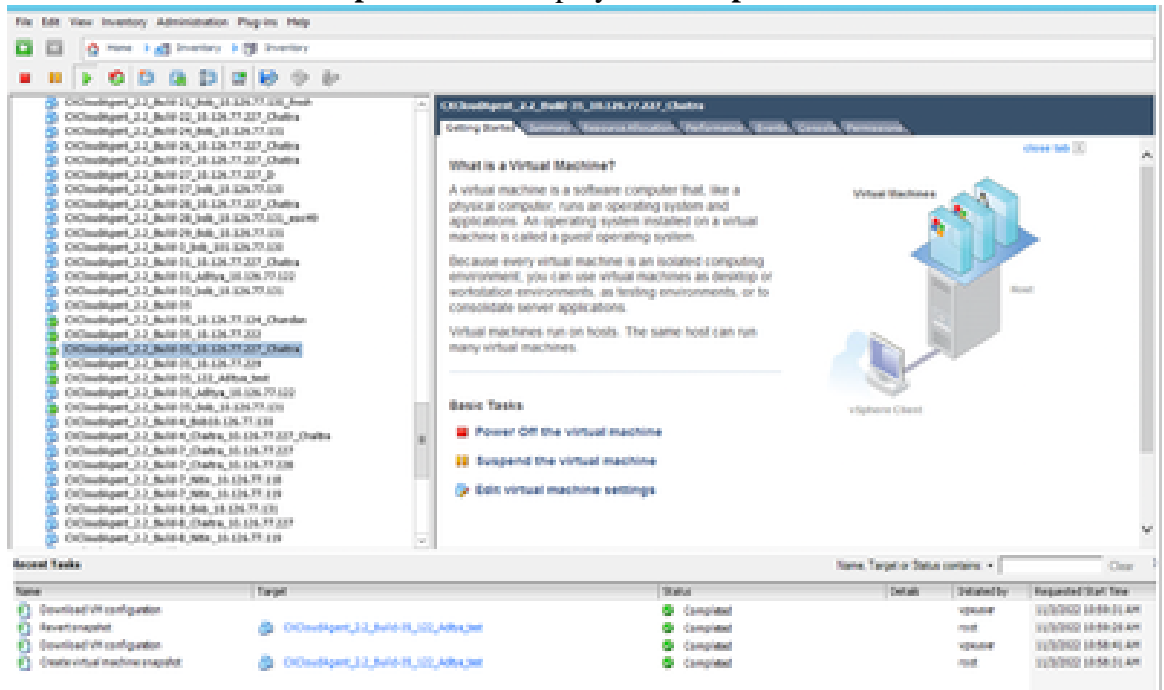
Snapshots window

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



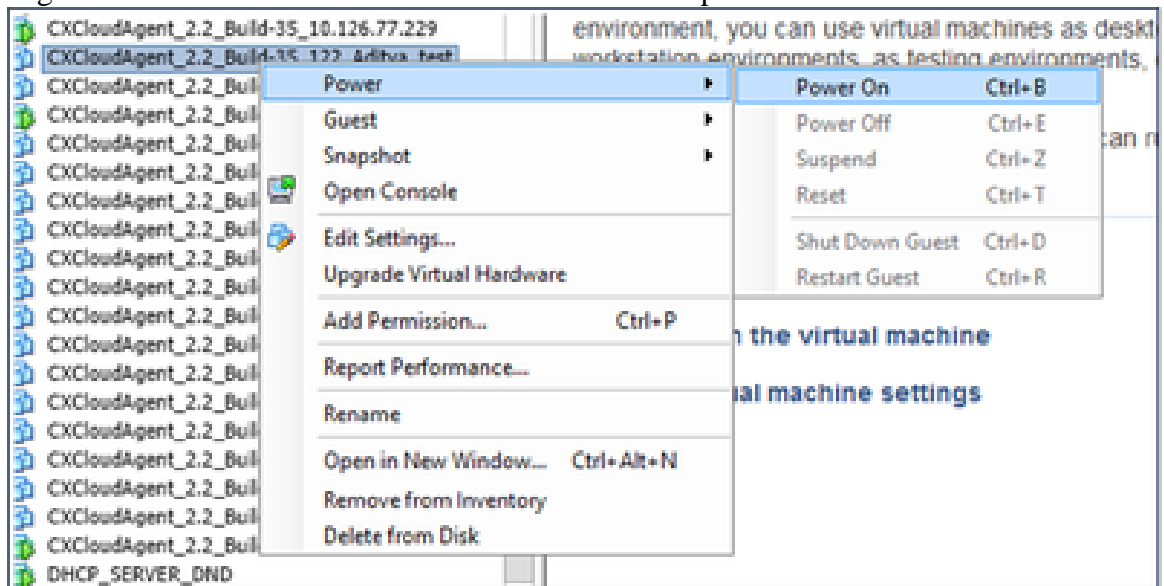
Confirm window

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



Recent Tasks

- 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 (<https://swims.cisco.com/abraxas/decrypt>). 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 DNA 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, etc. 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 DNA 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 FAQ to set his bootloader (single user mode) password.
User Access	SSH: <ul style="list-style-type: none"> · Access to appliance using cxcadmin user requires credentials created during installation · Access to appliance using excroot user requires credentials to be decrypted using SWIM portal by authorized personnel
User Accounts	<ul style="list-style-type: none"> · cxcadmin: default user account created; User can execute CX Cloud Agent application commands using cxcli and has least privileges on the appliance; excroot user and its encrypted password is generated using cxcadmin user · excroot: cxcadmin can create this user using the utility "remoteaccount"; User can gain root privileges with this account
cxcadmin password policy	<ul style="list-style-type: none"> · Password is one-way hashed using SHA-256 and stored securely · Minimum eight (8) characters, containing three of the following categories: uppercase, lowercase, numbers, and special characters
excroot password policy	<ul style="list-style-type: none"> · excroot password is RSA/ECB/PKCS1v1_5 encrypted · The passphrase generated needs to be decrypted in SWIM portal

	<ul style="list-style-type: none"> · The cxroot user and password is valid for two days and can be regenerated using cxcadmin user
ssh login password policy	<ul style="list-style-type: none"> · Minimum of eight characters that contains three of the following categories: uppercase, lowercase, numbers, and special characters · Five failed log in attempts lock the box for 30 minutes; Password expires in 90 days
Ports	Open Incoming Ports – 514(Syslog) and 22 (SSH)
Data Security	<ul style="list-style-type: none"> · No Customer information stored · No Device data stored · Cisco DNA Center server credentials encrypted and stored in the database