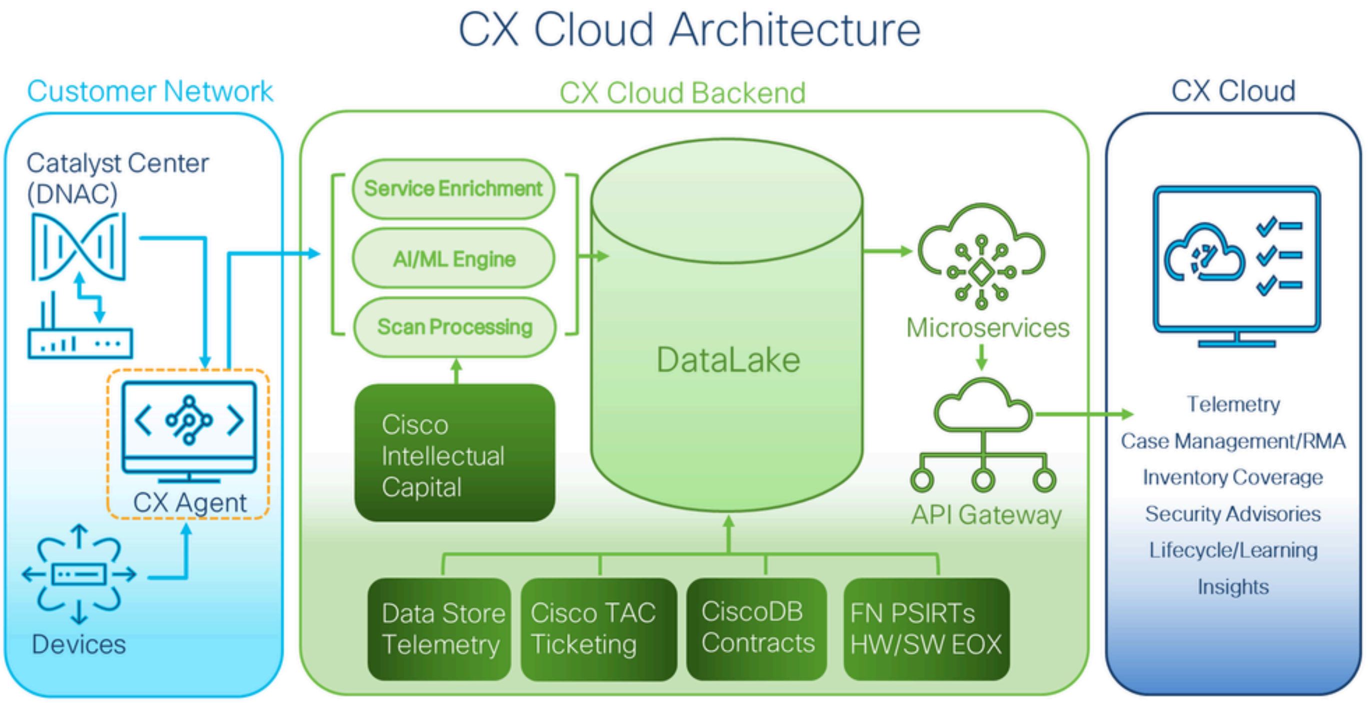
CX Agent Overview Guide v3.1

Contents

Introduction

This document describes Cisco's Customer Experience (CX) Agent. Cisco's CX Agent is a highly scalable platform that collects telemetry data from customer network devices to deliver actionable insights for customers. CX Agent enables the Artificial Intelligence (AI)/Machine Learning (ML) transformation of active running configuration data into proactive and predictive insights displayed in CX Cloud (including Success Tracks, Smart Net Total Care (SNTC) and Business Critical Services (BCS) or Lifecycle Services (LCS) offers).



CX Cloud Architecture

This guide is intended for CX Cloud and Partner Administrators only. Users with Super User Admin (SUA) and Admin roles have the necessary permissions to perform the actions described in this guide.

This guide is specific to CX Agent v3.1. Refer to the Cisco CX Agent page to access prior versions.

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

Prerequisites

CX 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 and version 2025
- The configurations in the following table are required for deploying VM:

CX Agent Deployment Type	**Number of CPU Cores**	**RAM**	**Hard Disk**	***Maximum number of Assets directly connected to CX Agent**	**Supported Hypervisors**
Small OVA	8C	16GB	200GB	10,000	VMware ESXi, Oracle VirtualBox, and Windows Hyper-V
Medium OVA	16C	32GB	600GB	20,000	VMware ESXi
Large OVA	32C	64GB	1200GB	50,000 :	VMware ESXi

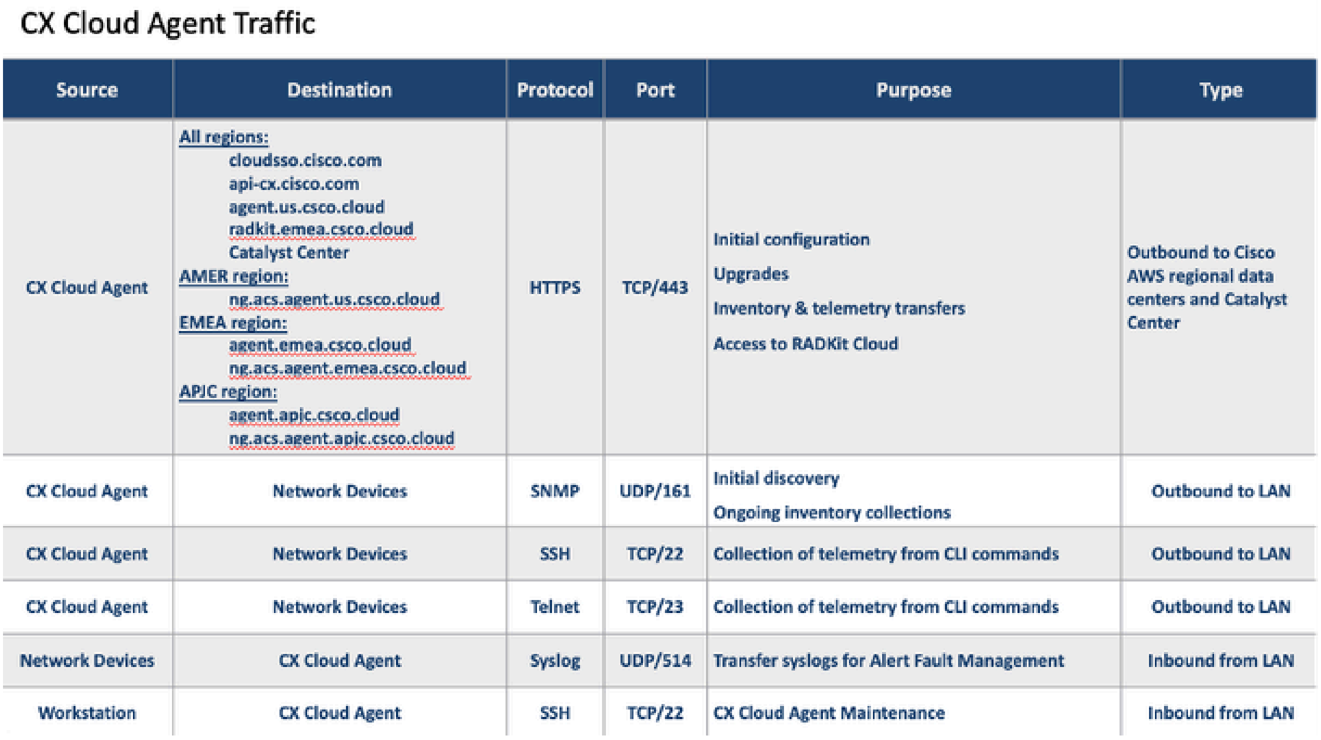
*In addition to connecting 20 Cisco Catalyst Center (Catalyst Center) non-clusters or 10 Catalyst Center clusters for each CX Cloud Agent instance.

Note:RADKit service is available exclusively for CX Agent deployments of Medium and Large OVA types.

- For customers using designated US data centers as the primary data region to store CX Cloud data, the CX 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.csco.cloud
  - FQDN: ng.acs.agent.us.csco.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 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.csco.cloud
  - FQDN: agent.emea.csco.cloud
  - FQDN: ng.acs.agent.emea.csco.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 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.csco.cloud
  - FQDN: agent.apjc.csco.cloud
  - FQDN: ng.acs.agent.apjc.csco.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.csco.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.
- For customers using RADKit using the FQDN, and HTTPS on TCP port 443:
  - US FQDN: radkit.us.csco.cloud
  - EMEA FQDN: radkit.emea.csco.cloud

- APJC FQDN: radkit.apjc.csco.cloud

- To enable RADKit to attach output to a Service Request, the FQDN cxd.cisco.com must be accessible for the CX Agent.
- 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	All regions: cloudsso.cisco.com api-cx.cisco.com agent.us.csco.cloud radkit.emea.csco.cloud Catalyst Center AMER region: ng.acs.agent.us.csco.cloud EMEA region: agent.emea.csco.cloud ng.acs.agent.emea.csco.cloud APJC region: agent.apjc.csco.cloud ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/443	Initial configuration Upgrades Inventory & telemetry transfers Access to RADKit Cloud	Outbound to Cisco AWS regional data centers and Catalyst 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 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 Agent Portal

Major Domains	Other Domains
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com

	appdynamics.com
	tiqcdn.com
	jquery.com

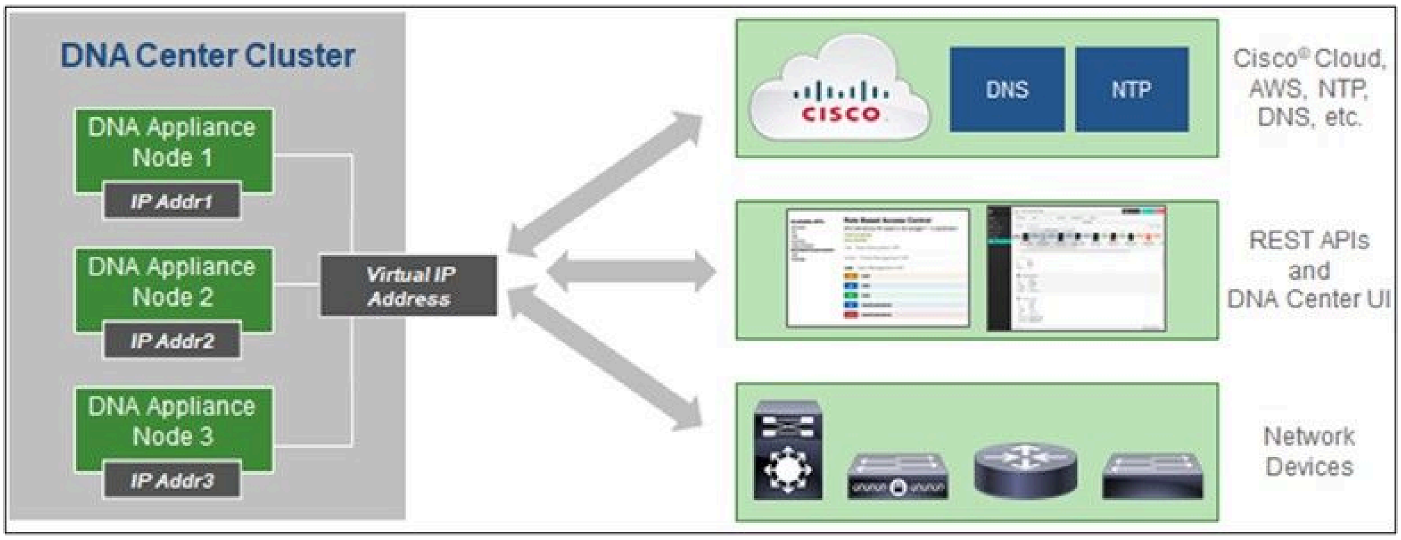
Domains Specific to CX Agent OVA

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.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agent.emea.csco.cloud	agent.apjc.csco.cloud
	ng.acs.agent.emea.csco.cloud	ng.acs.agent.apjc.csco.cloud

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

Catalyst Center Supported Versions

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.



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 Agent, refer to the *Supported Product List*.

Upgrading/Installing CX Agent v3.1

- Existing customers upgrading to the new version should refer to Upgrading CX Agent v3.1.
- New customers implementing a fresh flexible OVA v3.1 install should refer to Adding CX Agent.

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.

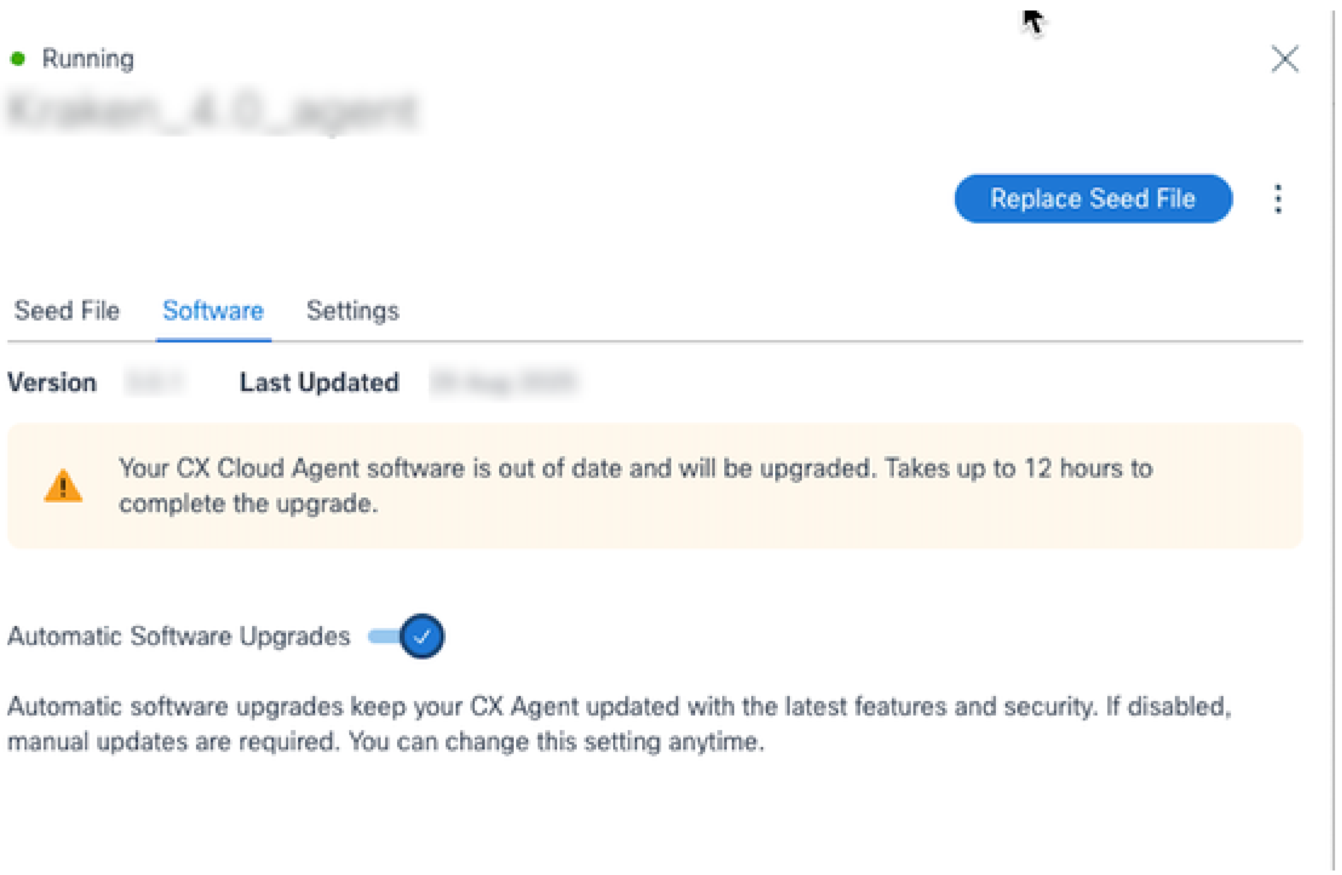
To upgrade the existing VM configuration from small to medium or large, refer to section Upgrading CX Agent VMs to medium and large configuration.

Upgrading to CX Agent v3.1

Existing customers can upgrade to the latest version by enabling automatic upgrades or by choosing to upgrade manually from their existing version.

Automatic Upgrades

Customers can enable the **Automatic Software Upgrade** toggle to ensure their system is updated when the new versions are released. This option is enabled by default for new installations but can be modified at any time to align with company policies or to schedule upgrades during planned maintenance windows.



Running

[redacted]

Version [redacted] **Last Updated** [redacted]

⚠ Your CX Cloud Agent software is out of date and will be upgraded. Takes up to 12 hours to complete the upgrade.

Automatic Software Upgrades ✓

Automatic software upgrades keep your CX Agent updated with the latest features and security. If disabled, manual updates are required. You can change this setting anytime.

Automatic Upgrades

Note: The automatic upgrades are disabled by default for existing CX Agent instance(s) but users can enable them at any time.

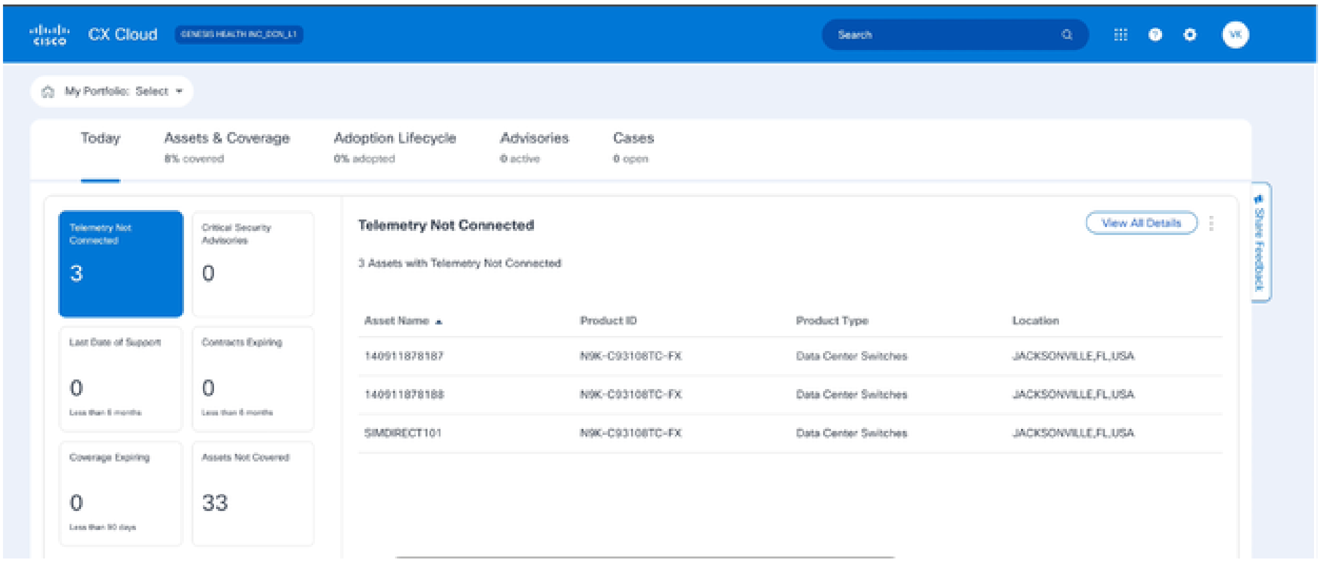
Manual Upgrades

Customers who prefer not to use automatic upgrades and have not enabled **Automatic Software Upgrades** can choose to upgrade manually. CX Agent v2.4.x and above support a direct upgrade to v3.1 by following the steps outlined in this section.

Note: Customers on CX Agent v2.3.x and below should incrementally upgrade to v2.4.x before upgrading to v3.1 or perform a fresh OVA install.

To install the CX Agent upgrade v3.1 from CX Cloud:

1. Log in CX Cloud. The **Home** page displays.



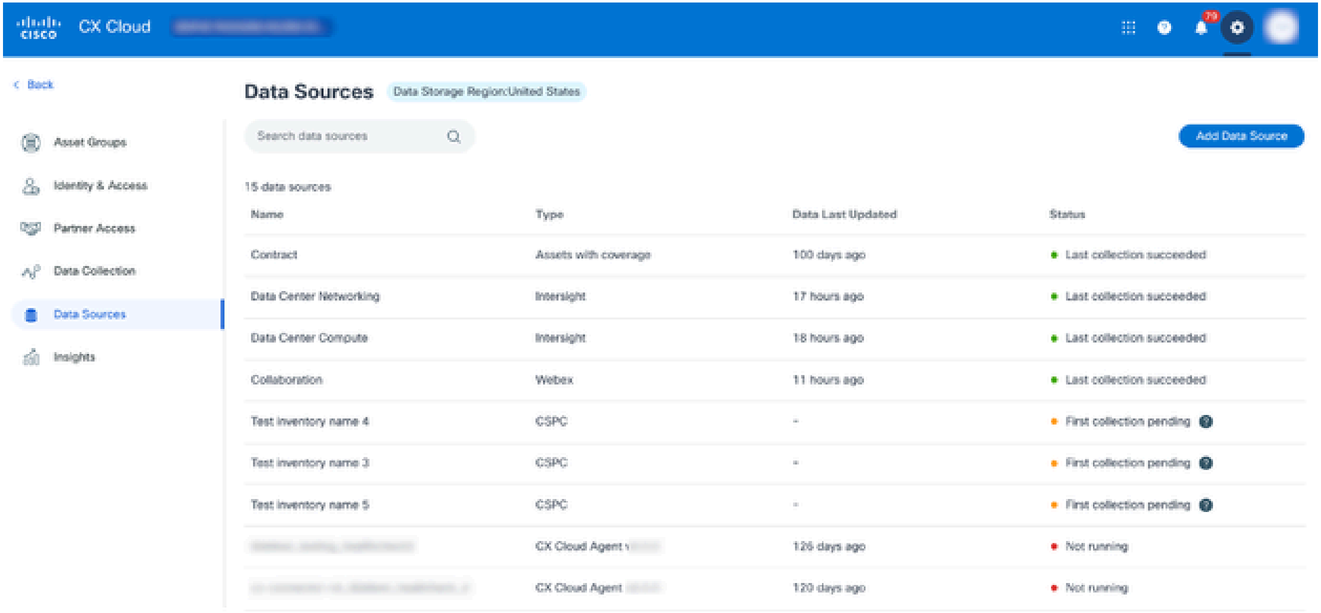
Telemetry Not Connected

3 Assets with Telemetry Not Connected

Asset Name ▲	Product ID	Product Type	Location
140911878187	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA
140911878188	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA
SIMDIRECT101	N9K-C93108TC-FX	Data Center Switches	JACKSONVILLE,FL,USA

CX Cloud Home Page

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



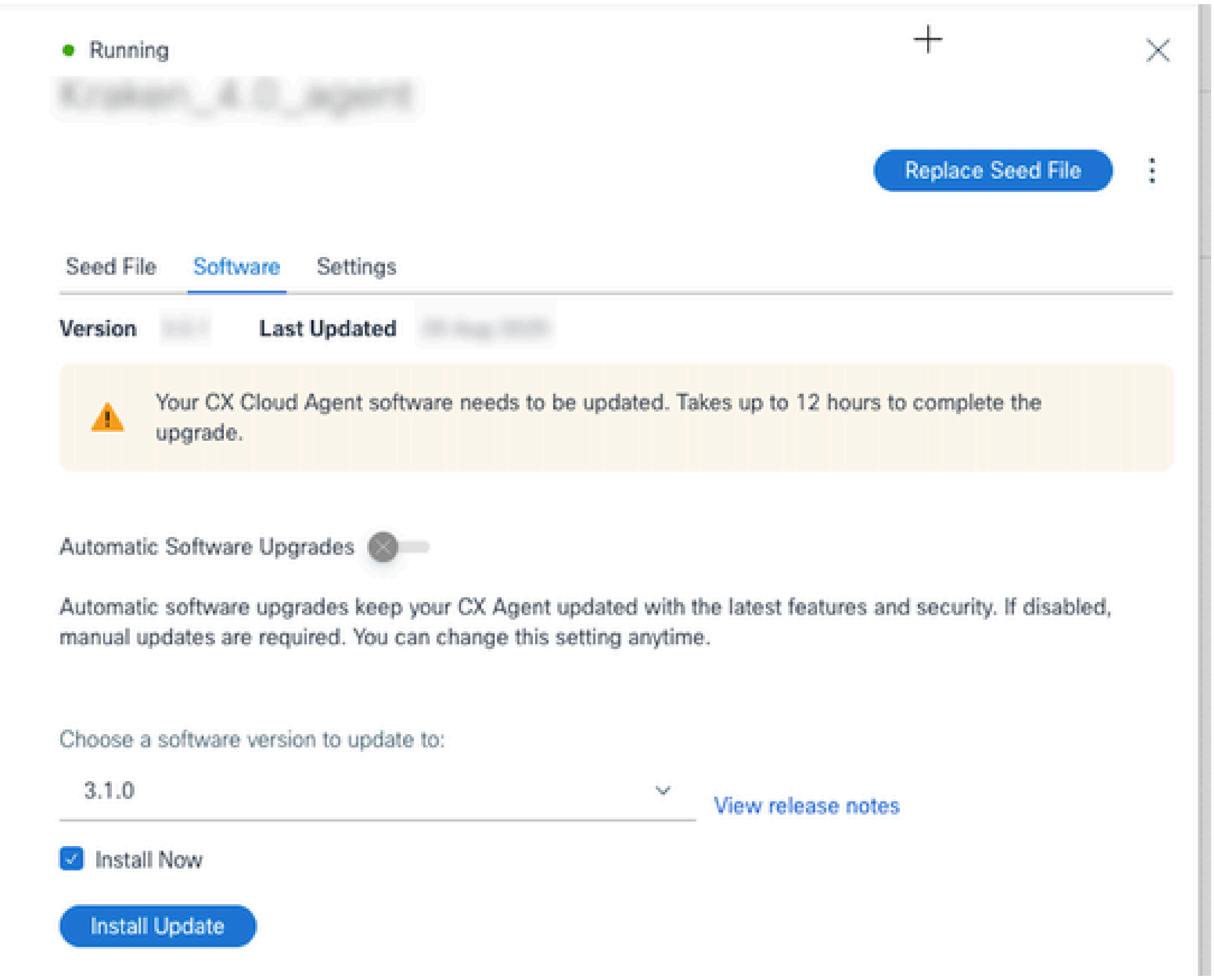
Data Sources Data Storage Region:United States

15 data sources

Name	Type	Data Last Updated	Status
Contract	Assets with coverage	100 days ago	● Last collection succeeded
Data Center Networking	Intersight	17 hours ago	● Last collection succeeded
Data Center Compute	Intersight	18 hours ago	● Last collection succeeded
Collaboration	Webex	11 hours ago	● Last collection succeeded
Test inventory name 4	CSPC	-	● First collection pending
Test inventory name 3	CSPC	-	● First collection pending
Test inventory name 5	CSPC	-	● First collection pending
[redacted]	CX Cloud Agent [redacted]	126 days ago	● Not running
[redacted]	CX Cloud Agent [redacted]	120 days ago	● Not running

Data Sources

3. Click the **CX Agent** Data Source. The **CX Agent** details window opens.



● Running

[redacted]

Replace Seed File

Seed File | Software | Settings

Version [redacted] **Last Updated** [redacted]

⚠ Your CX Cloud Agent software needs to be updated. Takes up to 12 hours to complete the upgrade.

Automatic Software Upgrades ○

Automatic software upgrades keep your CX Agent updated with the latest features and security. If disabled, manual updates are required. You can change this setting anytime.

Choose a software version to update to:

3.1.0

View release notes

☑ Install Now

Install Update

Manual Upgrades

4. Select the software version **3.1.0** from **Choose a software version to update to** drop-down list.
5. Click **Install Update** to install CX Agent v3.1.

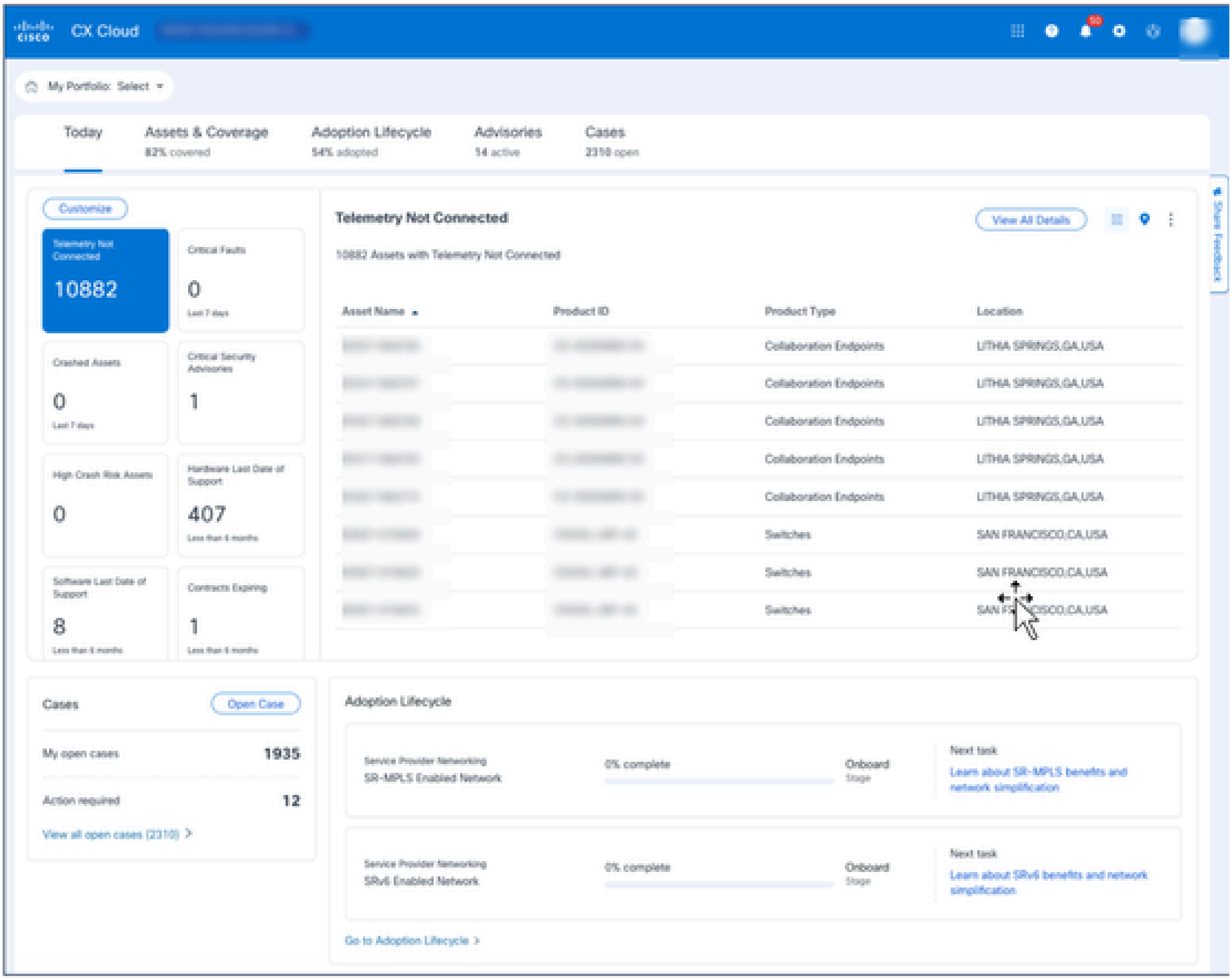
Note: Customers can schedule the update for later by clearing the **Install Now** check box which displays scheduling options.

Adding CX Agent

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

To add a CX Agent:

1. Log in to CX Cloud. The **Home** page displays.



Telemetry Not Connected

10882 Assets with Telemetry Not Connected

Asset Name ▲	Product ID	Product Type	Location
[redacted]	[redacted]	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
[redacted]	[redacted]	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
[redacted]	[redacted]	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
[redacted]	[redacted]	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
[redacted]	[redacted]	Collaboration Endpoints	LITHIA SPRINGS,GA,USA
[redacted]	[redacted]	Switches	SAN FRANCISCO,CA,USA
[redacted]	[redacted]	Switches	SAN FRANCISCO,CA,USA
[redacted]	[redacted]	Switches	SAN FRANCISCO,CA,USA

Cases	
My open cases	1935
Action required	12

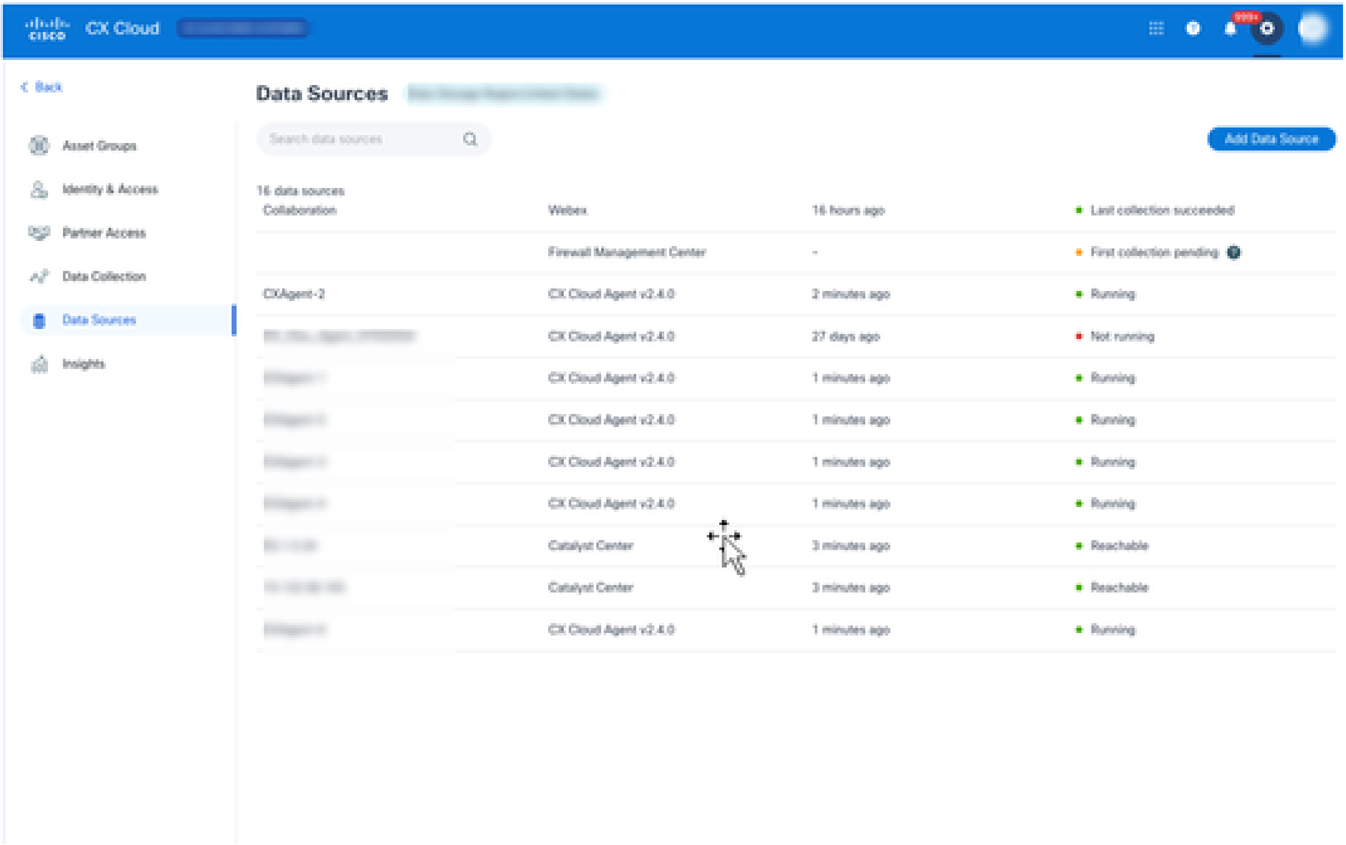
View all open cases (2310) >

Service Provider Networking SR-MPLS Enabled Network	0% complete	Onboard Stage	Next task Learn about SR-MPLS benefits and network simplification
Service Provider Networking SRv6 Enabled Network	0% complete	Onboard Stage	Next task Learn about SRv6 benefits and network simplification

Go to Adoption Lifecycle >

CX Cloud Home page

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

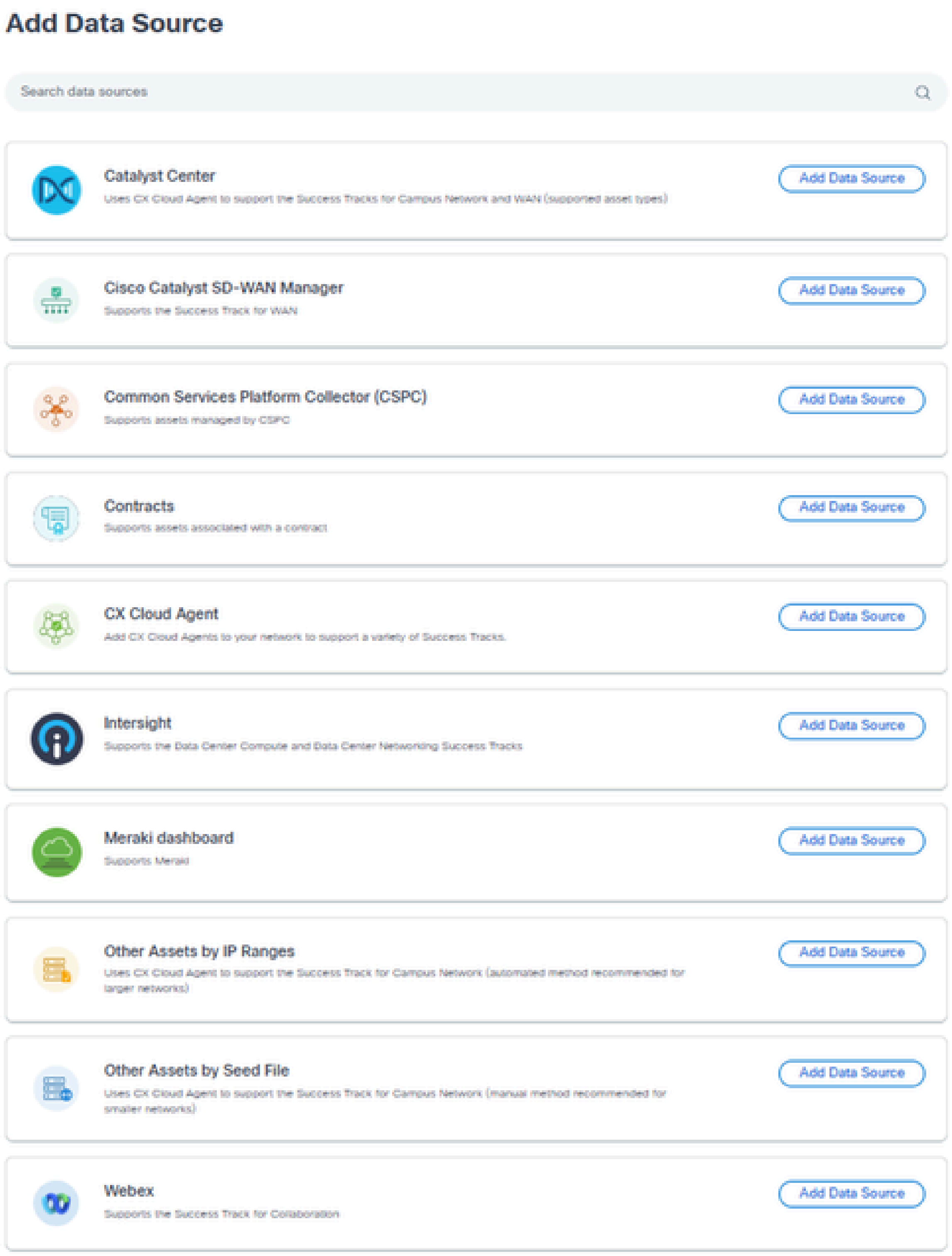


16 data sources

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
[redacted]	CX Cloud Agent v2.4.0	27 days ago	● Not running
[redacted]	CX Cloud Agent v2.4.0	1 minutes ago	● Running
[redacted]	CX Cloud Agent v2.4.0	1 minutes ago	● Running
[redacted]	CX Cloud Agent v2.4.0	1 minutes ago	● Running
[redacted]	CX Cloud Agent v2.4.0	1 minutes ago	● Running
[redacted]	Catalyst Center	3 minutes ago	● Reachable
[redacted]	Catalyst Center	3 minutes ago	● Reachable
[redacted]	CX Cloud Agent v2.4.0	1 minutes ago	● Running

Data Sources

3. Click **Add Data Source**. The **Add Data Source** page opens. Displayed options vary based on customer subscriptions.



Add Data Source

Search data sources

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

Common Services Platform Collector (CSPC)
Supports assets managed by CSPC

Contracts
Supports assets associated with a contract

CX Cloud Agent
Add CX Cloud Agents to your network to support a variety of Success Tracks.

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

Meraki dashboard
Supports Meraki

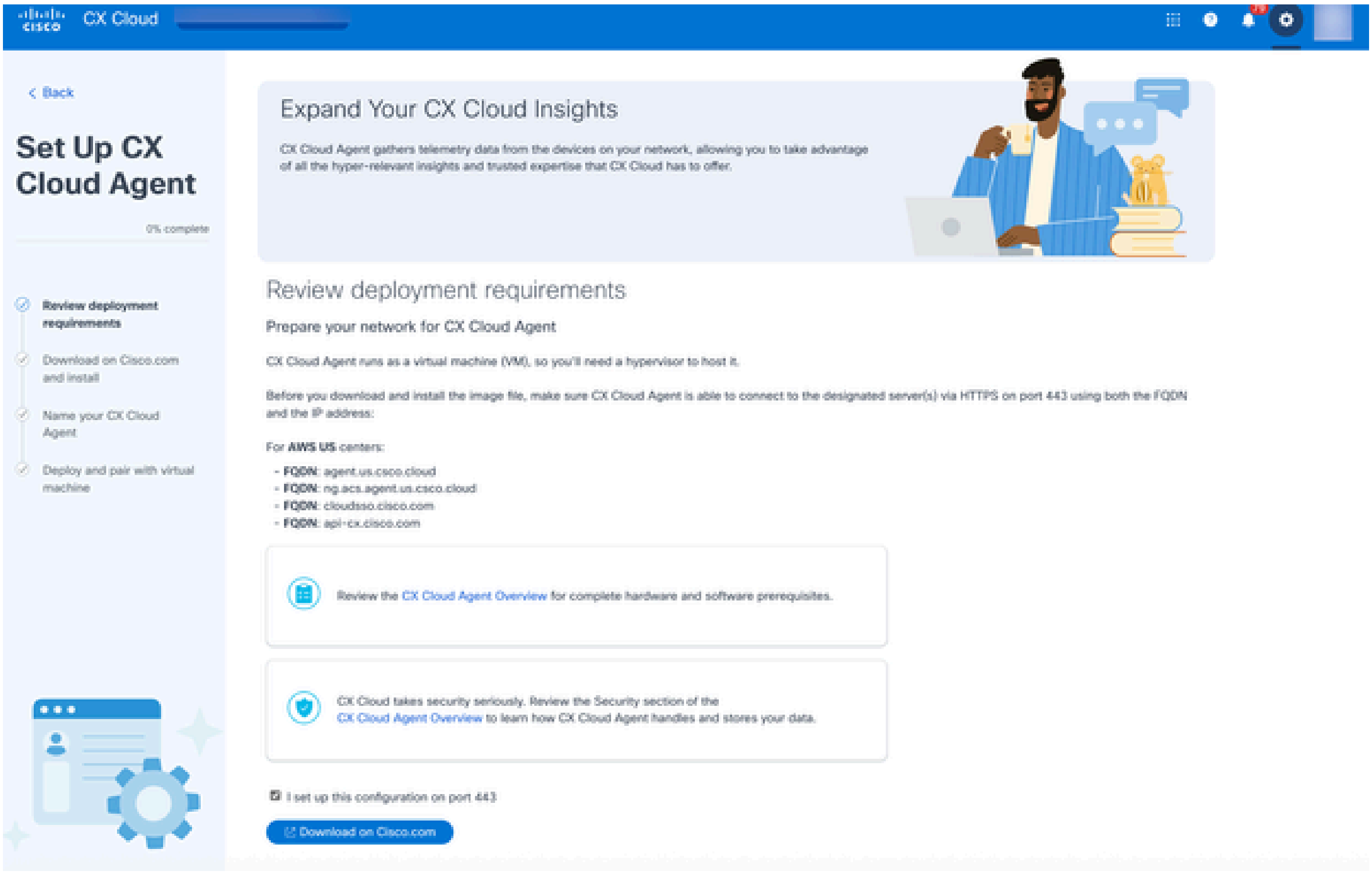
Other Assets by IP Ranges
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

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

Webex
Supports the Success Track for Collaboration

Add Data Source

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



< Back

Set Up CX Cloud Agent

0% complete

- Review deployment requirements
- Download on Cisco.com and install
- Name your CX Cloud Agent
- Deploy and pair with virtual machine

Expand Your CX Cloud Insights

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** centers:

- **FQDN**: agent.us.csco.cloud
- **FQDN**: ng.acs.agent.us.csco.cloud
- **FQDN**: cloudsso.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.

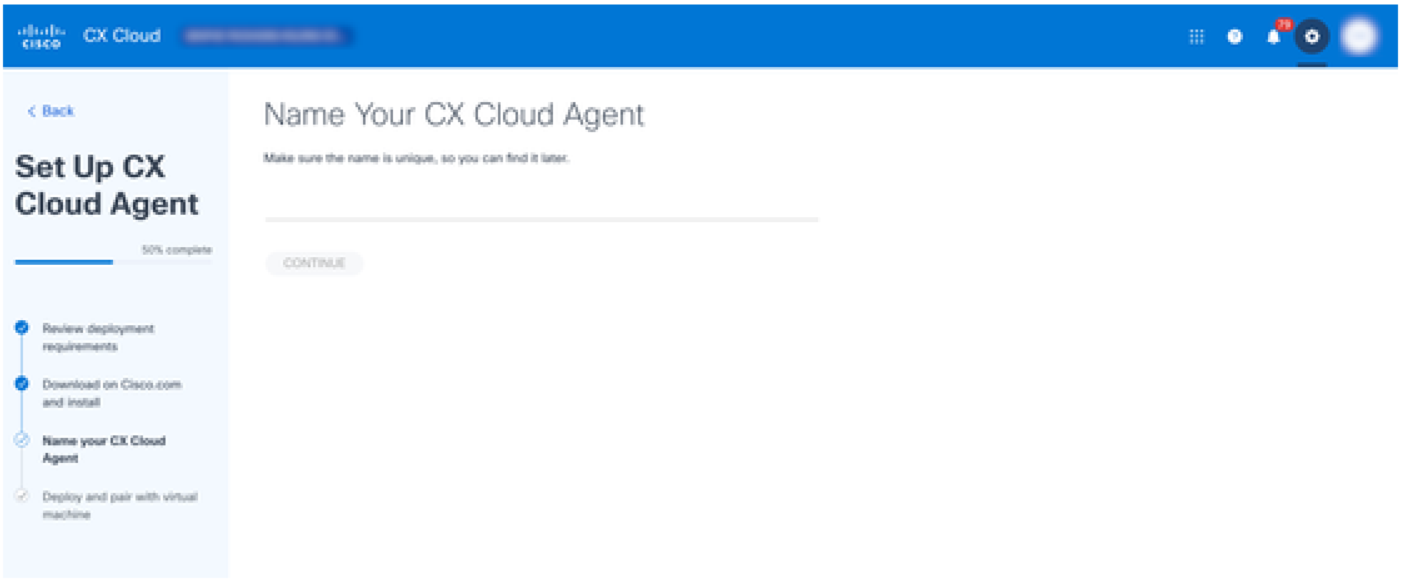
☑ I set up this configuration on port 443

Adding CX 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** window opens in another tab.
7. Download the “CX Agent v3.1.0 OVA” file.

Note: A Pairing Code required to complete the CX Agent setup is generated after deploying the “OVA” file.

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



< Back

Set Up CX Cloud Agent

50% complete

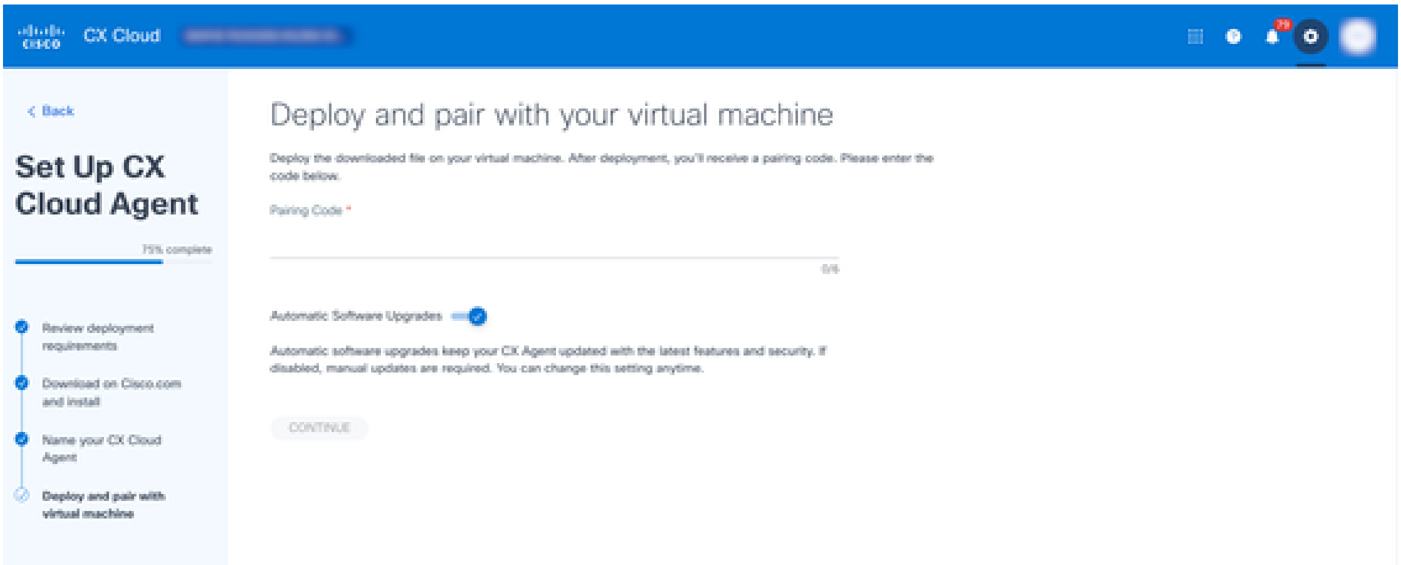
- Review deployment requirements
- Download on Cisco.com and install
- Name your CX Cloud Agent
- Deploy and pair with virtual machine

Name Your CX Cloud Agent

Make sure the name is unique, so you can find it later.

Name CX Agent

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


CX Cloud
< Back
Set Up CX Cloud Agent
75% complete
Review deployment requirements
Download on Cisco.com and install
Name your CX Cloud Agent
Deploy and pair with virtual machine
0/6
CONTINUE

Deploy and pair with your virtual machine

Deploy the downloaded file on your virtual machine. After deployment, you'll receive a pairing code. Please enter the code below.

Pairing Code *

Automatic Software Upgrades

Automatic software upgrades keep your CX Agent updated with the latest features and security. If disabled, manual updates are required. You can change this setting anytime.

Pairing Code

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

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

Note: Repeat the steps above to add additional CX Agent instances as a Data Source.

Configuring CX Agent for BCS/LCS

Cisco’s new Converged Collection feature streamlines CX Agent v3.1 configuration for BCS/LCS, simplifying the customer experience.

Note:This configuration is specific to Cisco Support Engineers responsible for Collector setup for BCS/LCS customers.

BCS/LCS customers can visit the CX Cloud Community to learn more about user onboarding and other related information.

Prerequisites

Support Engineers with Super User Administrator (SUA) and Administrator access can only perform CX Agent configuration for BCS/LCS.

Configuring CX Agent

To configure CX Agent for BCS/LCS, contact Cisco Support.

Configuring RADKit Capabilities

CX Agent v3.1 provides an optional RADKit configuration designed to enhance remote management and troubleshooting of Cisco devices in CX Cloud. When enabled, authorized users can securely perform operations such as data capture, configuration, and software upgrades remotely. These settings can be enabled or disabled at any time based on customer's operational requirements.

For comprehensive details on RADKit, refer to Cisco RADKit.

Integrating RADKit Client Through CLI

To integrate the RADKit client service, create an administrator account and enroll the service by completing the following steps:

Note: The following steps require root access to the CX Agent VM.

1. Open the terminal and Secure Shell (SSH) into a VM using the appropriate credentials, for example:

```
ssh your_username@your_vm_ip
```

2. Run the following command to enable network connectivity:

```
kubectl get netpol deny-from-other-namespaces -o yaml >
/home/cxcadmin/deny-from-other-namespaces.yaml
```

```
kubectl delete netpol deny-from-other-namespaces
```

3. On the local machine, send a POST request to the manager endpoint to create an administrator account. The request body should include:

- **admin_name** (required): The username for the administrator account
- **email** (optional): The email address for the administrator account
- **full_name** (optional): The full name of the Administrator
- **description** (optional): A description of the administrator account

The following example shows how to send this request using cURL:

```
curl -X POST \
  http://<your_vm_ip>:30100/radkitmanager/v1/createAdmin \
  -H "Content-Type: application/json" \
  -d '{
        "admin_name": "admin_user123",
        "email": "admin@example.com",
        "full_name": "Admin User",
        "description": "Administrator account for managing the system"
      }'
```

Upon successful creation of an administrator account, the server responds with a confirmation message indicating that the administrator account has been successfully created. This response also includes a temporary password that must be changed upon the first login. However, if the administrator account already exists, the server returns a 400 status code with the message “Admin already created”.

4. Open the web browser and navigate to the RADKit web UI: https://<your_vm_ip>:30101/.
5. Log in using the administrator username (admin_name) and the temporary password provided in the response.

Note: Upon first login, users are prompted to change the password. Follow the instructions to set a new password.

6. Run the RADKit client on the local machine to enroll the service.
7. After authentication, generate a one-time password by running the following command:

```
grant_service_otp()
```

8. On the local machine, send a POST request to the manager endpoint to enroll the service. The request body should include:

- OTP (required): The one-time password string

The following example shows how to send this request using cURL:

```
curl -X POST \

  http://<your_vm_ip>:30100/radkitmanager/v1/enrollService \

  -H "Content-Type: application/json" \

  -d '{

        "one_time_password": "PROD:1234-1234-1234"

      }'
```

Upon successful enrolment, a confirmation message displays and users can manage the RADKit service using an administrator account.

To disable network connectivity, run the following command:

```
kubectl apply -f /home/cxcadmin/deny-from-other-namespaces.yaml
```

Configuring Vault for Existing CX Agents

The optional Vault configuration feature enables CX Cloud to securely connect to a vault service for accessing sensitive data, such as tokens and inventory lists, using the latest credentials. When enabled, CX Cloud automatically uses the configured address and token. This setting can be enabled or disabled at any time. Currently, only HashiCorp's vault configuration is supported.

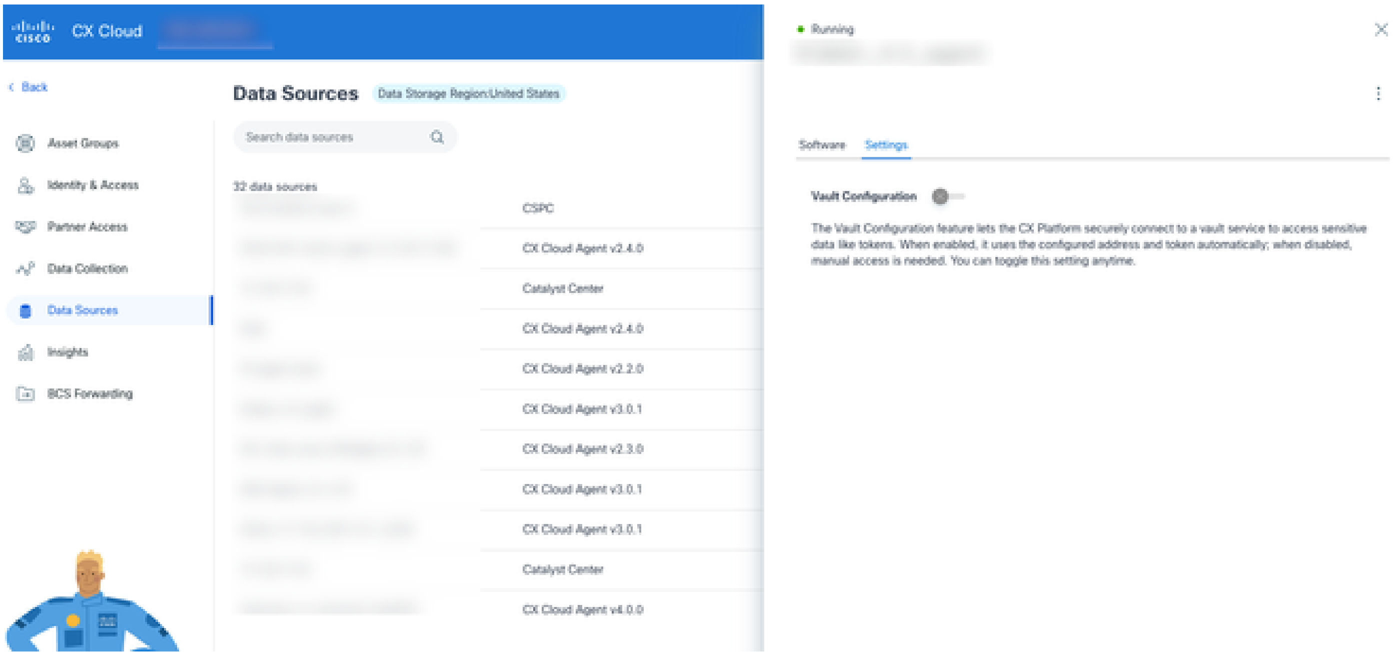
The vault can be configured in two ways:

- Though CX Cloud UI
- Through CLI

Configuring HashiCorp Vault in CX Cloud UI

To configure the HashiCorp vault for an existing CX Agent:

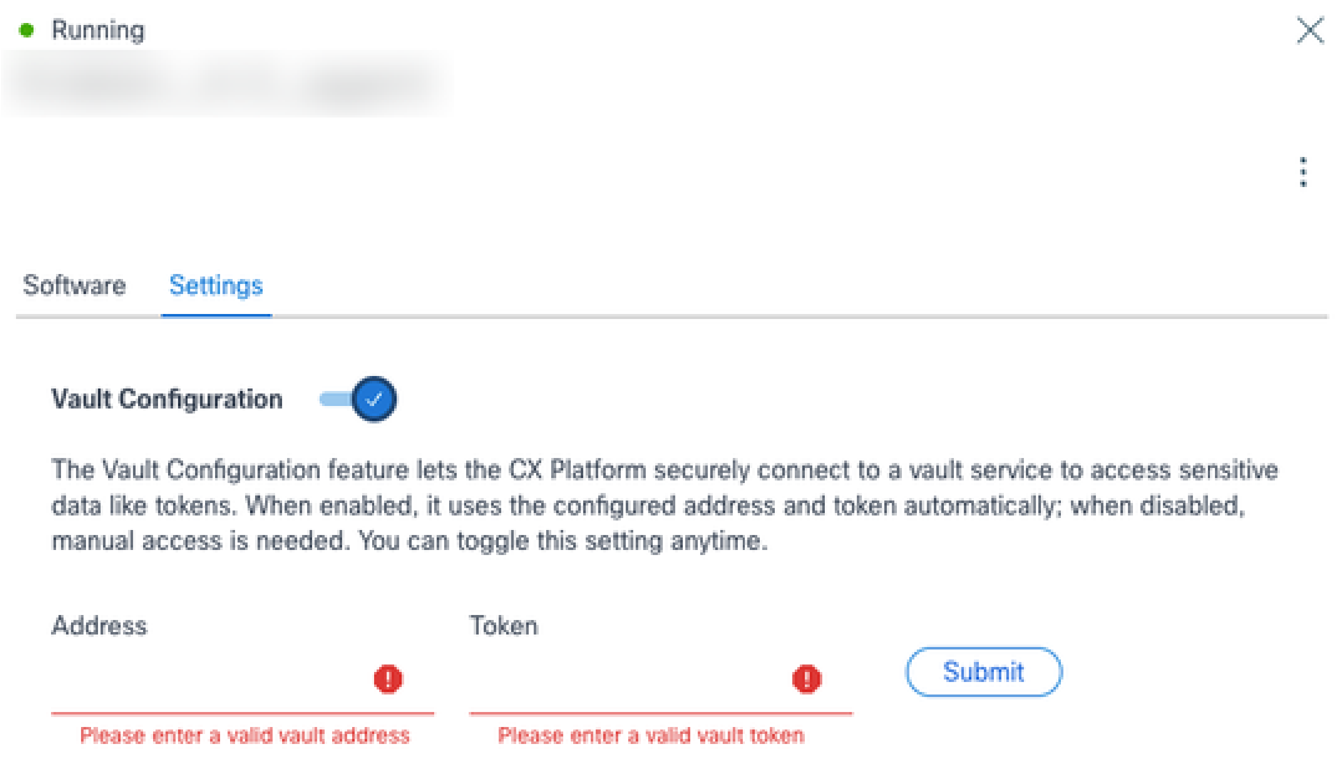
1. Select the **Admin Center** icon. The Data Sources window opens.
2. Click the CX Agent data source. The CX Agent details window opens.



The Vault Configuration feature lets the CX Platform securely connect to a vault service to access sensitive data like tokens. When enabled, it uses the configured address and token automatically; when disabled, manual access is needed. You can toggle this setting anytime.

Settings

3. Click the **Settings** tab.
4. Enable the **Vault Configuration** toggle.



The Vault Configuration feature lets the CX Platform securely connect to a vault service to access sensitive data like tokens. When enabled, it uses the configured address and token automatically; when disabled, manual access is needed. You can toggle this setting anytime.

Please enter a valid vault address

Please enter a valid vault token

5. Enter details in the **Address** and **Token** fields.

6. Click **Submit**. A confirmation and the added IP address displays.

Customers can remove the configured vault by clicking **Remove**.

Integrating CX Agent with HashiCorp Vault Through CLI

This section outlines the procedure for configuring the connection between the Cisco CX Agent and a HashiCorp Vault instance. This integration allows for secure storage and retrieval of device credentials, enhancing the overall security posture.

Prerequisites

- cxcroot access to CX Agent VM
- A running and accessible vault instance

Integrating with HashiCorp Vault

- To enable vault integration, run the following command:

```
cxcli agent vault on
```

- To disable vault integration, run the following command:

```
cxcli agent vault off
```

- To check current vault integration status, run the following command:

```
cxcli agent vault status
```

Enabling HashiCorp Vault Integration

To enable vault integration:

1. Log in to the CX Agent via SSH using the cxcroot user account to access the CX Agent.
2. Switch to the root user to elevate privileges by running the following command:

```
sudo su
```

3. Run the following command to check current vault Integration Status:

```
root@cxcloudagent: /home/cxcroot# cxcli agent vault status

vault integration disabled
```

4. Run the following command to enable vault Integration:

```
cxcli agent vault on
```

5. Update the following fields:

- Vault Address

- Vault Root Token

6. To verify, check the status of integration with vault. The response message should confirm that the integration is enabled:

```
root@cxcloudagent: /home/cxcroot# cxcli agent vault on

Enter HashiCorp Vault Address:

Enter HashiCorp Vault Token:

vault integration enabled root@cxcloudagent: /home/cxcroot#
```

Disabling HashiCorp Vault Integration

To access the CX Agent:

1. Log in to the CX Agent via SSH using the cxcroot user account.
2. Switch to the root user to elevate privileges by running the following command:

```
sudo su
```

3. Run the following command to disable HashiCorp Vault Integration:

```
root@cxcloudagent: /home/cxcroot# cxcli agent vault off

vault integration disabled

root@cxcloudagent: /home/cxcroot# |
```

HashiCorp Vault Device Credentials Schema

Vault Credentials Schema: For detailed information about available options and supported fields for device credentials, download the “Vault credentials schema” file (vault-credentials-schema.json).

Example: The following is an example of a JSON credential based on the schema:

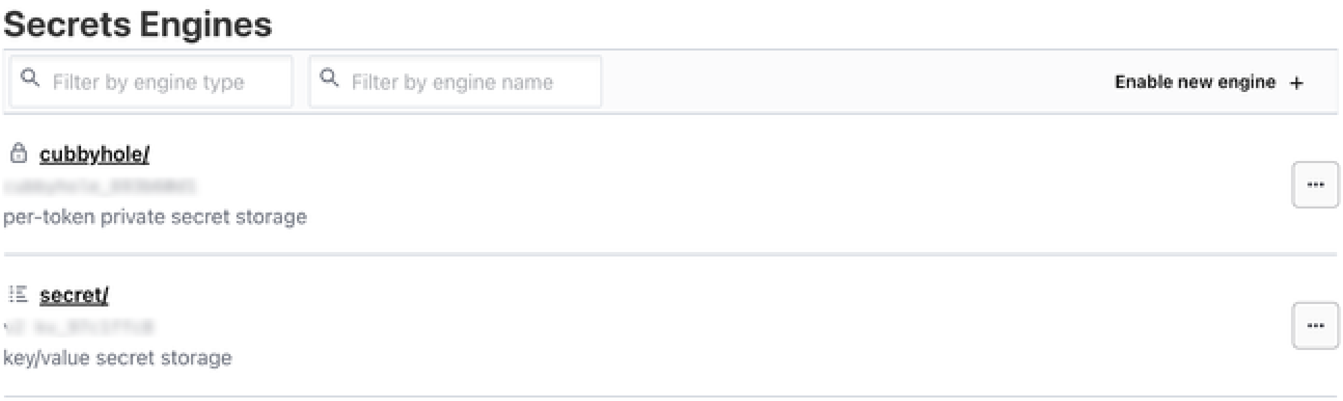
-

```
{
"targetIp": "5.0.1.*",
"credentials": {
"snmpv3": {
"user": "cisco",
"authPassword": "*******",
"authAlgorithm": "MD5",
"privacyPassword": "*******",
"privacyAlgorithm": "AES-256"
},
"telnet": {
"user": "cisco",
"password": "*******",
"enableUser": "cisco",
"enablePassword": "*******"
}
}
}
```

Note:Users can specify multiple protocols within a single credential JSON file. However, avoid including duplicate protocols from the same family (e.g., do not include both SNMPv2c and SNMPv3 in the same credential file).

Configuring Device Credentials in HashiCorp Vault (First Time)

1. Log in to a Vault instance.



Secrets Engines

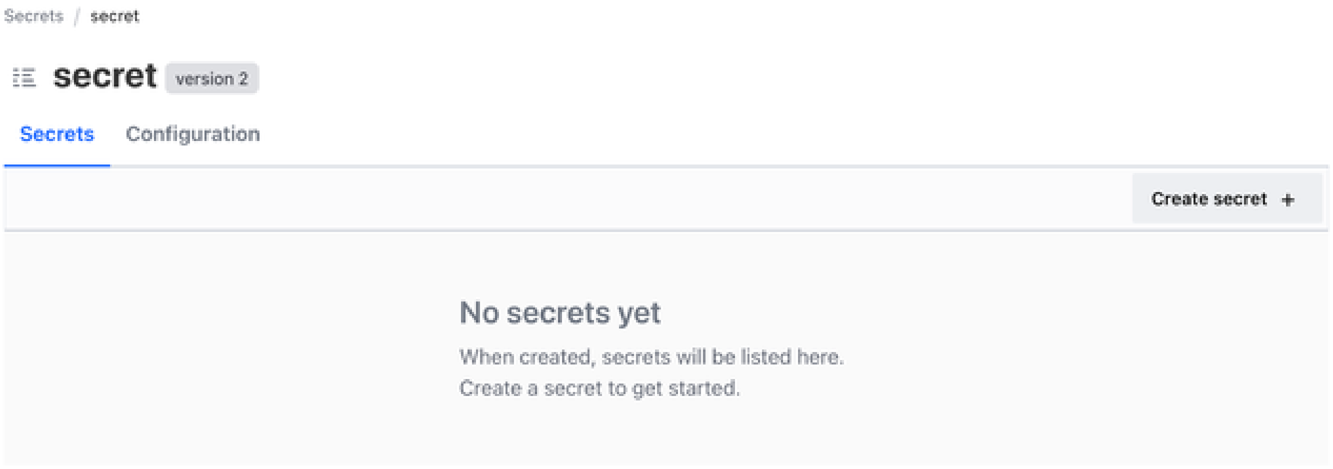
Filter by engine type | Filter by engine name | Enable new engine +

cubbyhole/
[redacted]
per-token private secret storage

secret/
[redacted]
key/value secret storage

Secret

2. Create a new key-value secret using the following path: *secret/seed/credentials*.
3. Choose the key-value secret storage engine (secret/).



Secrets / secret

secret version 2

Secrets | Configuration

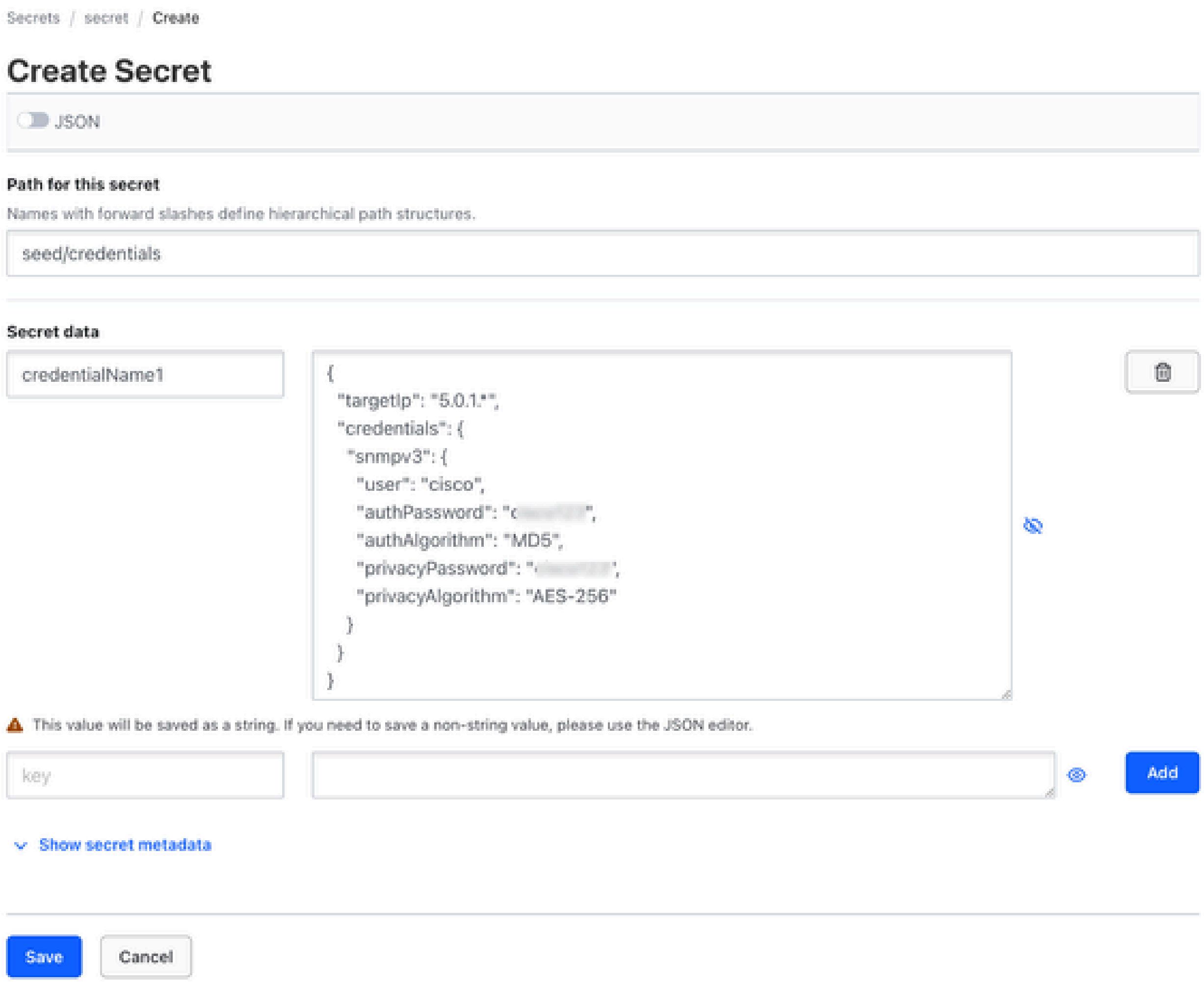
Create secret +

No secrets yet

When created, secrets will be listed here.
Create a secret to get started.

Key value secret

4. Click **Create secret**. The **Create Secret** window opens.



Create Secret

Path for this secret

Names with forward slashes define hierarchical path structures.

seed/credentials

Secret data

credentialName1

```
{
  "targetIp": "5.0.1.*",
  "credentials": {
    "snmpv3": {
      "user": "cisco",
      "authPassword": "[redacted]",
      "authAlgorithm": "MD5",
      "privacyPassword": "[redacted]",
      "privacyAlgorithm": "AES-256"
    }
  }
}
```

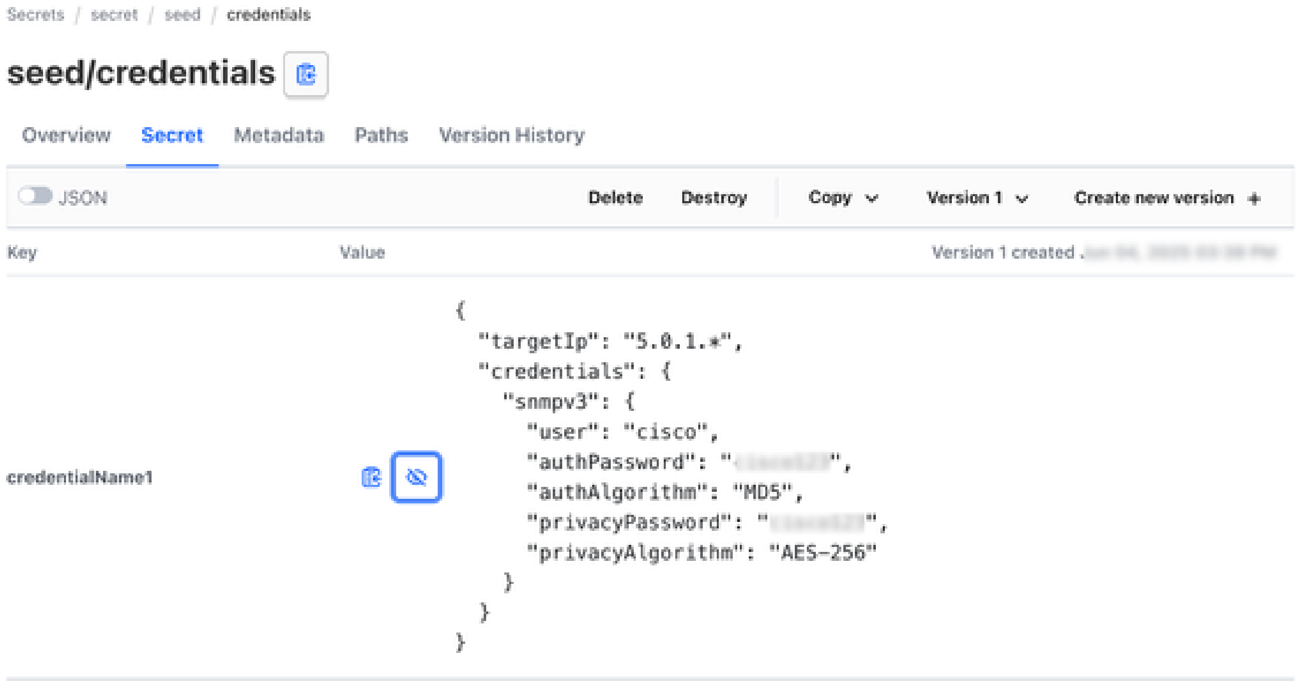
This value will be saved as a string. If you need to save a non-string value, please use the JSON editor.

Client Secret

5. Update the following fields:

- **Path for secret**: seed/credentials
- **Secret data**: collection of key - value secrets
- **key**: custom unique credential name
- **value**: credentials JSON

6. Click **Save**. The secret should now be stored in the HashiCorp Vault.

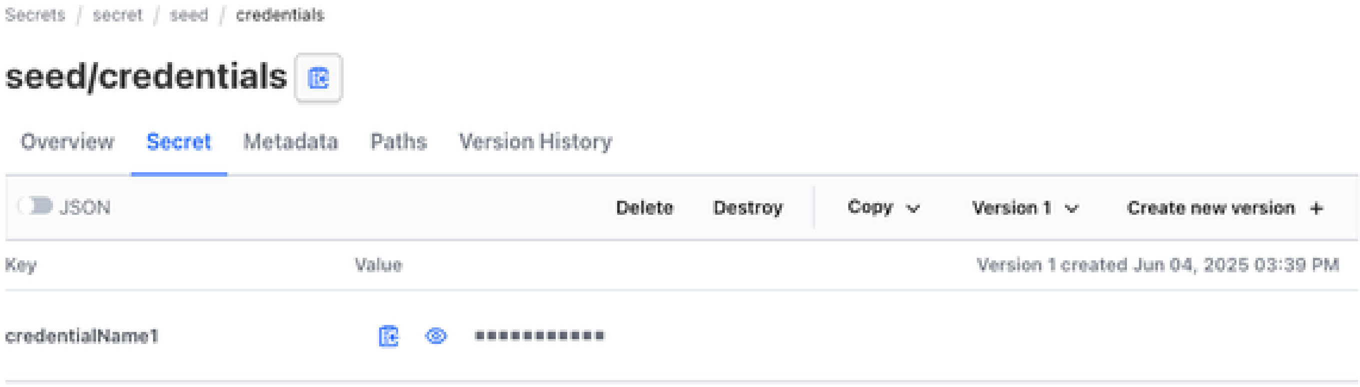


```
{
  "targetIp": "5.0.1.*",
  "credentials": {
    "snmpv3": {
      "user": "cisco",
      "authPassword": "[redacted]",
      "authAlgorithm": "MD5",
      "privacyPassword": "[redacted]",
      "privacyAlgorithm": "AES-256"
    }
  }
}
```

Credentials

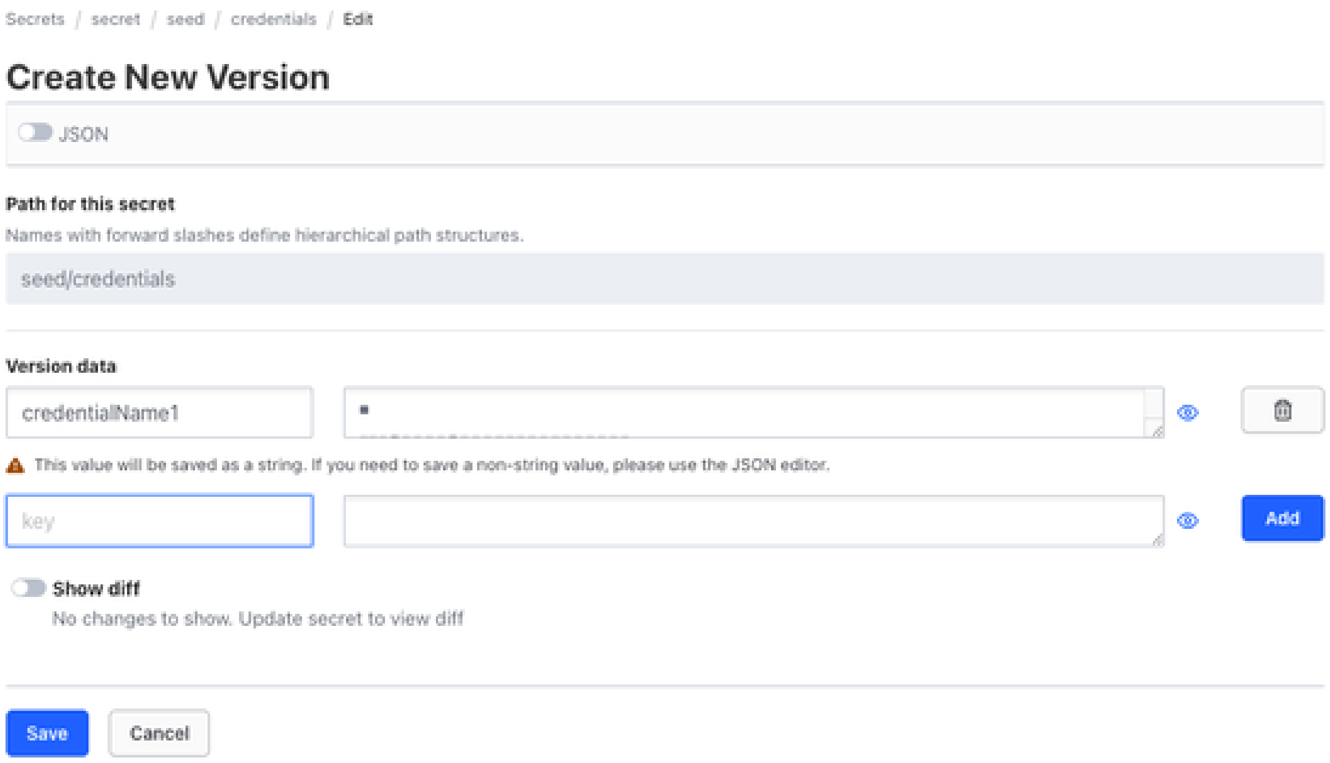
Adding More Credentials to HashiCorp Vault

1. Log in to a HashiCorp vault instance.



Add Credentials

2. Navigate to the already created Secret “secret/seed/credentials”.



Secrets / secret / seed / credentials / Edit

Create New Version

JSON

Path for this secret

Names with forward slashes define hierarchical path structures.

seed/credentials

Version data

credentialName1

This value will be saved as a string. If you need to save a non-string value, please use the JSON editor.

key

Show diff

No changes to show. Update secret to view diff

Create Version

3. Click **Create new version.**

4. Add new secrets by providing any number of key-value pairs as needed.

5. Click **Save**.

CX Cloud Seed File with Default Credentials

- **Simplify Seed File**: When using credentials configured through Hashicorp vault, simplify the Seed File by omitting sensitive information
- **Specify only IP Address or Hostname**: Users can pass only the IP Address or Hostname in the Seed File, leaving other fields blank

```
5.0.1.2,,,,,,,,,,,,,,,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

IP or Hostname

- **Use both HashiCorp vault and Seed File credentials**: Provide credentials for some devices in the Seed File while relying on the vault to manage credentials for other devices

```
5.0.1.1,snmpv3,,username,,,,,,,,cliUser,cliPassword,,enablePassword,,,
25.0.1.2,snmpv2c,readOnlyPassword,,,,,,,sshv2,,cliUser,cliPassword,,,,
5.0.1.3,,,,,,,,,,,,,,,,,,
5.0.1.4,,,,,,,,,,,,,,,,,,
```

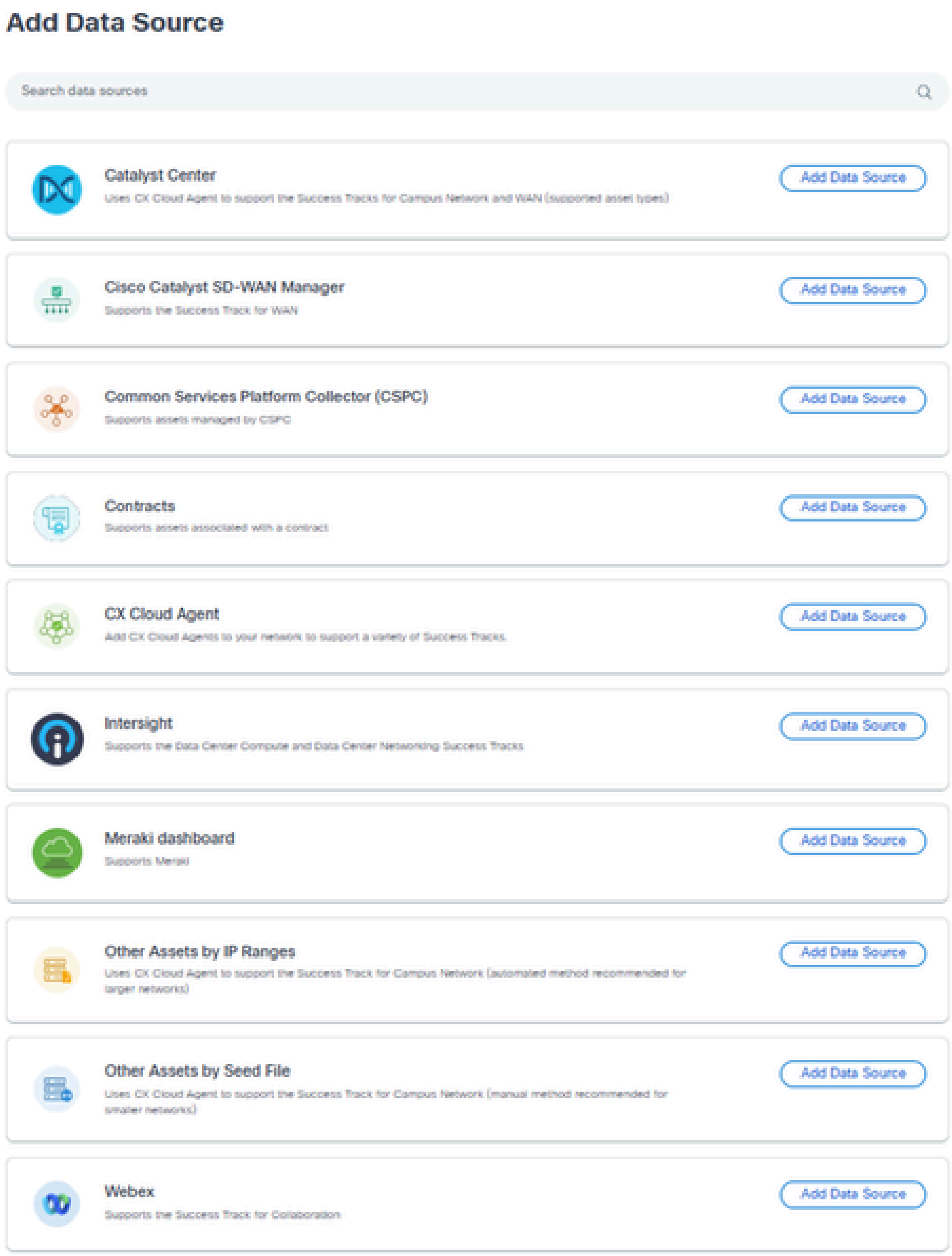
IP or Hostname

Adding Catalyst Center as Data Source

Users with the Super Administrator User role can add the Catalyst Center Data Source.

To add Catalyst Center as a Data Source:

1. Select the **Admin Center** icon. The **Data Sources** window opens.
2. Click **Add Data Source**. The **Add Data Source** page displays.



Add Data Source

Search data sources

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

Common Services Platform Collector (CSPC)
Supports assets managed by CSPC

Contracts
Supports assets associated with a contract

CX Cloud Agent
Add CX Cloud Agents to your network to support a variety of Success Tracks.

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

Meraki dashboard
Supports Meraki

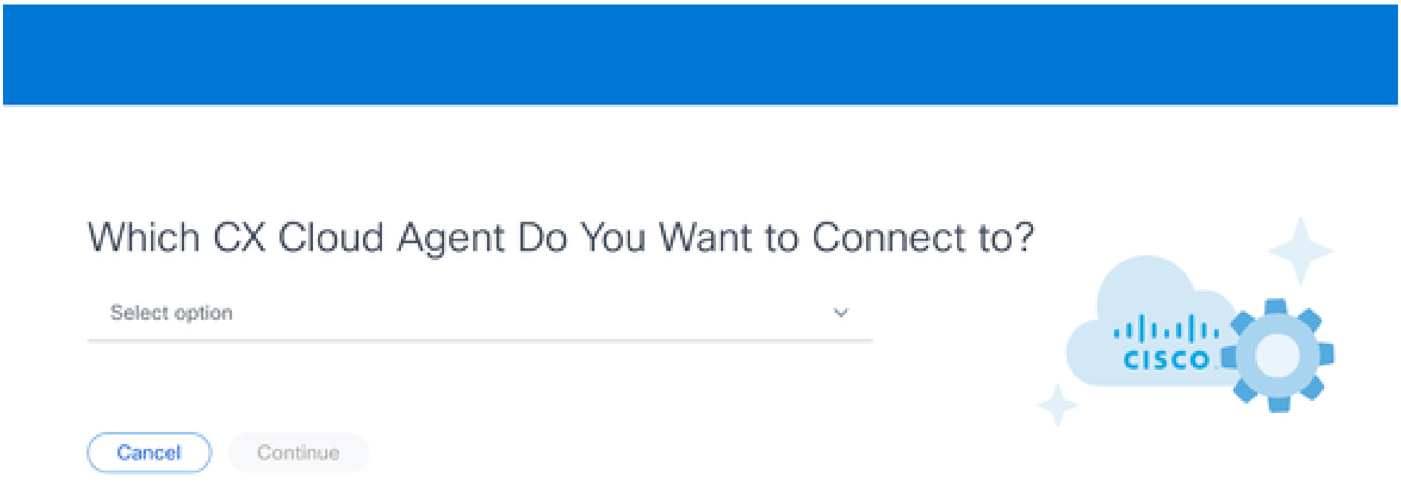
Other Assets by IP Ranges
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

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

Webex
Supports the Success Track for Collaboration

Add Data Source

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

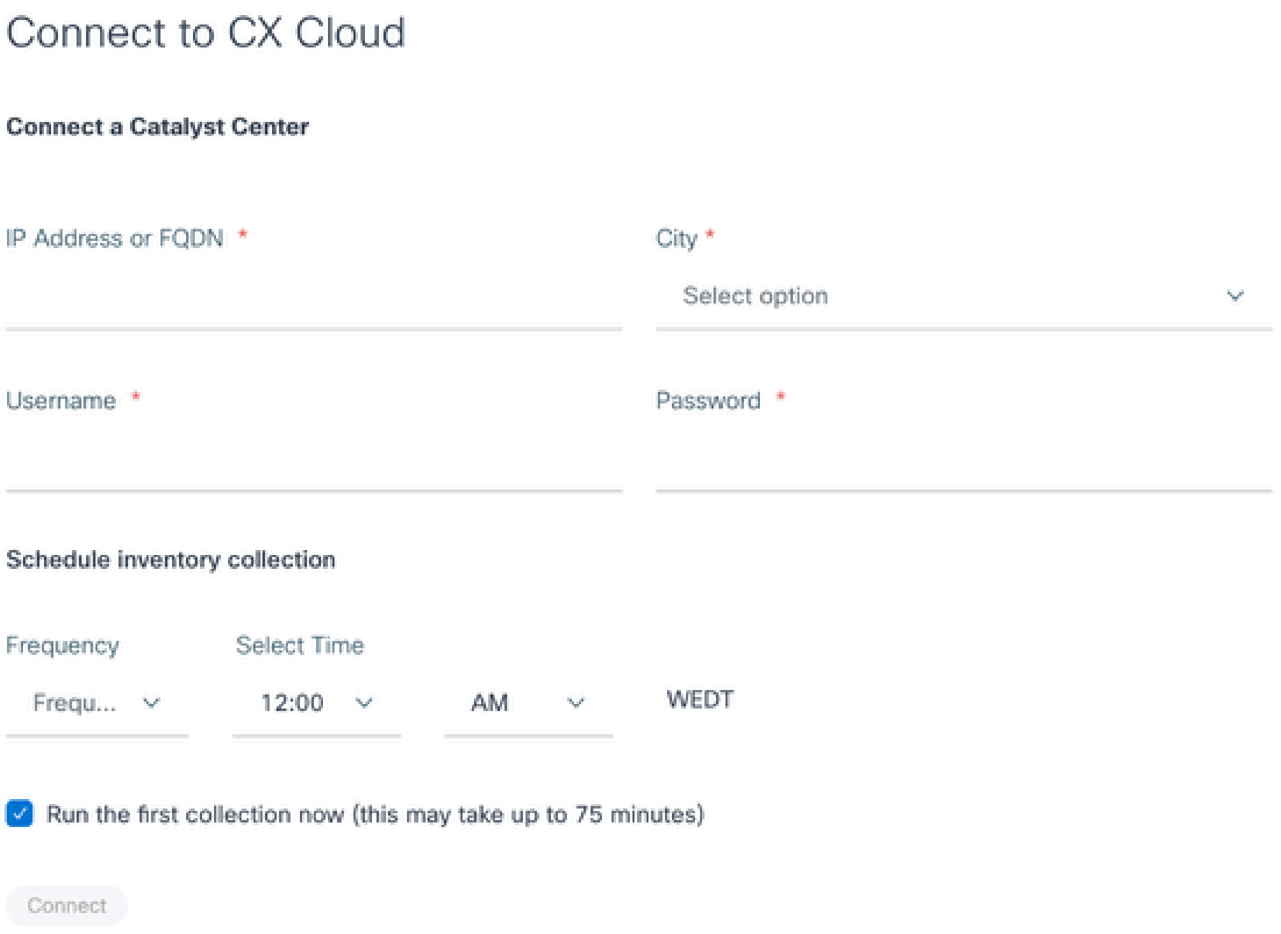


Which CX Cloud Agent Do You Want to Connect to?

Select option

Select CX Agent

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



Connect to CX Cloud

Connect a Catalyst Center

IP Address or FQDN *

City *
Select option

Username *

Password *

Schedule inventory collection

Frequency: Frequ...

Select Time: 12:00 AM WEDT

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

Frequency

6. 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 and Select Time** to indicate how often the CX Agent should perform network scans in **Schedule Inventory Collection** sections

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

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

Adding SolarWinds® as a Data Source

Note: If there is a requirement to add the SolarWinds® Data Source, contact Cisco Support for assistance.

BCS/LCS customers can now use the CX Agent capability to externally integrate with SolarWinds®, providing greater transparency, improved manageability, and an enhanced user experience through increased automation. The CX Agent collects inventory and other required data to generate various reports that are consistent in terms of format, data completeness, and data accuracy to current reports generated by Operational Insights Collector CX Agent supports integration with SolarWinds® by allowing a BCS/LCS customer to replace OIC with CX Agent for collecting data from Solarwinds®. This feature, including the Solarwinds® Data Source, is available exclusively to BCS/LCS customers.

The CX Agent must be configured in **BCS Forwarding** before the first collection; otherwise, files remain unprocessed. Refer to the section Configuring CX Agent for BCS or LCS for more information about BCS Forwarding configuration.

Notes:

- Multiple collections from the same SolarWinds® instance overwrite previous files (later uploads take precedence)
- Multiple sources are supported, but each SolarWinds® instance must have a unique IP and Appliance ID

Adding Other Assets as Data Sources

Telemetry collection has been extended to devices not managed by the Catalyst Center, enabling users to view and interact with telemetry-derived insights and analytics for a broader range of devices. After the initial CX Agent setup, users have the option to configure CX 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 should be scanned by CX Agent. Both approaches rely on Simple Network Management Protocol (SNMP) for the purpose of discovery and on Secure Shell (SSH) for connectivity. These must be properly configured to enable successful telemetry collection.

To add other assets as data sources, use any of the following options:

- 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 Agent supports SNMPv2c and SNMPv3 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, then the CX Agent attempts, by default, to communicate with each respective device using SNMPv3 and reverts 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 (e.g., usernames and passwords) submitted through telnet are not encrypted and therefore vulnerable to compromise, absent additional security.

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.
- If a device from the seed file or IP range collections is also part of the Catalyst Center inventory, the device is reported only once for the Catalyst Center entry. The respective devices within the seed file or IP range entry are skipped to avoid duplication.
- Cisco IP phones are not supported in CX Cloud for data collection by CX Agent. As a result, Cisco IP phones do not display in the assets list.

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 should be collected by CX 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 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.

Users can upload a Common Services Platform Collector (CSPC) Seed File in the same way as a standard CX Cloud Seed File, and any required reformatting is managed in the CX Cloud.

For CX Agent v3.1 and later, customers can upload Seed Files in either the CSPC or CX format; only the CX format Seed File is supported for earlier CX Agent versions.

It is important that the format of the sample seed file, including column headers, not be altered in any way.

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 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	SNMPv3 protocol permits Authentication via either the Message Digest (MD5) or Secure Hash Algorithm (SHA). If the device is configured with secure authentication, then the respective Auth Algorithm must be provided.

Seed File Column	Column Header / Identifier	Purpose of the Column
		Note: MD5 is considered insecure, and SHA can 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 Data Encryption Standard (DES) are considered too short to provide cryptographic security, and that

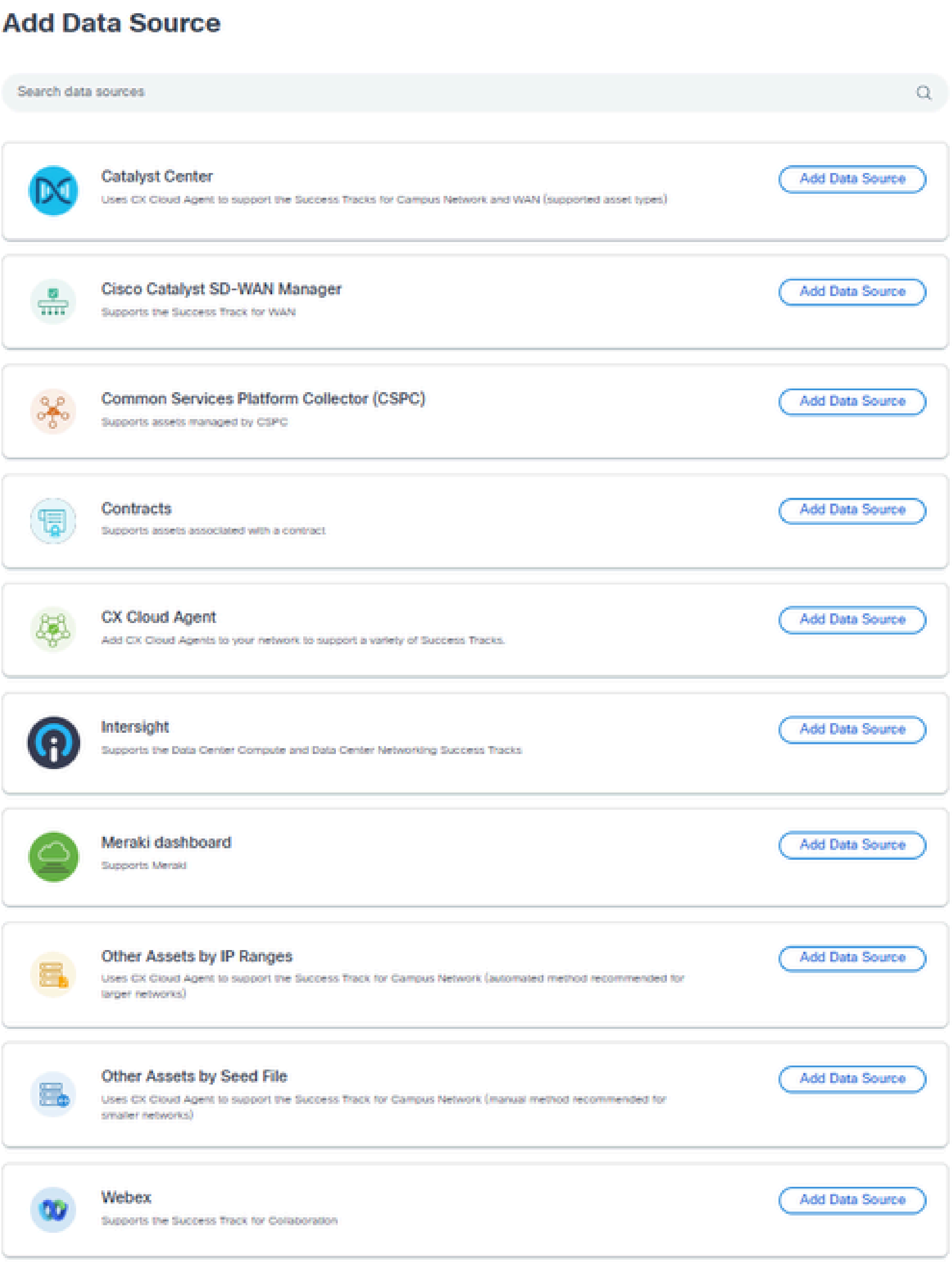
Seed File Column	Column Header / Identifier	Purpose of the Column
		Triple Data Encryption Standard (3DES) can be used on all devices that support it.
H	snmpv3PrivPassword : password	If the SNMPv3 privacy algorithm is configured on the device, then its respective privacy password needs to be provided 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 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 can set to 'sshv2' by default	The Command Line Interface (CLI) is intended to interact with the device directly. CX 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 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

Seed File Column	Column Header / Identifier	Purpose of the Column
		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

Adding 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)

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

Common Services Platform Collector (CSPC)
Supports assets managed by CSPC

Contracts
Supports assets associated with a contract

CX Cloud Agent
Add CX Cloud Agents to your network to support a variety of Success Tracks.

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

Meraki dashboard
Supports Meraki

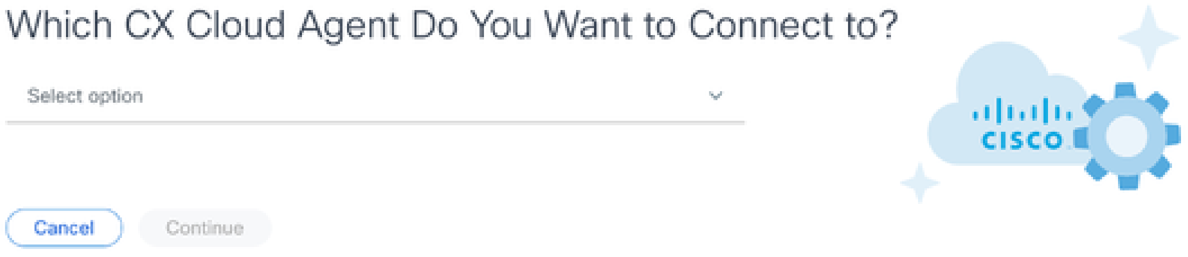
Other Assets by IP Ranges
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

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

Webex
Supports the Success Track for Collaboration

Add Data Source

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

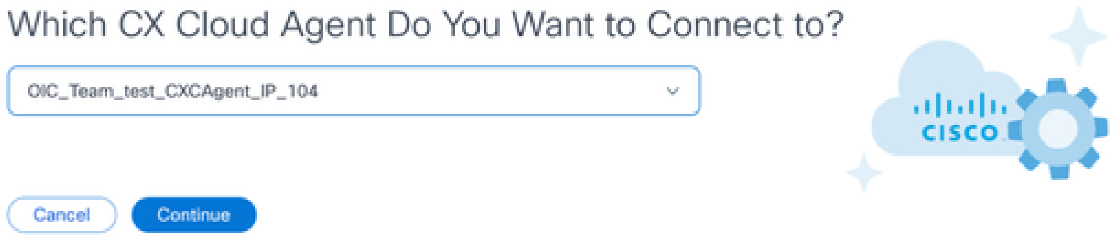


Which CX Cloud Agent Do You Want to Connect to?

Select option

Select CX Agent

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

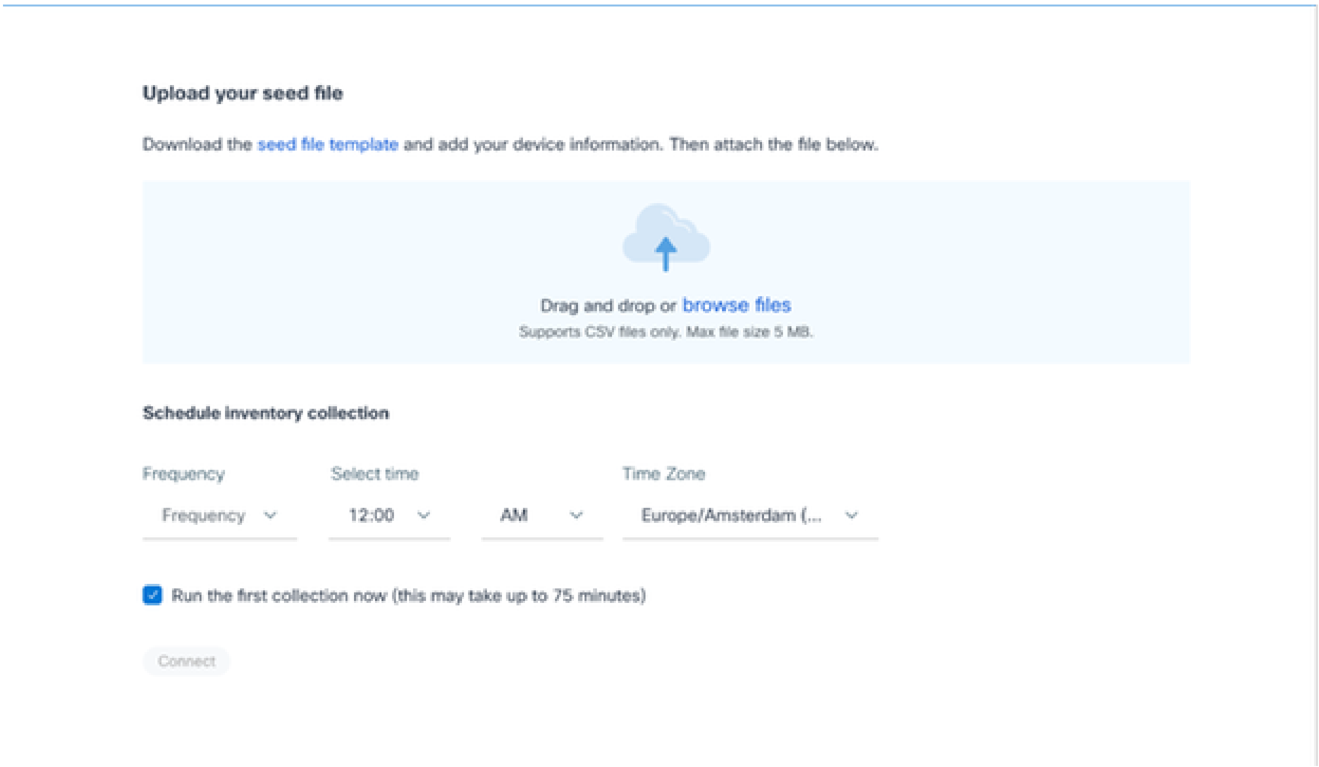


Which CX Cloud Agent Do You Want to Connect to?

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.

Drag and drop or browse files

Supports CSV files only. Max file size 5 MB.

Schedule inventory collection

Frequency: Frequency

Select time: 12:00 AM

Time Zone: Europe/Amsterdam (...

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

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 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.

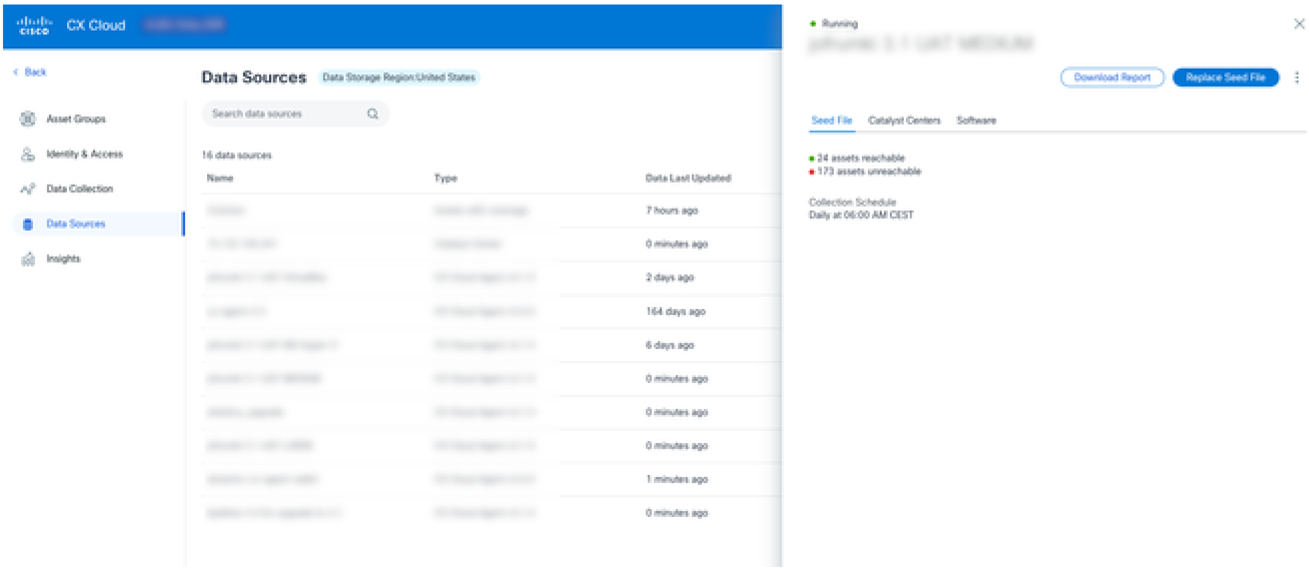
Adding Other Assets Using a Modified Seed File

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 Agent data source that requires an updated seed file. The **CX Cloud Agent** details window opens.



Data Sources Data Storage Region:United States

16 data sources

Name	Type	Data Last Updated
[redacted]	[redacted]	7 hours ago
[redacted]	[redacted]	0 minutes ago
[redacted]	[redacted]	2 days ago
[redacted]	[redacted]	164 days ago
[redacted]	[redacted]	6 days ago
[redacted]	[redacted]	0 minutes ago
[redacted]	[redacted]	0 minutes ago
[redacted]	[redacted]	0 minutes ago
[redacted]	[redacted]	1 minutes ago
[redacted]	[redacted]	0 minutes ago

● Running

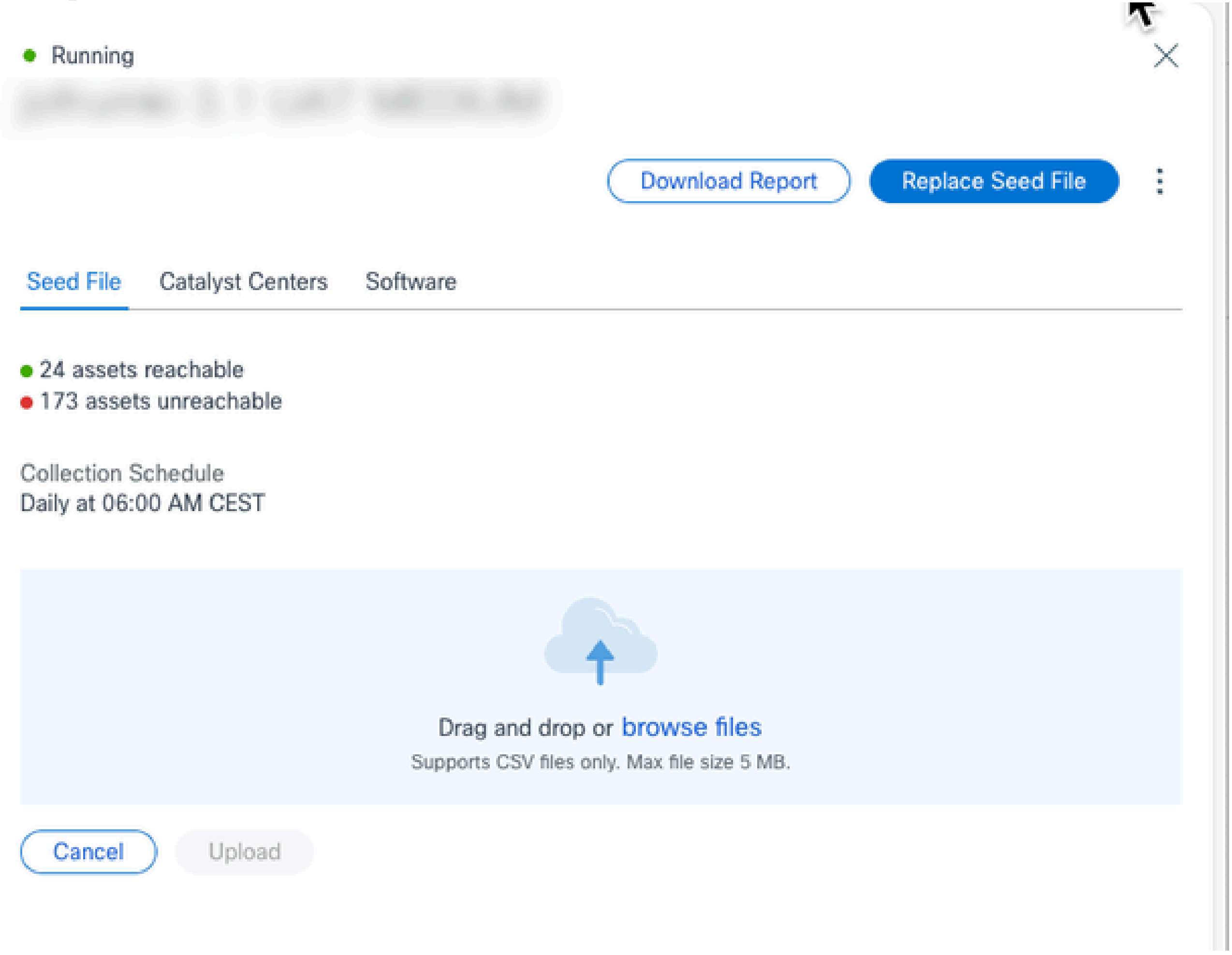
[redacted]

● 24 assets reachable
● 173 assets unreachable

Collection Schedule
Daily at 06:00 AM CEST

Seed File

3. Click **Replace Seed File**.



● Running

[redacted]

● 24 assets reachable
● 173 assets unreachable

Collection Schedule
Daily at 06:00 AM CEST

Supports CSV files only. Max file size 5 MB.

Replace Seed File

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

Default Credentials for the Seed File

CX Agent provides default credentials that customers can set up locally in Agent, eliminating the need to include sensitive passwords directly in the Seed File. This enhances security by reducing exposure of confidential information, addressing a key customer concern.

Adding 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 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 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 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 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 Agent collection inventory.

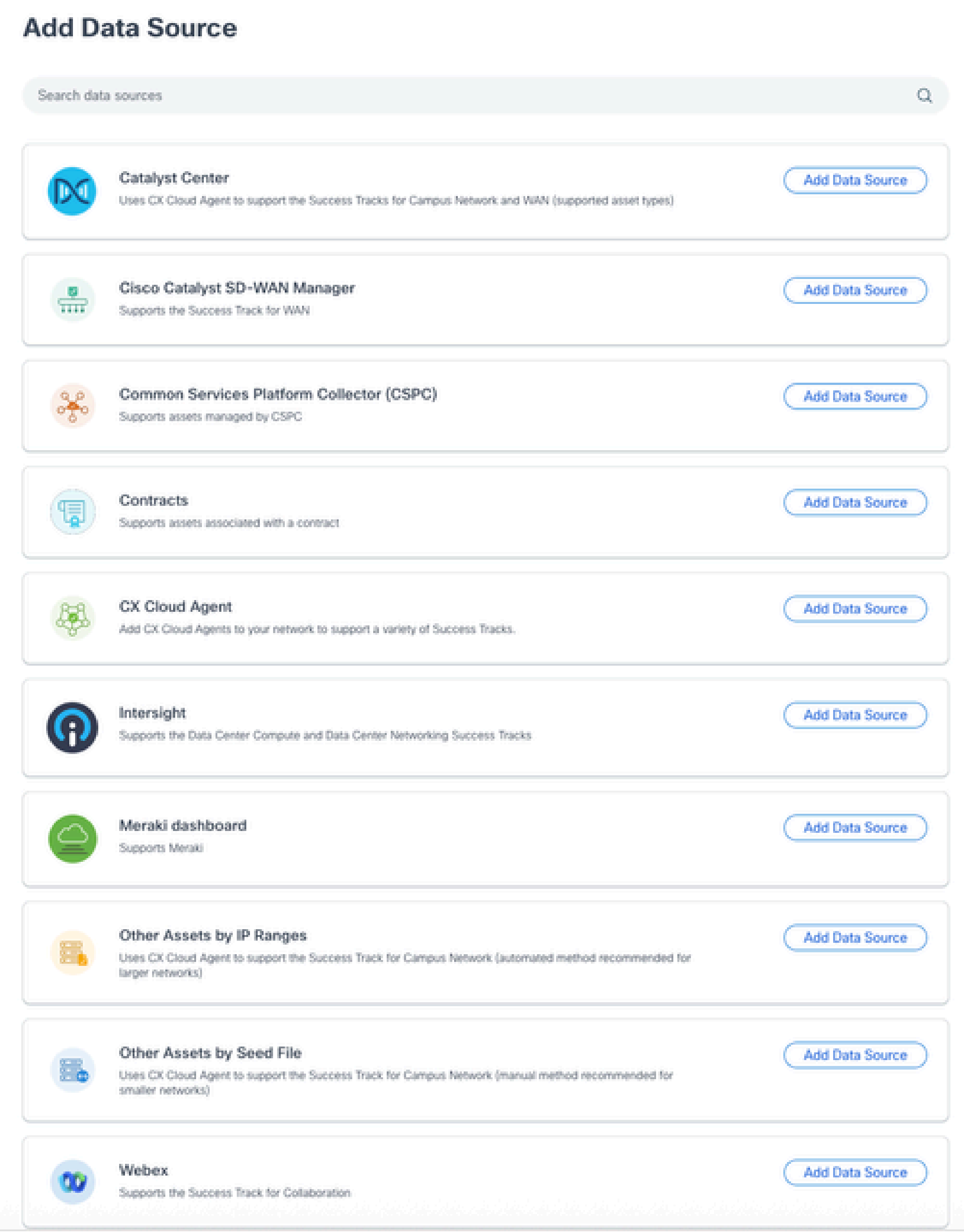
Adding devices using an IP range requires users to specify all applicable credentials through the configuration UI. The fields visible vary depending on the protocols selected on the previous windows. If multiple selections are made for the same protocol, for example, selecting both SNMPv2c and SNMPv3 or selecting both SSHv2 and SSHv1, CX 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. Select the **Admin Center** icon. The **Data Sources** window opens.
2. 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)

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

Common Services Platform Collector (CSPC)
Supports assets managed by CSPC

Contracts
Supports assets associated with a contract

CX Cloud Agent
Add CX Cloud Agents to your network to support a variety of Success Tracks.

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

Meraki dashboard
Supports Meraki

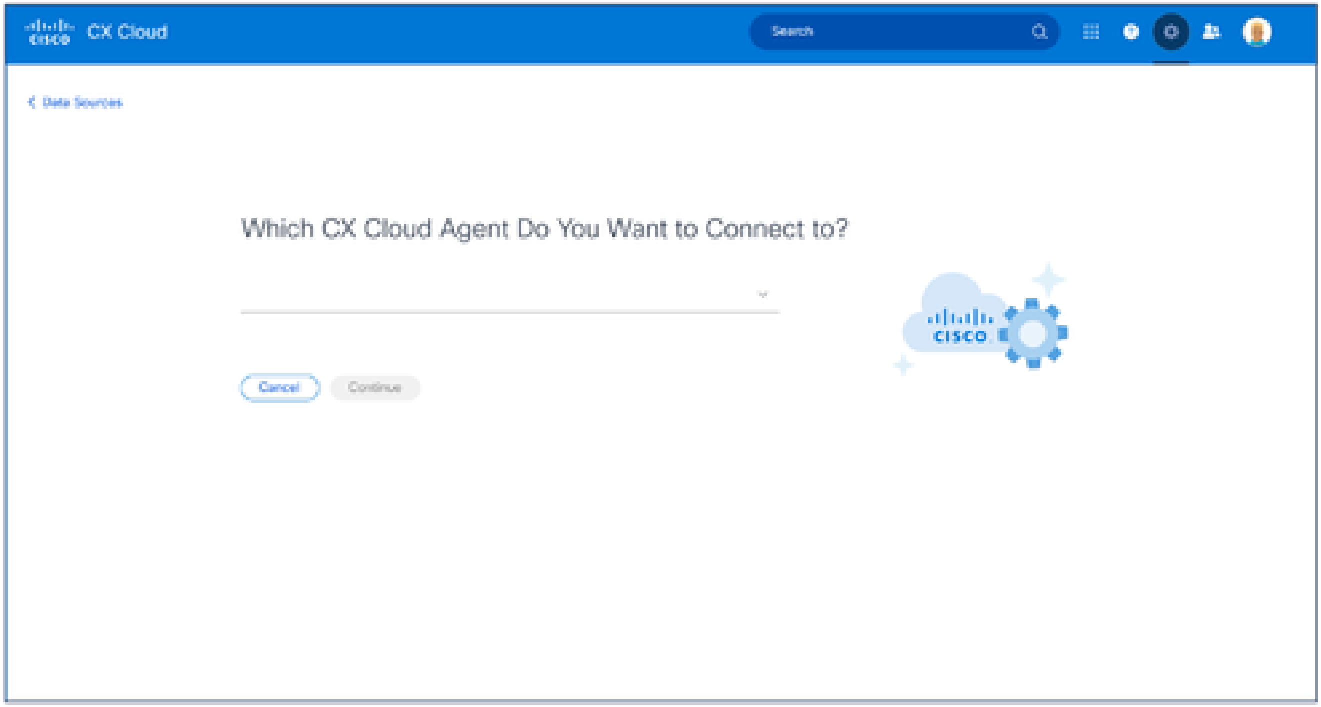
Other Assets by IP Ranges
Uses CX Cloud Agent to support the Success Track for Campus Network (automated method recommended for larger networks)

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

Webex
Supports the Success Track for Collaboration

Add Data Source

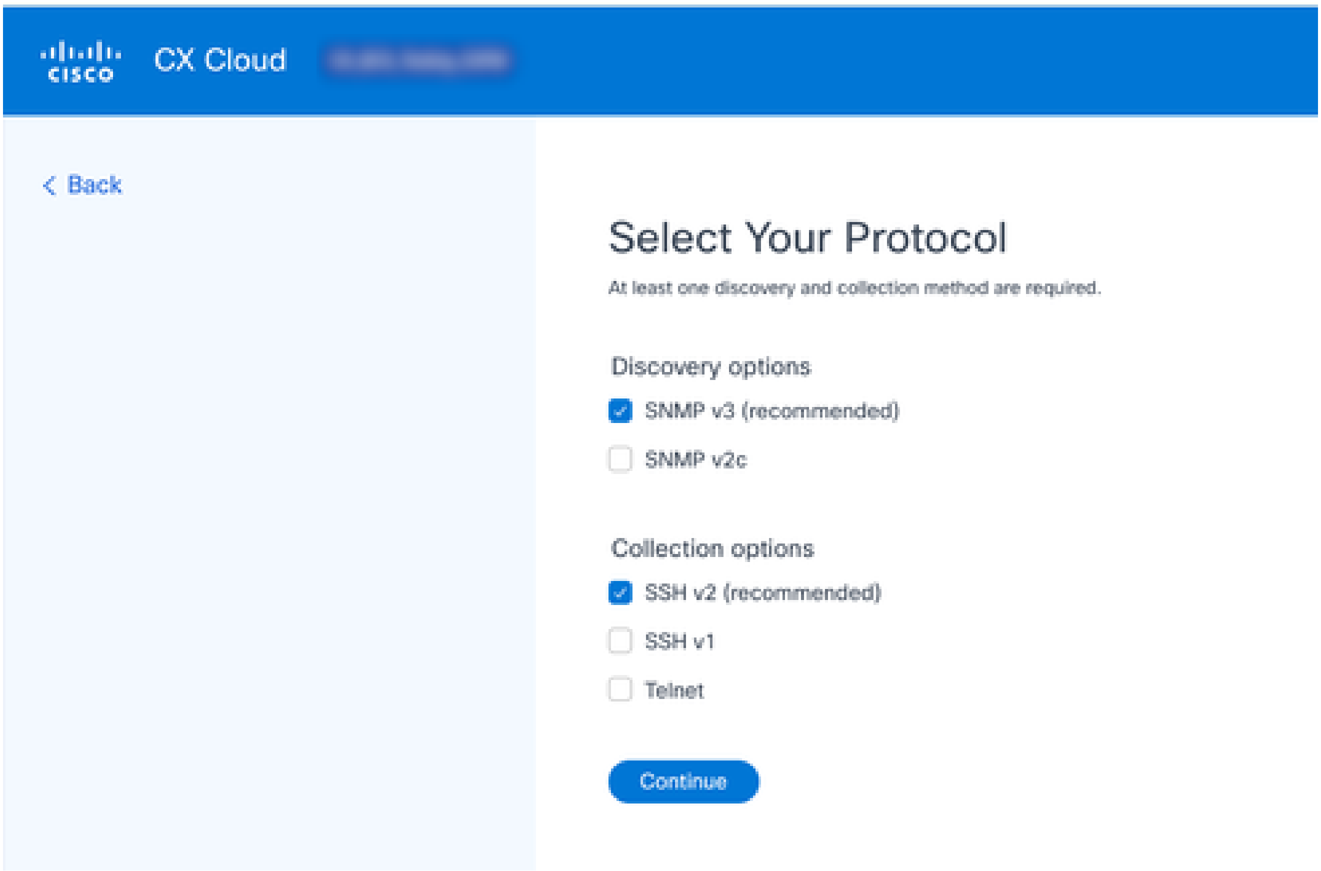
3. Click **Add Data Source** in the **Other Assets by IP Ranges** option.



Which CX Cloud Agent Do You Want to Connect to?

Select CX Cloud Agent

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



Select Your Protocol

At least one discovery and collection method are required.

Discovery options

☑ SNMP v3 (recommended)

☐ SNMP v2c

Collection options

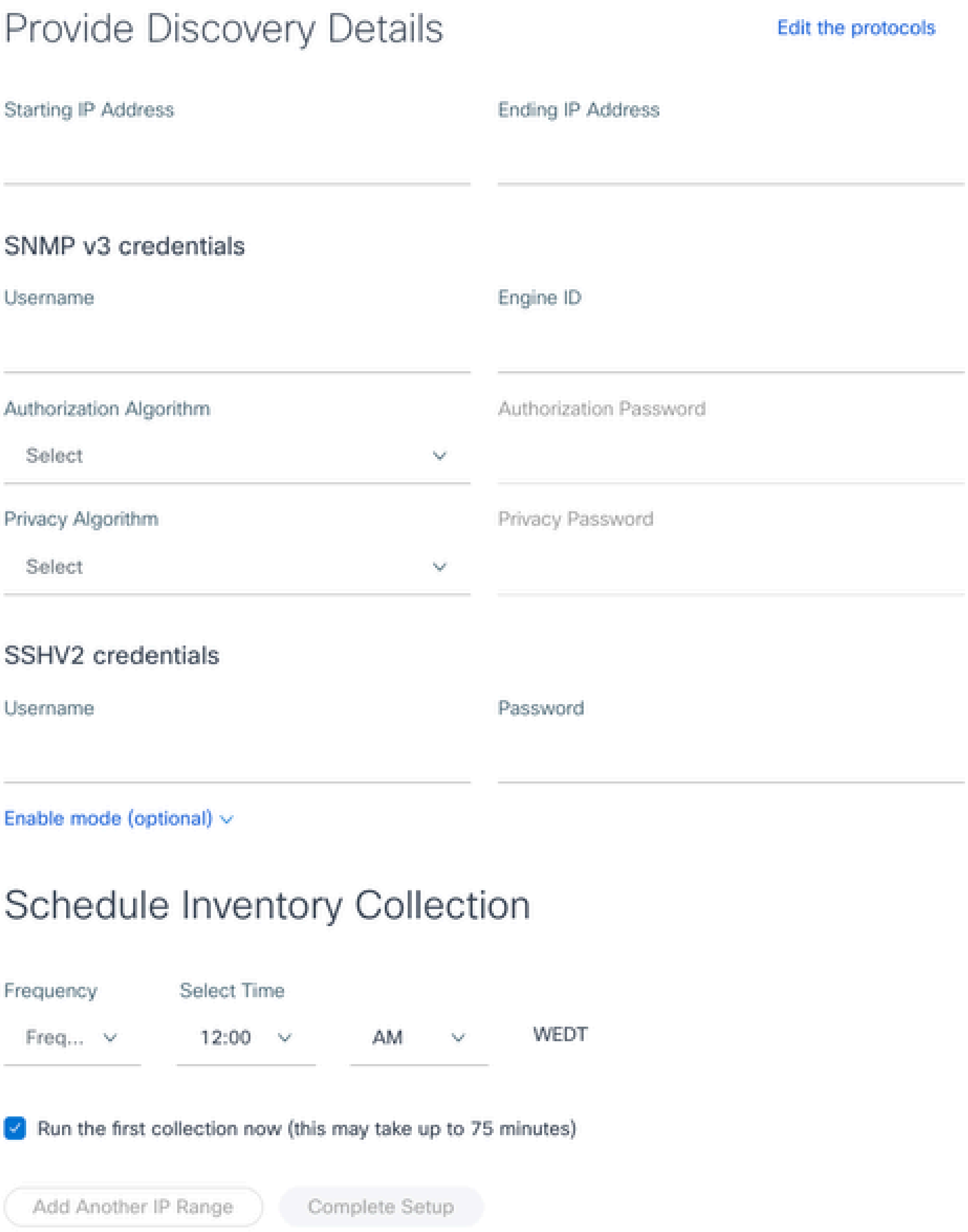
☑ SSH v2 (recommended)

☐ SSH v1

☐ Telnet

Select Your Protocol

6. Select the applicable check boxes for **Discovery options** and **Collection options**.
7. Click **Continue**.



Provide Discovery Details

Edit the protocols

Starting IP Address

Ending IP Address

SNMP v3 credentials

Username

Engine ID

Authorization Algorithm: Select

Authorization Password

Privacy Algorithm: Select

Privacy Password

SSHV2 credentials

Username

Password

Enable mode (optional)

Schedule Inventory Collection

Frequency: Freq...

Select Time: 12:00 AM WEDT

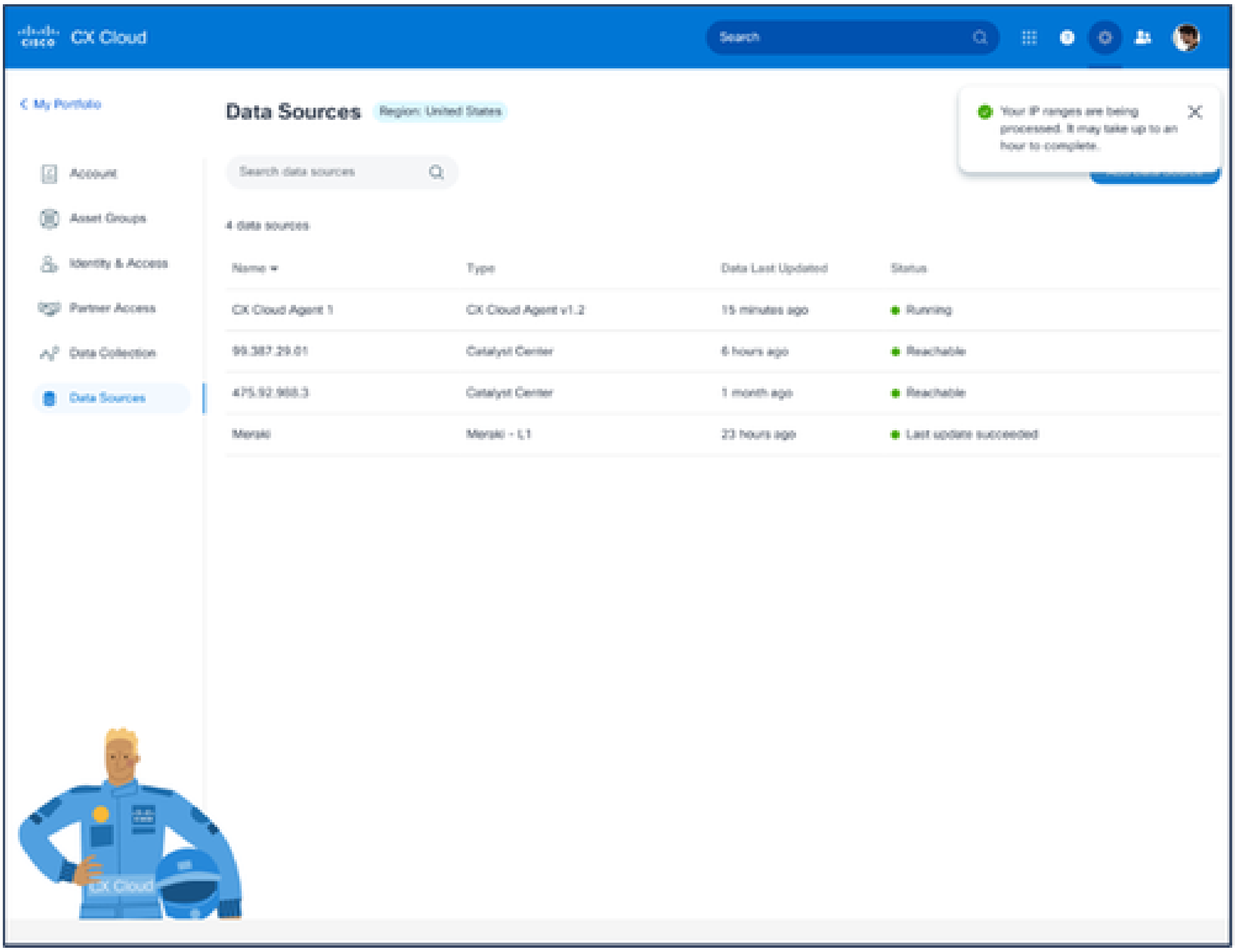
☑ Run the first collection now (this may take up to 75 minutes)

Discovery details

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

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

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



Data Sources Region: United States

Your IP ranges are being processed. It may take up to an hour to complete.

Search data sources

4 data sources

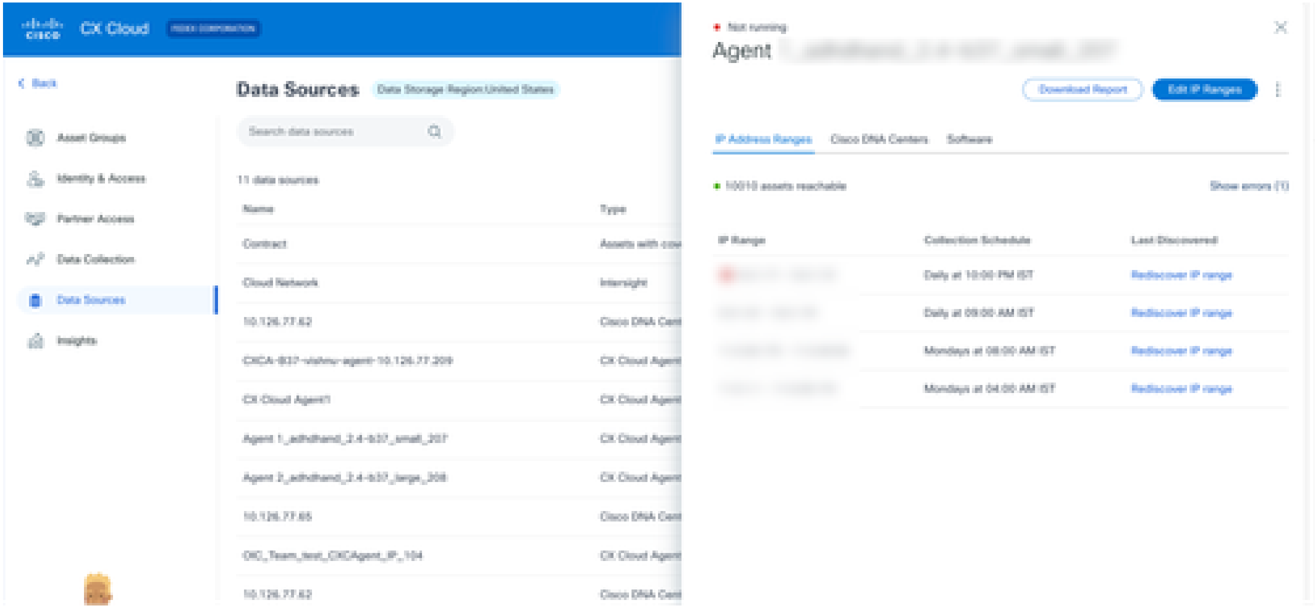
Name ▾	Type	Data Last Updated	Status
CX Cloud Agent 1	CX Cloud Agent v1.2	15 minutes ago	● Running
99.387.29.01	Catalyst Center	6 hours ago	● Reachable
475.92.988.3	Catalyst Center	1 month ago	● Reachable
Meraki	Meraki - L1	23 hours ago	● Last update succeeded

Confirmation Message

Editing IP Ranges

To edit an IP range:

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



Data Sources Data Storage Region United States

Search data sources

11 data sources

Name	Type
Contract	Assets with cov
Cloud Network	Intersight
10.126.77.62	Cisco DNA Cent
CXCA-837-vishnu-agent-10.126.77.209	CX Cloud Agent
CX Cloud Agent1	CX Cloud Agent
Agent 1_adhdhand_2.4-b37_small_207	CX Cloud Agent
Agent 2_adhdhand_2.4-b37_large_208	CX Cloud Agent
10.126.77.65	Cisco DNA Cent
CXC_Team_test_CXCAgent_IP_104	CX Cloud Agent
10.126.77.62	Cisco DNA Cent

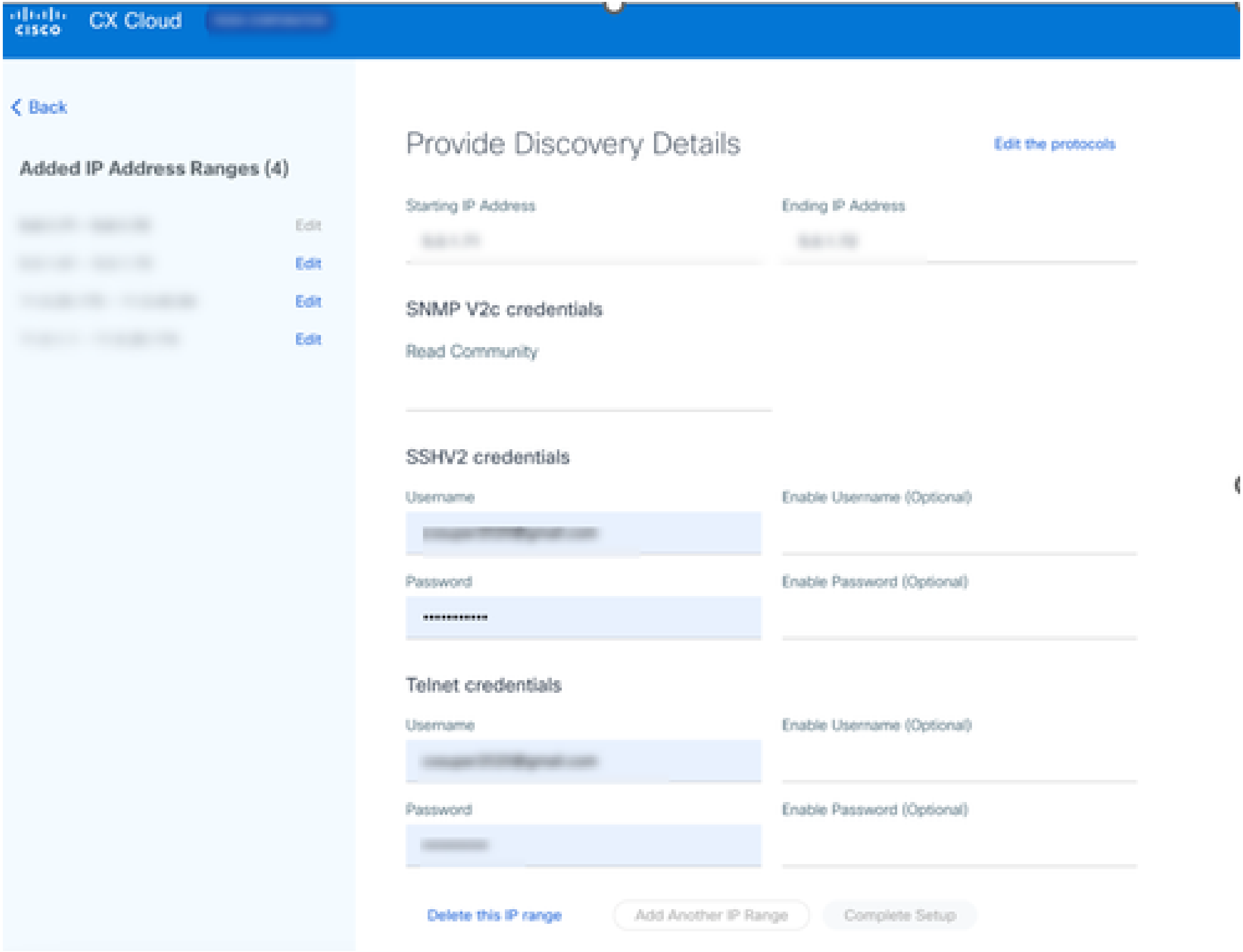
● Not running

Agent [redacted]

● 10010 assets reachable

IP Range	Collection Schedule	Last Discovered
[redacted]	Daily at 10:00 PM IST	Rediscover IP range
[redacted]	Daily at 09:00 AM IST	Rediscover IP range
[redacted]	Mondays at 08:00 AM IST	Rediscover IP range
[redacted]	Mondays at 04:00 AM IST	Rediscover IP range

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



CX Cloud [redacted]

< Back

Added IP Address Ranges (4)

[redacted] Edit

[redacted] Edit

[redacted] Edit

[redacted] Edit

Provide Discovery Details

Edit the protocols

Starting IP Address: [redacted]

Ending IP Address: [redacted]

SNMP V2c credentials

Read Community

SSHV2 credentials

Username: [redacted]

Enable Username (Optional)

Password: ••••••••••••

Enable Password (Optional)

Telnet credentials

Username: [redacted]

Enable Username (Optional)

Password: [redacted]

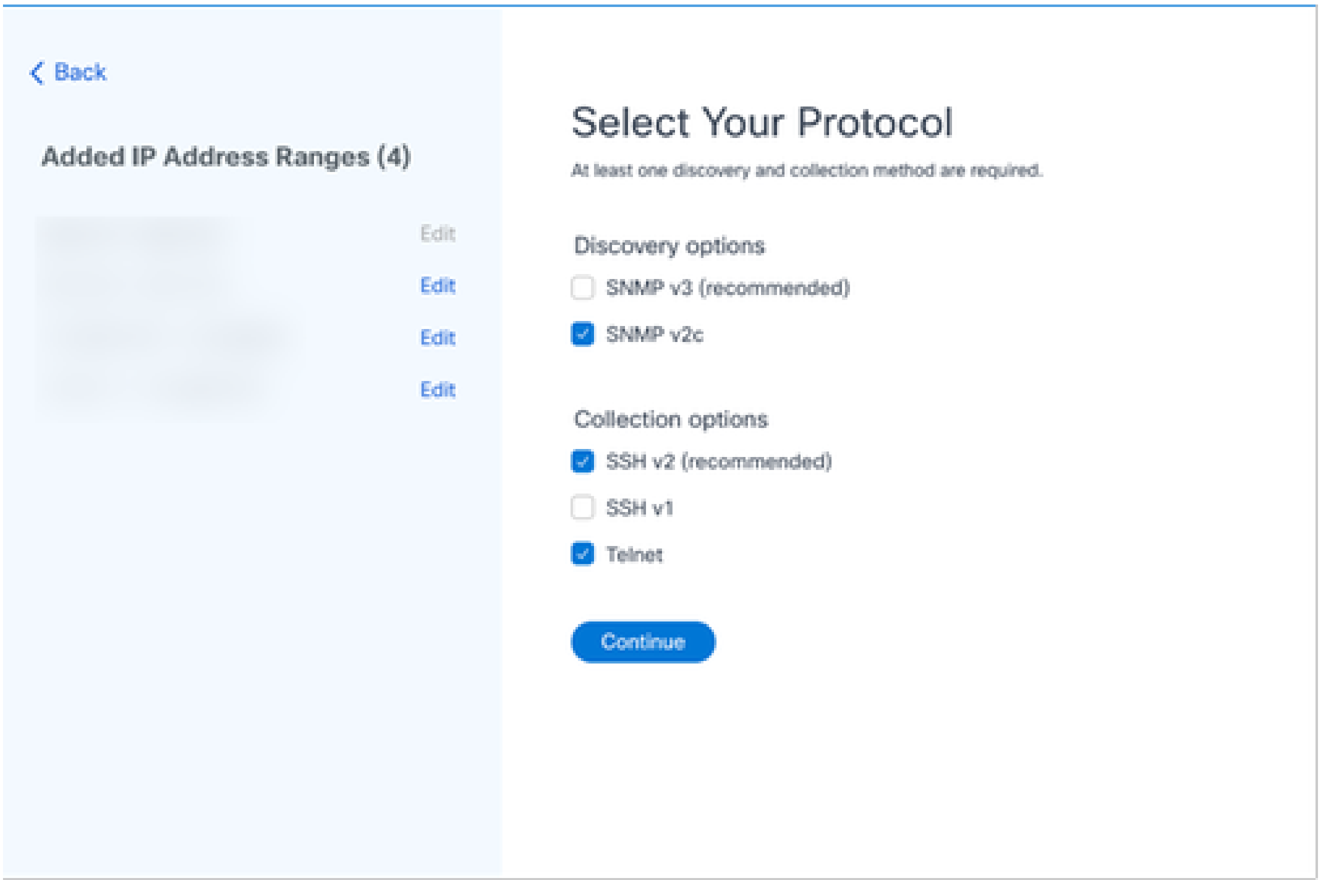
Enable Password (Optional)

Delete this IP range

Add Another IP Range

Complete Setup

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



Added IP Address Ranges (4)

Select Your Protocol

At least one discovery and collection method are required.

Discovery options

□ SNMP v3 (recommended)

☑ SNMP v2c

Collection options

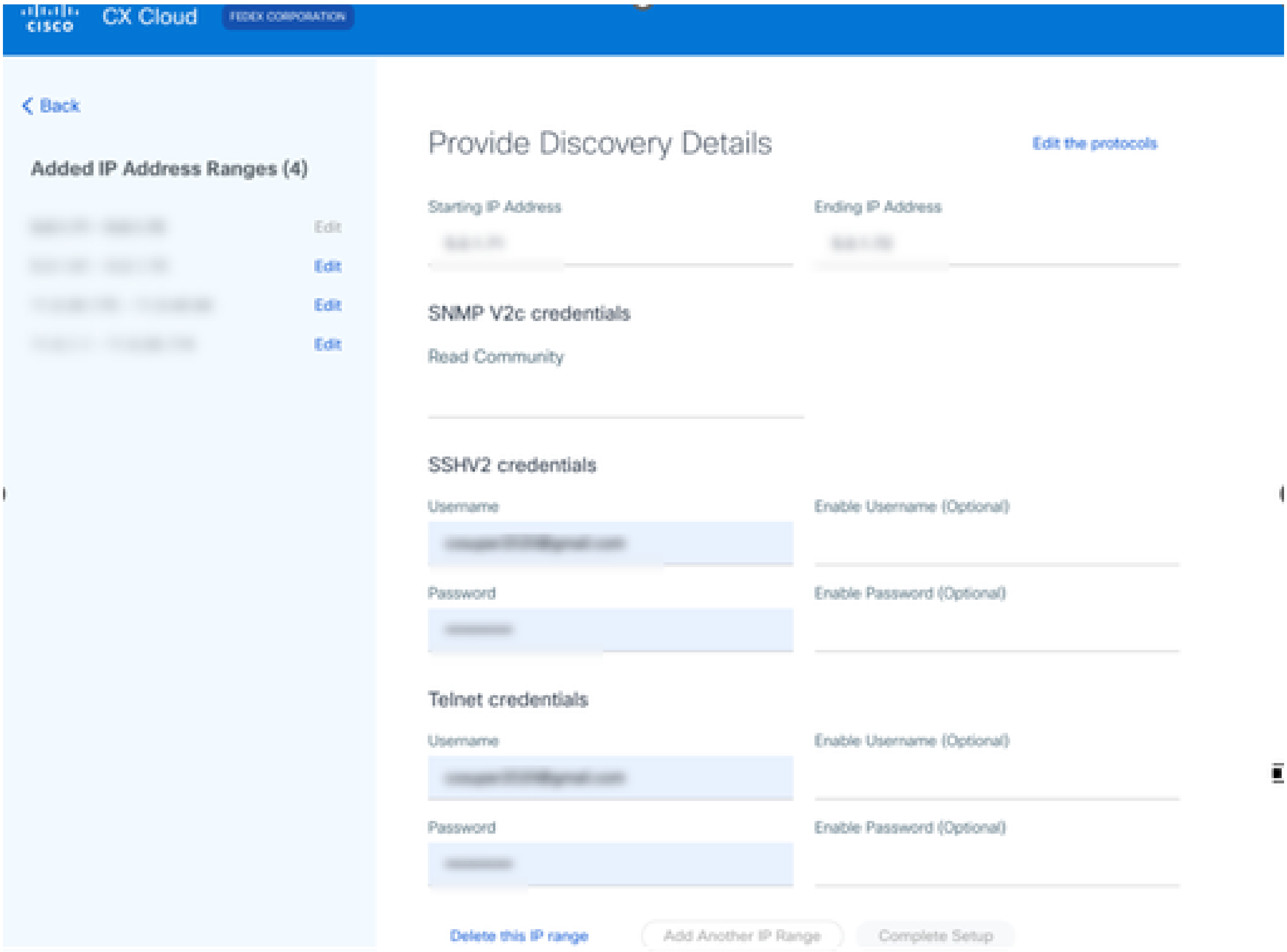
☑ SSH v2 (recommended)

□ SSH v1

☑ Telnet

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.



CX Cloud FEDEX CORPORATION

< Back

Added IP Address Ranges (4)

Edit

Edit

Edit

Edit

Provide Discovery Details

Edit the protocols

Starting IP Address

Ending IP Address

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

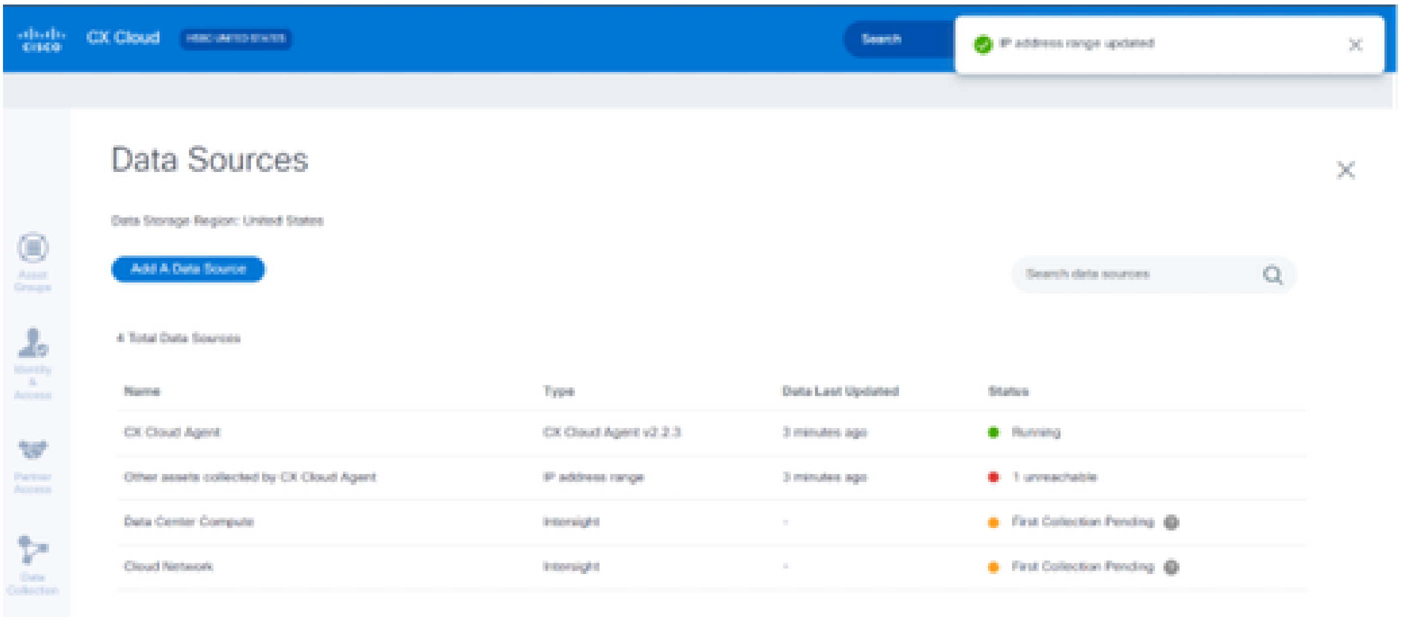
Add Another IP Range

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.



IP address range updated

Data Sources

Data Storage Region: United States

Add A Data Source

Search data sources

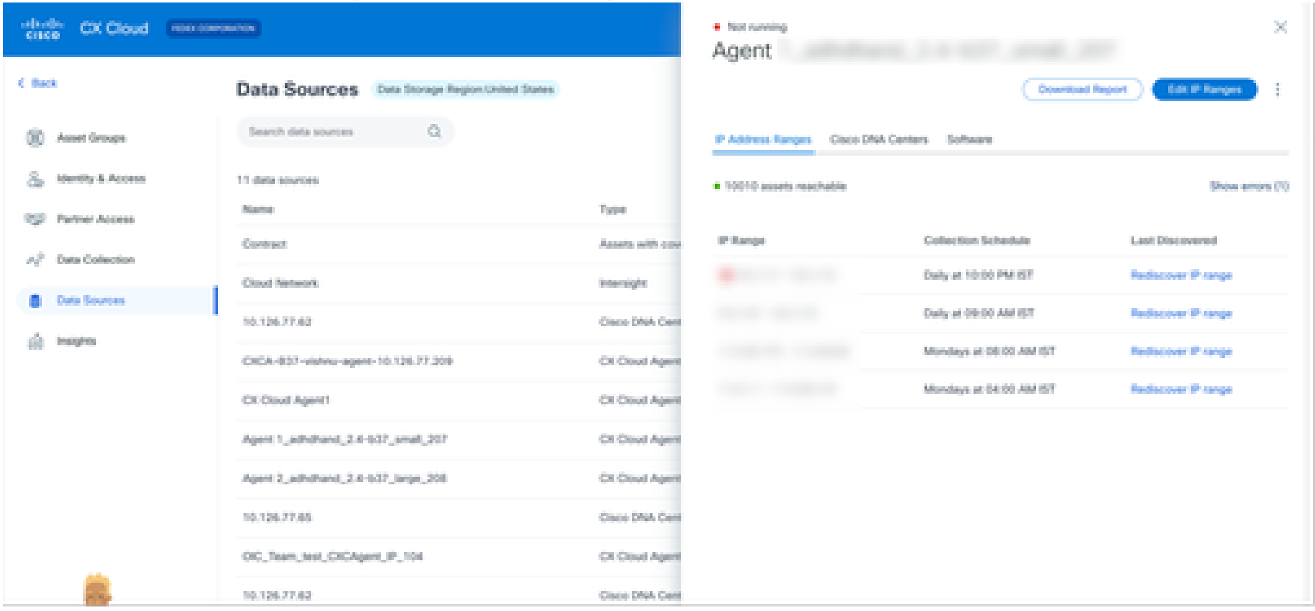
4 Total Data Sources

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

Deleting IP Range

To delete an IP range:

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



Data Sources Data Storage Region United States

Search data sources

11 data sources

Name	Type
Contract	Assets with cov
Cloud Network	Intersight
10.126.77.62	Cisco DNA Cent
CXCA-837-vishnu-agent-10.126.77.209	CX Cloud Agent
CX Cloud Agent1	CX Cloud Agent
Agent 1_adhdhand_2.4-b37_small_207	CX Cloud Agent
Agent 2_adhdhand_2.4-b37_large_208	CX Cloud Agent
10.126.77.65	Cisco DNA Cent
OIC_Team_test_CXCAgent_IP_104	CX Cloud Agent
10.126.77.62	Cisco DNA Cent

● Not running

Agent [redacted]

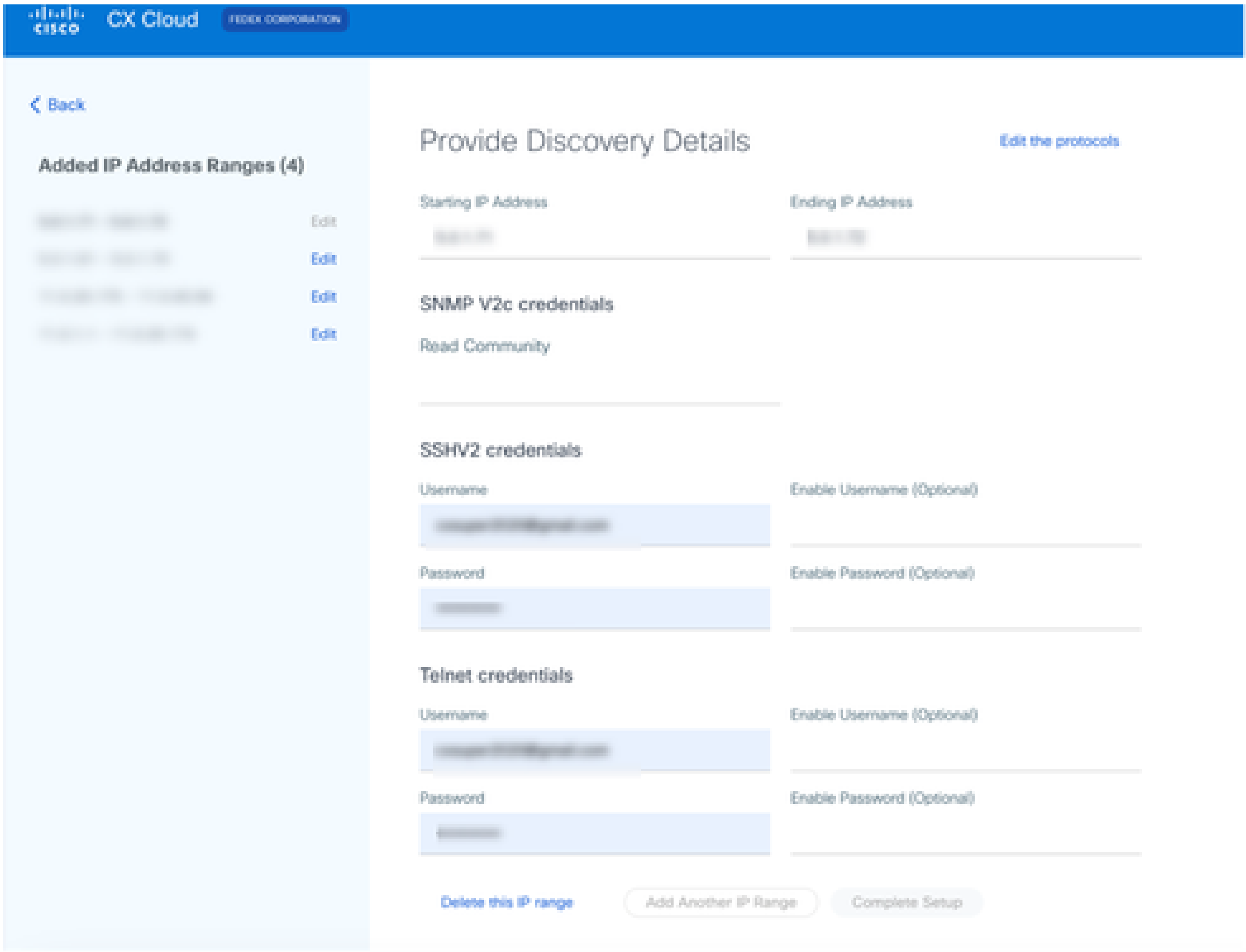
● 10010 assets reachable

Show errors (1)

IP Range	Collection Schedule	Last Discovered
[redacted]	Daily at 10:00 PM IST	Rediscover IP range
[redacted]	Daily at 09:00 AM IST	Rediscover IP range
[redacted]	Mondays at 08:00 AM IST	Rediscover IP range
[redacted]	Mondays at 04:00 AM IST	Rediscover IP range

Data Sources

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



CX Cloud FEDEX CORPORATION

Back

Added IP Address Ranges (4)

Edit

Edit

Edit

Edit

Provide Discovery Details

Edit the protocols

Starting IP Address

Ending IP Address

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)

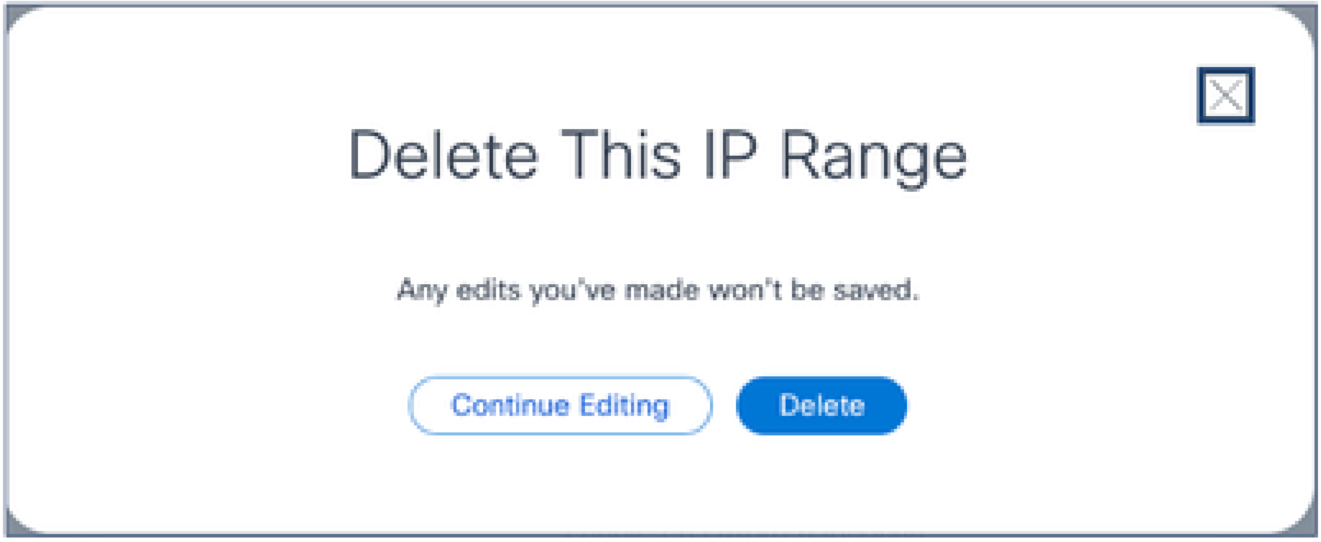
Delete this IP range

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

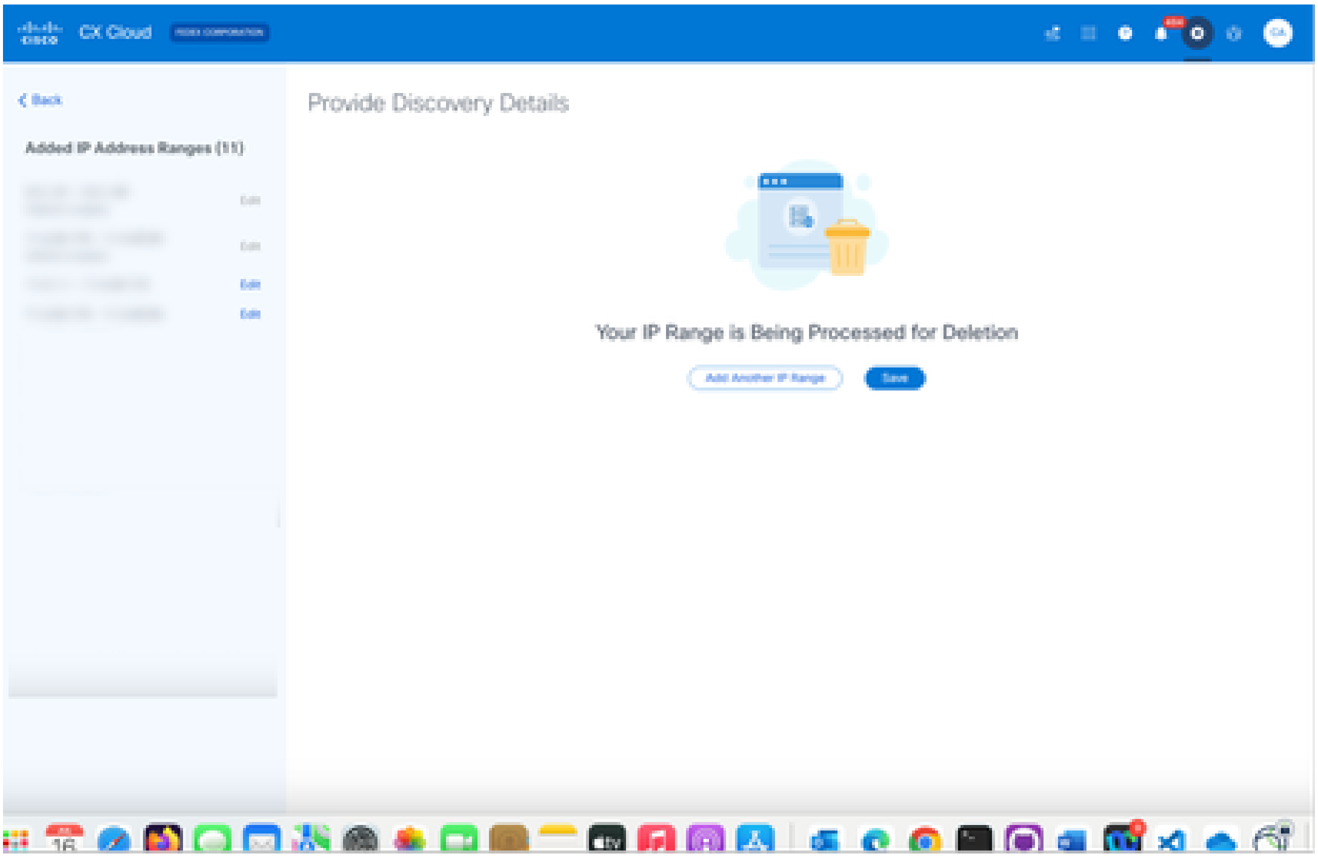
Any edits you've made won't be saved.

Continue Editing

Delete

Confirmation Delete Message

5. Click **Delete**.



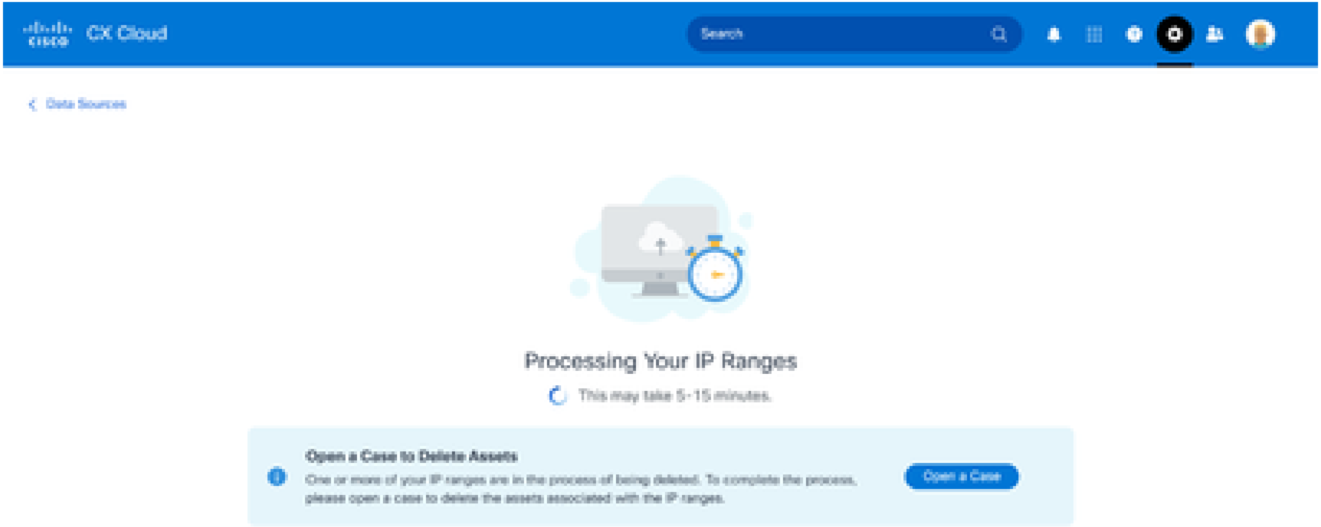
Added IP Address Ranges (11)

Provide Discovery Details

Your IP Range is Being Processed for Deletion

IP Range Delete

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



Processing Your IP Ranges

This may take 5-15 minutes.

Open a Case to Delete Assets

One or more of your IP ranges are in the process of being deleted. To complete the process, please open a case to delete the assets associated with the IP ranges.

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

If the Catalyst Center and Other Assets Collected by CX Agent (Direct Device Connection) are on the same CX Agent, then it is possible that some devices could be discovered by both the Cisco Catalyst Center and direct device connection to CX 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 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 Agent and then rediscovered by Cisco Catalyst Center, Cisco Catalyst Center takes precedence in controlling the device.

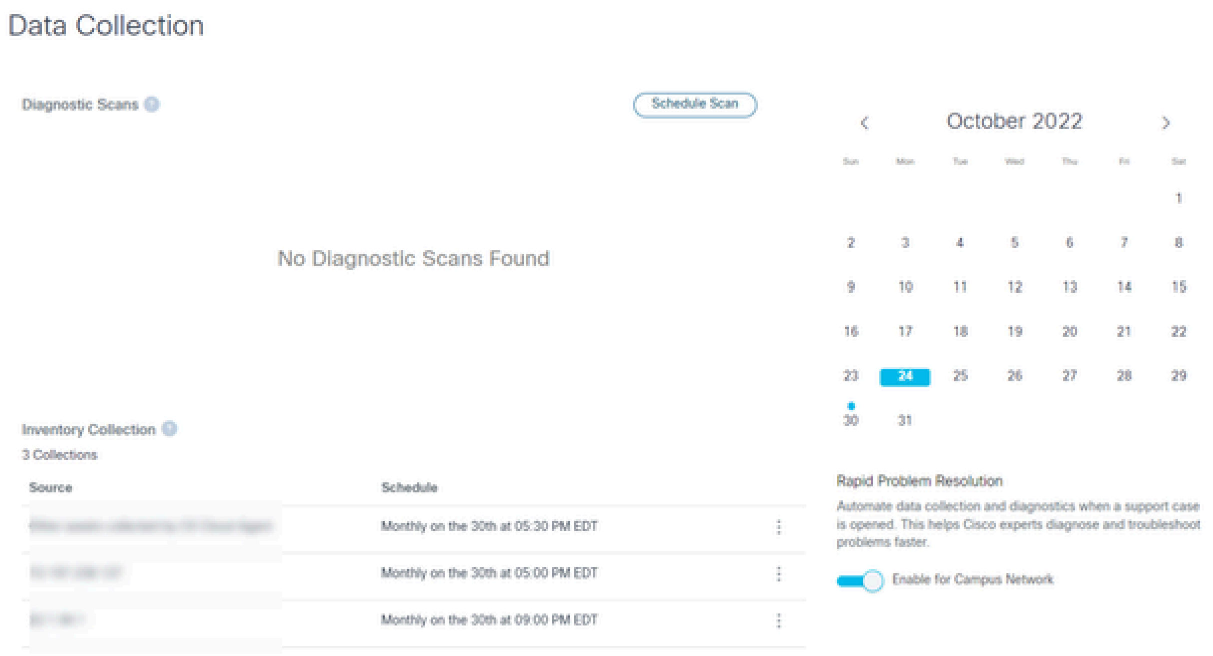
Scheduling Diagnostics Scans

Customers can schedule on demand diagnostic scans in CX Cloud for eligible Success Tracks and their covered devices to populate the **Priority Bugs** in **Advisories**.

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

No Diagnostic Scans Found

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

October 2022

Inventory Collection

3 Collections

Source	Schedule
[redacted]	Monthly on the 30th at 05:30 PM EDT
[redacted]	Monthly on the 30th at 05:00 PM EDT
[redacted]	Monthly on the 30th at 09:00 PM EDT

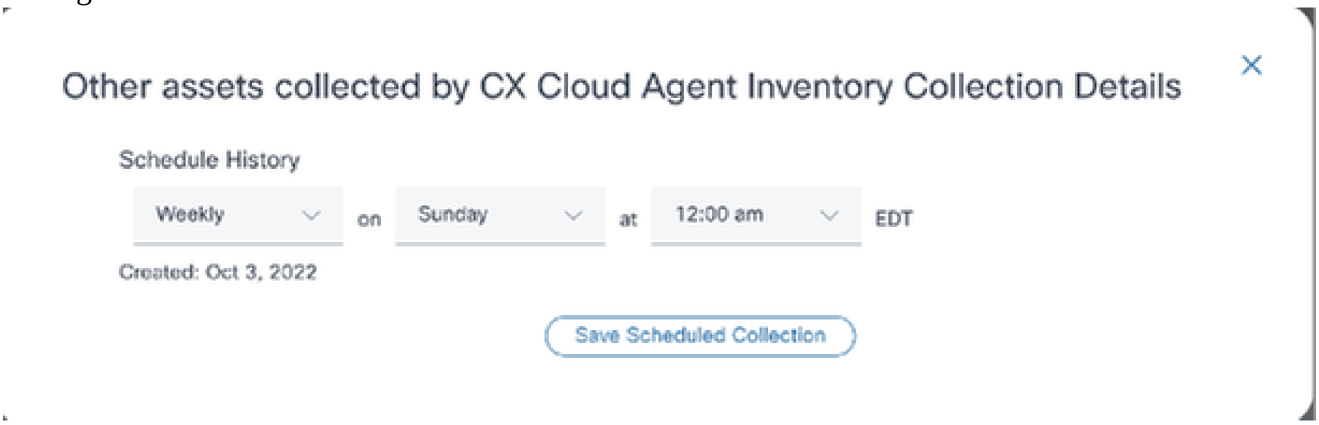
Rapid Problem Resolution

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

Enable for Campus Network

Scheduling Scans

4. Configure a schedule for this scan.



Other assets collected by CX Cloud Agent Inventory Collection Details

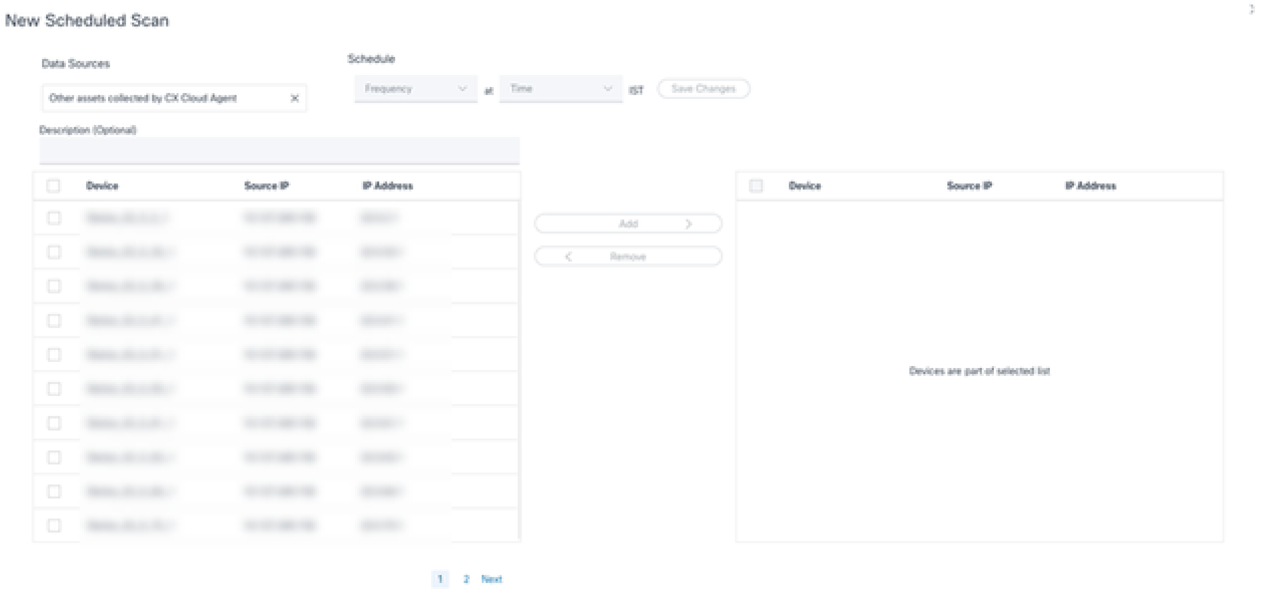
Schedule History

Weekly on Sunday at 12:00 am EDT

Created: Oct 3, 2022

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 IST

Description (Optional)

	Device	Source IP	IP Address
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]

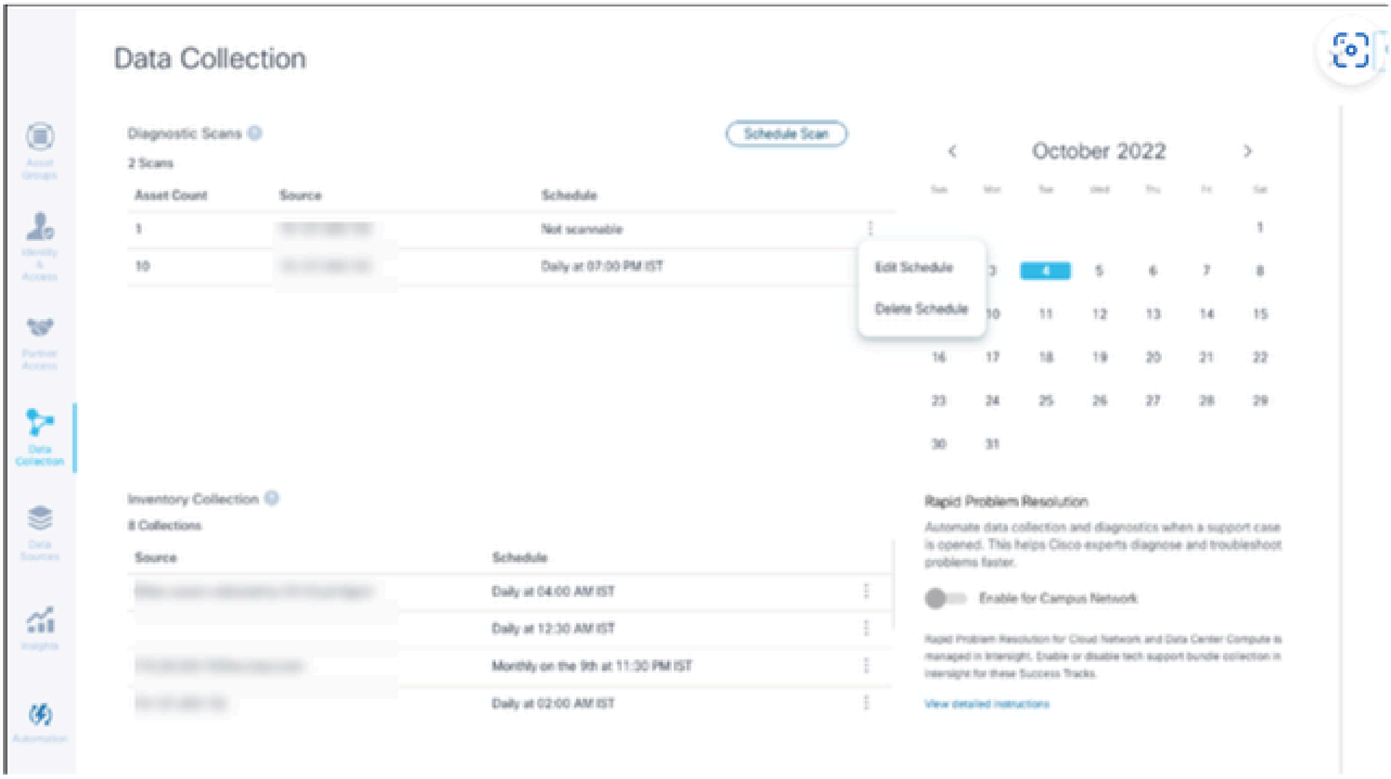
□	Device	Source IP	IP Address

Devices are part of selected list

Schedule 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

Asset Count	Source	Schedule
1	[redacted]	Not scannable
10	[redacted]	Daily at 07:00 PM IST

Inventory Collection

8 Collections

Source	Schedule
[redacted]	Daily at 04:00 AM IST
	Daily at 12:30 AM IST
[redacted]	Monthly on the 9th at 11:30 PM IST
[redacted]	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	22
23	24	25	26	27	28	29
30	31					

Rapid Problems Resolution

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

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.

Data Collection with Edit and Delete Schedule options

Upgrading CX Agent VMs to Medium and Large Configurations

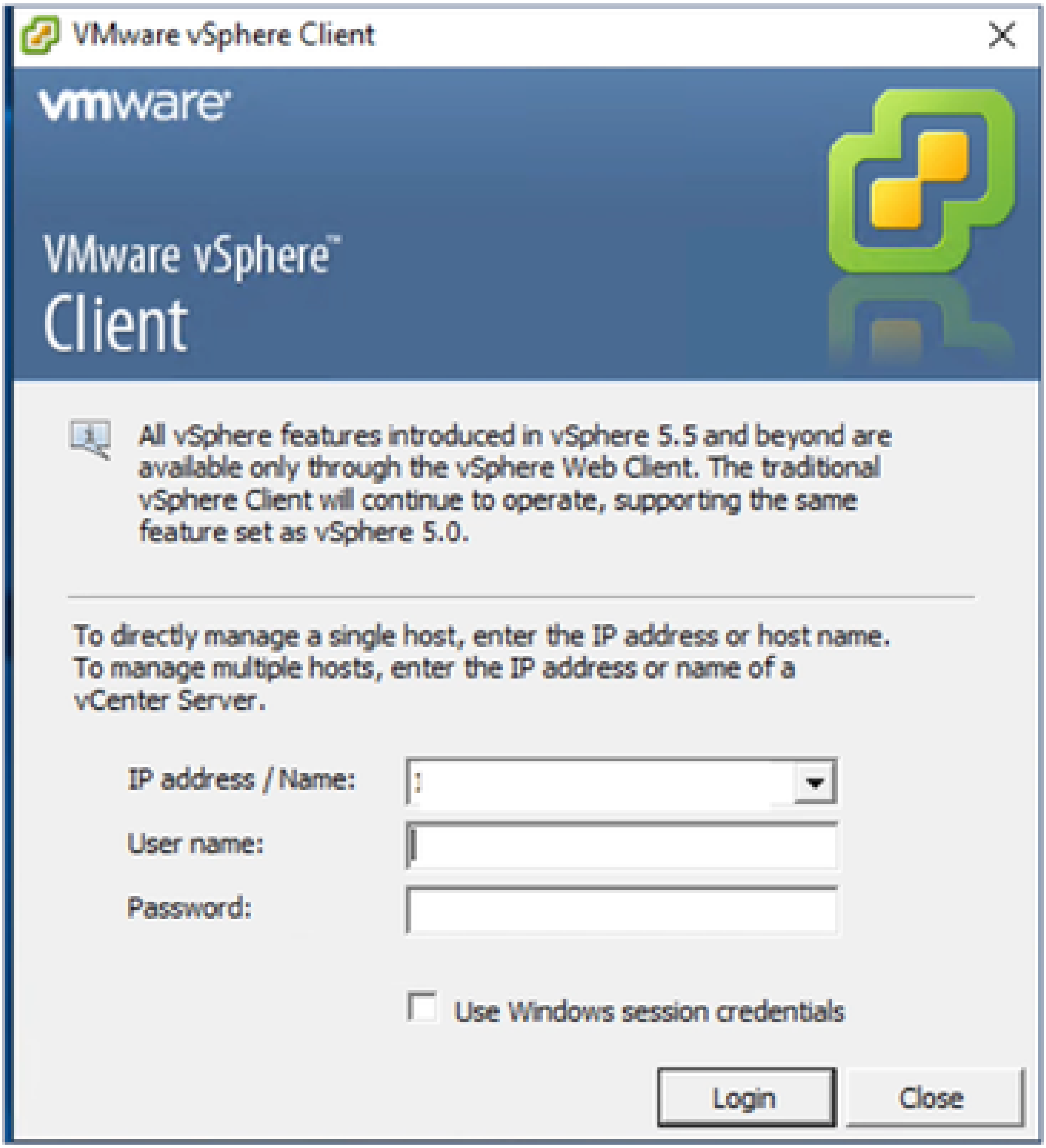
Once VMs are upgraded, it is not possible to:

- 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:

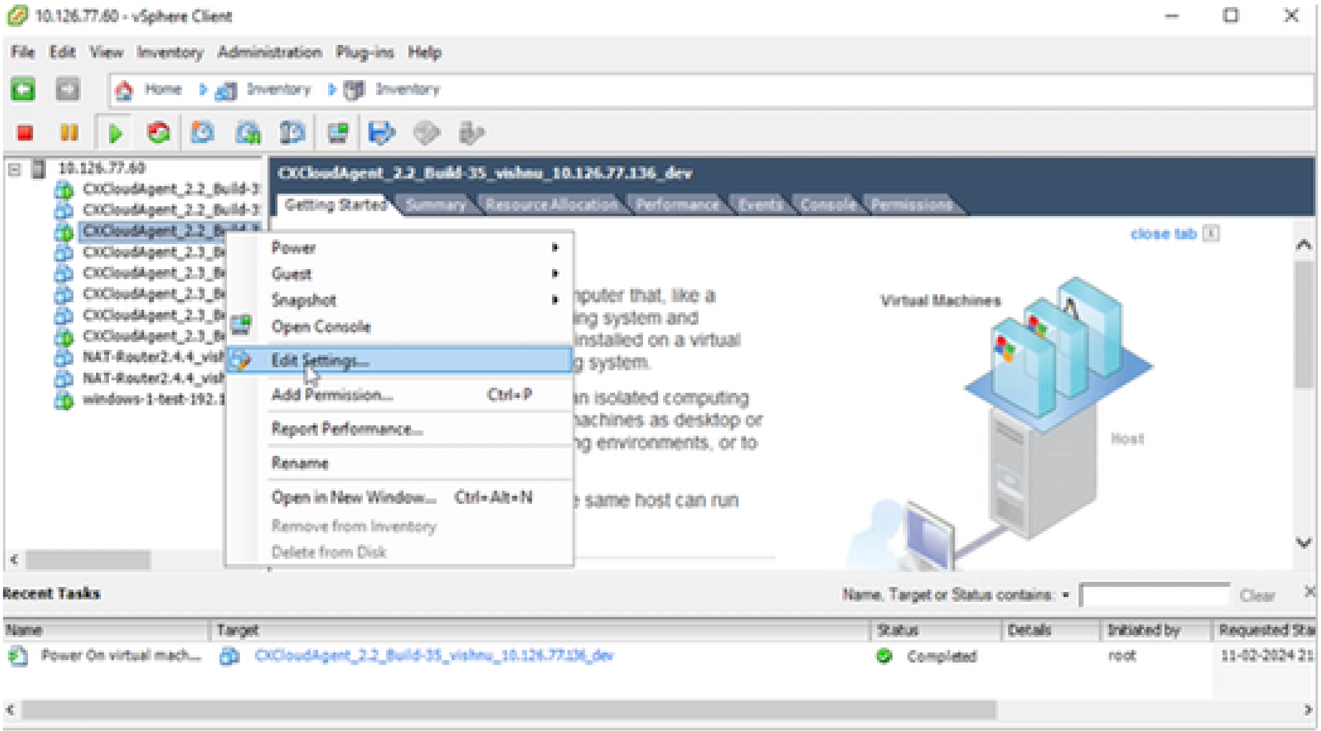


All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

vSphere Client

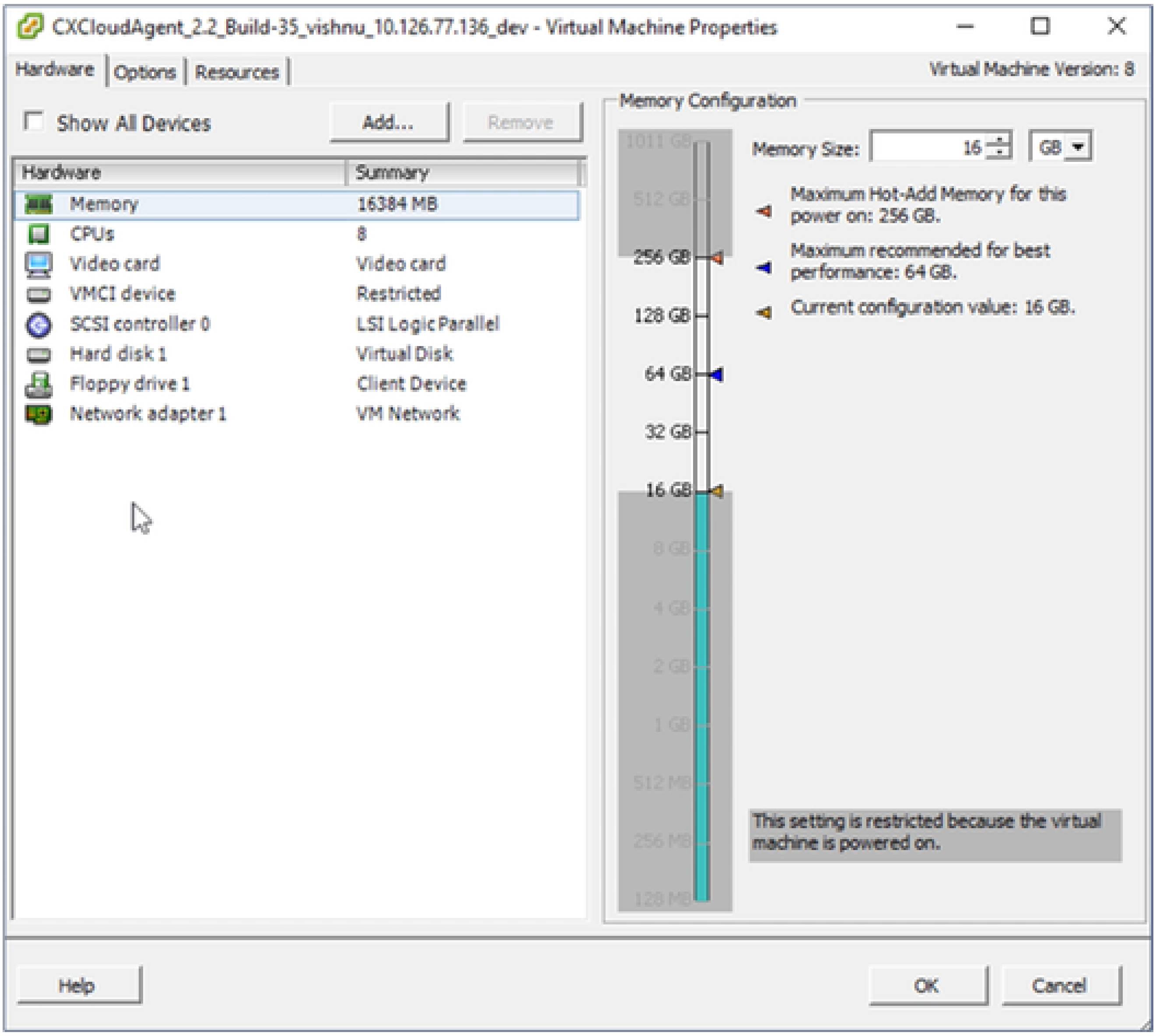
1. Log in to the VMware vSphere Client. The **Home** page displays a list of VMs.



Name	Target	Status	Details	Initiated by	Requested Sta
Power On virtual mach...	CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev	Completed		root	11-02-2024 21

Edit Settings

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



CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev - Virtual Machine Properties

Hardware	Summary
Memory	16384 MB
CPUs	8
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VM Network

Memory Configuration

Memory Size: 16 GB

Maximum Hot-Add Memory for this power on: 256 GB.

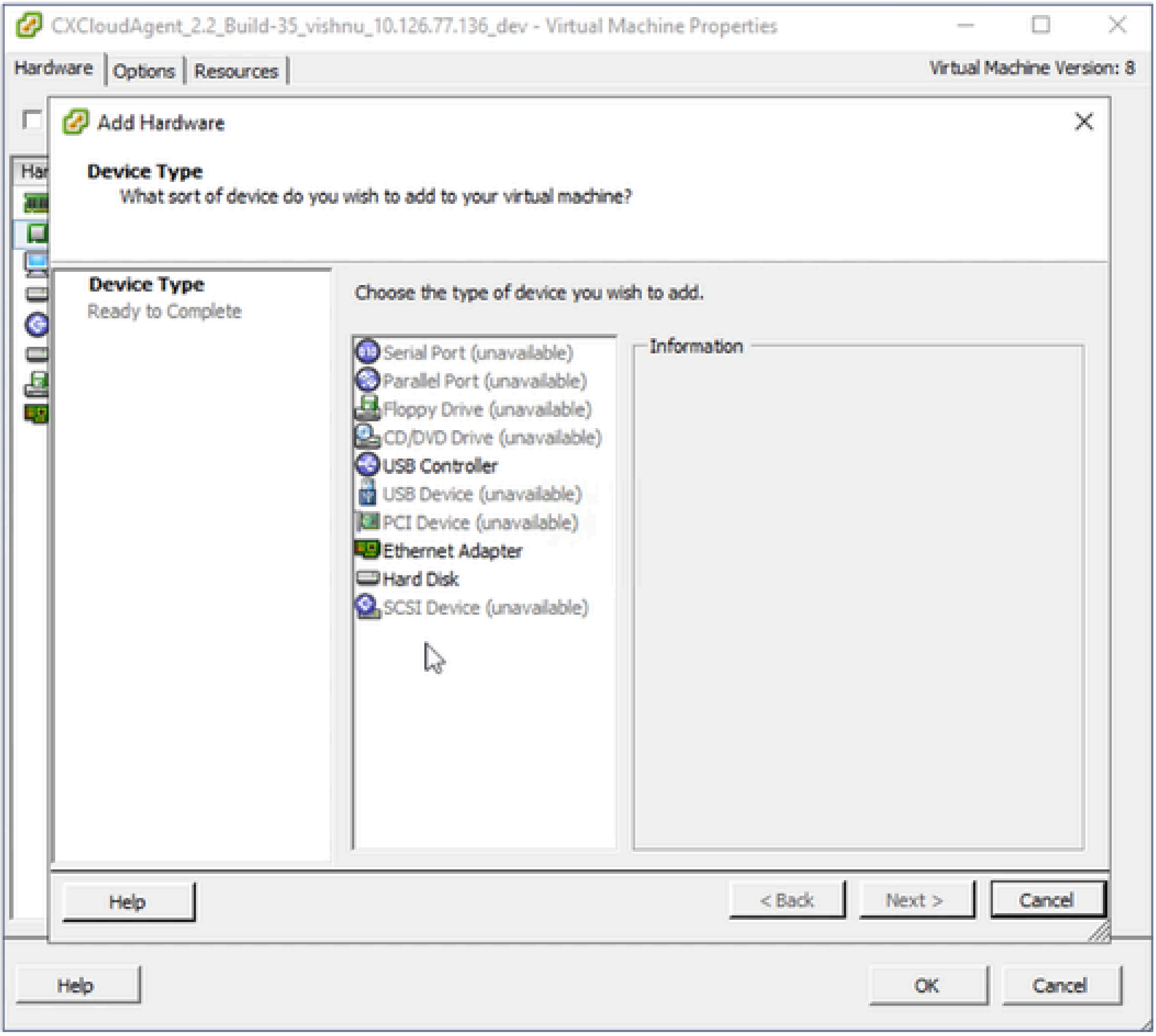
Maximum recommended for best performance: 64 GB.

Current configuration value: 16 GB.

This setting is restricted because the virtual machine is powered on.

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.


CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev - Virtual Machine Properties

Add Hardware

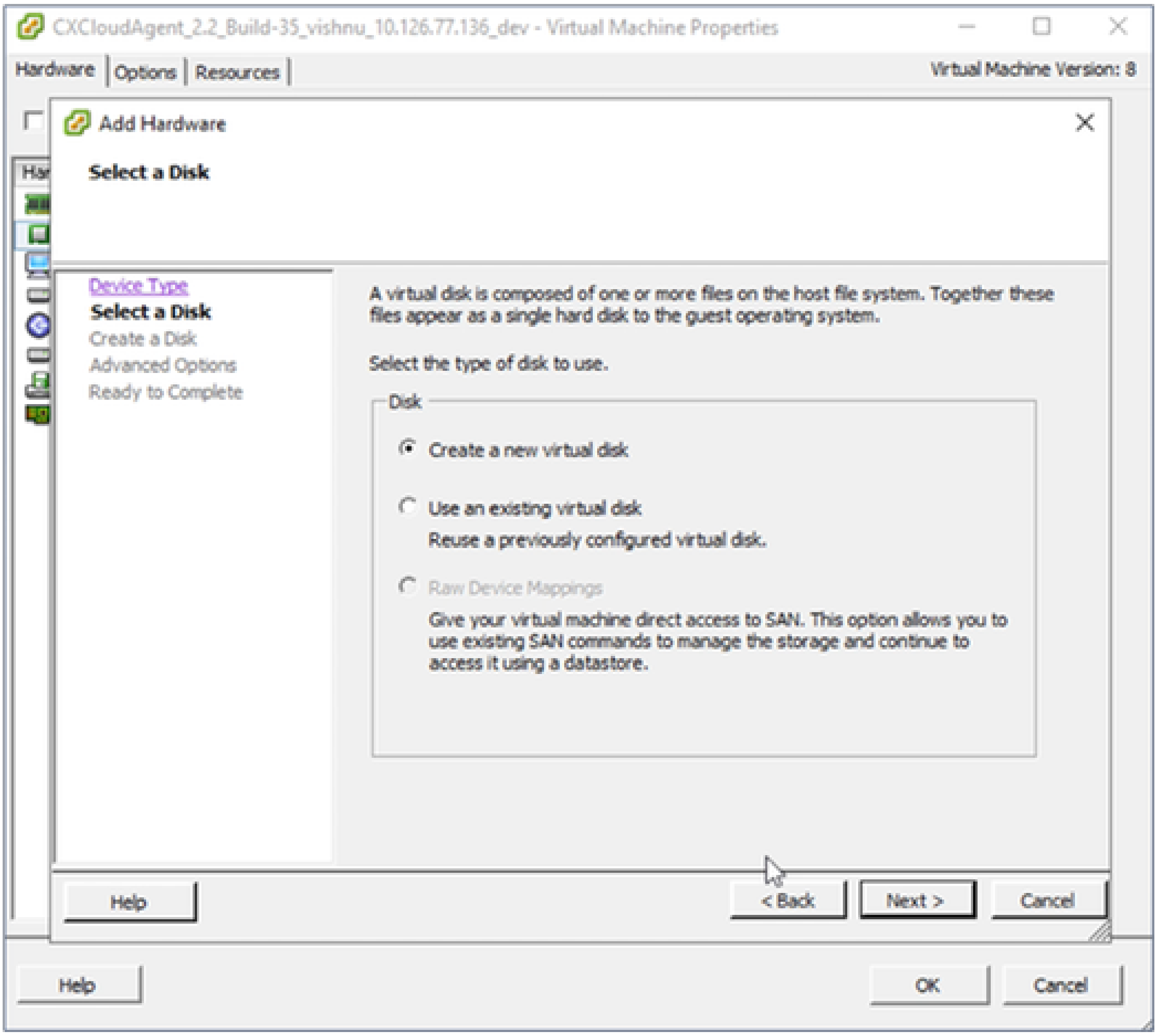
Device Type

What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

Device Type

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



Select a Disk

A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

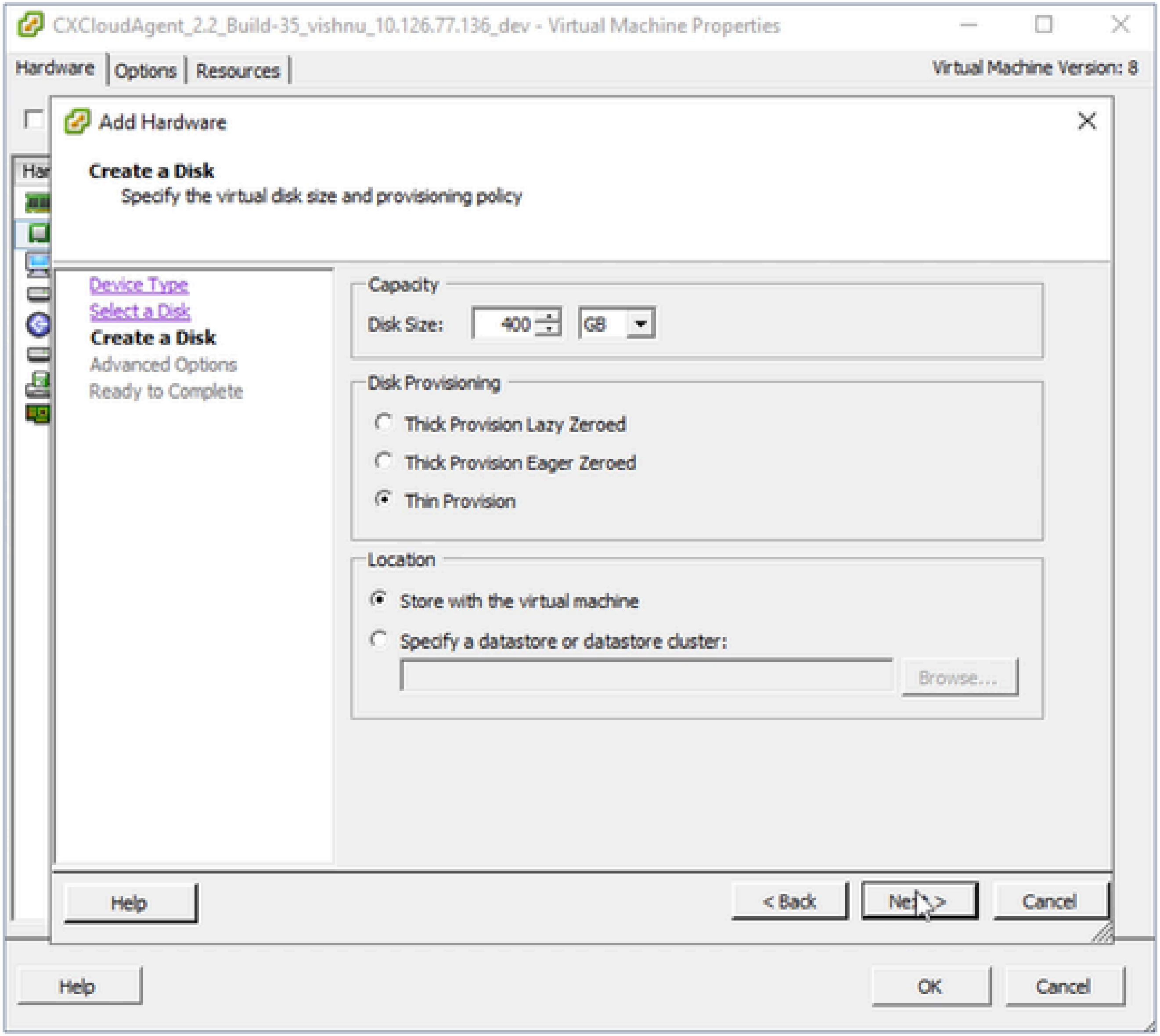
● Create a new virtual disk

○ Use an existing virtual disk
Reuse a previously configured virtual disk.

○ Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

Select Disk

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



CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev - Virtual Machine Properties

Add Hardware

Create a Disk

Specify the virtual disk size and provisioning policy

Capacity

Disk Size: 400 GB

Disk Provisioning

○ Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

● Thin Provision

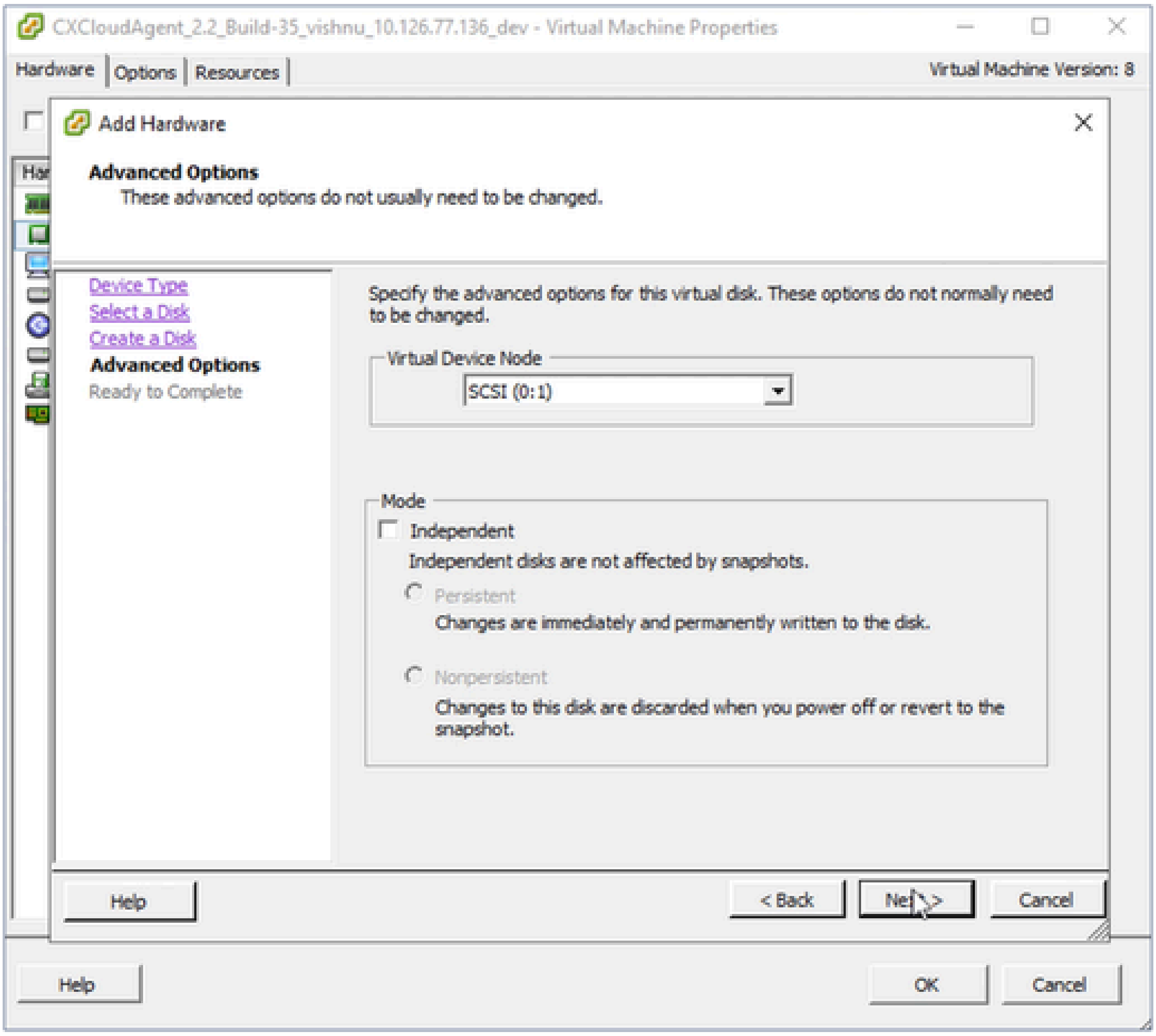
Location

● Store with the virtual machine

○ Specify a datastore or datastore cluster:

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.



CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev - Virtual Machine Properties

Hardware | Options | Resources

Virtual Machine Version: 8

Add Hardware

Advanced Options

These advanced options do not usually need to be changed.

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node: SCSI (0:1)

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

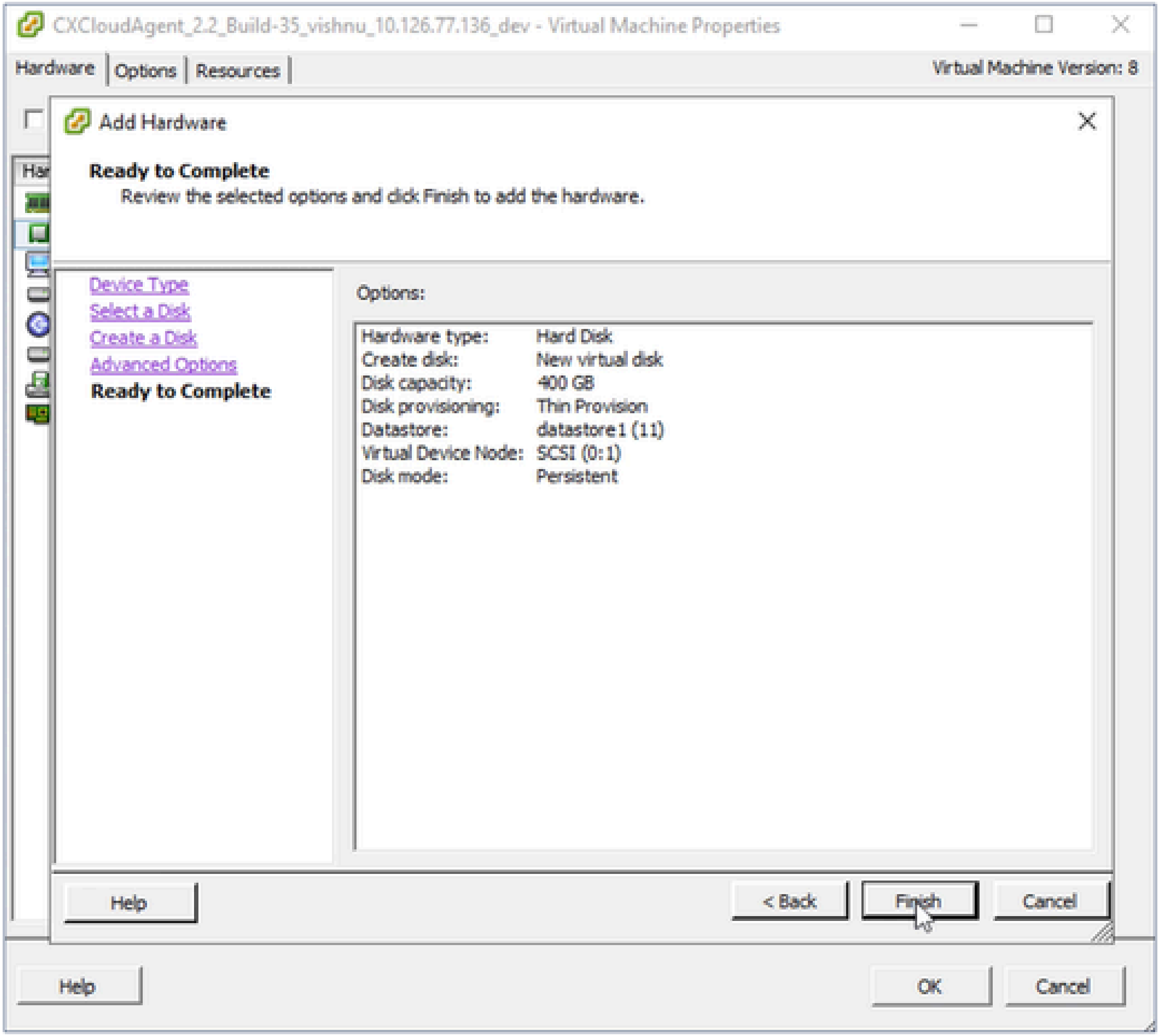
Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

Advanced Options

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



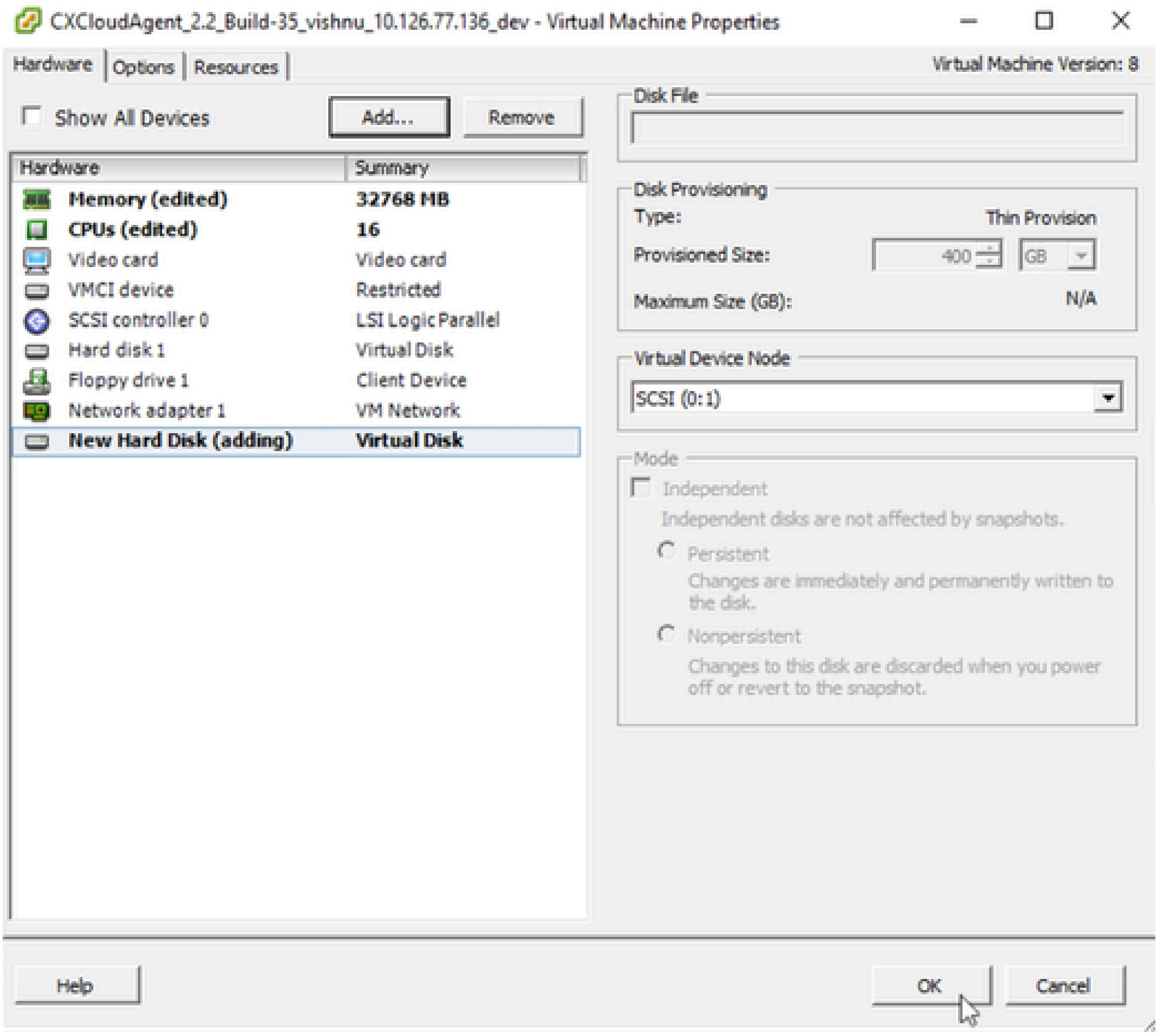
Ready to Complete

Review the selected options and click Finish to add the hardware.

Hardware type:	Hard Disk
Create disk:	New virtual disk
Disk capacity:	400 GB
Disk provisioning:	Thin Provision
Datastore:	datastore1 (11)
Virtual Device Node:	SCSI (0:1)
Disk mode:	Persistent

Ready to Complete

13. Click **Finish**.



CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev - Virtual Machine Properties

Virtual Machine Version: 8

☐ Show All Devices

Hardware	Summary
Memory (edited)	**32768 MB**
CPUs (edited)	**16**
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VM Network
New Hard Disk (adding)	**Virtual Disk**

Disk File

Disk Provisioning

Type: Thin Provision

Provisioned Size: 400 GB

Maximum Size (GB): N/A

Virtual Device Node

SCSI (0:1)

Mode

☐ Independent

Independent disks are not affected by snapshots.

○ Persistent

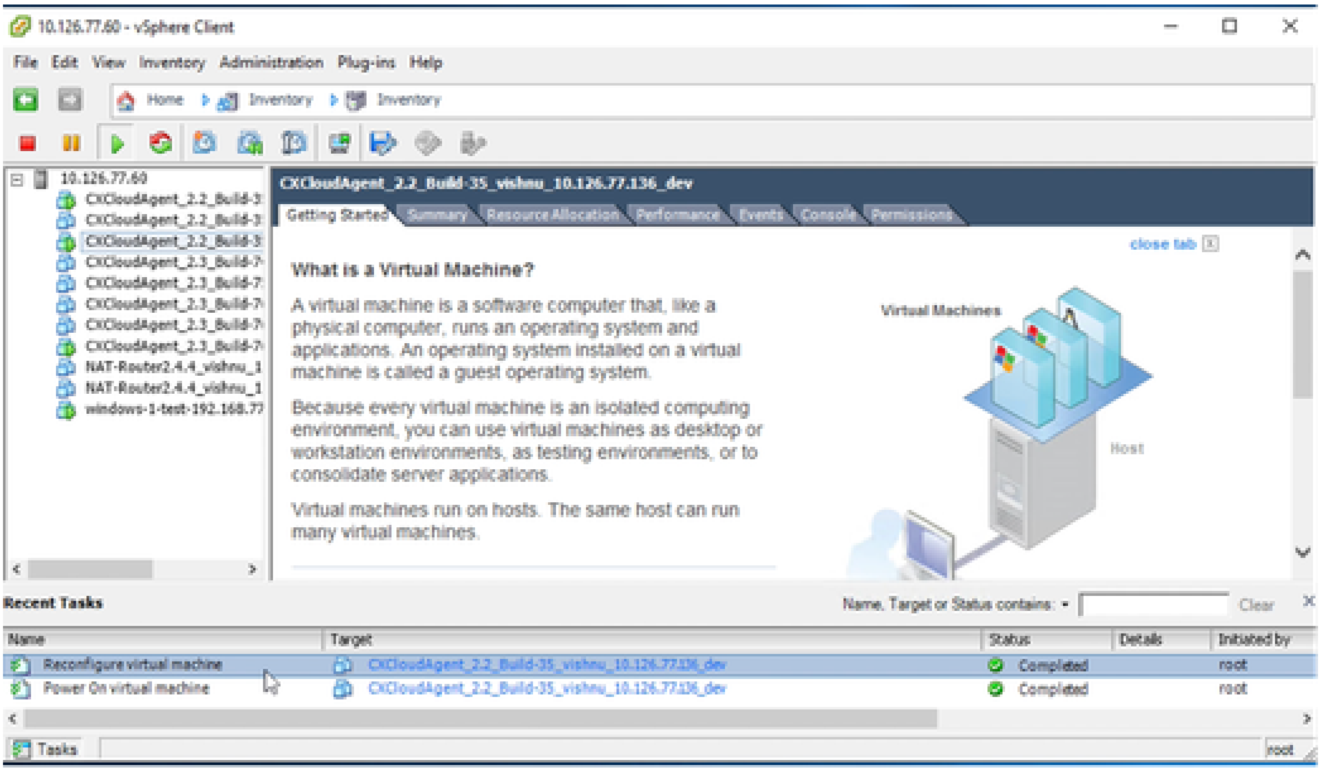
Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

Hardware

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



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.

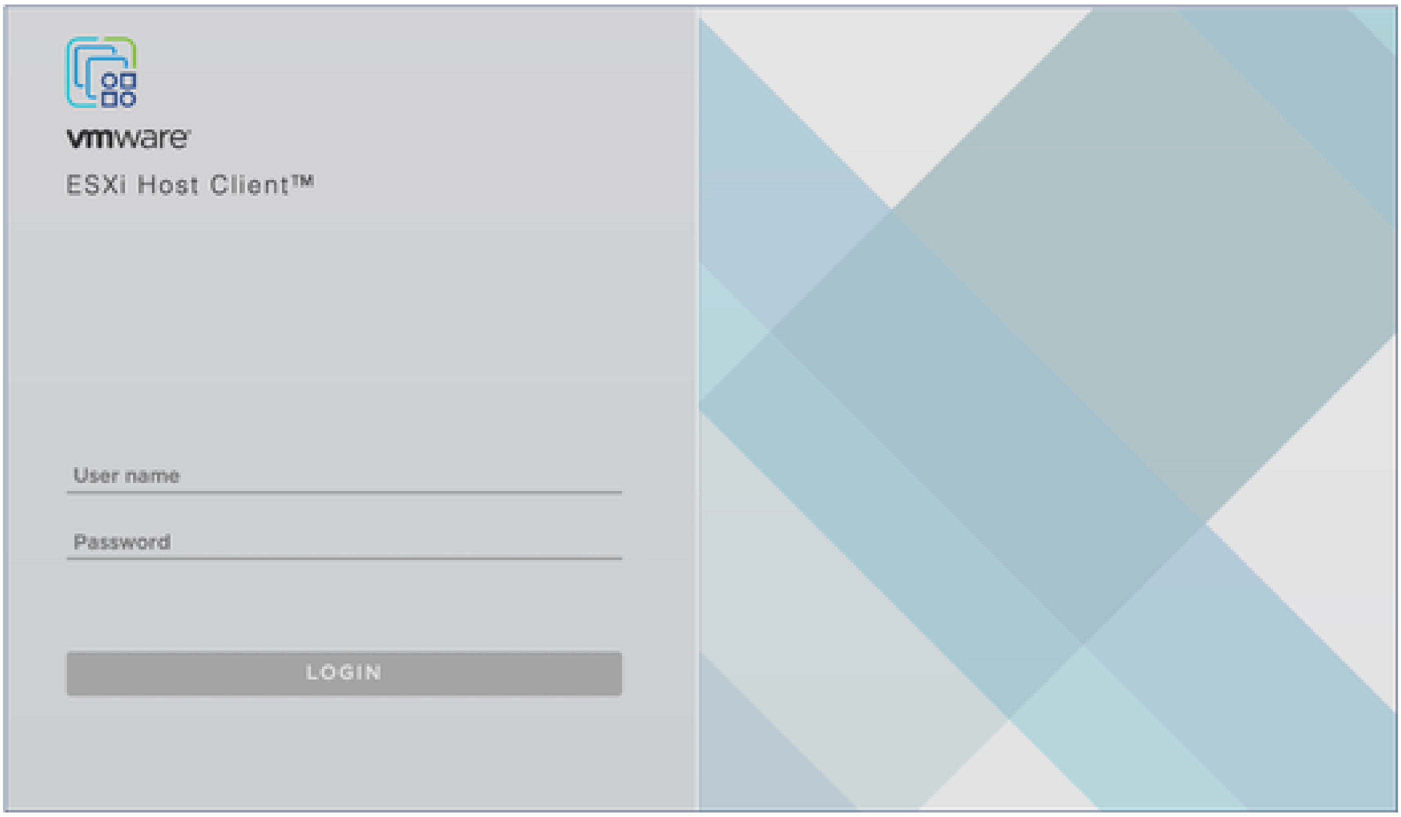
Name	Target	Status	Details	Initiated by
Reconfigure virtual machine	CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev	Completed		root
Power On virtual machine	CXCloudAgent_2.2_Build-35_vishnu_10.126.77.136_dev	Completed		root

Recent Tasks

Note: Configuration changes take approximately five minutes to complete.

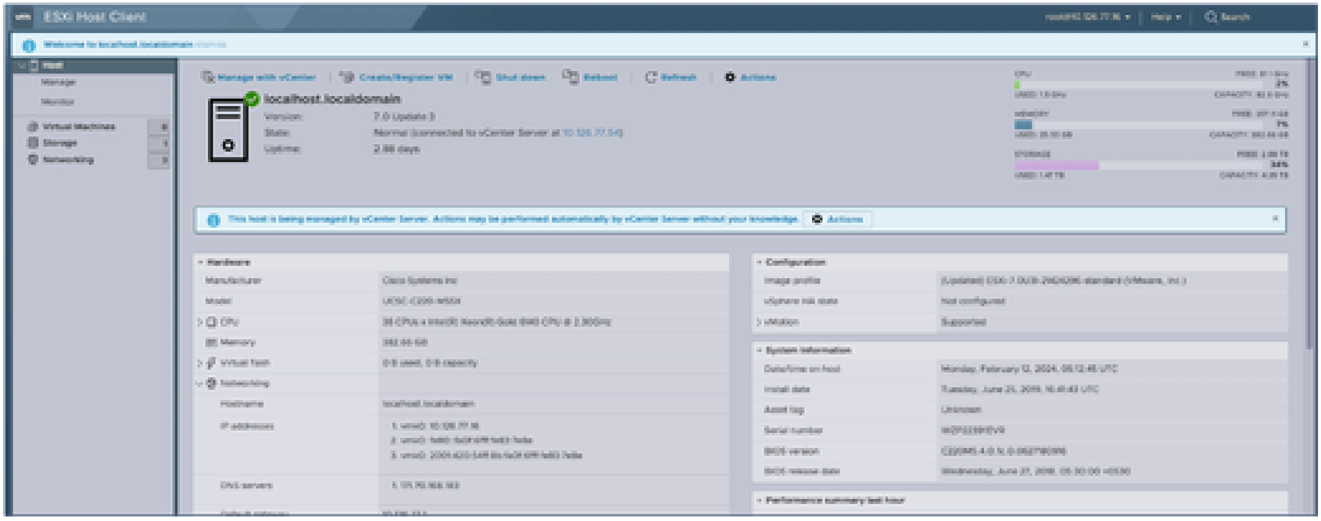
Reconfiguring Using Web Client ESXi v6.0

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



ESXi Client

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



Welcome to localhost.localdomain

localhost.localdomain
Version: 7.0 Update 3
State: Normal (connected to vCenter Server at 10.126.77.54)
Uptime: 2.88 days

CPU FREE: 81.1 GHz 2% USED: 1.5 GHz CAPACITY: 82.6 GHz
MEMORY FREE: 357.1 GB 7% USED: 25.55 GB CAPACITY: 382.66 GB
STORAGE FREE: 2.88 TB 34% USED: 1.47 TB CAPACITY: 4.35 TB

This host is being managed by vCenter Server. Actions may be performed automatically by vCenter Server without your knowledge.

Hardware
Manufacturer: Cisco Systems Inc
Model: UCSC-C220-M5SX
CPU: 36 CPUs x Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz
Memory: 382.66 GB
Virtual flash: 0 B used, 0 B capacity
Networking
Hostname: localhost.localdomain
IP addresses: 1. vmk0: 10.126.77.16
2. vmk0: fe80::[illegible]
3. vmk0: 2001:420:[illegible]
DNS servers: 1. 171.70.168.183

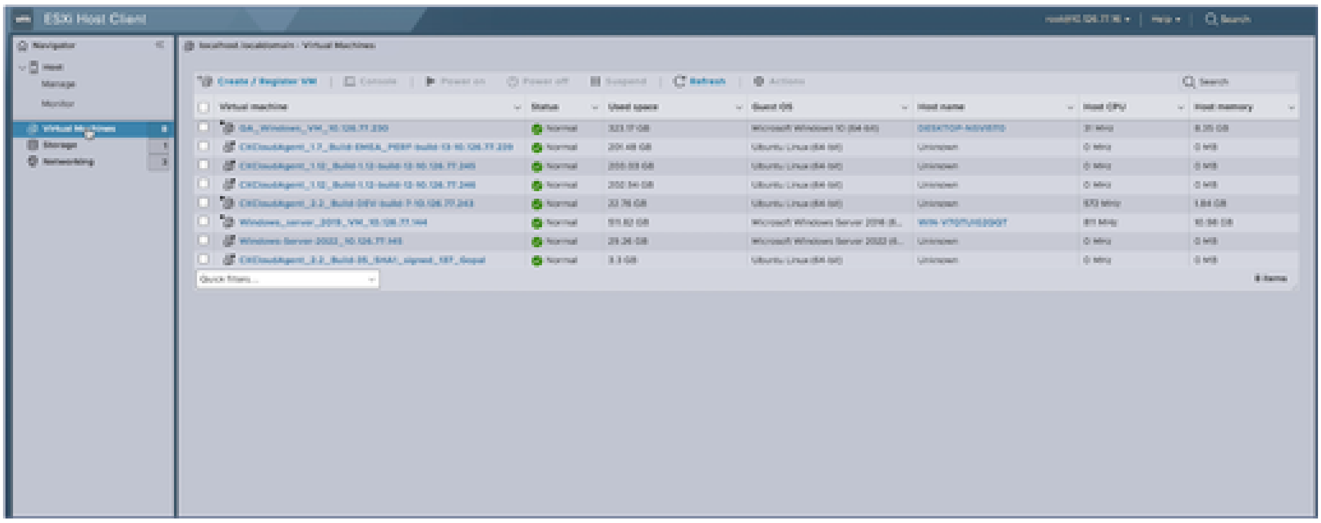
Configuration
Image profile: (Updated) ESXi-7.0U3i-20842708-standard (VMware, Inc.)
vSphere HA state: Not configured
vMotion: Supported

System information
Date/time on host: Monday, February 12, 2024, 09:12:48 UTC
Install date: Tuesday, June 25, 2019, 16:41:43 UTC
Asset tag: Unknown
Serial number: WZP22391EVR
BIOS version: C220M5.4.0.1c.0.0627180916
BIOS release date: Wednesday, June 27, 2018, 05:30:00 +0530

Performance summary last hour

ESXi Home Page

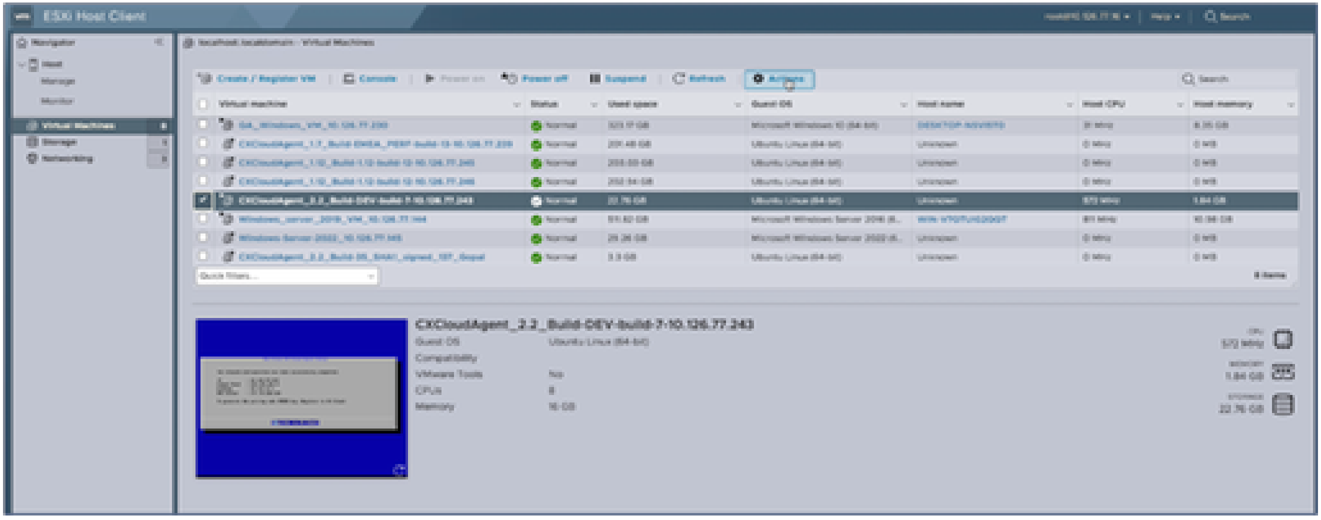
2. Click **Virtual Machine** to display a list of VMs.



Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
GA_Windows_VM_10.126.77.230	Normal	323.17 GB	Microsoft Windows 10 (64-bit)	DESKTOP-N5VI5TO	31 MHz	8.35 GB
CXCloudAgent_1.7_Build-EMEA_PERF-build-13-10.126.77.239	Normal	201.48 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB
CXCloudAgent_1.12_Build-1.12-build-13-10.126.77.245	Normal	200.03 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB
CXCloudAgent_1.12_Build-1.12-build-13-10.126.77.246	Normal	202.94 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB
CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243	Normal	22.76 GB	Ubuntu Linux (64-bit)	Unknown	572 MHz	1.84 GB
Windows_server_2019_VM_10.126.77.144	Normal	511.82 GB	Microsoft Windows Server 2016 (6...	WIN-V7GTUIG2GGT	811 MHz	10.98 GB
Windows Server 2022_10.126.77.145	Normal	29.26 GB	Microsoft Windows Server 2022 (6...	Unknown	0 MHz	0 MB
CXCloudAgent_2.2_Build-35_SHA1_signed_137_Gopal	Normal	3.3 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB

List of VMs

3. Select the target VM.



CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243

Guest OS: Ubuntu Linux (64-bit)

Compatibility

VMware Tools: No

CPUs: 8

Memory: 16 GB

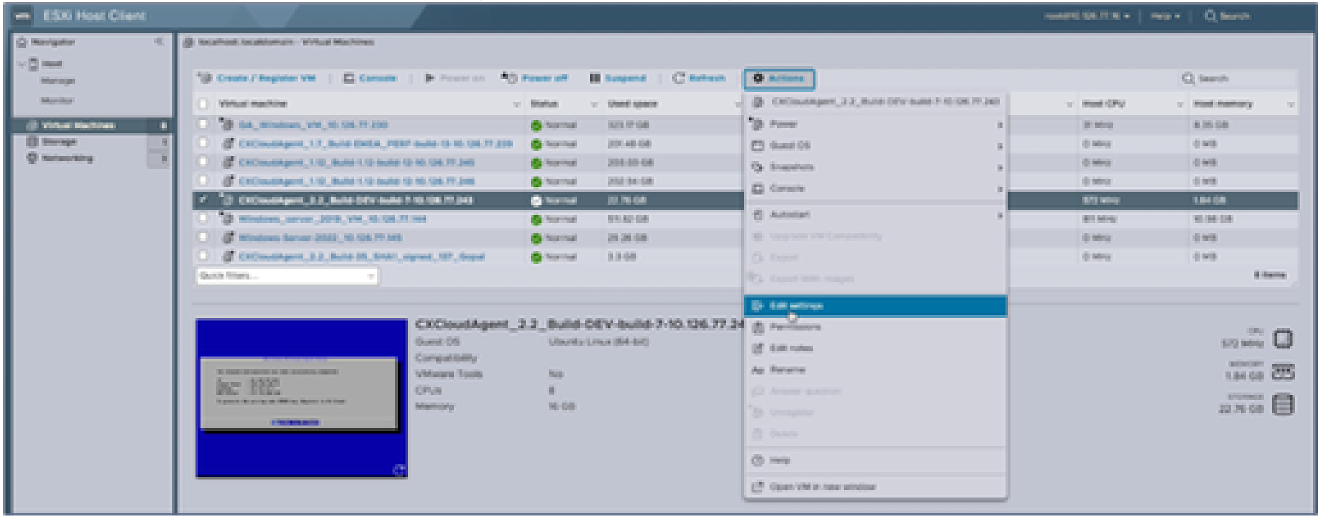
CPU: 572 MHz

Memory: 1.84 GB

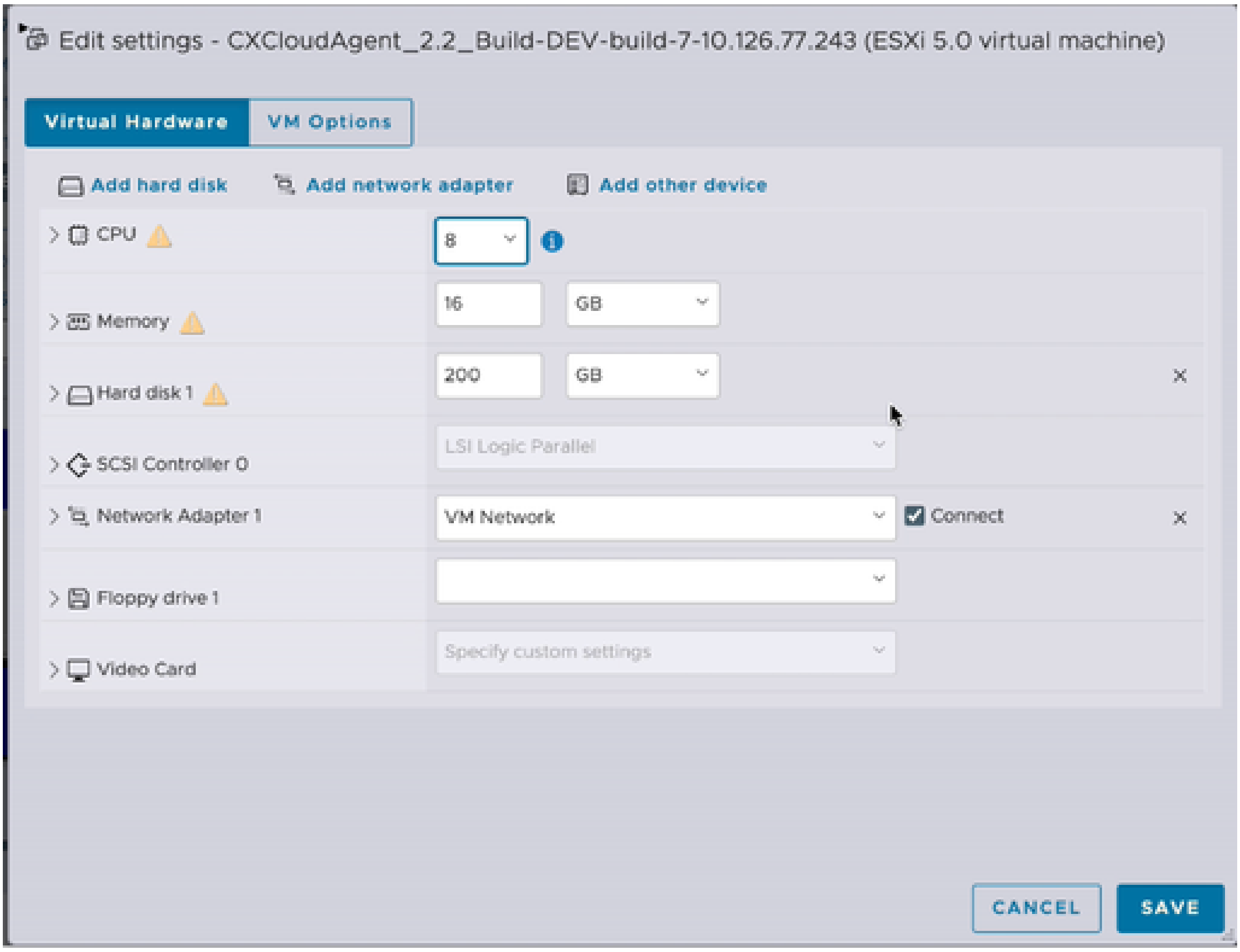
Storage: 22.76 GB

Target VM

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



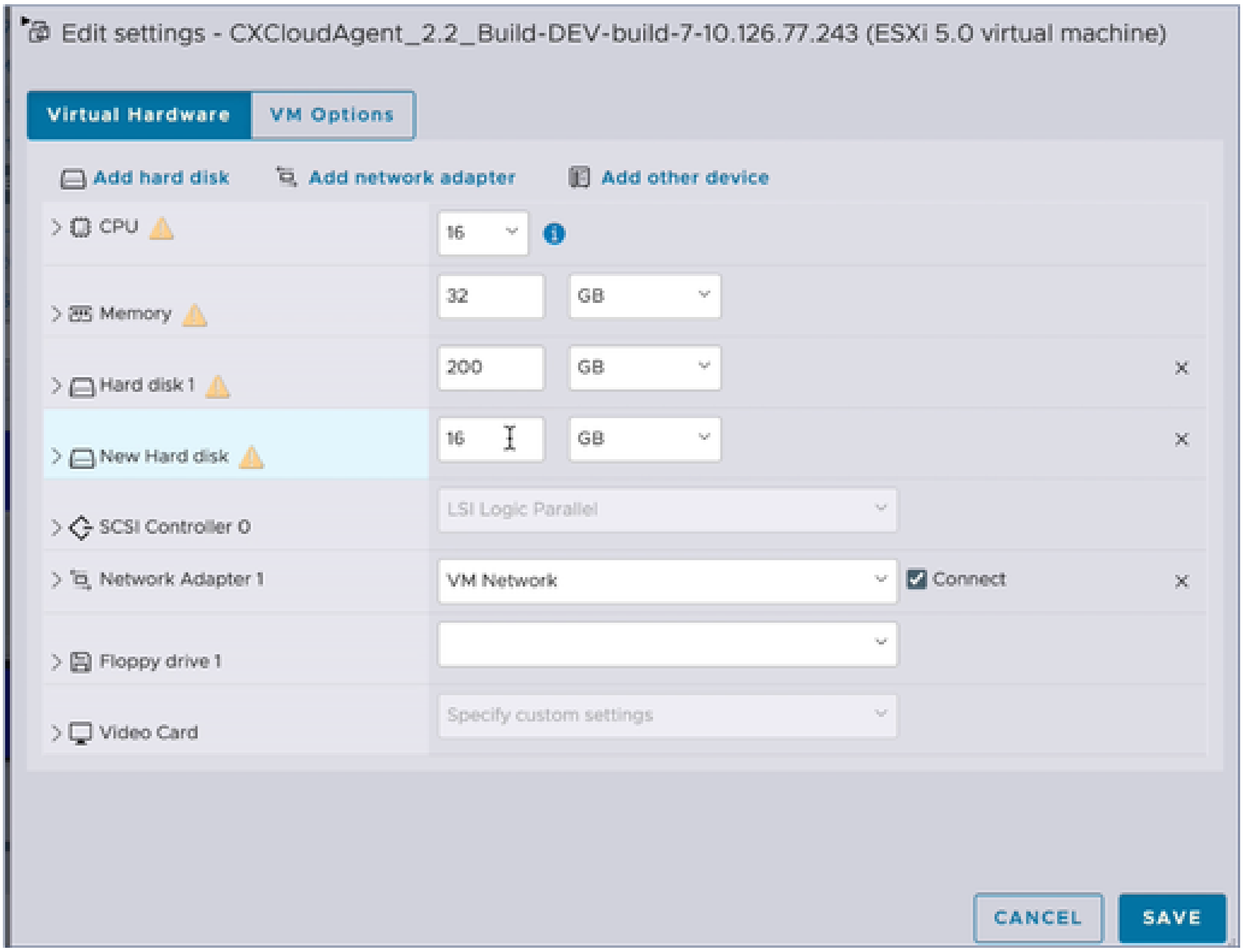
Actions


Edit settings - CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243 (ESXi 5.0 virtual machine)

CPU ⚠	8		
Memory ⚠	16	GB	
Hard disk 1 ⚠	200	GB	×
SCSI Controller 0	LSI Logic Parallel		
Network Adapter 1	VM Network	☑ Connect	×
Floppy drive 1			
Video Card	Specify custom settings		

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 - CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243 (ESXi 5.0 virtual machine)

CPU 16

Memory 32 GB

Hard disk 1 200 GB

New Hard disk 16 GB

SCSI Controller 0 LSI Logic Parallel

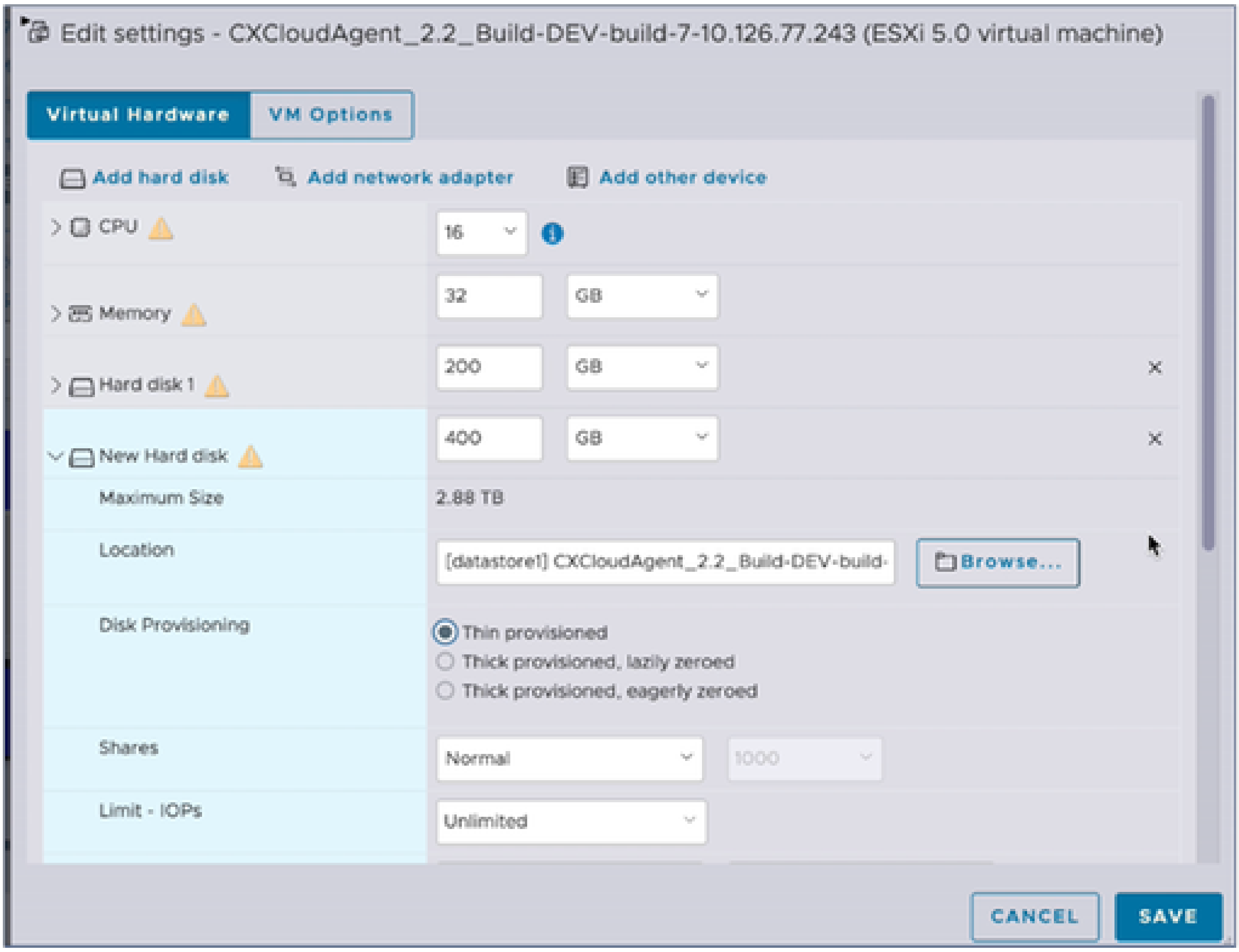
Network Adapter 1 VM Network ☑ Connect

Floppy drive 1

Video Card Specify custom settings

Edit Settings

8. 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)
9. Click the arrow to expand **New Hard disk**. The properties display.



Edit settings - CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243 (ESXi 5.0 virtual machine)

CPU: 16

Memory: 32 GB

Hard disk 1: 200 GB

New Hard disk: 400 GB

Maximum Size: 2.88 TB

Location: [datastore1] CXCloudAgent_2.2_Build-DEV-build-

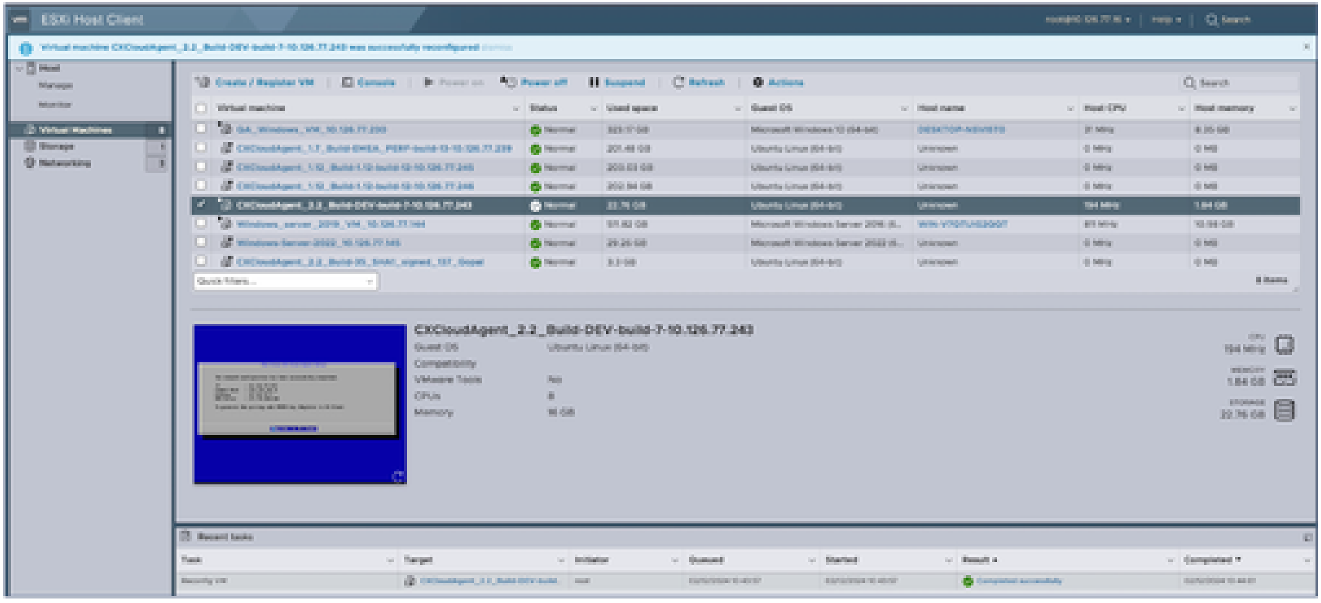
Disk Provisioning: ● Thin provisioned ○ Thick provisioned, lazily zeroed ○ Thick provisioned, eagerly zeroed

Shares: Normal 1000

Limit - IOPs: Unlimited

Edit Settings

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

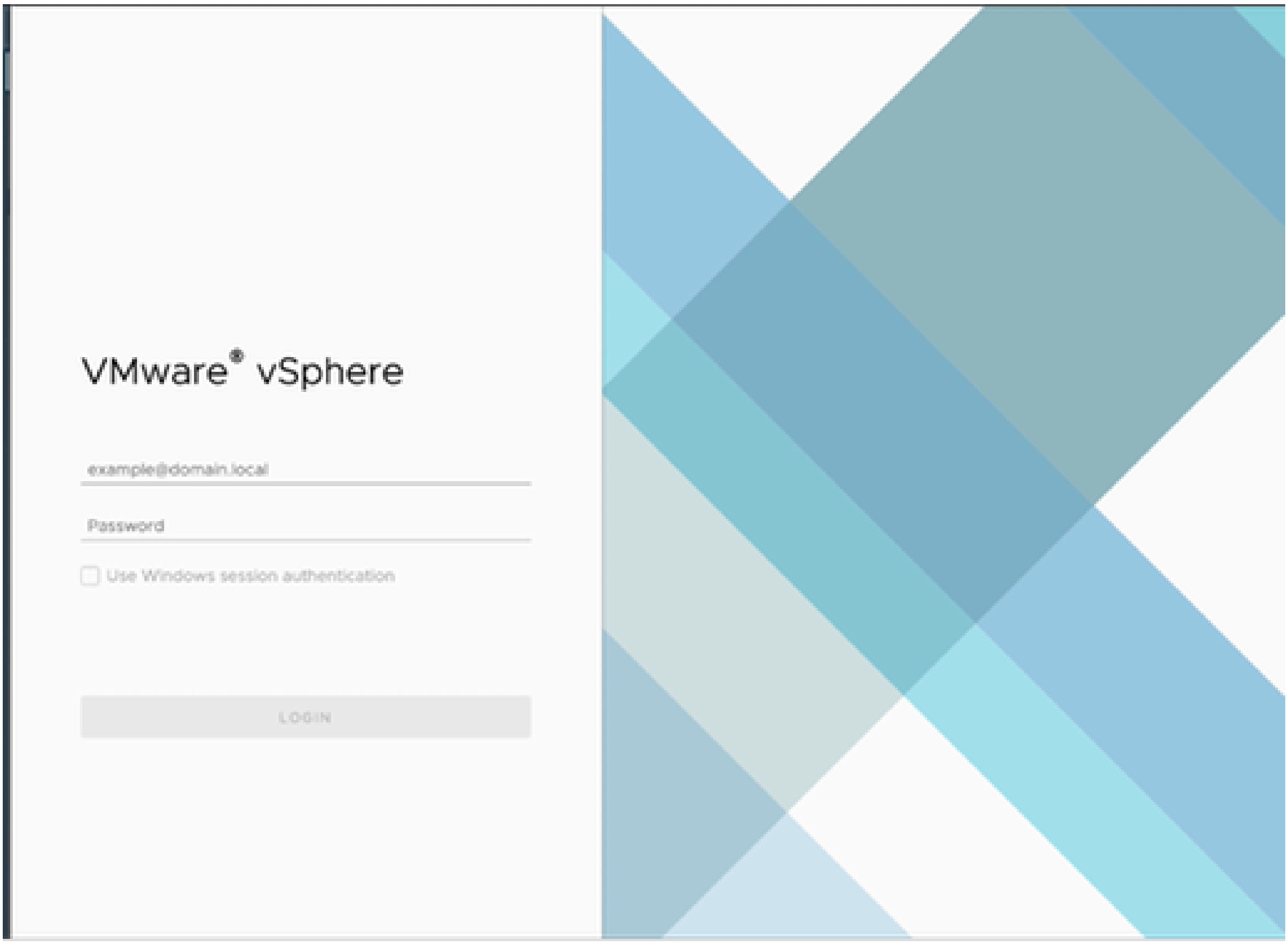


CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243

Recent Tasks

Reconfiguring Using Web Client vCenter

To update the VM configurations using the Web Client vCenter:



VMware® vSphere

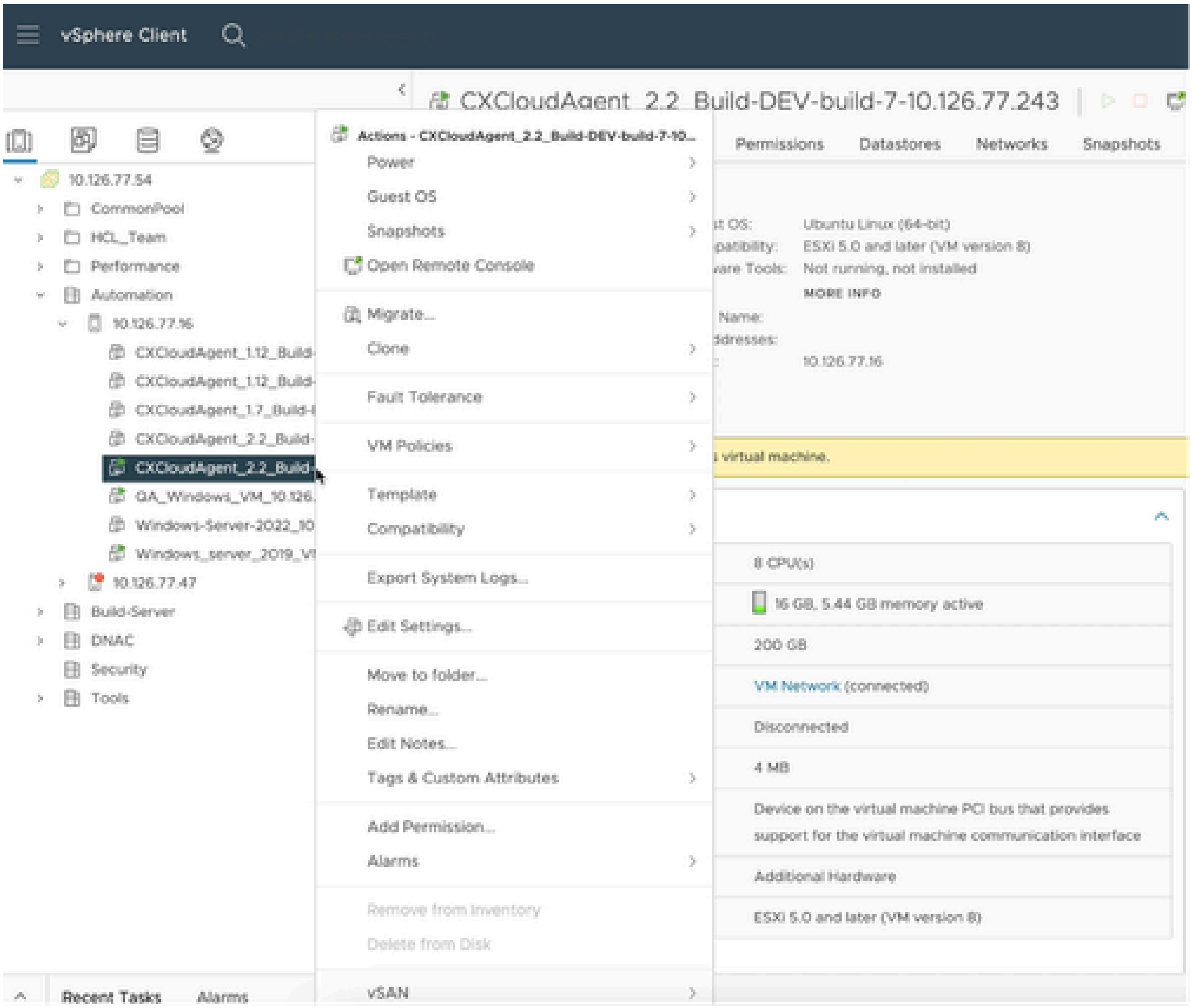
example@domain.local

Password

□ Use Windows session authentication

vCenter

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



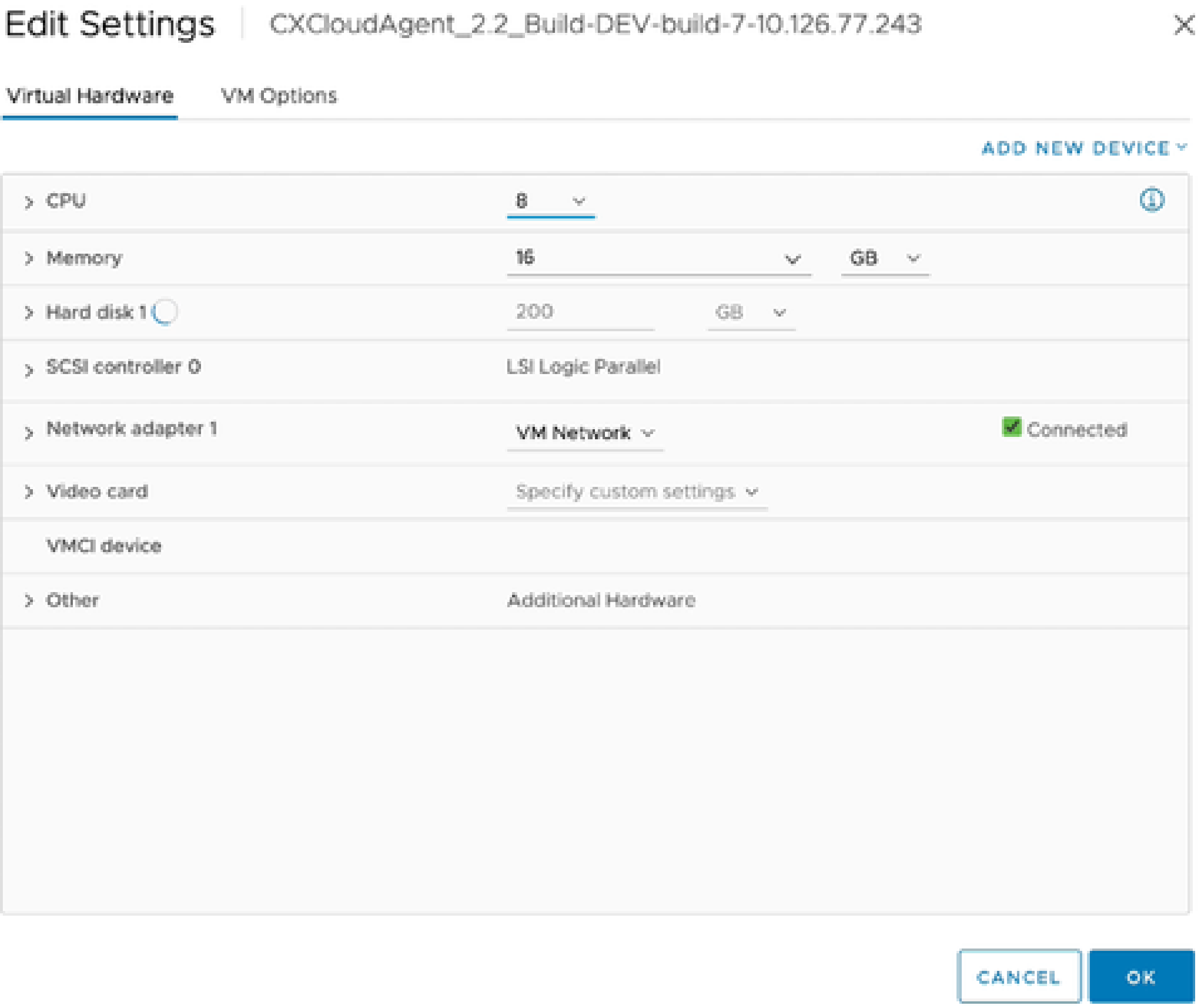
t OS: Ubuntu Linux (64-bit)
patibility: ESXi 5.0 and later (VM version 8)
are Tools: Not running, not installed
Name:
ddresses:
: 10.126.77.16

virtual machine.

8 CPU(s)
16 GB, 5.44 GB memory active
200 GB
VM Network (connected)
Disconnected
4 MB
Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Additional Hardware
ESXi 5.0 and later (VM version 8)

List of VMs

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

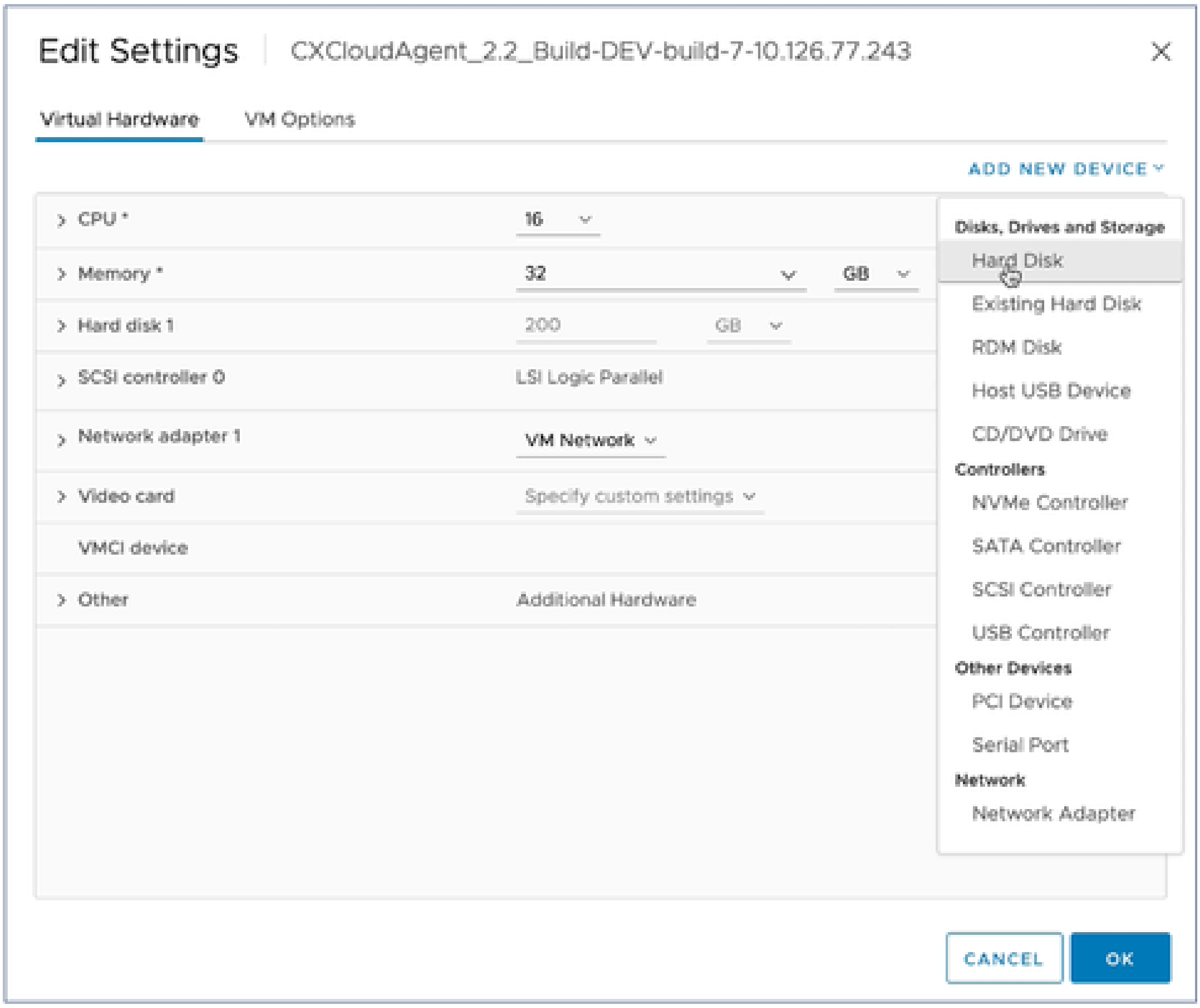


Edit Settings | CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243

CPU	8	
Memory	16 GB	
Hard disk 1	200 GB	
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	VM Network	☑ Connected
Video card	Specify custom settings	
VMCI device		
Other	Additional Hardware	

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

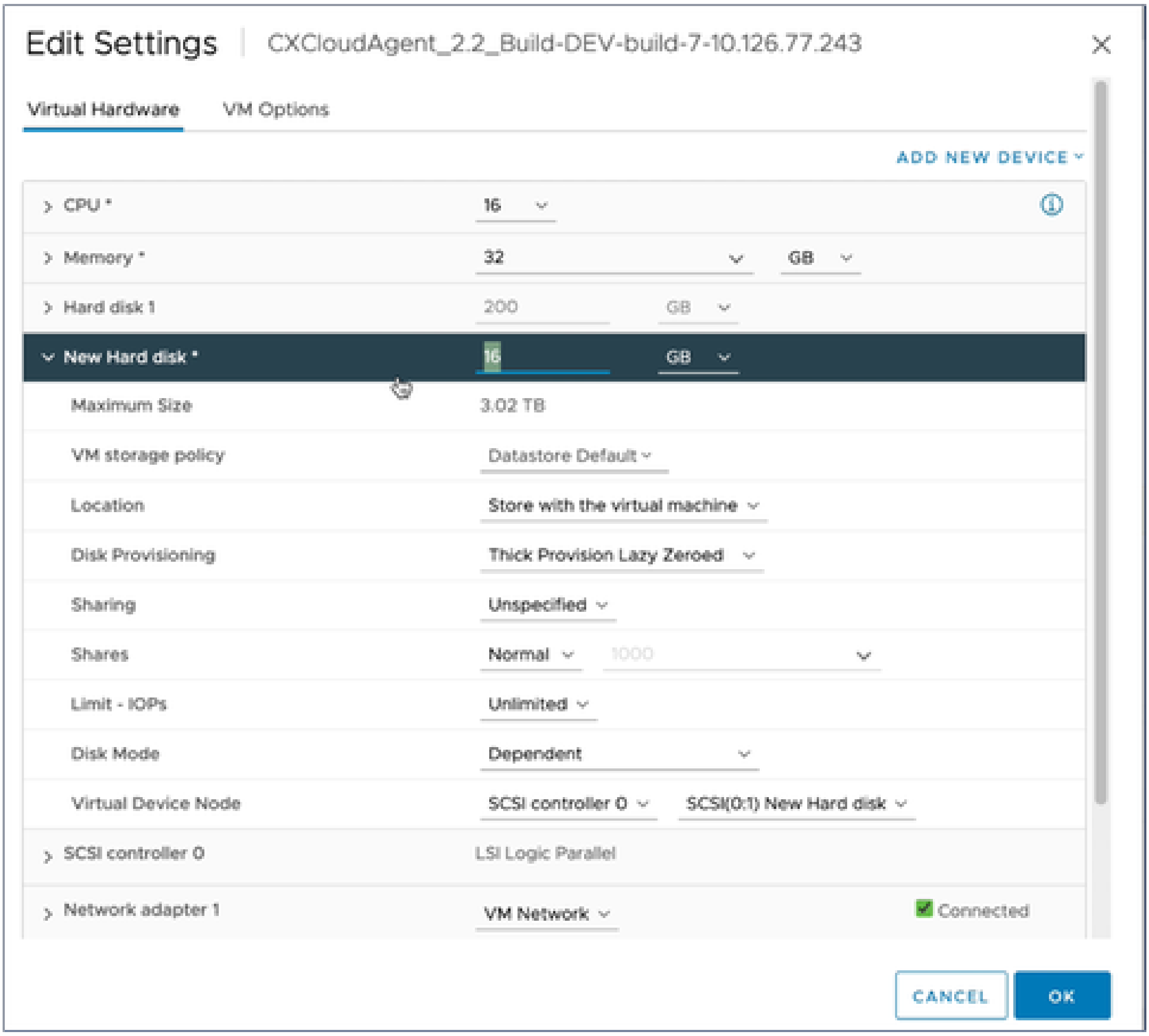


Edit Settings | CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243

CPU *	16
Memory *	32 GB
Hard disk 1	200 GB
SCSI controller 0	LSI Logic Parallel
Network adapter 1	VM Network
Video card	Specify custom settings
VMCI device	
Other	Additional Hardware

Edit Settings

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



Edit Settings | CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243

CPU * 16

Memory * 32 GB

Hard disk 1 200 GB

New Hard disk * 16 GB

Maximum Size 3.02 TB

VM storage policy Datastore Default

Location Store with the virtual machine

Disk Provisioning Thick Provision Lazy Zeroed

Sharing Unspecified

Shares Normal 1000

Limit - IOPs Unlimited

Disk Mode Dependent

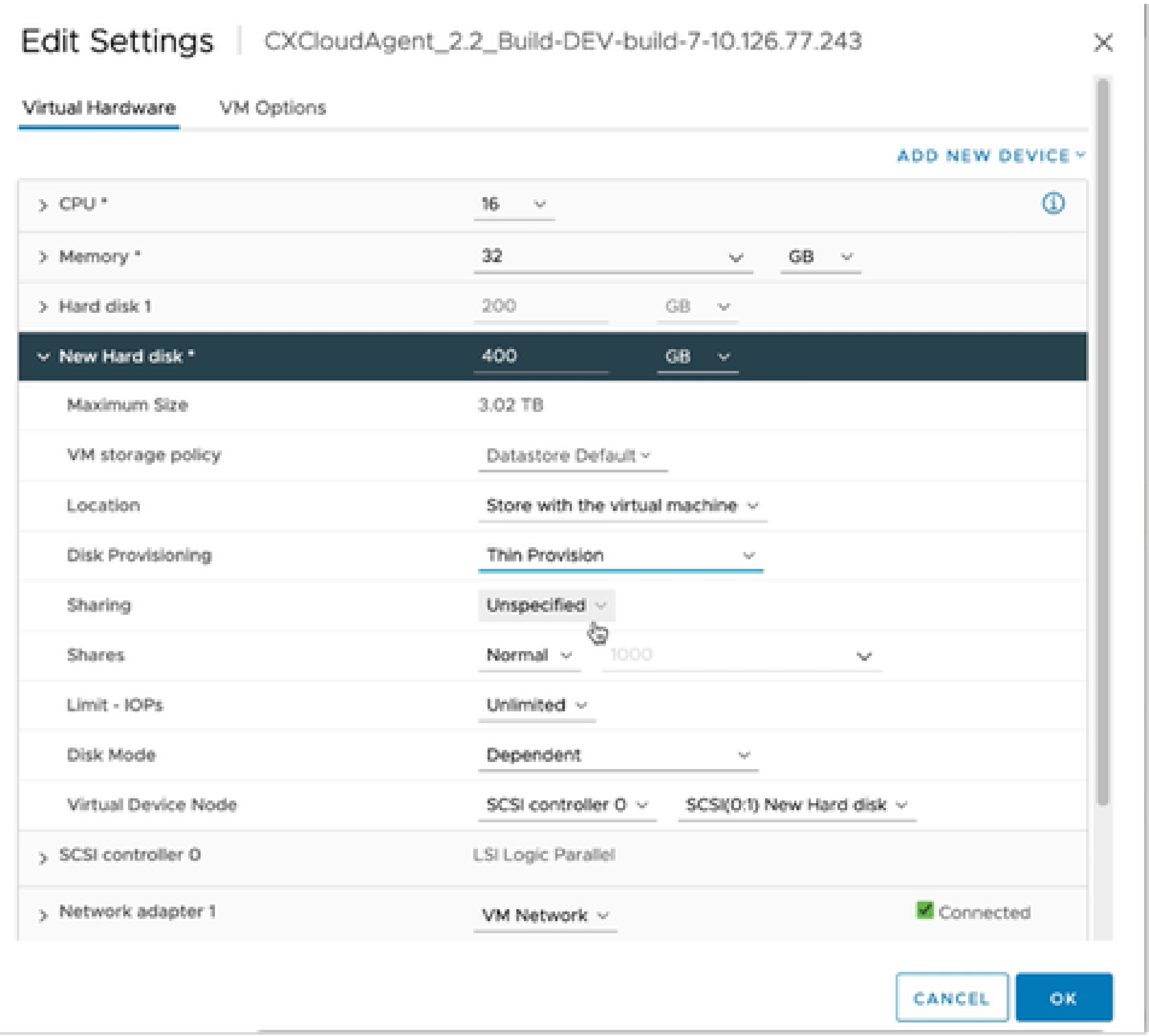
Virtual Device Node SCSI controller 0 SCSI(0:1) New Hard disk

SCSI controller 0 LSI Logic Parallel

Network adapter 1 VM Network ☑ Connected

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 | CXCloudAgent_2.2_Build-DEV-build-7-10.126.77.243

CPU *	16	
Memory *	32	GB
Hard disk 1	200	GB
New Hard disk *	400	GB
Maximum Size	3.02 TB	
VM storage policy	Datastore Default	
Location	Store with the virtual machine	
Disk Provisioning	Thin Provision	
Sharing	Unspecified	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Disk Mode	Dependent	
Virtual Device Node	SCSI controller 0	SCSI(0:1) New Hard disk
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	VM Network	☑ Connected

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 Agent:

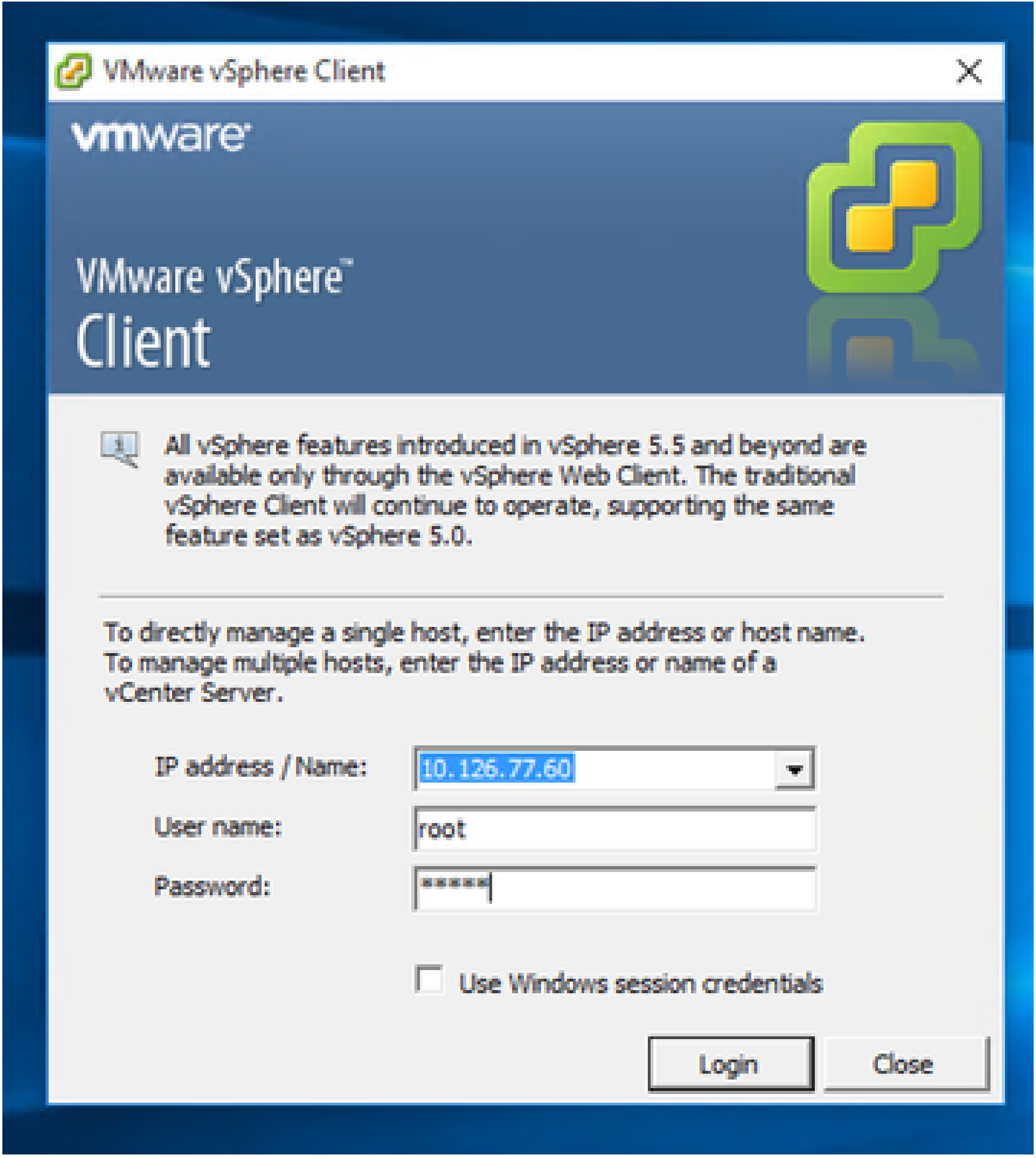
- VMware vSphere/vCenter Thick Client ESXi 5.5/6.0
- VMware vSphere/vCenter Web Client ESXi 6.0 or Web Client vCenter Installation
- Oracle Virtual Box 7.0.12
- Microsoft Hyper-V Installation

OVA Deployment

Thick Client ESXi 5.5/6.0 Installation

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

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



VMware vSphere Client

All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 10.126.77.60

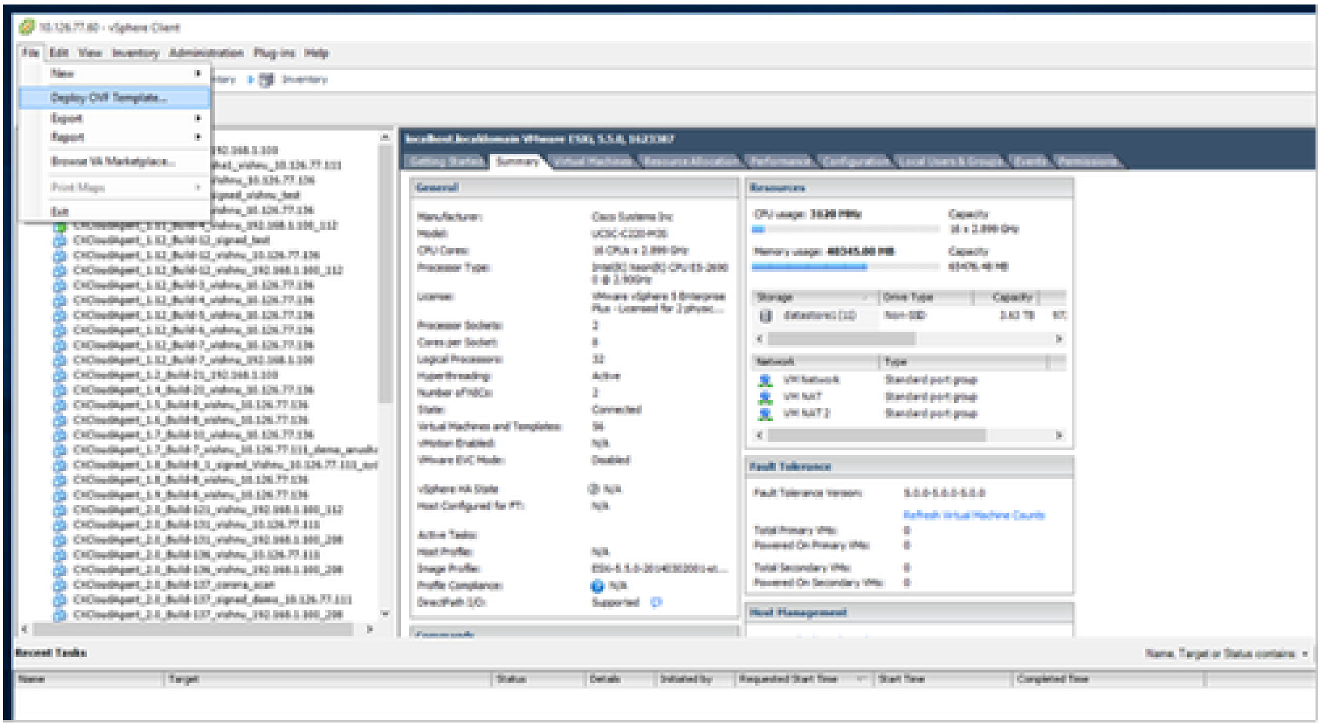
User name: root

Password: *****

□ Use Windows session credentials

Login

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



Manufacturer: Cisco Systems Inc
Model: UCSC-C220-M3S
CPU Cores: 16 CPUs x 2.899 GHz
Processor Type: Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz
License: VMware vSphere 5 Enterprise Plus - Licensed for 2 physic...
Processor Sockets: 2
Cores per Socket: 8
Logical Processors: 32
Hyperthreading: Active
Number of NICs: 2
State: Connected
Virtual Machines and Templates: 56
vMotion Enabled: N/A
VMware EVC Mode: Disabled
vSphere HA State: N/A
Host Configured for FT: N/A
Active Tasks:
Host Profile: N/A
Image Profile: ESXi-5.5.0-20140302001-st...
Profile Compliance: N/A
DirectPath I/O: Supported

CPU usage: 3638 MHz — Capacity 16 x 2.899 GHz
Memory usage: 48545.00 MB — Capacity 65476.48 MB

Storage	Drive Type	Capacity
datastore1 (12)	Non-SSD	3.63 TB

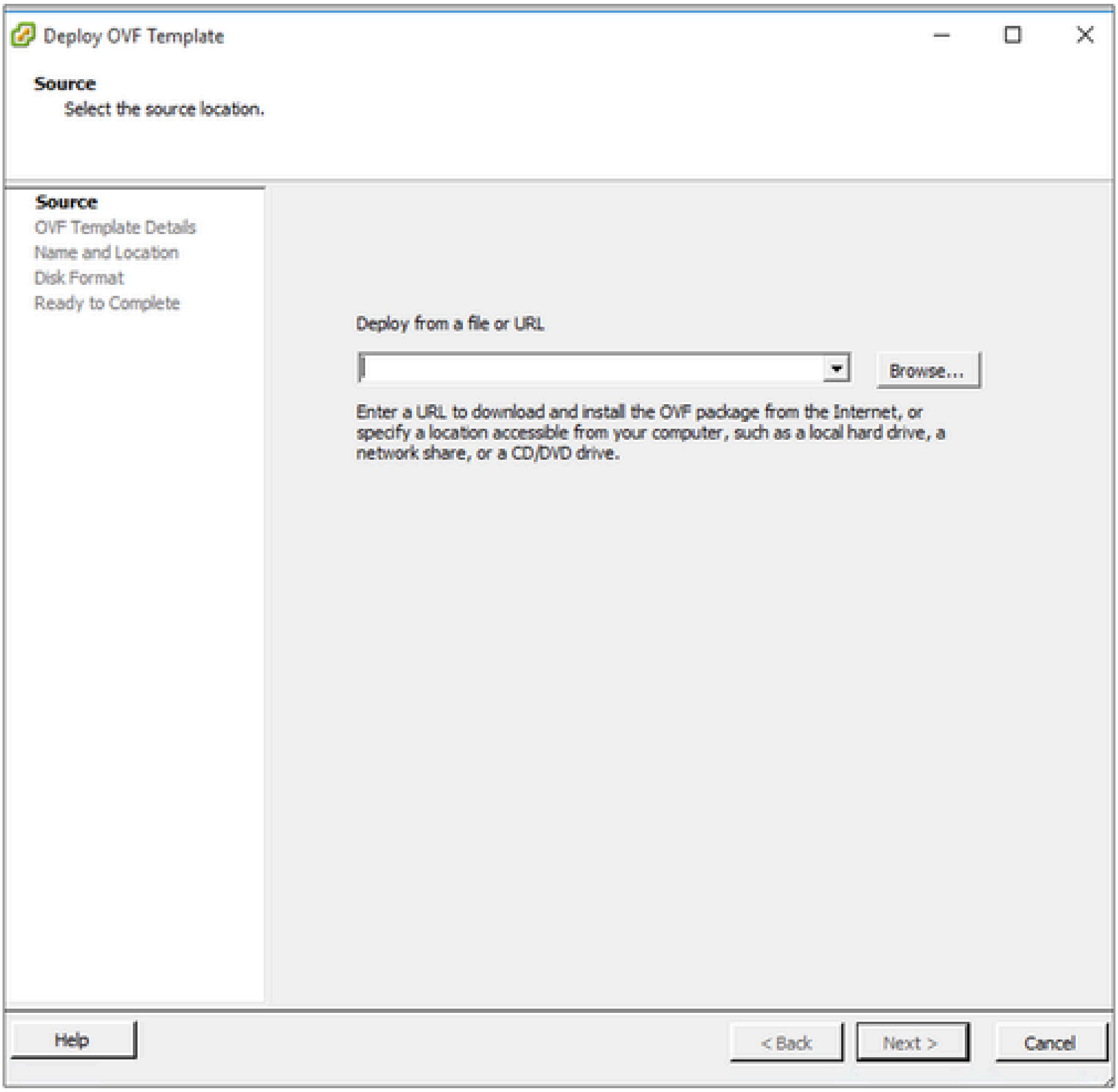
Network	Type
VM Network	Standard port group
VM NAT	Standard port group
VM NAT 2	Standard port group

Fault Tolerance Version: 5.0.0-5.0.0-5.0.0
Refresh Virtual Machine Counts
Total Primary VMs: 0
Powered On Primary VMs: 0
Total Secondary VMs: 0
Powered On Secondary VMs: 0

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completed Time

vSphere Client

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



Deploy OVF Template

Source

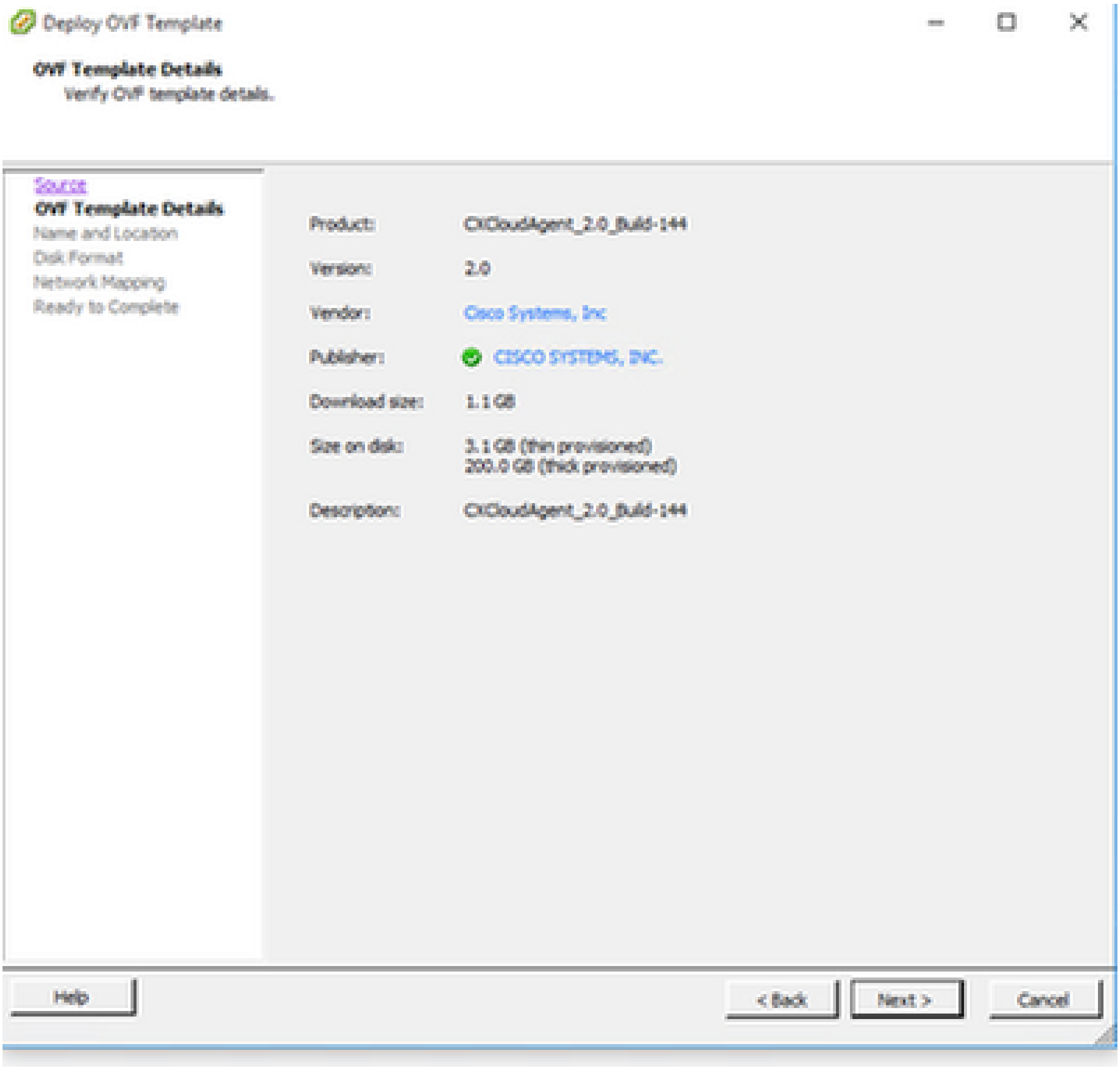
Select the source location.

Deploy from a file or URL

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

OVA Path

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



Product: CXCloudAgent_2.0_Build-144

Version: 2.0

Vendor: Cisco Systems, Inc

Publisher: CISCO SYSTEMS, INC.

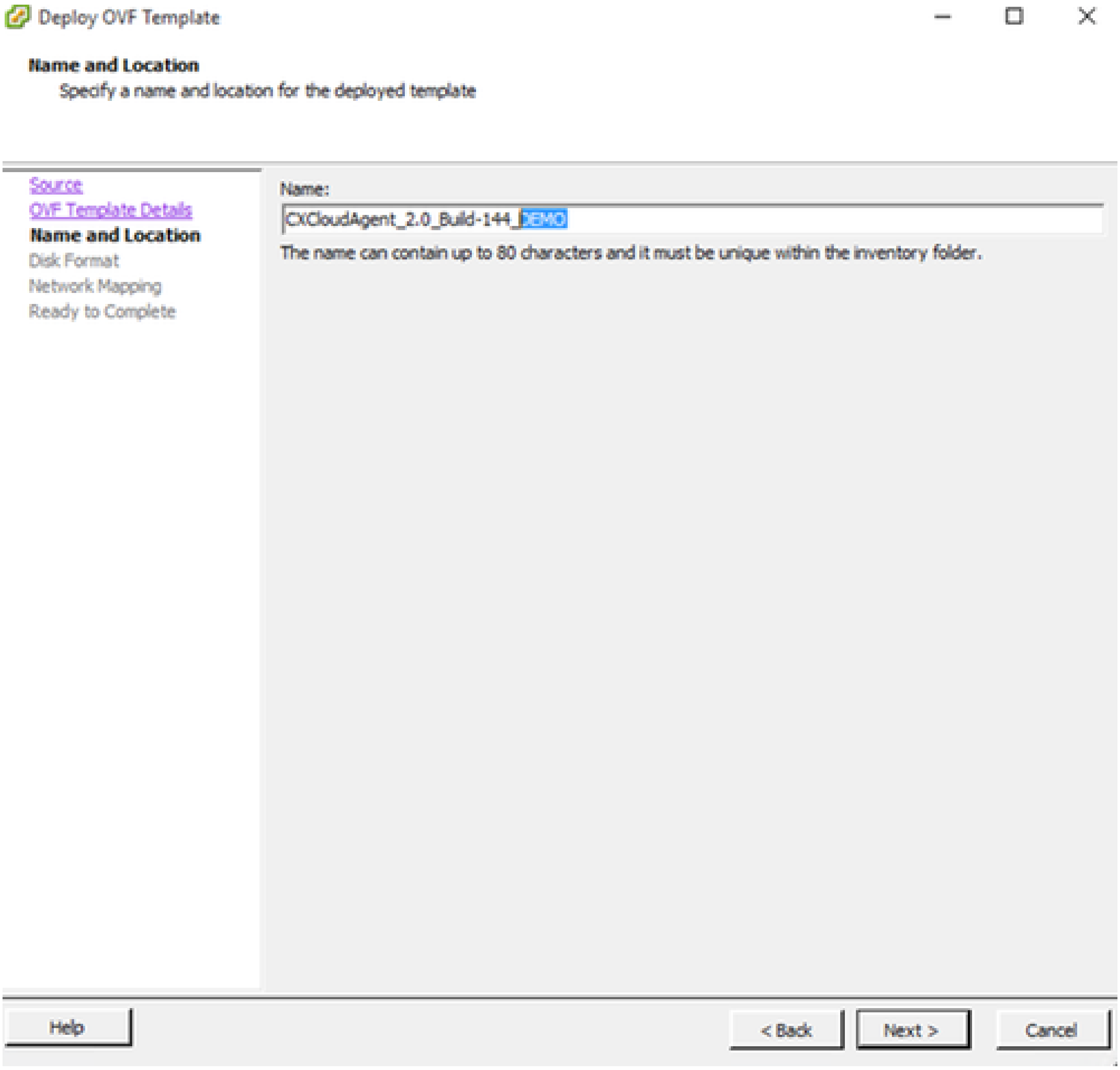
Download size: 1.1 GB

Size on disk: 3.1 GB (thin provisioned)
200.0 GB (thick provisioned)

Description: CXCloudAgent_2.0_Build-144

Template Details

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



Name and Location

Specify a name and location for the deployed template

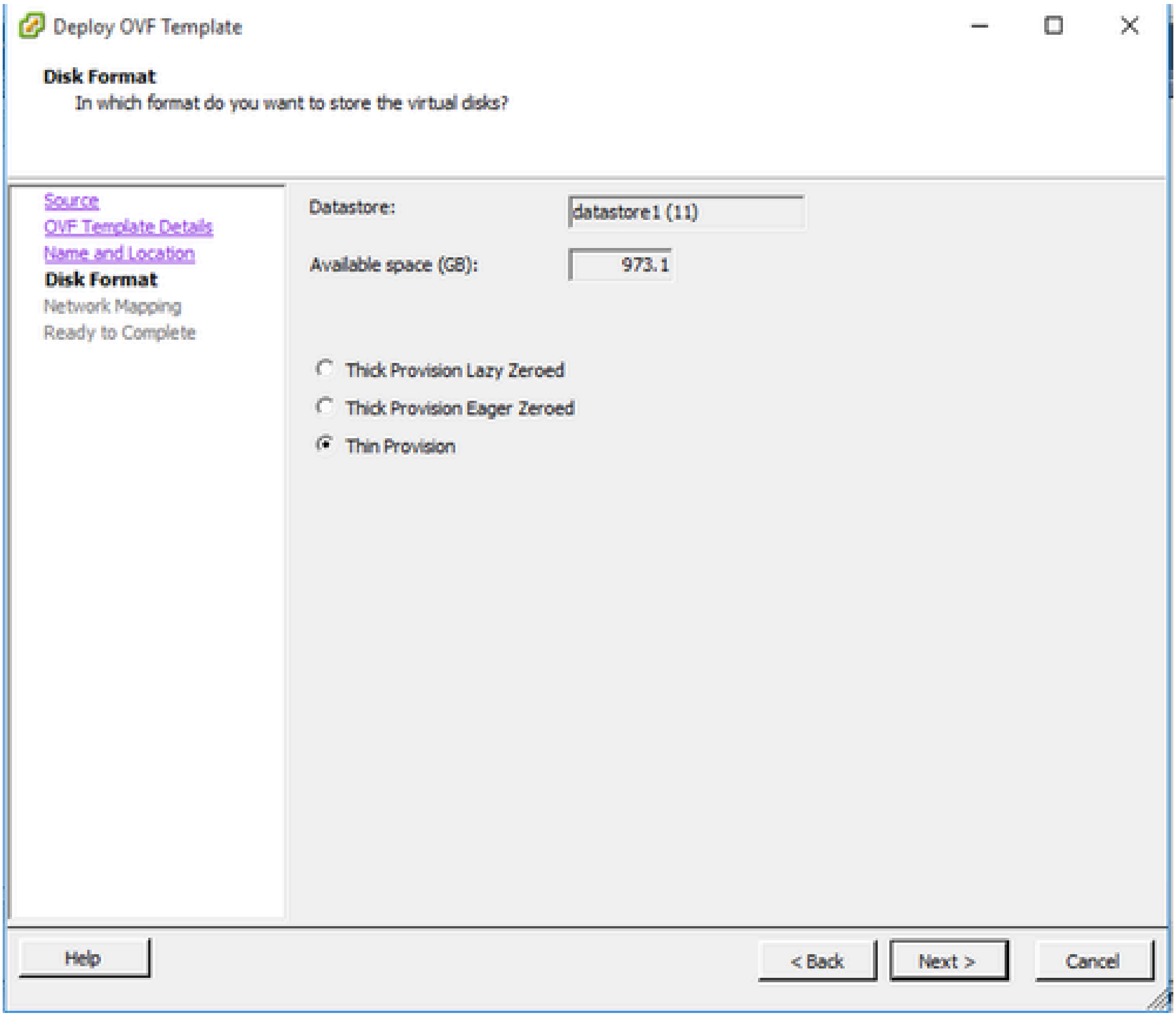
Name:

CXCloudAgent_2.0_Build-144_DEMO

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

Name and Location

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



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1 (11)

Available space (GB): 973.1

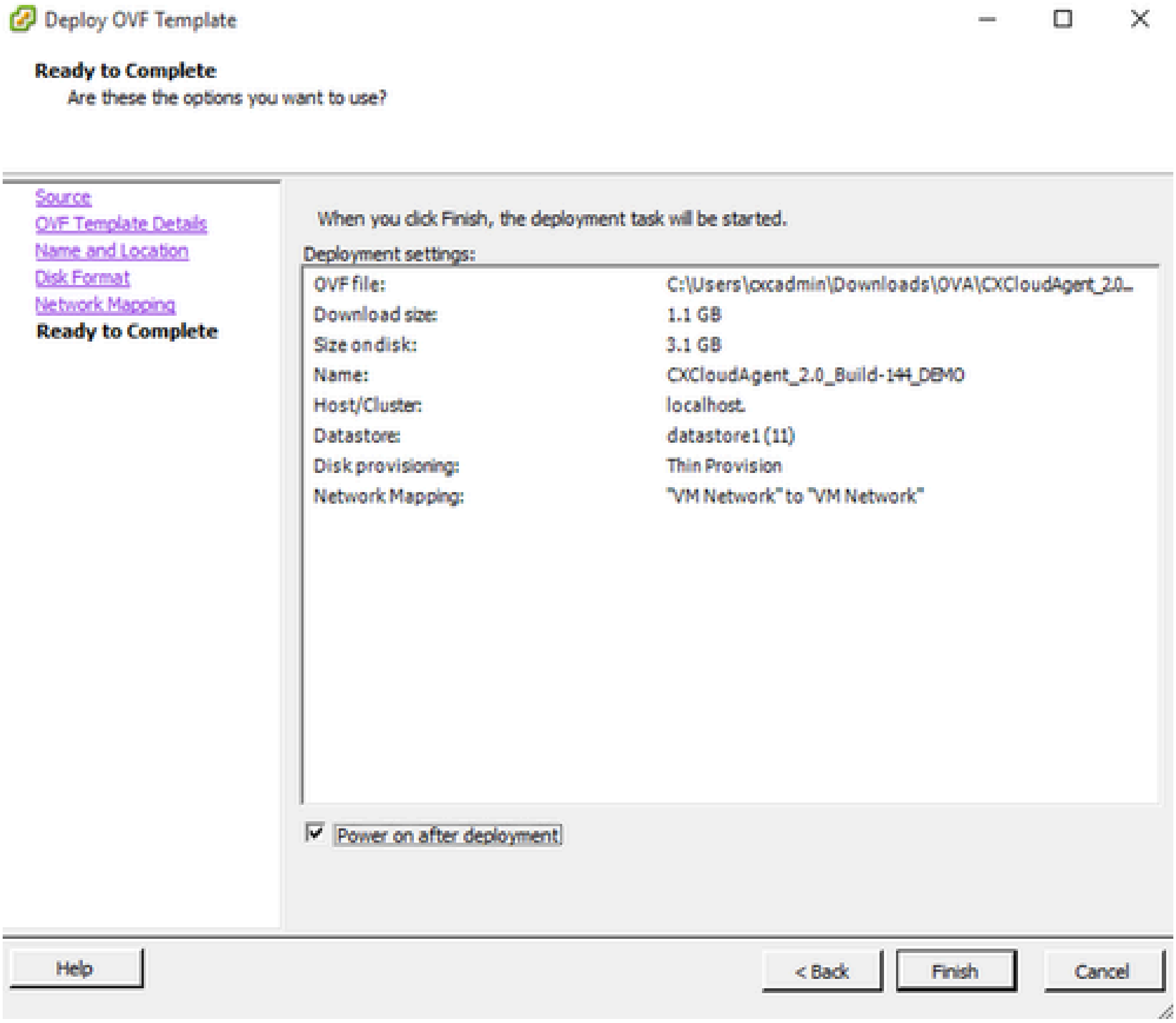
○ Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

● Thin Provision

Disk Format

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



Deploy OVF Template

Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

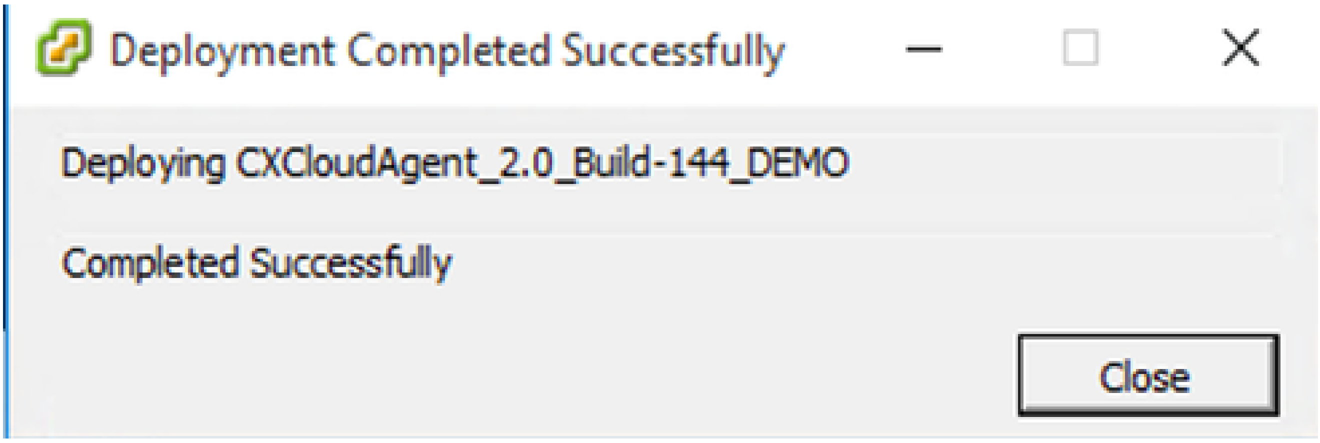
Deployment settings:

OVF file:	C:\Users\cxadmin\Downloads\OVA\CXCloudAgent_2.0...
Download size:	1.1 GB
Size on disk:	3.1 GB
Name:	CXCloudAgent_2.0_Build-144_DEMO
Host/Cluster:	localhost.
Datastore:	datastore1 (11)
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"

☑ Power on after deployment

Ready to Complete

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



Deployment Completed Successfully

Deploying CXCloudAgent_2.0_Build-144_DEMO

Completed Successfully

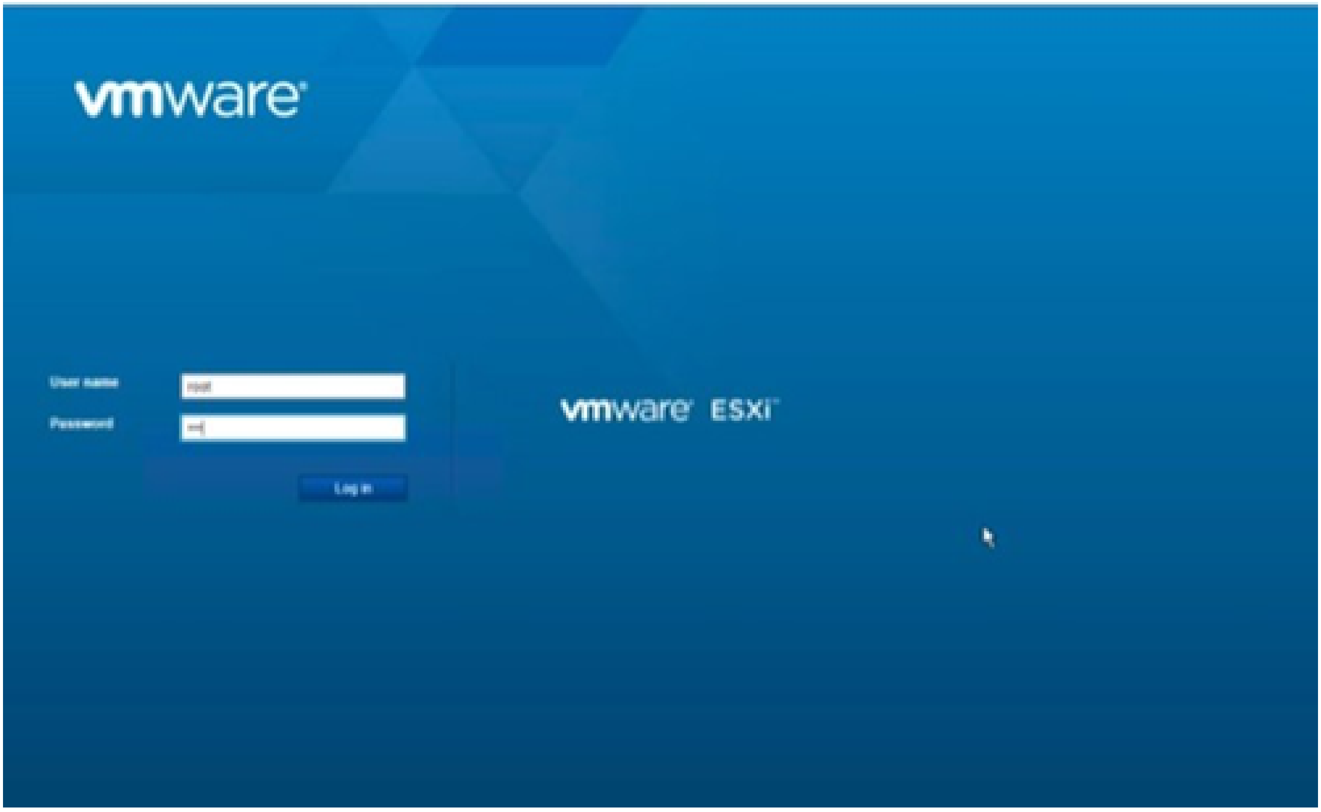
Deployment Complete

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 OVA by use of the vSphere web.

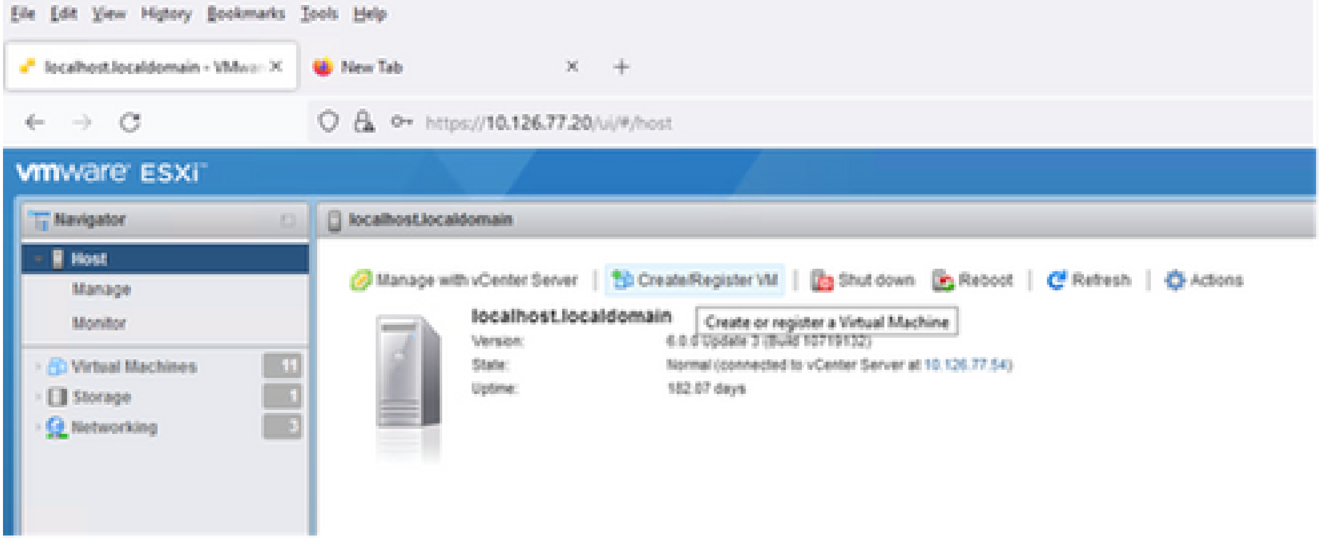
1. Log in to the VMWare UI with the ESXi/hypervisor credentials used for deploying VM.



User name: root

VMWare ESXi Login

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


File Edit View History Bookmarks Tools Help
localhost.localdomain - VMwa
New Tab
https://10.126.77.20/ui/#/host
vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
11
Storage
1
Networking
3
localhost.localdomain
Manage with vCenter Server
Create/Register VM
Shut down
Reboot
Refresh
Actions
Create or register a Virtual Machine

localhost.localdomain

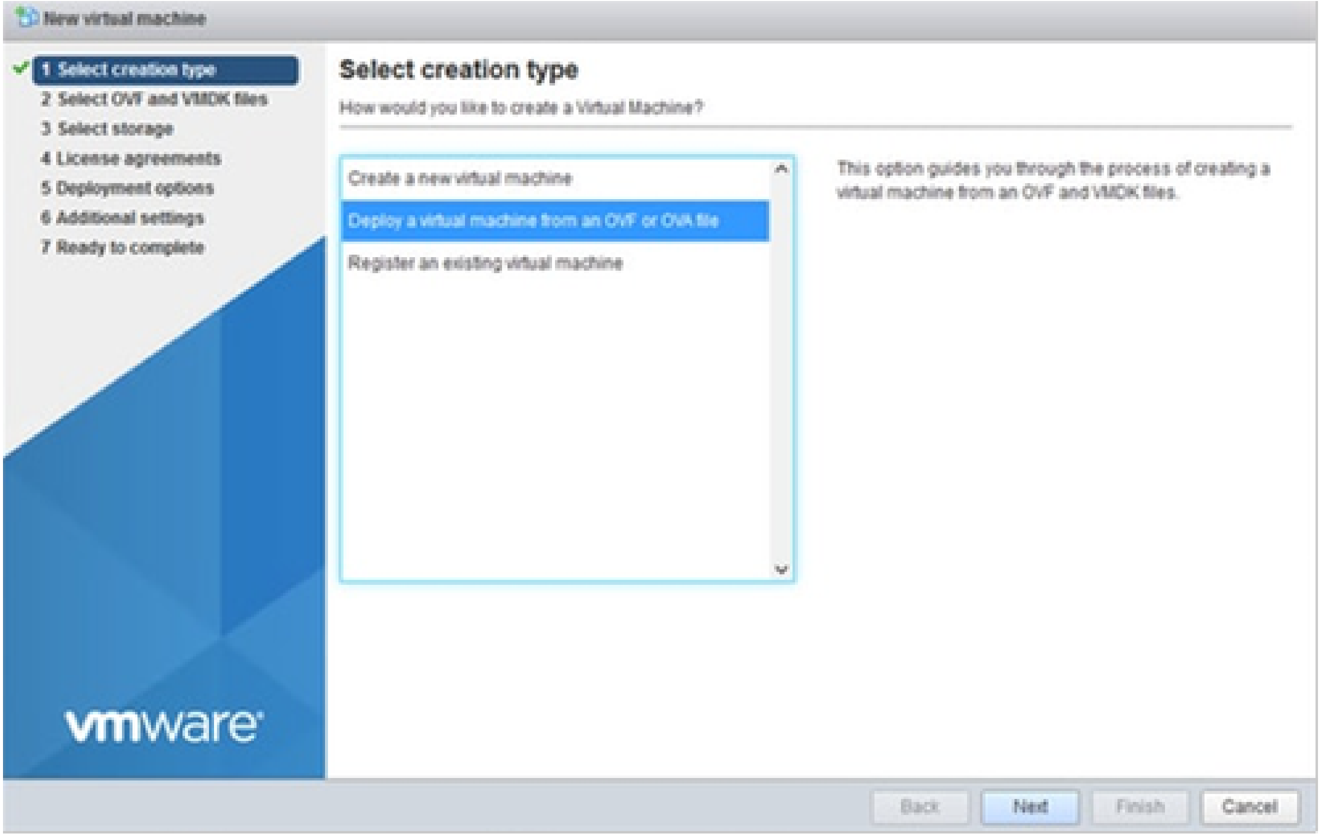
Version: 6.0.0 Update 3 (Build 10719132)

State: Normal (connected to vCenter Server at 10.126.77.54)

Uptime: 182.07 days

Create VM

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



Select creation type

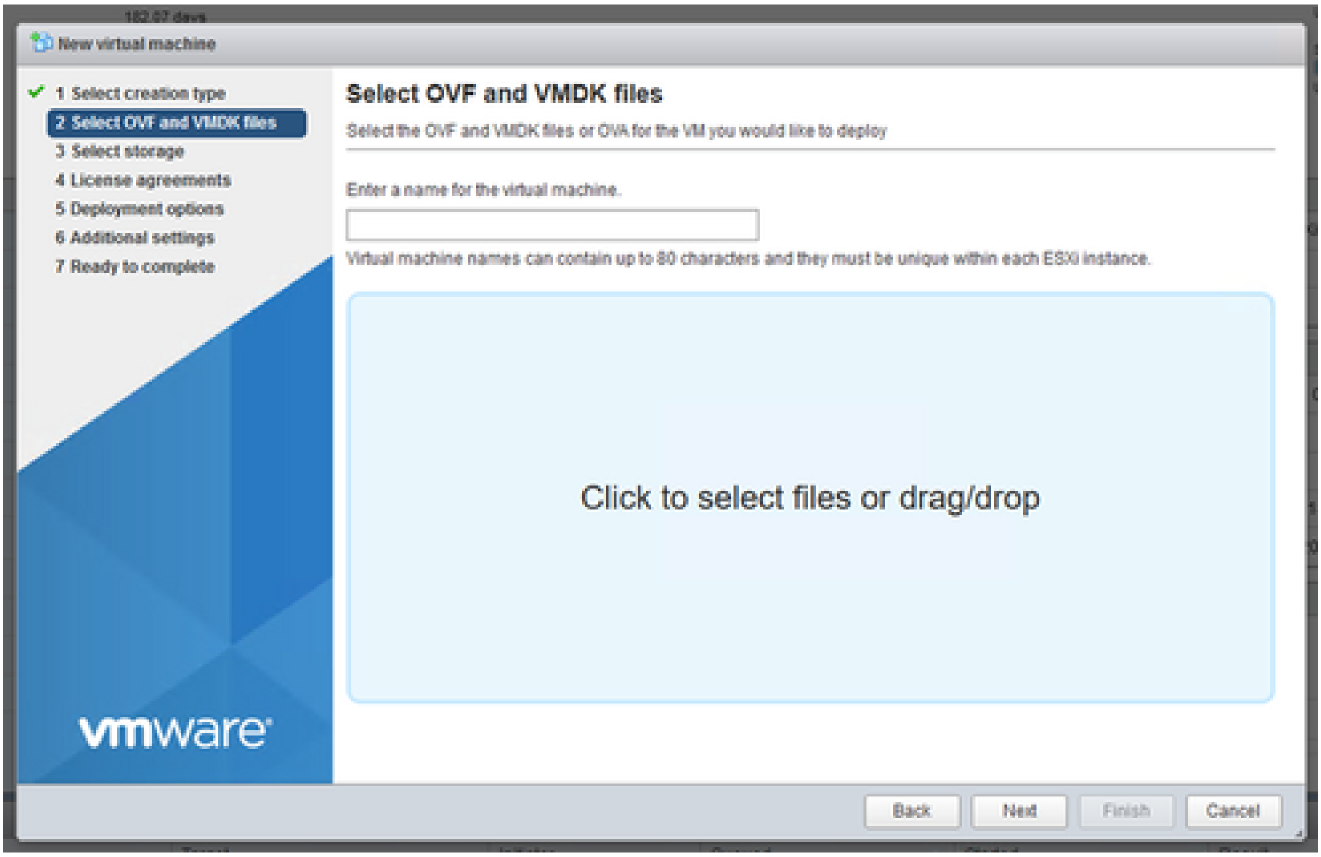
How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

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**.



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

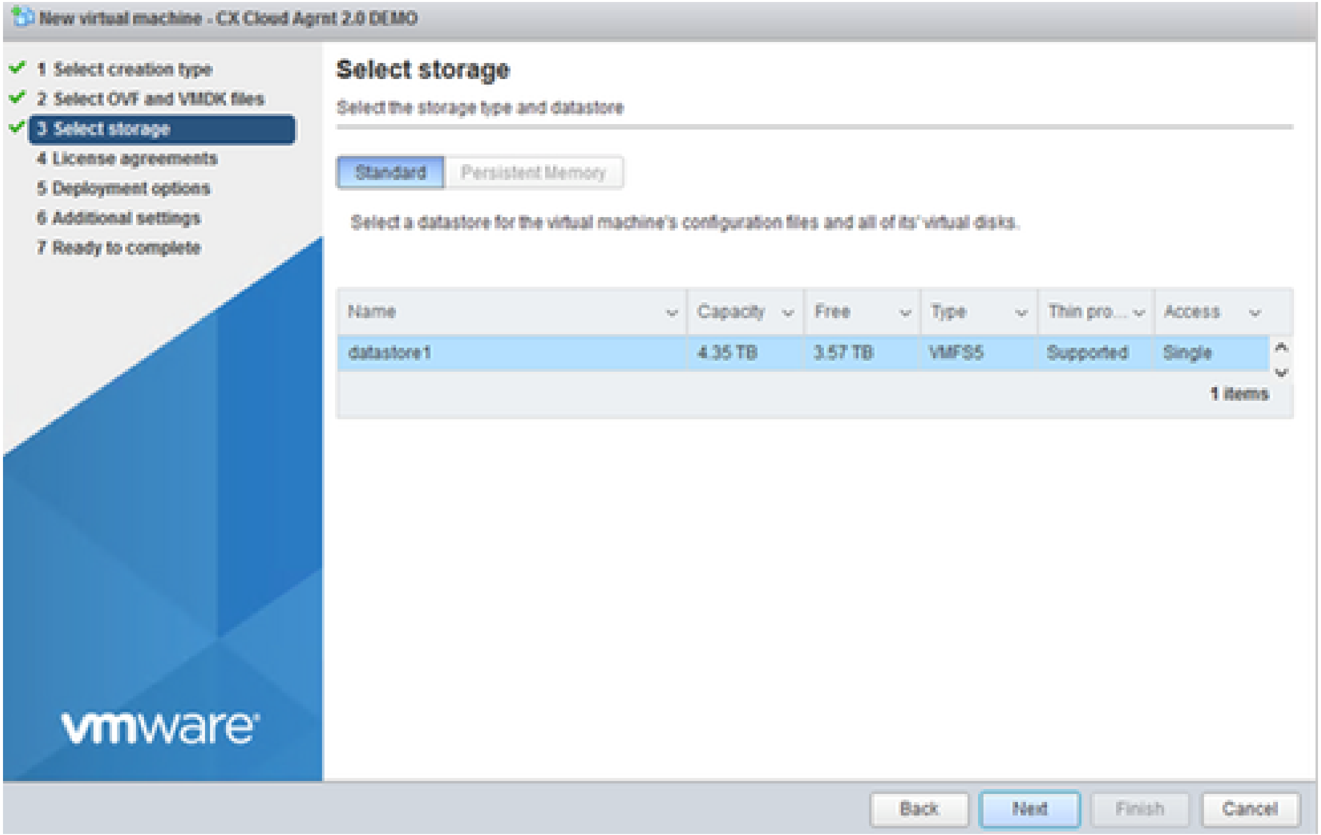
Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Click to select files or drag/drop

OVA Selection

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



Select storage

Select the storage type and datastore

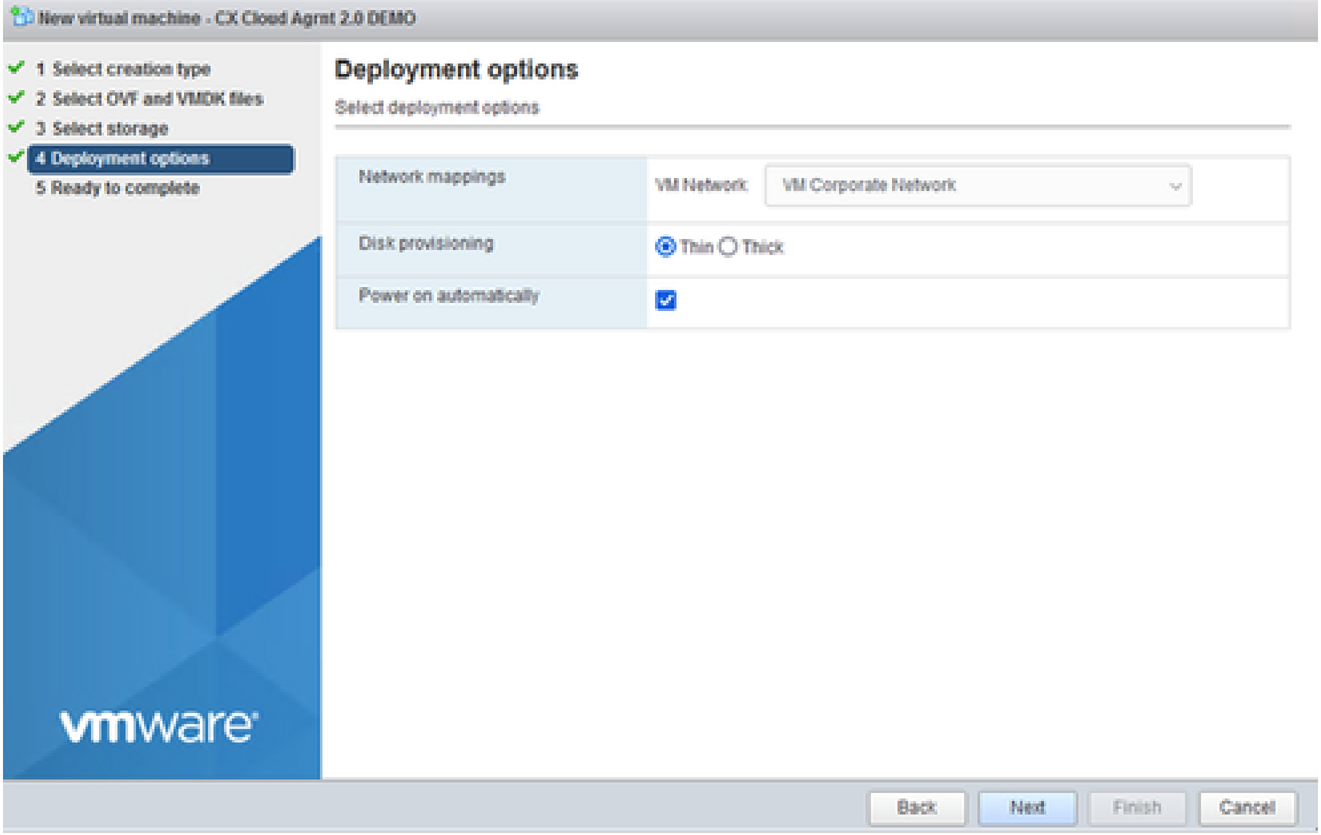
Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	4.35 TB	3.57 TB	VMFS5	Supported	Single

1 items

Select Storage

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



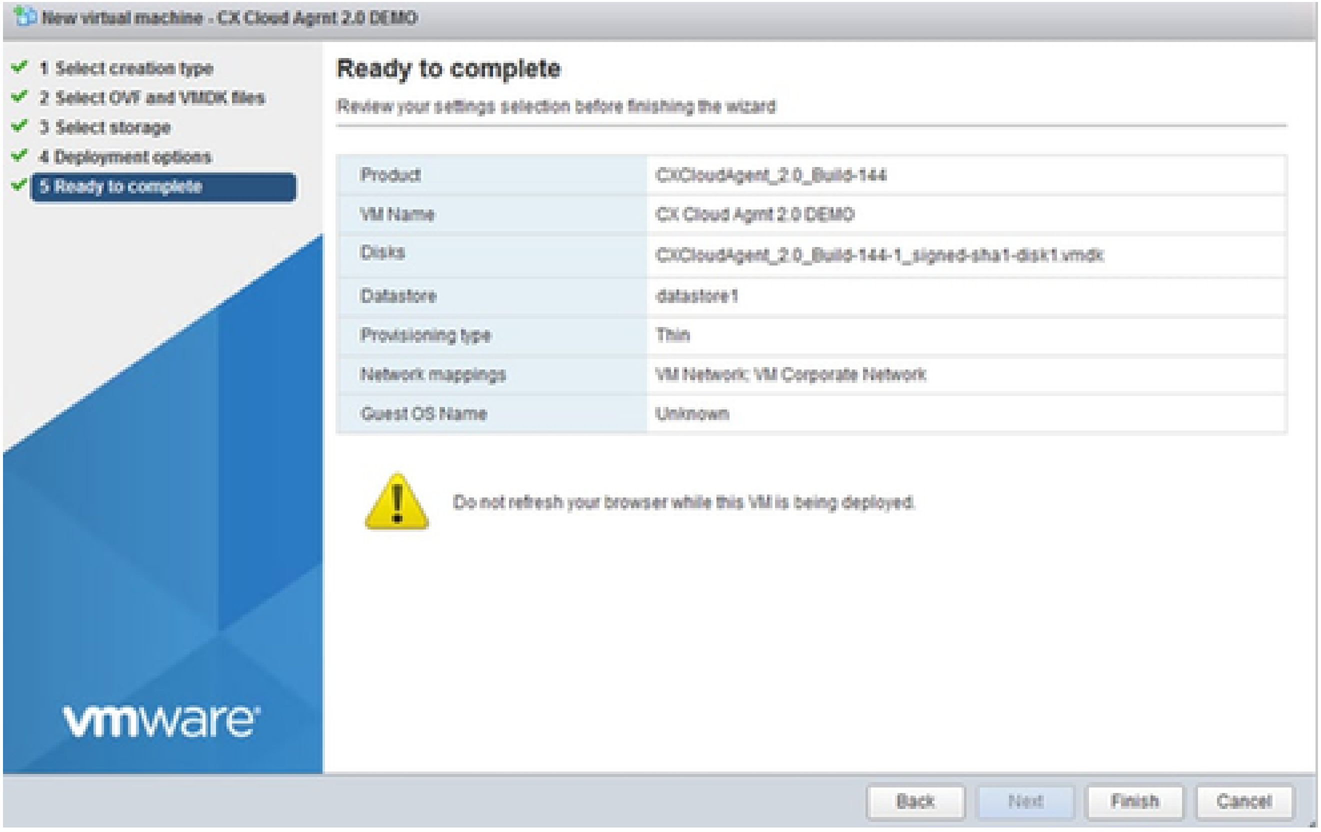
Deployment options

Select deployment options

Network mappings	VM Network: VM Corporate Network
Disk provisioning	● Thin ○ Thick
Power on automatically	☑

Deployment Options

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



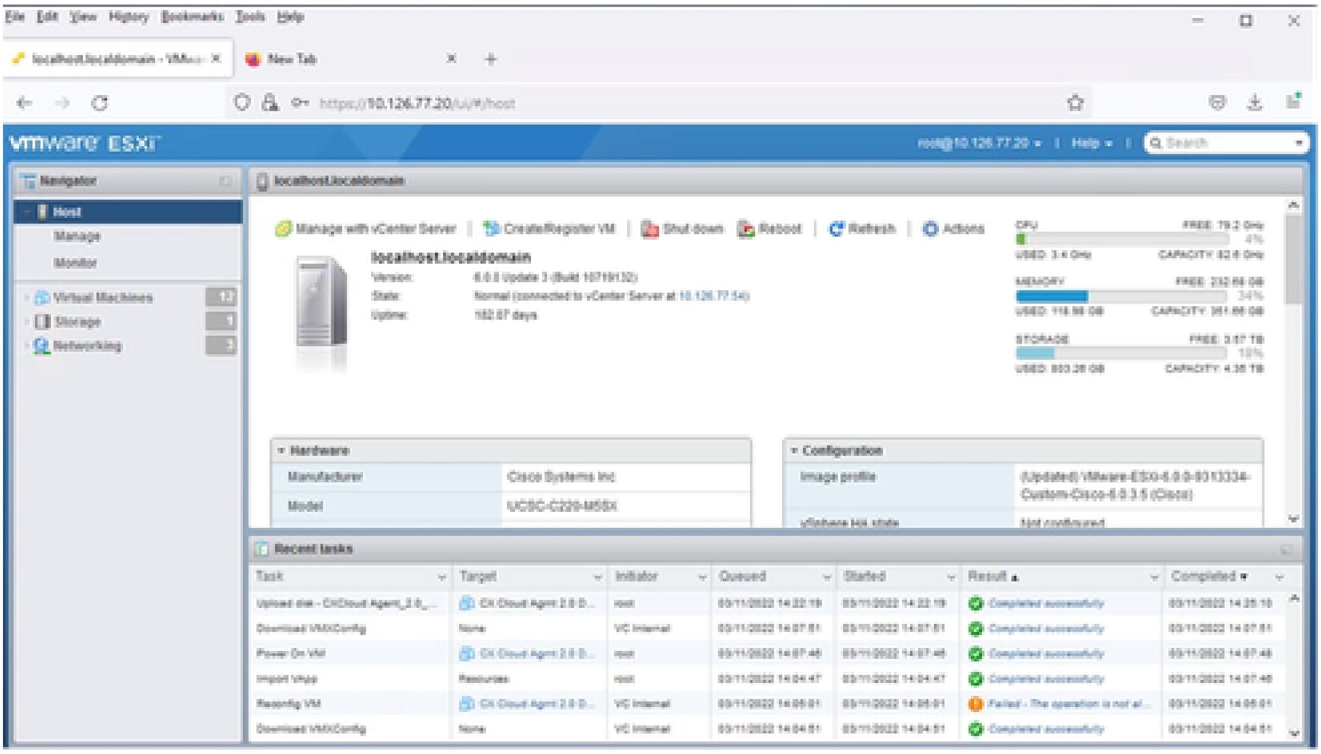
Ready to complete

Review your settings selection before finishing the wizard

Product	CXCloudAgent_2.0_Build-144
VM Name	CX Cloud Agmt 2.0 DEMO
Disks	CXCloudAgent_2.0_Build-144-1_signed-sha1-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: VM Corporate Network
Guest OS Name	Unknown

Do not refresh your browser while this VM is being deployed.

Ready to Complete



localhost.localdomain

Version: 6.0.0 Update 3 (Build 10719132)

State: Normal (connected to vCenter Server at 10.126.77.54)

Uptime: 152.07 days

CPU FREE: 79.2 GHz 4% USED: 3.4 GHz CAPACITY: 82.6 GHz

MEMORY FREE: 232.69 GB 34% USED: 118.96 GB CAPACITY: 351.66 GB

STORAGE FREE: 3.57 TB 18% USED: 803.28 GB CAPACITY: 4.38 TB

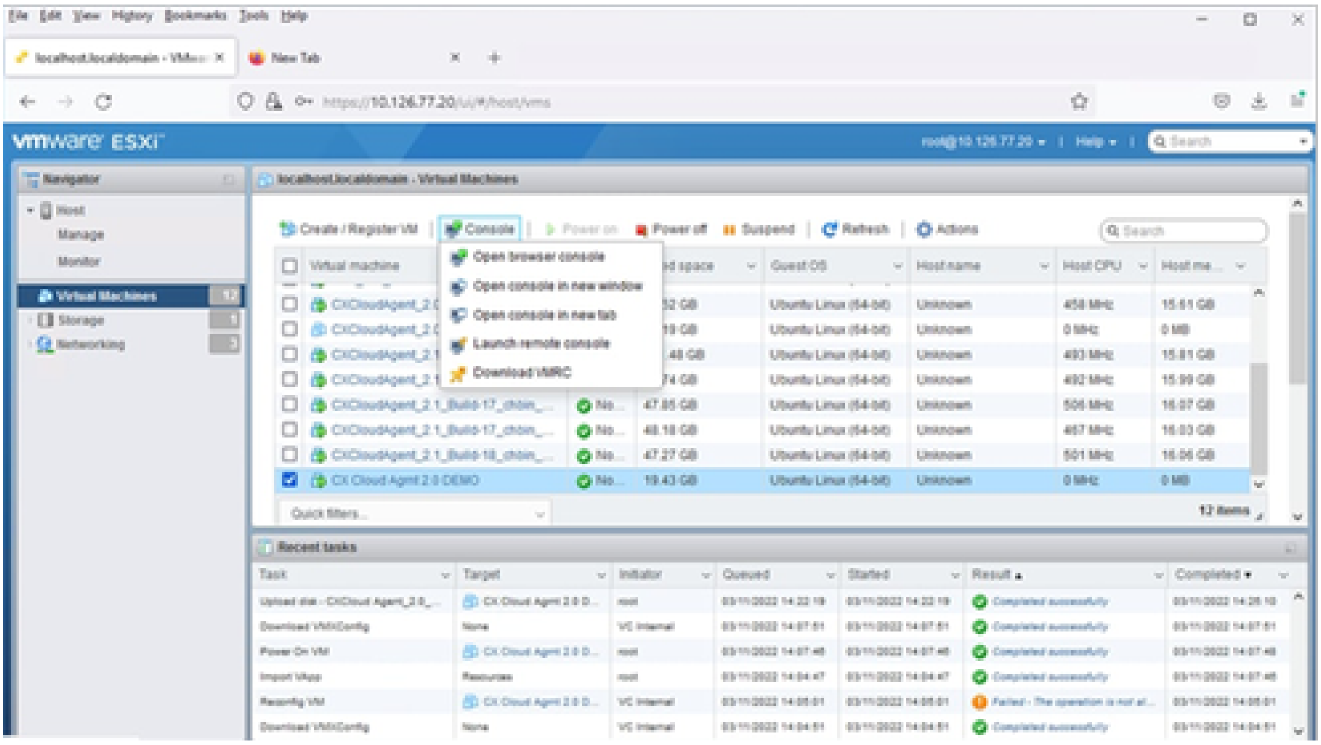
Hardware	
Manufacturer	Cisco Systems Inc
Model	UCSC-C220-M5SX

Configuration	
Image profile	(Updated) VMware-ESXi-6.0.0-9313334-Custom-Cisco-6.0.3.5 (Cisco)
vSphere HA state	Not configured

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Upload disk - CXCloud Agent_2.0_...	CX Cloud Agmt 2.0 D...	root	03/11/2022 14:22:19	03/11/2022 14:22:19	Completed successfully	03/11/2022 14:25:10
Download VMXConfig	None	VC Internal	03/11/2022 14:07:51	03/11/2022 14:07:51	Completed successfully	03/11/2022 14:07:51
Power On VM	CX Cloud Agmt 2.0 D...	root	03/11/2022 14:07:48	03/11/2022 14:07:48	Completed successfully	03/11/2022 14:07:48
Import VApp	Resources	root	03/11/2022 14:04:47	03/11/2022 14:04:47	Completed successfully	03/11/2022 14:07:48
Reconfig VM	CX Cloud Agmt 2.0 D...	VC Internal	03/11/2022 14:05:01	03/11/2022 14:05:01	Failed - The operation is not al...	03/11/2022 14:05:01
Download VMXConfig	None	VC Internal	03/11/2022 14:04:51	03/11/2022 14:04:51	Completed successfully	03/11/2022 14:04:51

Successful Completion

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



☐	Virtual machine		Used space	Guest OS	Host name	Host CPU	Host me...
☐	CXCloudAgent_2.0		52 GB	Ubuntu Linux (64-bit)	Unknown	458 MHz	15.61 GB
☐	CXCloudAgent_2.0		19 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB
☐	CXCloudAgent_2.1		48 GB	Ubuntu Linux (64-bit)	Unknown	493 MHz	15.81 GB
☐	CXCloudAgent_2.1		74 GB	Ubuntu Linux (64-bit)	Unknown	492 MHz	15.99 GB
☐	CXCloudAgent_2.1_Build-17_chbin_...	No...	47.85 GB	Ubuntu Linux (64-bit)	Unknown	506 MHz	16.07 GB
☐	CXCloudAgent_2.1_Build-17_chbin_...	No...	48.18 GB	Ubuntu Linux (64-bit)	Unknown	467 MHz	16.03 GB
☐	CXCloudAgent_2.1_Build-18_chbin_...	No...	47.27 GB	Ubuntu Linux (64-bit)	Unknown	501 MHz	16.06 GB
☑	CX Cloud Agnt 2.0 DEMO	No...	19.43 GB	Ubuntu Linux (64-bit)	Unknown	0 MHz	0 MB

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Upload disk - CXCloud Agent_2.0_...	CX Cloud Agnt 2.0 D...	root	03/11/2022 14:22:19	03/11/2022 14:22:19	Completed successfully	03/11/2022 14:26:10
Download VMXConfig	None	VC Internal	03/11/2022 14:07:51	03/11/2022 14:07:51	Completed successfully	03/11/2022 14:07:51
Power On VM	CX Cloud Agnt 2.0 D...	root	03/11/2022 14:07:48	03/11/2022 14:07:48	Completed successfully	03/11/2022 14:07:48
Import VApp	Resources	root	03/11/2022 14:04:47	03/11/2022 14:04:47	Completed successfully	03/11/2022 14:07:48
Reconfig VM	CX Cloud Agnt 2.0 D...	VC Internal	03/11/2022 14:05:01	03/11/2022 14:05:01	Failed - The operation is not al...	03/11/2022 14:05:01
Download VMXConfig	None	VC Internal	03/11/2022 14:04:51	03/11/2022 14:04:51	Completed successfully	03/11/2022 14:04:51

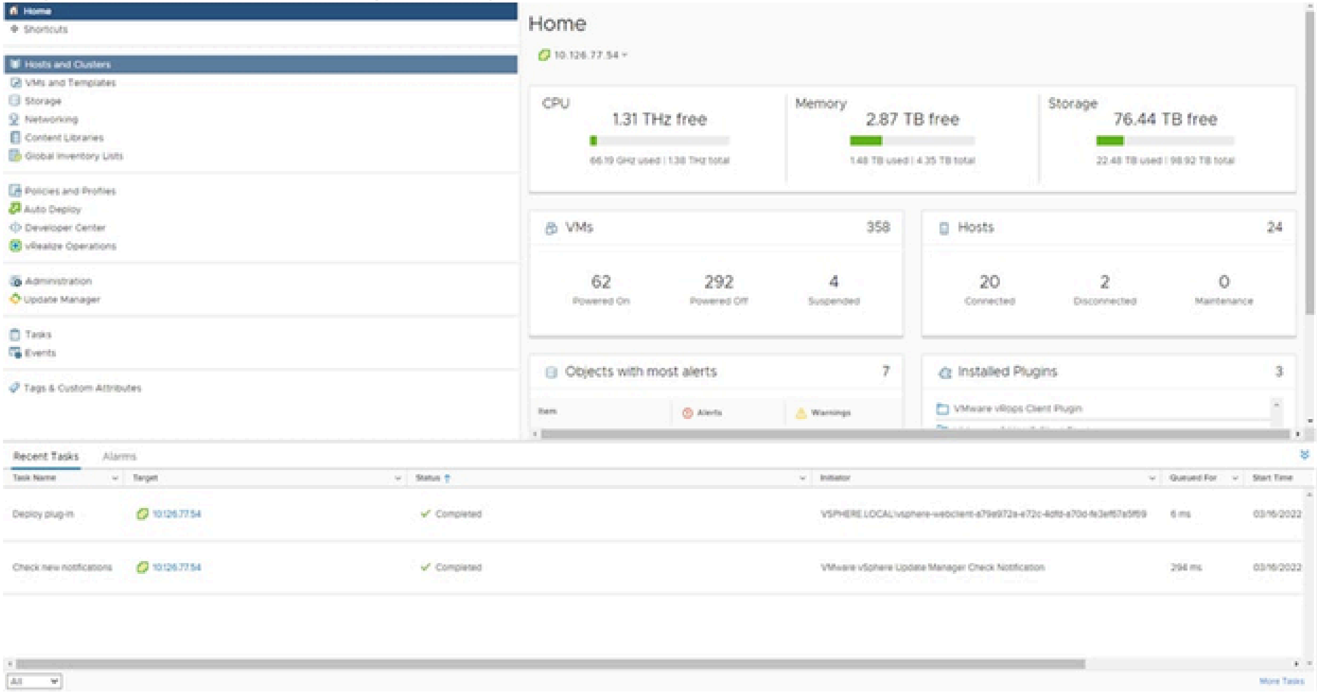
Console

10. Navigate to Network Configuration to proceed with the next steps.

Web Client vCenter Installation

This client allows deployment of CX Agent OVA by use of the Web Client vCenter.

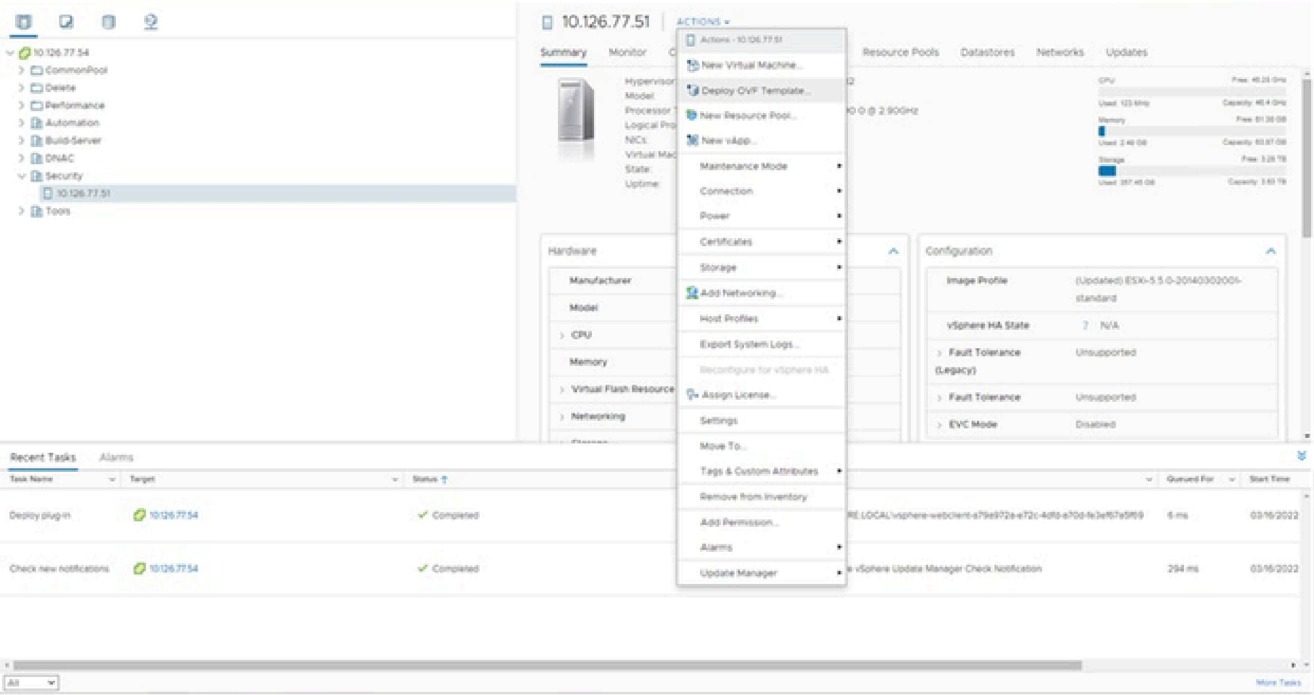
1. Log into vCenter Client using ESXi/hypervisor credentials.



Task Name	Target	Status ↑	Initiator	Queued For	Start Time
Deploy plug-in	10.126.77.54	✓ Completed	VSPHERE.LOCAL\vsphere-webclient-a79a972a-e72c-4dfd-a70d-fe3ef67a5f69	6 ms	03/16/2022
Check new notifications	10.126.77.54	✓ Completed	VMware vSphere Update Manager Check Notification	294 ms	03/16/2022

Home Page

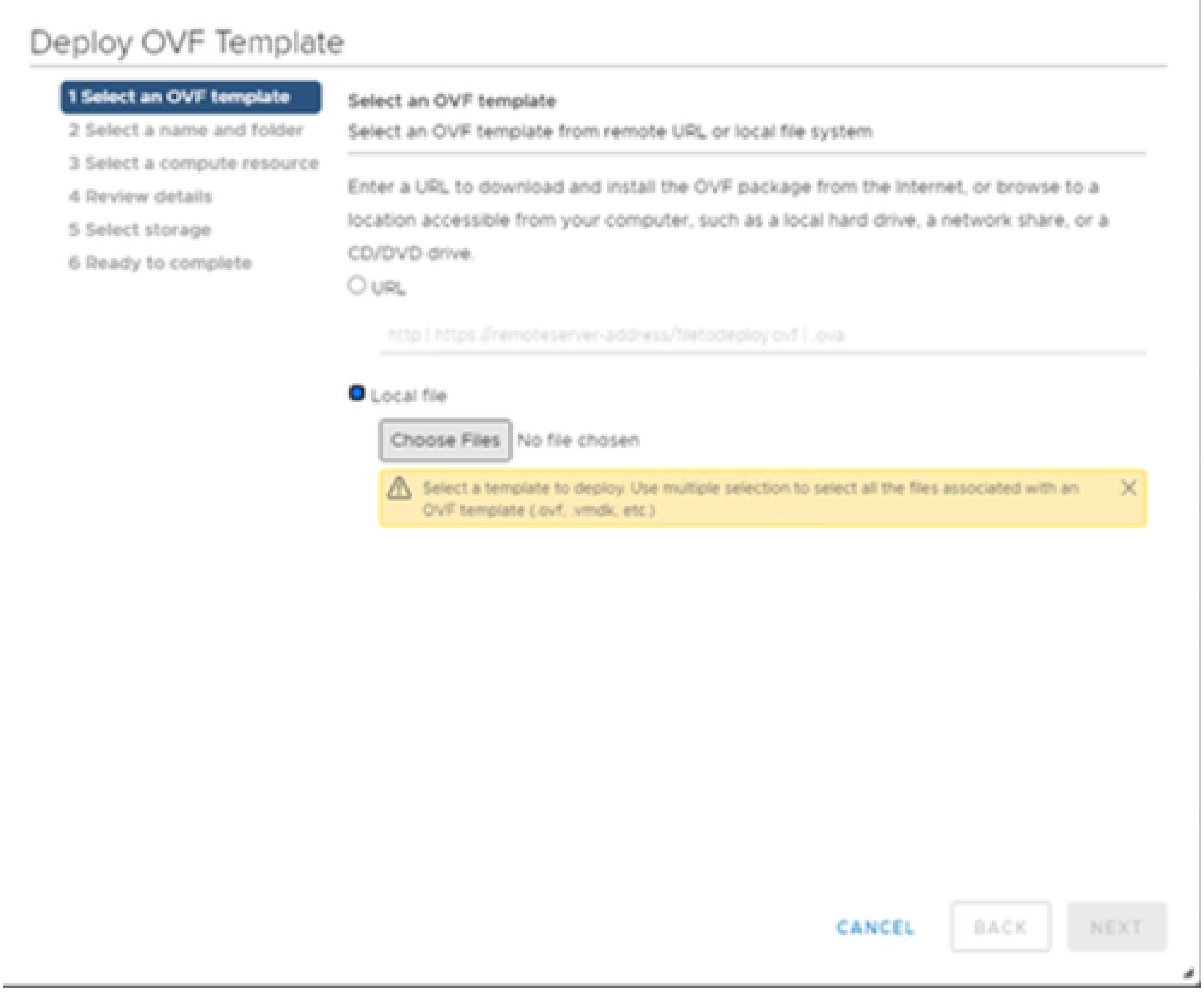
2. From the **Home** page, click **Hosts and Clusters**.



Task Name	Target	Status		Queued For	Start Time
Deploy plug-in	10.126.77.54	✓ Completed	RE.LOCAL\vsphere-webclient-a79e972a-e72c-4df0-a70d-fe3ef67a5f69	6 ms	03/16/2022
Check new notifications	10.126.77.54	✓ Completed	vSphere Update Manager Check Notification	294 ms	03/16/2022

Hosts and Clusters

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



Deploy OVF Template

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

http | https://remoteserver-address/filetodeploy.ovf | .ova

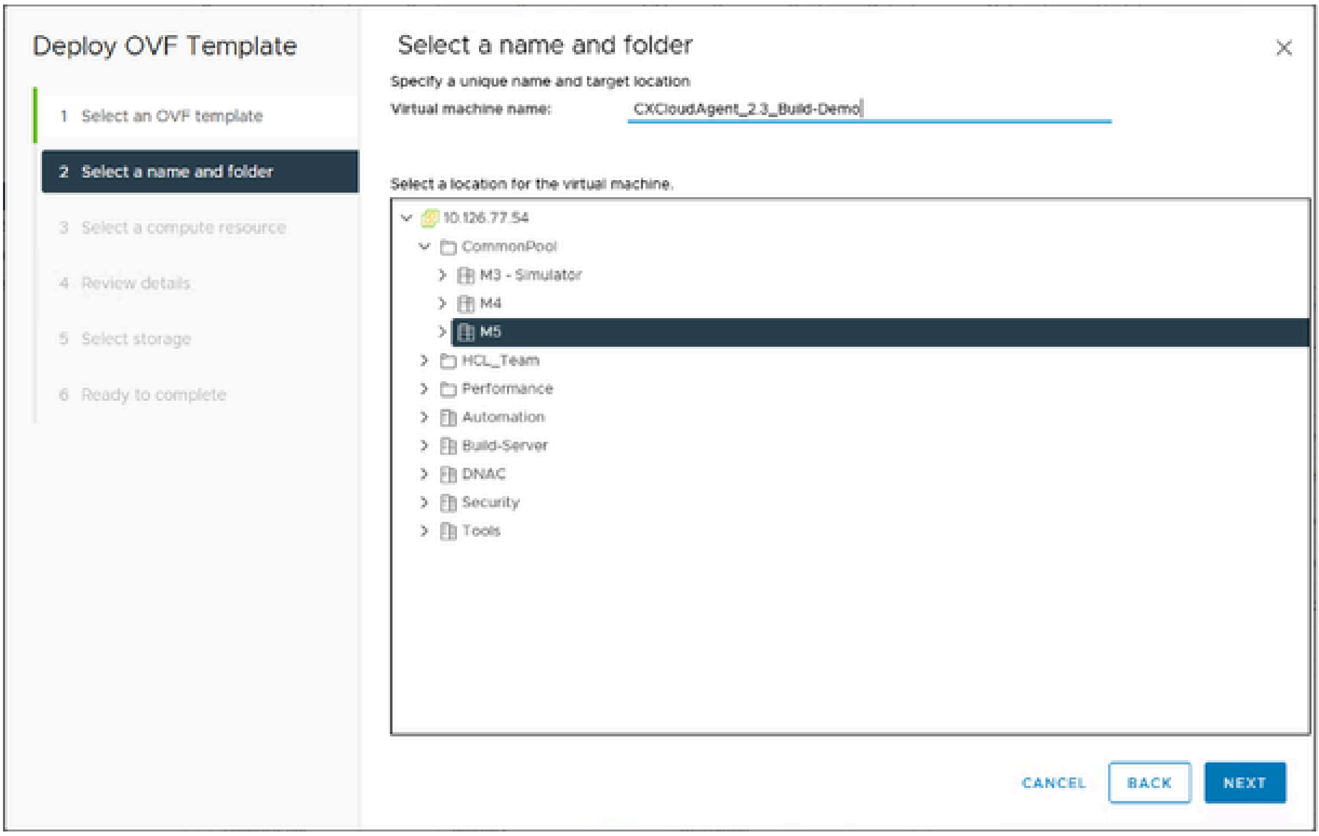
● Local file

Choose Files No file chosen

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

Deploy OVF

4. Add the URL directly or browse to select the OVA file.
5. Click **Next**.



Deploy OVF Template

Select a name and folder

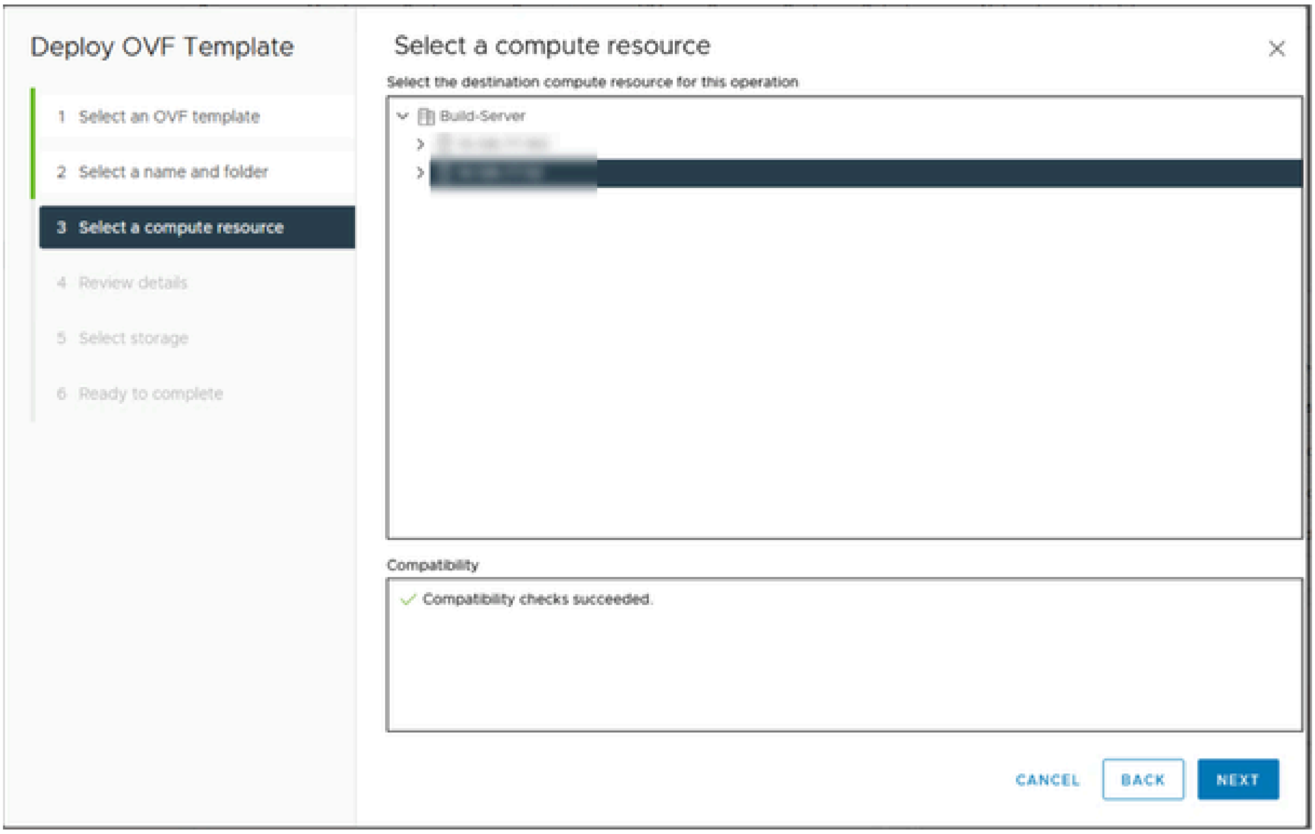
Specify a unique name and target location

Virtual machine name: CXCloudAgent_2.3_Build-Demo

Select a location for the virtual machine.

Name and Folder

6. Enter a unique name and browse to the location if required.
7. Click **Next**.



Deploy OVF Template

Select a compute resource

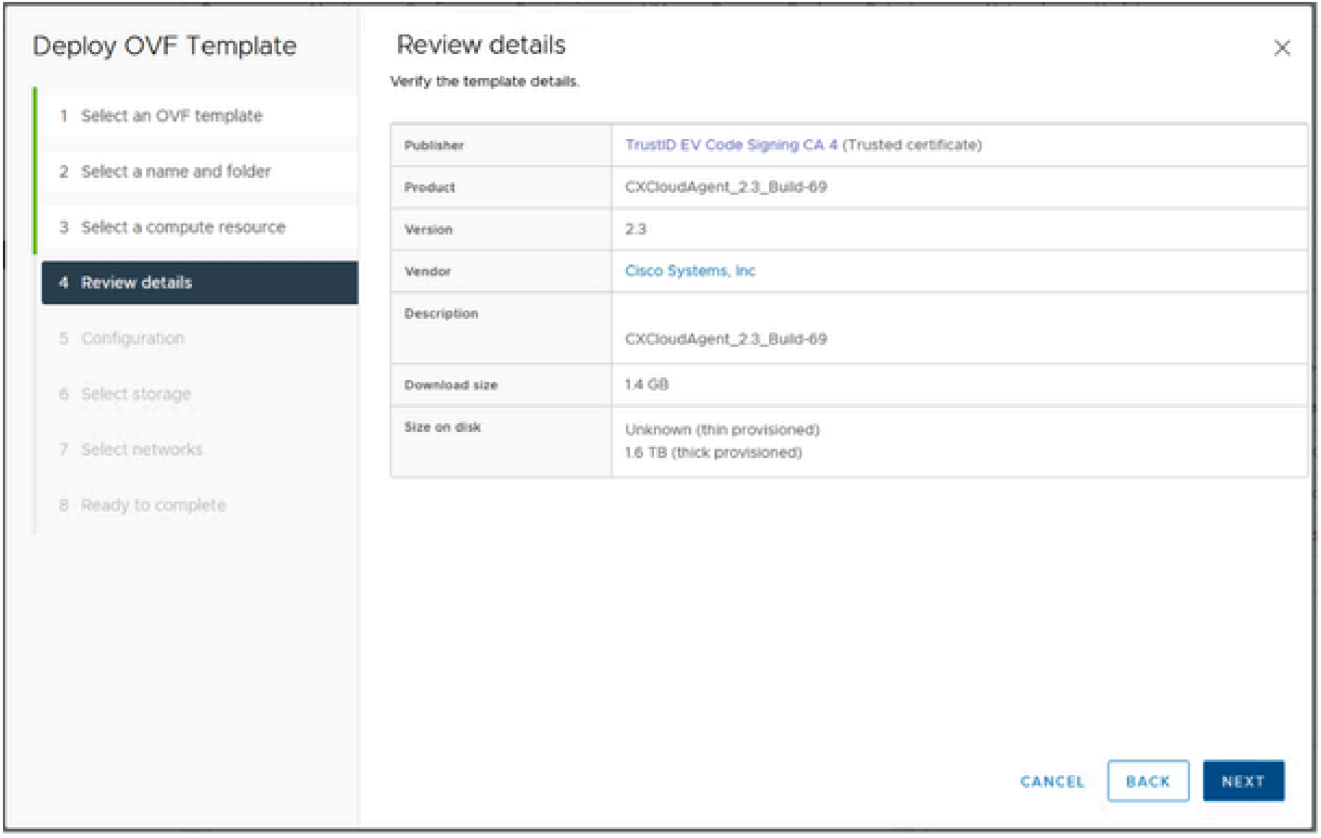
Select the destination compute resource for this operation

Compatibility

✓ Compatibility checks succeeded.

Select compute resource

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



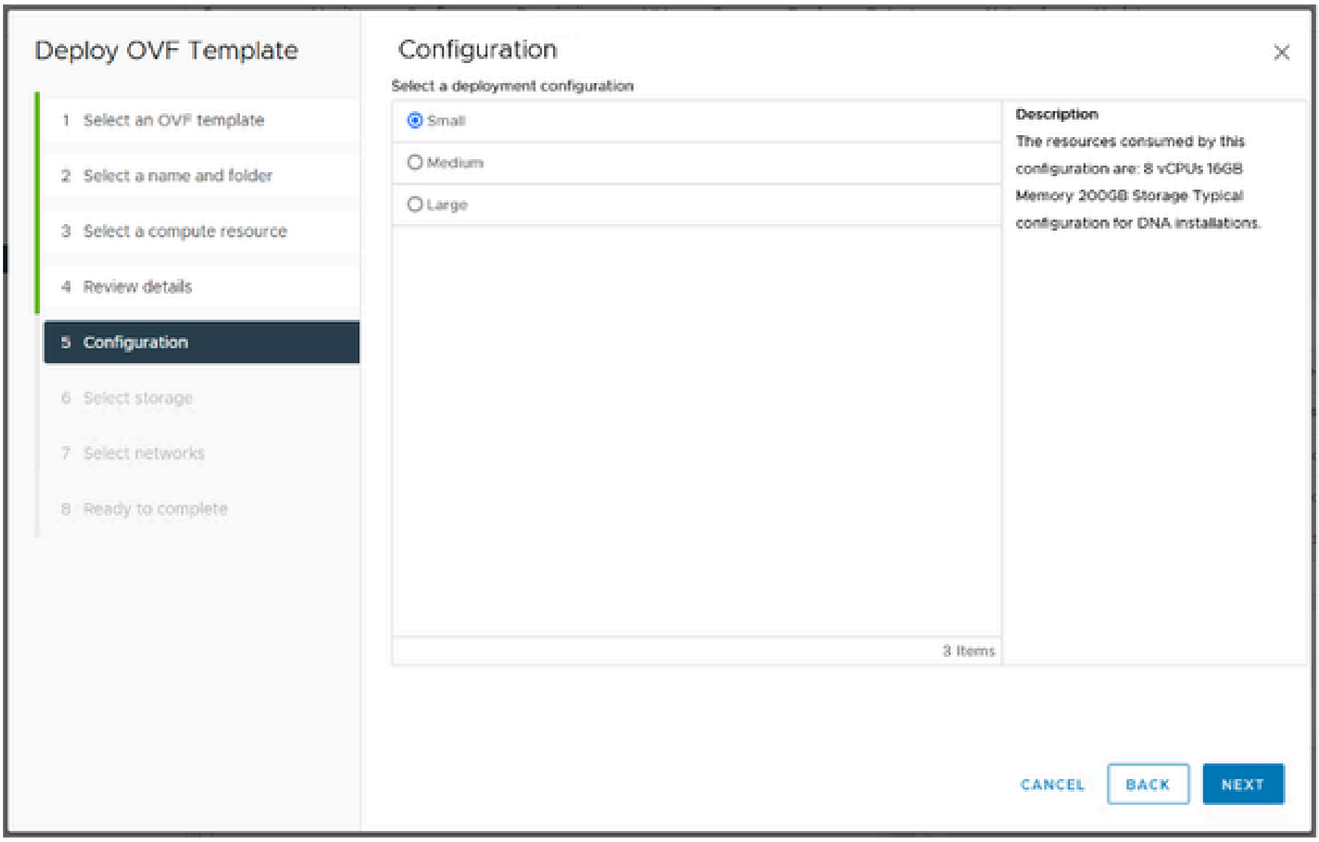
Review details

Verify the template details.

Publisher	TrustID EV Code Signing CA 4 (Trusted certificate)
Product	CXCloudAgent_2.3_Build-69
Version	2.3
Vendor	Cisco Systems, Inc
Description	CXCloudAgent_2.3_Build-69
Download size	1.4 GB
Size on disk	Unknown (thin provisioned) 1.6 TB (thick provisioned)

Review details

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



Configuration

Select a deployment configuration

● Small

○ Medium

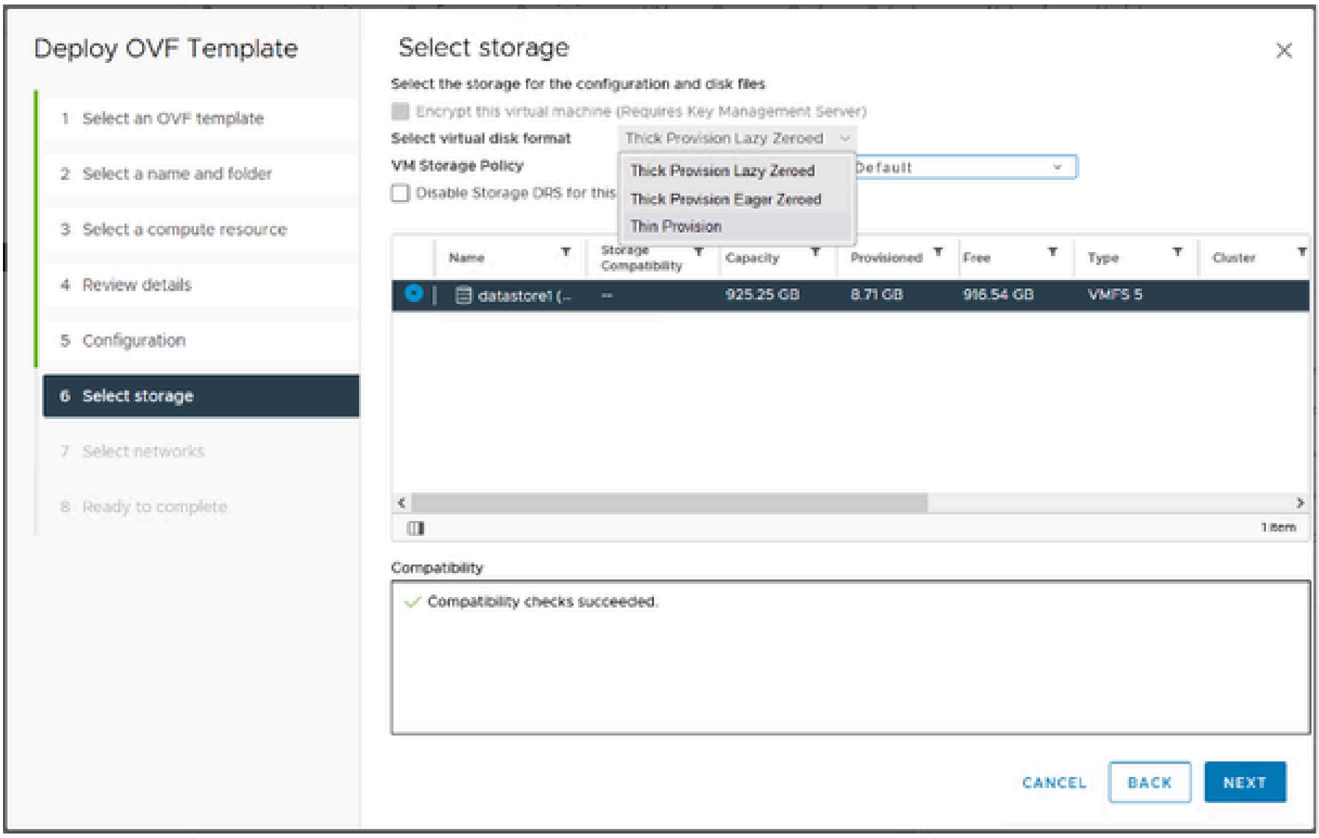
○ Large

Description

The resources consumed by this configuration are: 8 vCPUs 16GB Memory 200GB Storage Typical configuration for DNA installations.

Configuration

10. Select the the deployment **Configuration** and click **Next**.



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Default

□ Disable Storage DRS for this

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster
●	datastore1 (...	--	925.25 GB	8.71 GB	916.54 GB	VMFS 5	

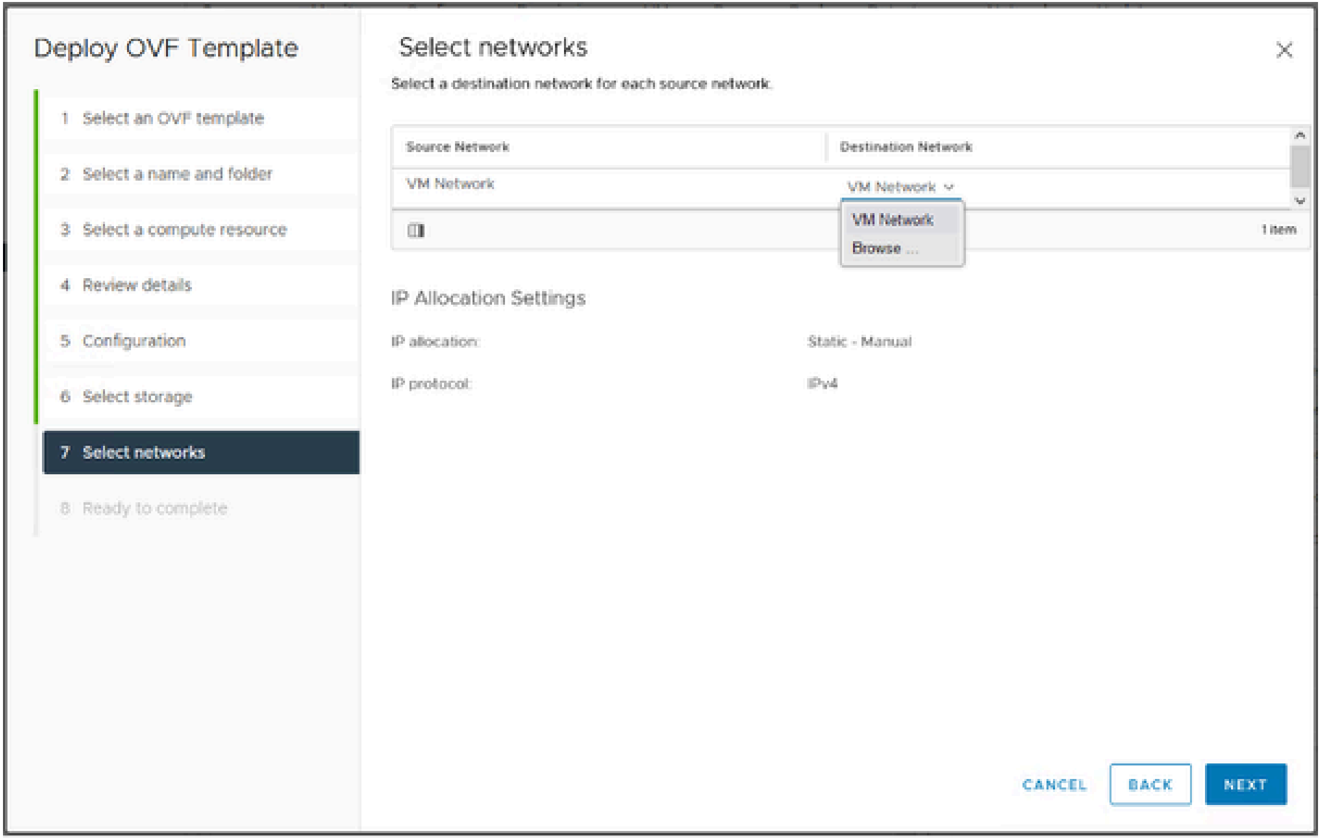
1 item

Compatibility

✓ Compatibility checks succeeded.

Configuration

11. Select **Storage** > **Select virtual disk format** from the drop-down list and click **Next**.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
VM Network	VM Network

1 item

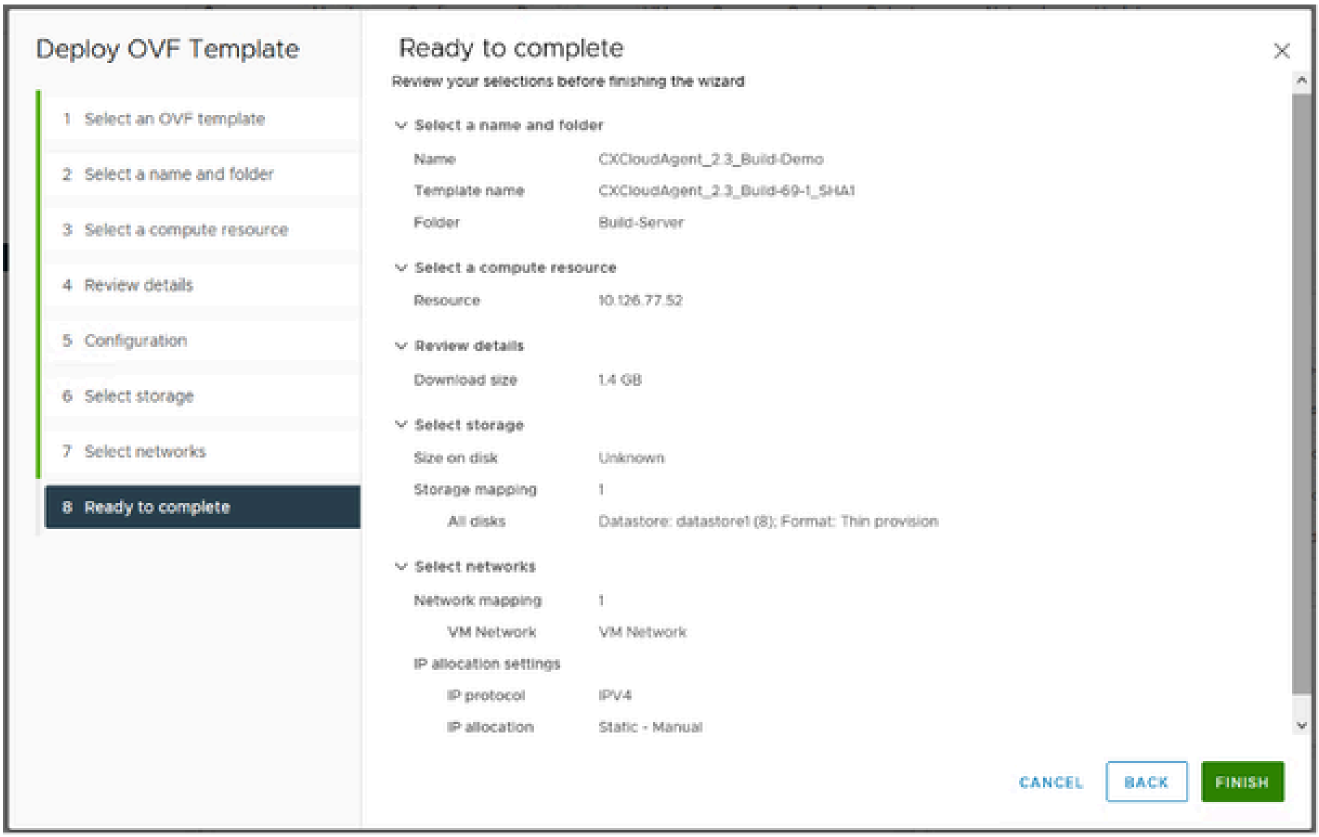
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Select Networks

12. Make the appropriate selections in the **Select networks** and click **Next**.



Ready to complete

Review your selections before finishing the wizard

Select a name and folder

Name	CXCloudAgent_2.3_Build-Demo
Template name	CXCloudAgent_2.3_Build-69-1_SHA1
Folder	Build-Server

Select a compute resource

Resource	10.126.77.52

Review details

Download size	1.4 GB

Select storage

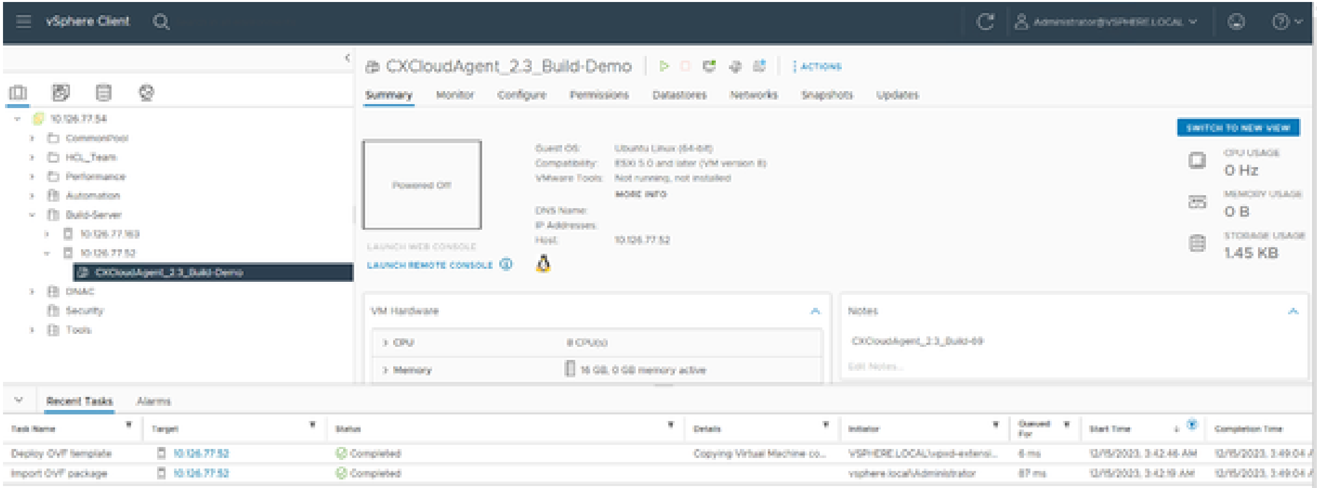
Size on disk	Unknown
Storage mapping	1
All disks	Datastore: datastore1 (8); Format: Thin provision

Select networks

Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

Ready to complete

13. Review selections and click **Finish**. The **Home** page displays.



CXCloudAgent_2.3_Build-Demo

Guest OS:	Ubuntu Linux (64-bit)
Compatibility:	ESXi 5.0 and later (VM version 8)
VMware Tools:	Not running, not installed
DNS Name:	
IP Addresses:	
Host:	10.126.77.52

CPU USAGE 0 Hz

MEMORY USAGE 0 B

STORAGE USAGE 1.45 KB

VM Hardware

CPU	8 CPU(s)
Memory	16 GB, 0 GB memory active

Notes

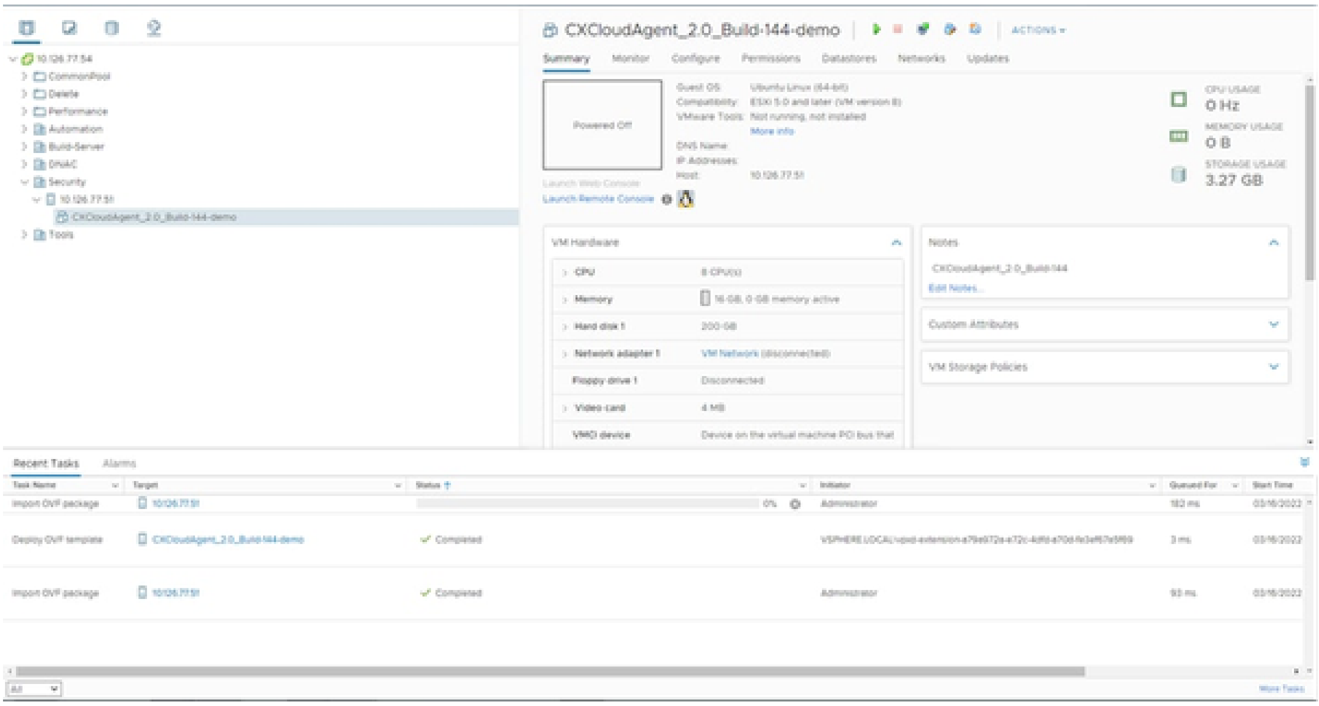
CXCloudAgent_2.3_Build-69

Edit Notes...

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Deploy OVF template	10.126.77.52	Completed	Copying Virtual Machine co...	VSPHERE.LOCAL\vpxd-extensi...	6 ms	12/15/2023, 3:42:46 AM	12/15/2023, 3:49:04 A
Import OVF package	10.126.77.52	Completed		vsphere.local\Administrator	87 ms	12/15/2023, 3:42:19 AM	12/15/2023, 3:49:04 A

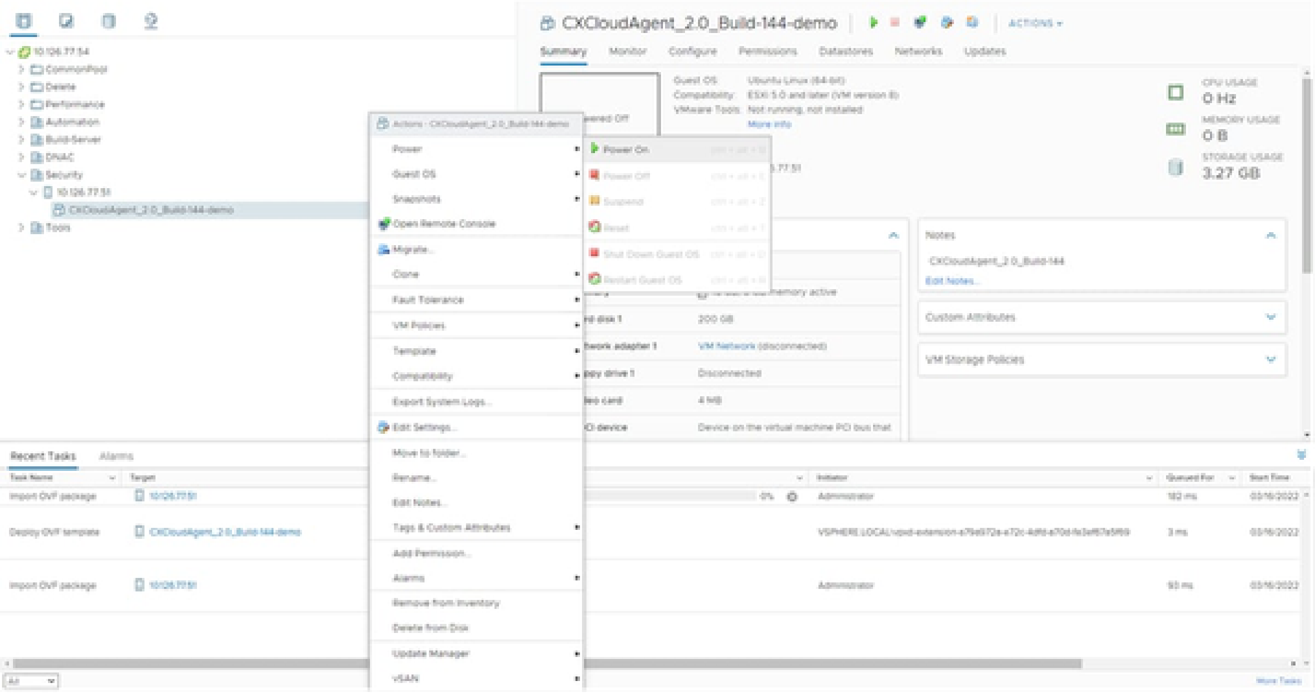
VM added

14. Click thenewly added VM to view the status.



VM Added

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



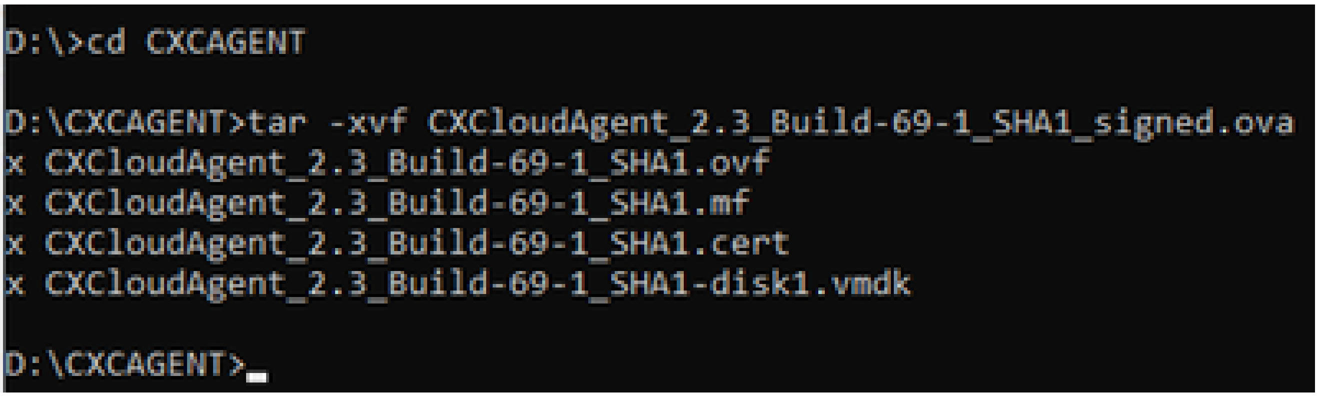
Open Console

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

Oracle Virtual Box 7.0.12 Installation

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

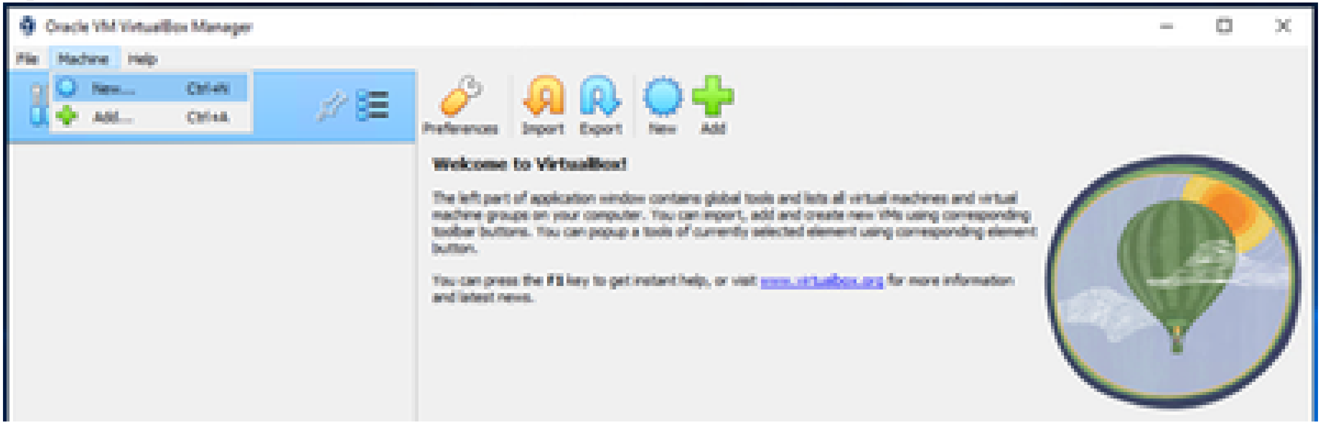
1. Download the *CXCloudAgent_3.1 OVA* into the windows box to any folder.
2. Browse to the folder using the command line interface.
3. Unzip the OVA file using the command tar *-xvf D:\CXCloudAgent_3.1_Build-xx.ova*.



```
D:\>cd CXCAGENT

D:\CXCAGENT>tar -xvf CXCloudAgent_2.3_Build-69-1_SHA1_signed.ova
x CXCloudAgent_2.3_Build-69-1_SHA1.ovf
x CXCloudAgent_2.3_Build-69-1_SHA1.mf
x CXCloudAgent_2.3_Build-69-1_SHA1.cert
x CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk

D:\CXCAGENT>_
```

Unzip OVA File

4. Open the Oracle VM UI.



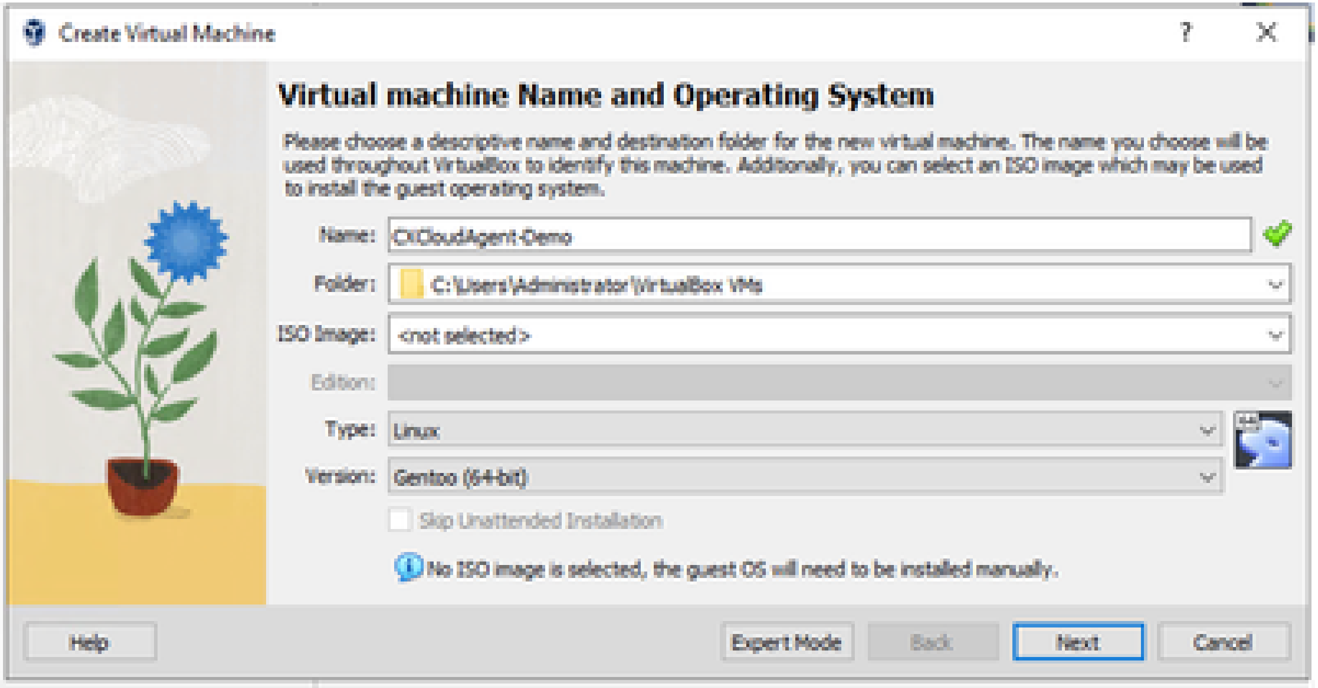
Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

Oracle VM

5. From the menu, select **Machine>New**. The **Create Virtual Machine** window opens.



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: CXCloudAgent-Demo

Folder: C:\Users\Administrator\VirtualBox VMs

ISO Image: <not selected>

Edition:

Type: Linux

Version: Gentoo (64-bit)

□ Skip Unattended Installation

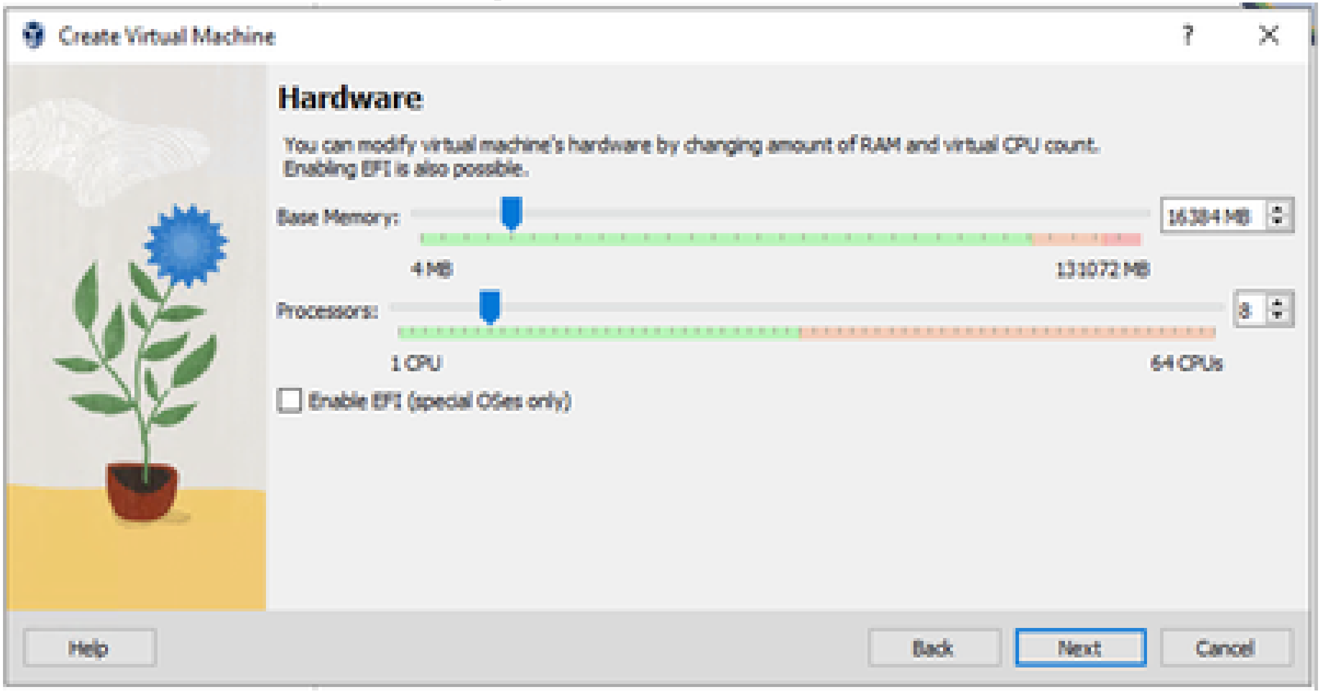
No ISO image is selected, the guest OS will need to be installed manually.

Create Virtual Machine

6. Enter the following details in the **Virtual machine Name and Operating System** window.
   Name: VM name
   Folder: Location where VM data to be stored

ISO image: none
Type: Linux
Version: Gentoo (64bit)

7. Click **Next**. The **Hardware** window opens.



Create Virtual Machine

Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

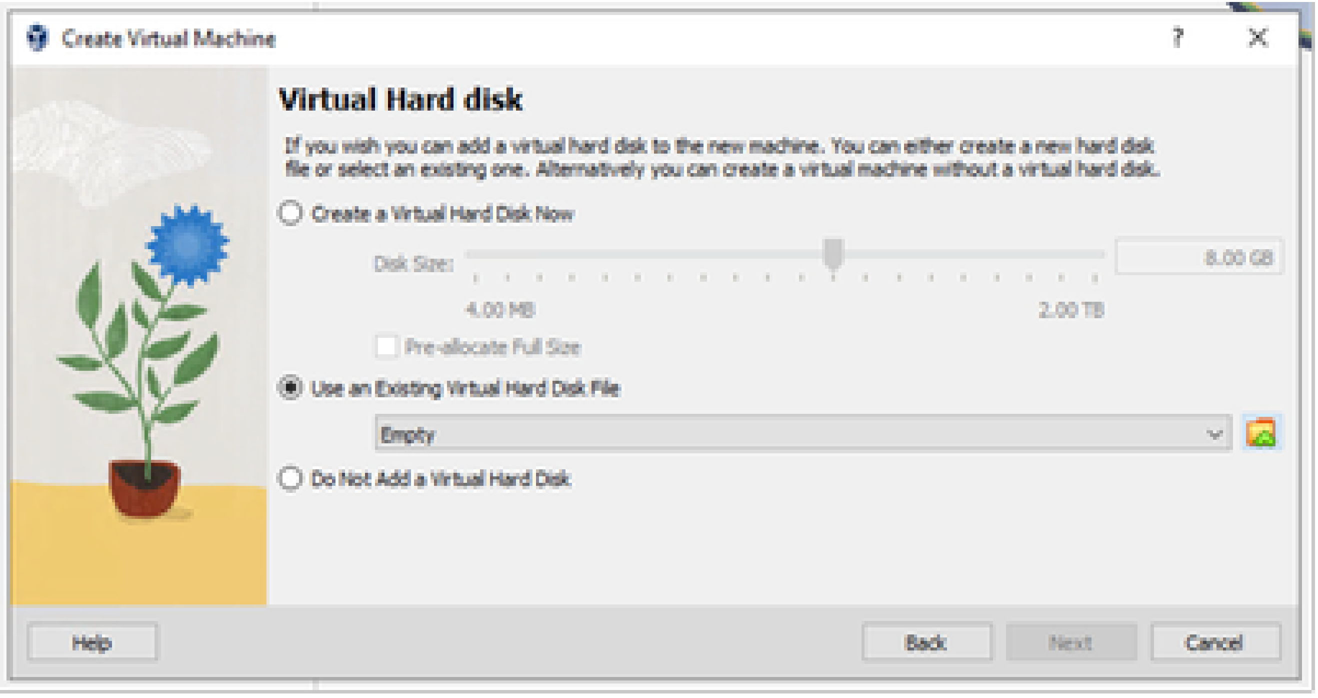
Base Memory: 16384 MB

Processors: 8

□ Enable EFI (special OSes only)

Hardware

8. Enter **Base Memory** (16384 MB) and **Processors** (8 CPU) and click **Next**. The **Virtual Hard Disk** window opens.



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

○ Create a Virtual Hard Disk Now

Disk Size: 8.00 GB

□ Pre-allocate Full Size

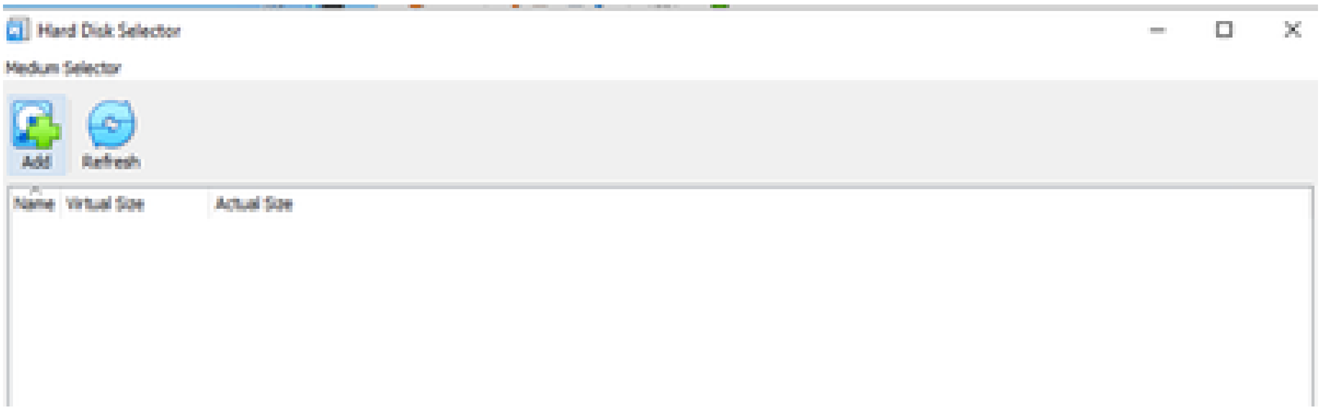
● Use an Existing Virtual Hard Disk File

Empty

○ Do Not Add a Virtual Hard Disk

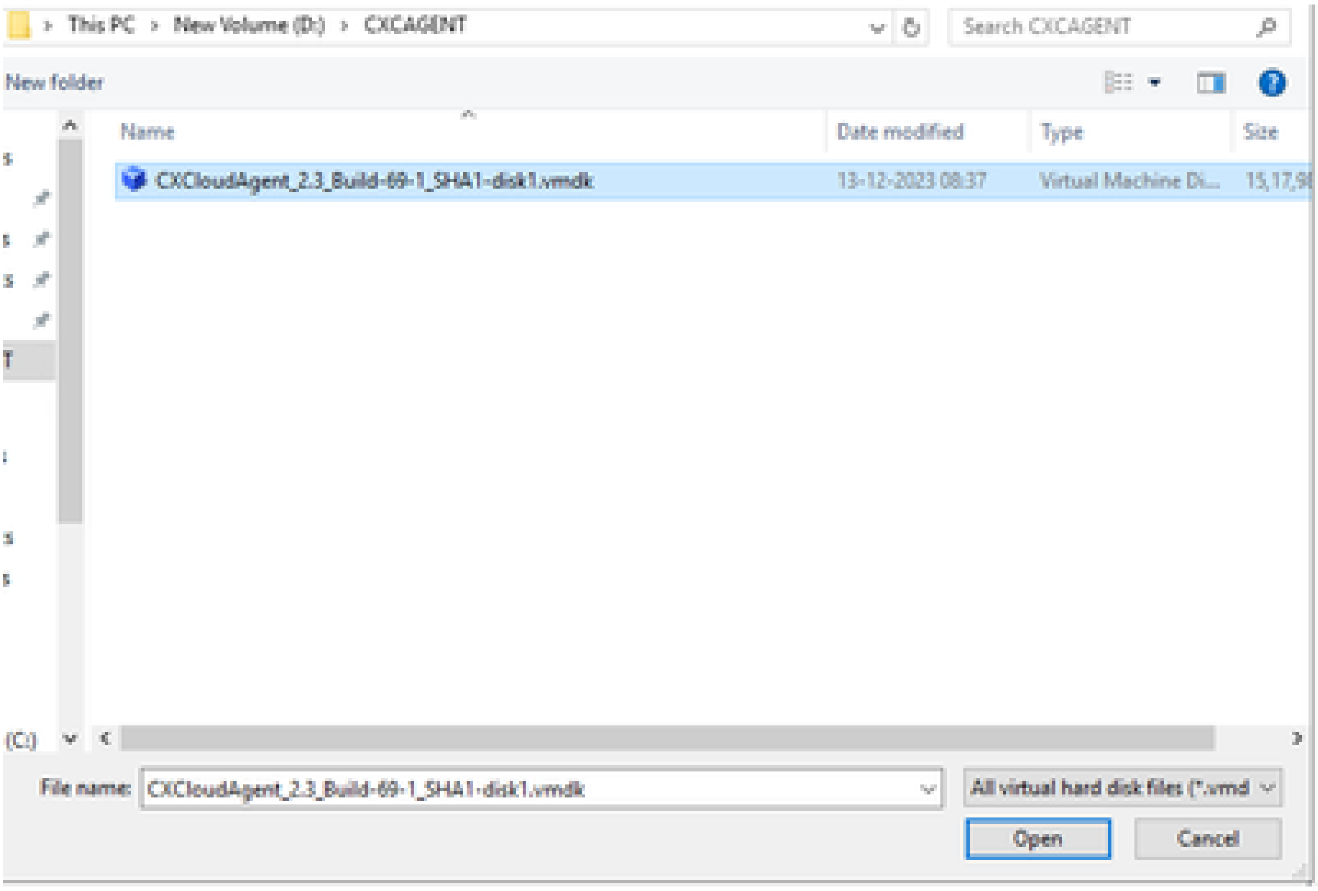
Virtual Hard Disk

9. Select the **Use an Existing Virtual Hard Disk File** radio button and select the **Browse** icon. The **Hard Disk Selector** window opens.



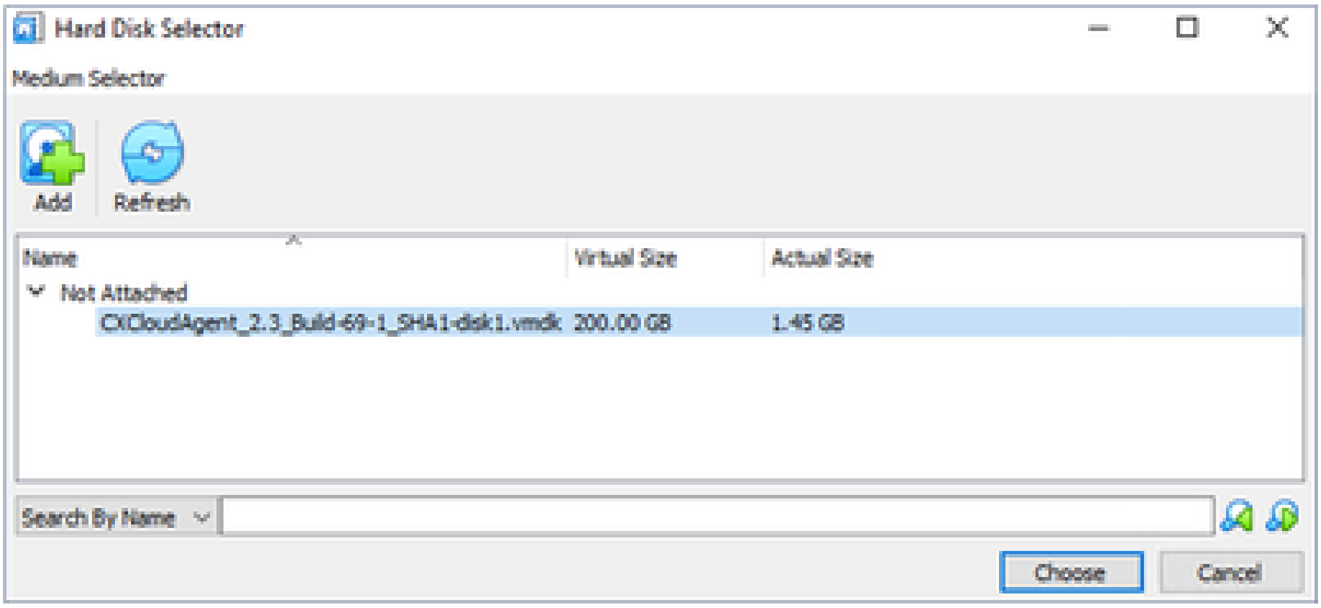
Hard Disk Selector

10. Browse to the OVA folder and select the VMDK file.



OVA Folder

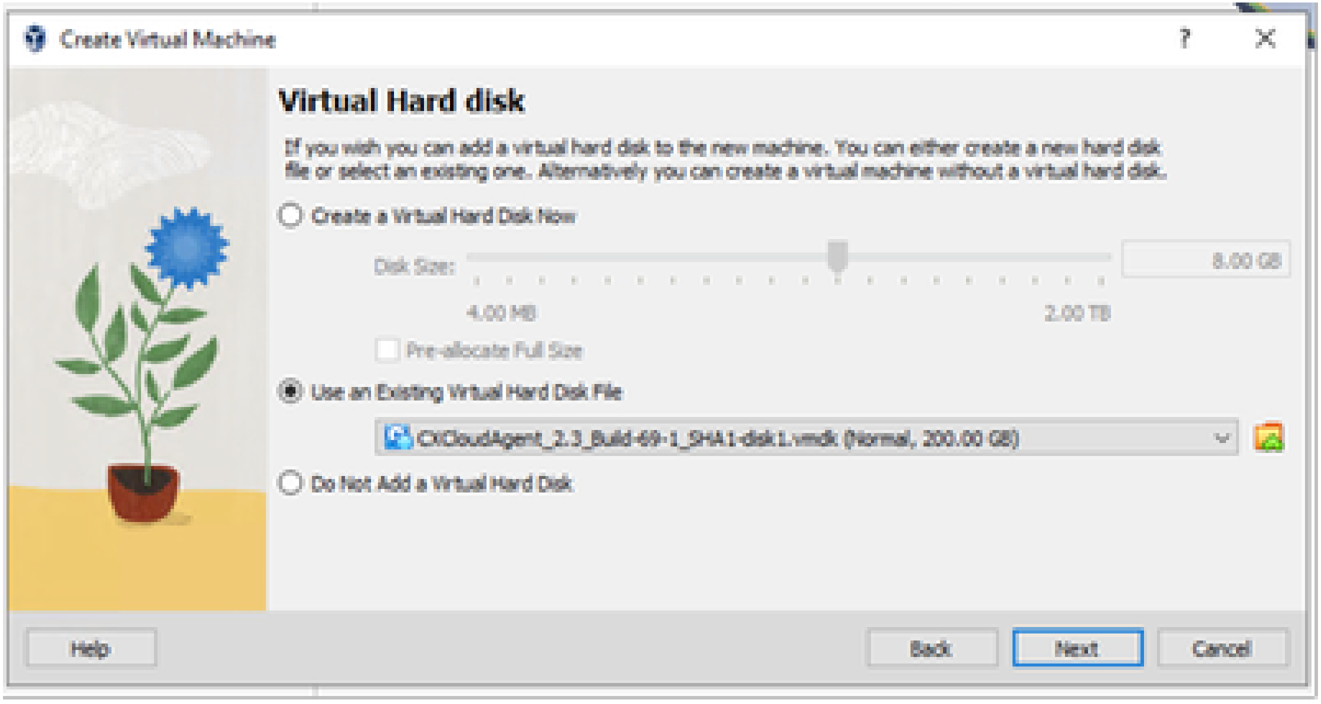
11. Click **Open**. The file displays in the **Hardware Disk Selector** window.



Name	Virtual Size	Actual Size
Not Attached		
CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk	200.00 GB	1.45 GB

Hard Disk Selector

12. Click **Choose**. The **Virtual Hard Disk** window opens. Confirm the displayed option is selected.



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

○ Create a Virtual Hard Disk Now

Disk Size: 8.00 GB (4.00 MB – 2.00 TB)

□ Pre-allocate Full Size

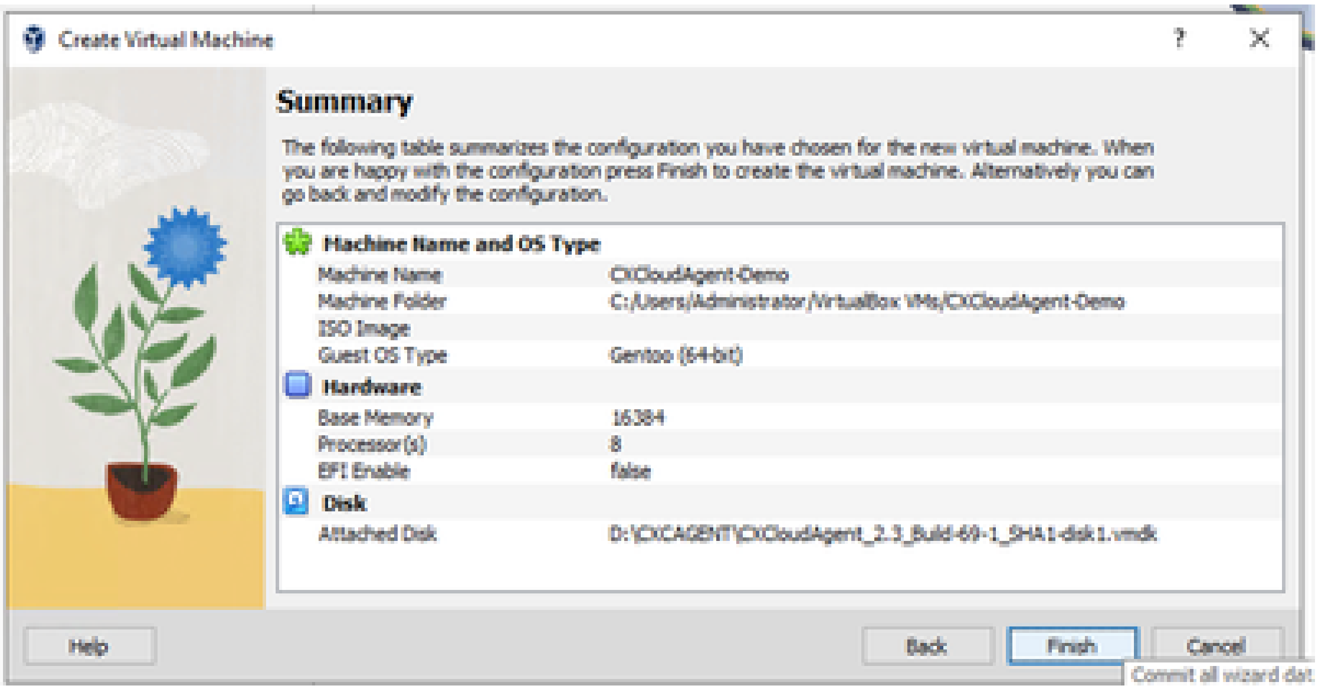
● Use an Existing Virtual Hard Disk File

CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk (Normal, 200.00 GB)

○ Do Not Add a Virtual Hard Disk

Select file

13. Click **Next**. The **Summary** window opens.



Create Virtual Machine

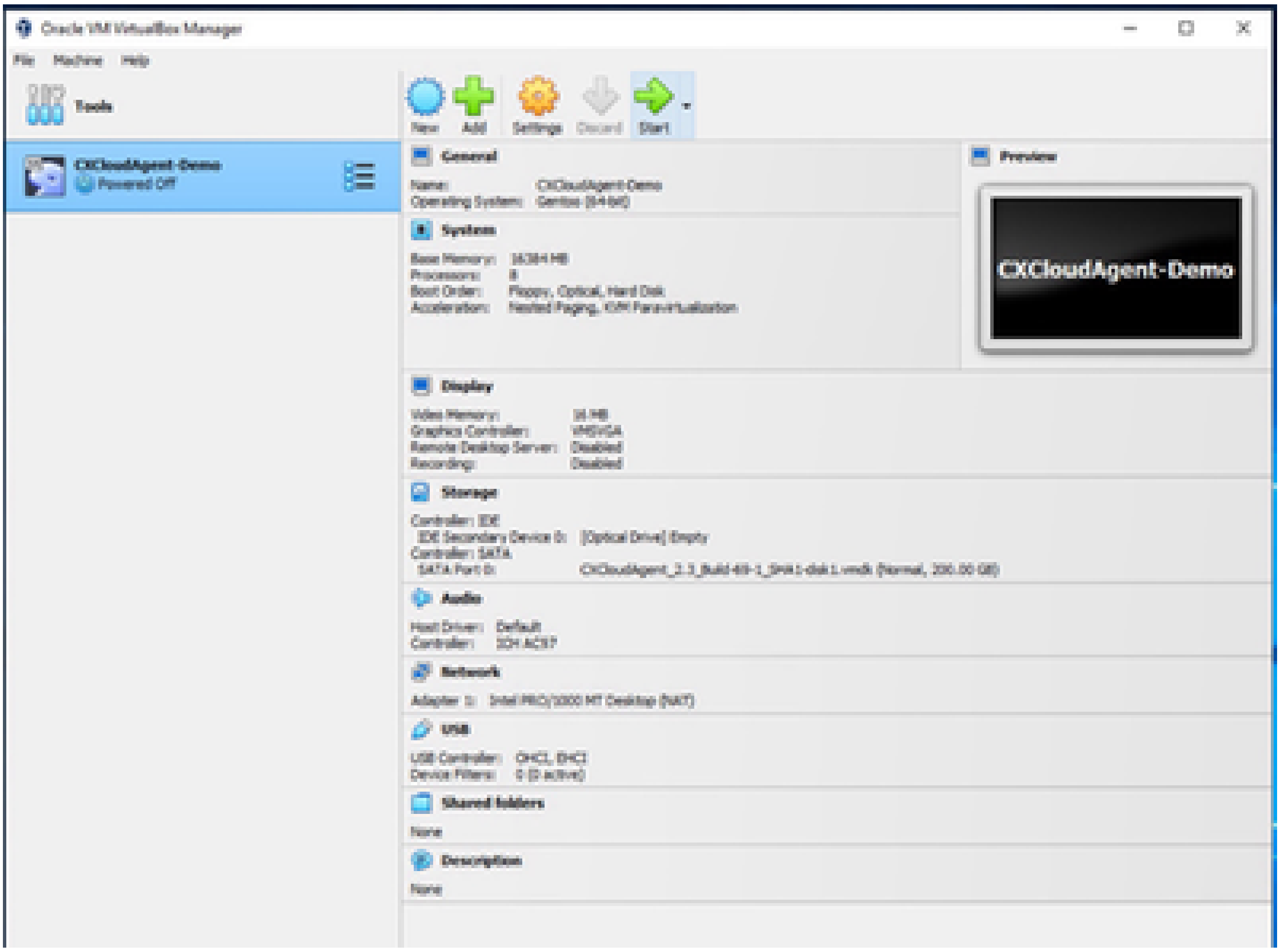
Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	CXCloudAgent-Demo
Machine Folder	C:/Users/Administrator/VirtualBox VMs/CXCloudAgent-Demo
ISO Image	
Guest OS Type	Gentoo (64-bit)
Hardware	
Base Memory	16384
Processor(s)	8
EFI Enable	false
Disk	
Attached Disk	D:\CXCAGENT\CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk

Summary

14. Click **Finish**.



Oracle VM VirtualBox Manager

General

Name: CXCloudAgent-Demo
Operating System: Gentoo (64-bit)

System

Base Memory: 16384 MB
Processors: 8
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: CXCloudAgent_2.3_Build-69-1_SHA1-disk1.vmdk (Normal, 200.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

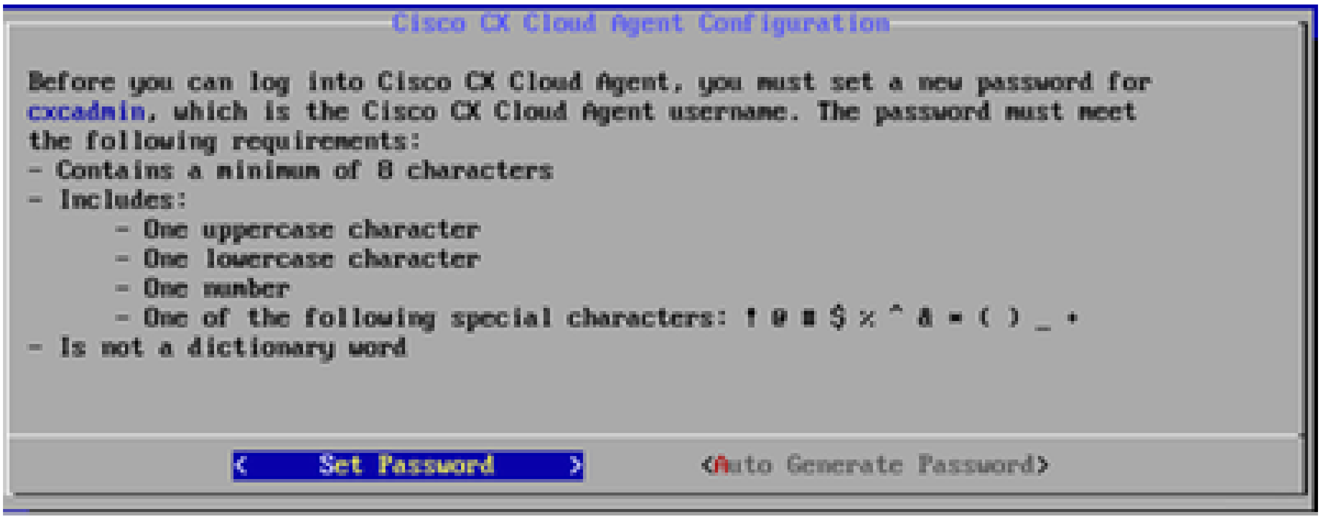
None

Description

None

VM Console Startup

15. Select the deployed VM and click **Start**. The VM powers in and the console screen displays for setup.



```
Cisco CX Cloud Agent Configuration

Before you can log into Cisco CX Cloud Agent, you must set a new password for
cxcadmin, which is the Cisco CX Cloud Agent username. The password must meet
the following requirements:
- Contains a minimum of 8 characters
- Includes:
      - One uppercase character
      - One lowercase character
      - One number
      - One of the following special characters: ! @ # $ % ^ & * ( ) _ +
- Is not a dictionary word

        <   Set Password   >        <Auto Generate Password>
```

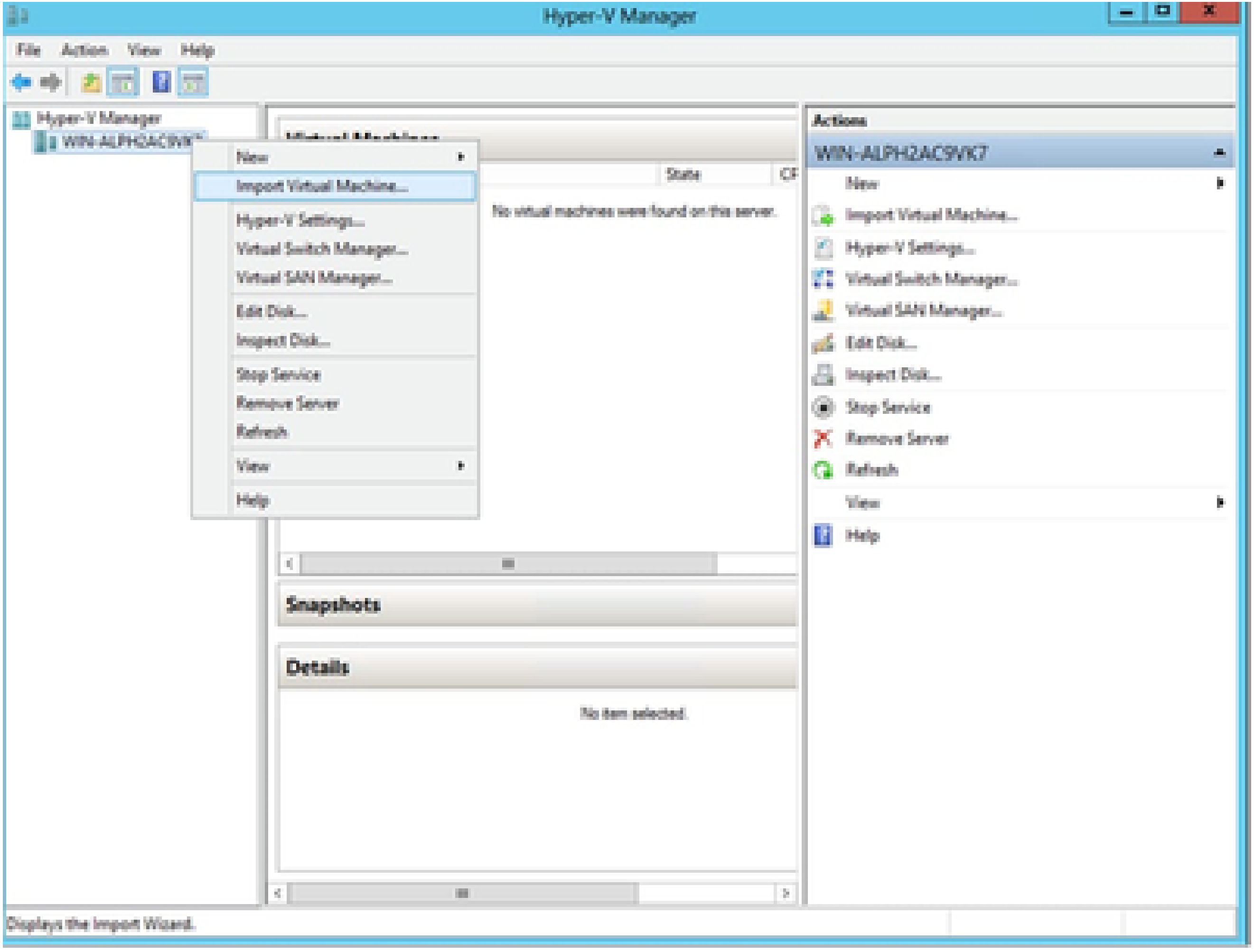
Open the console

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

Microsoft Hyper-V Installation

This client deploys CX Agent OVA though the Microsoft Hyper-V installation.

1. Login into the Hyper-V Manager.



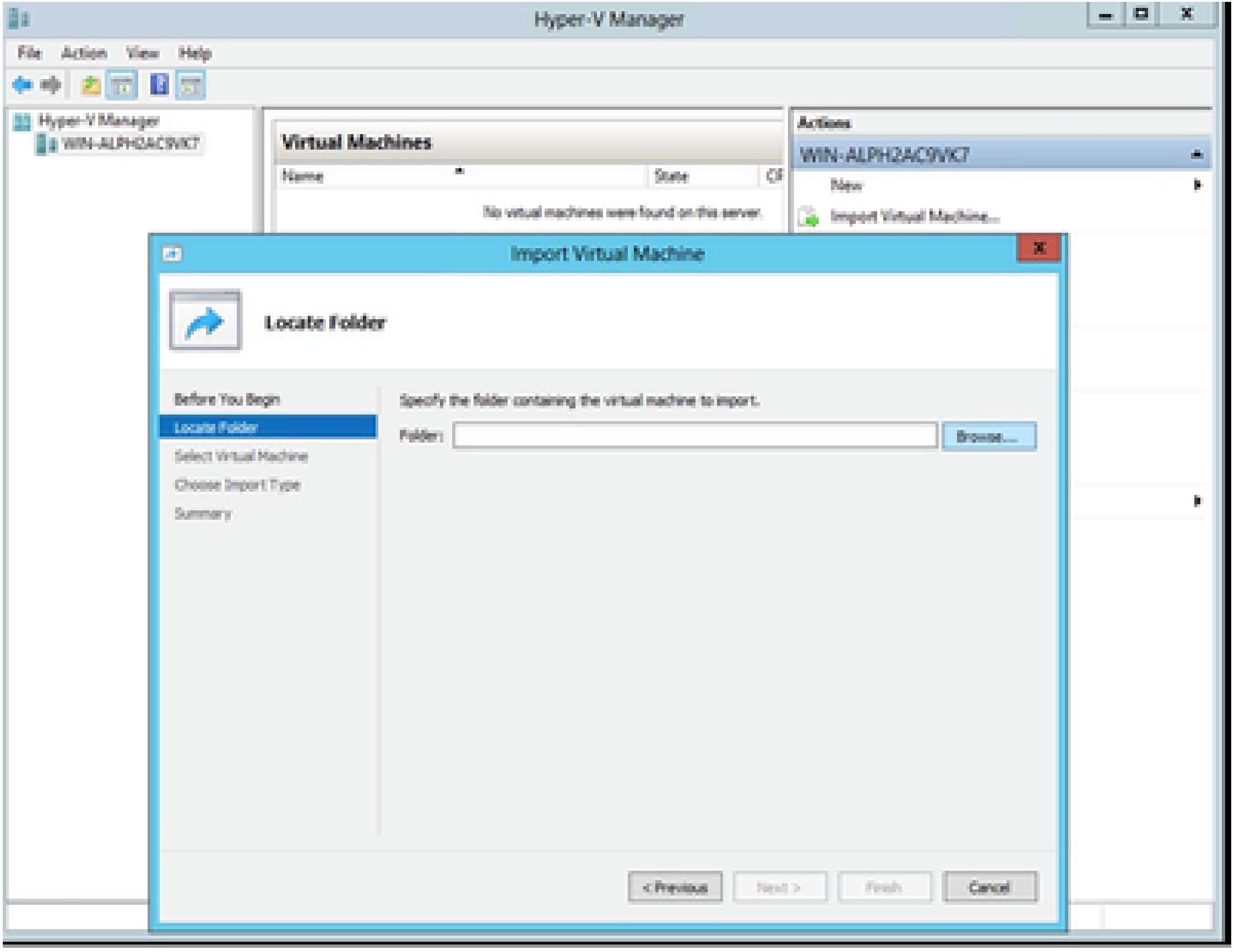
No virtual machines were found on this server.

No item selected.

Displays the Import Wizard.

Hyper V Manager

2. Select target VM, right-click to open menu, and select **Import Virtual Machine**.



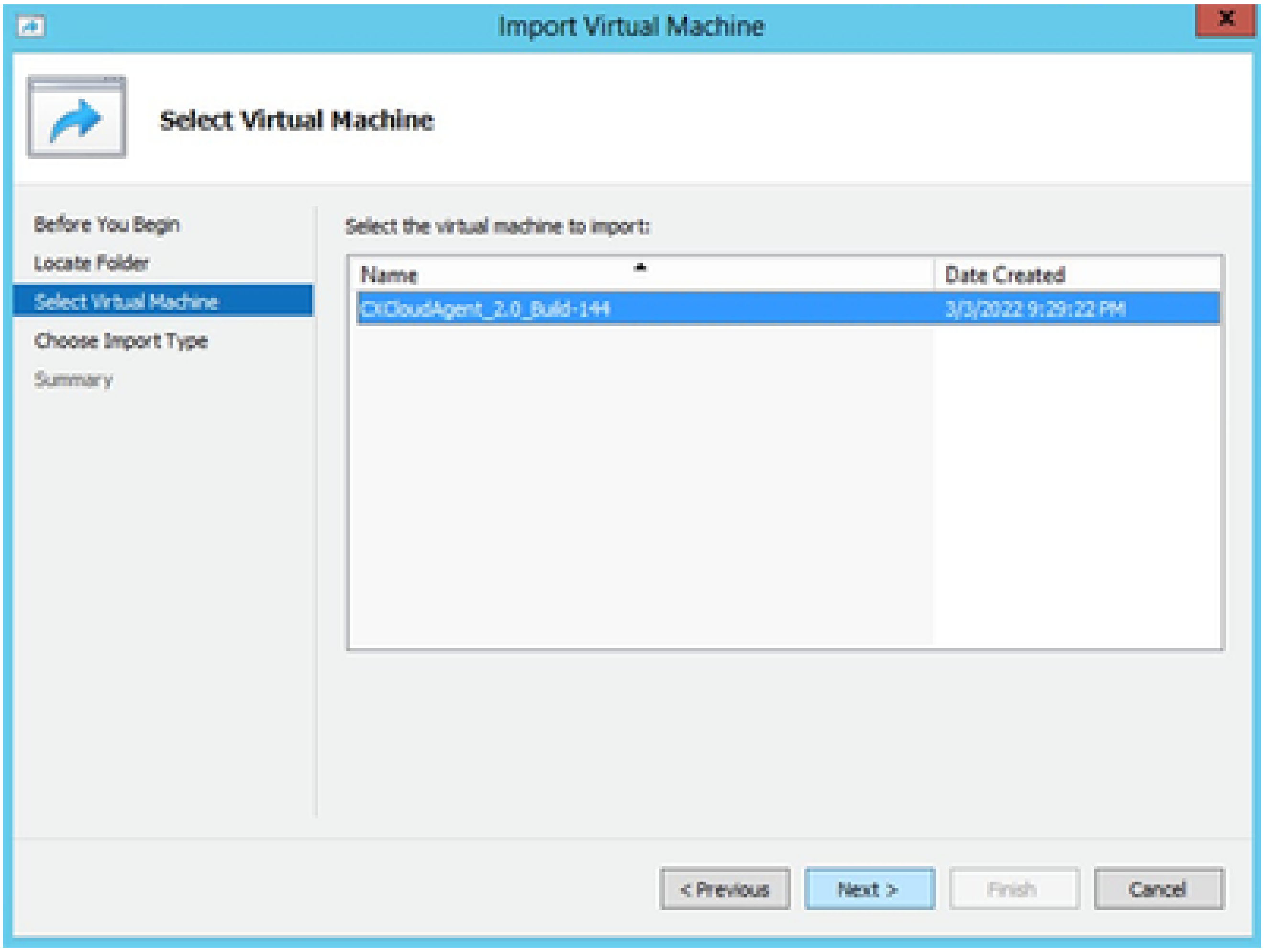
No virtual machines were found on this server.

Specify the folder containing the virtual machine to import.

Folder:

Folder to Import

3. Browse and select the **download folder** and click **Next**.

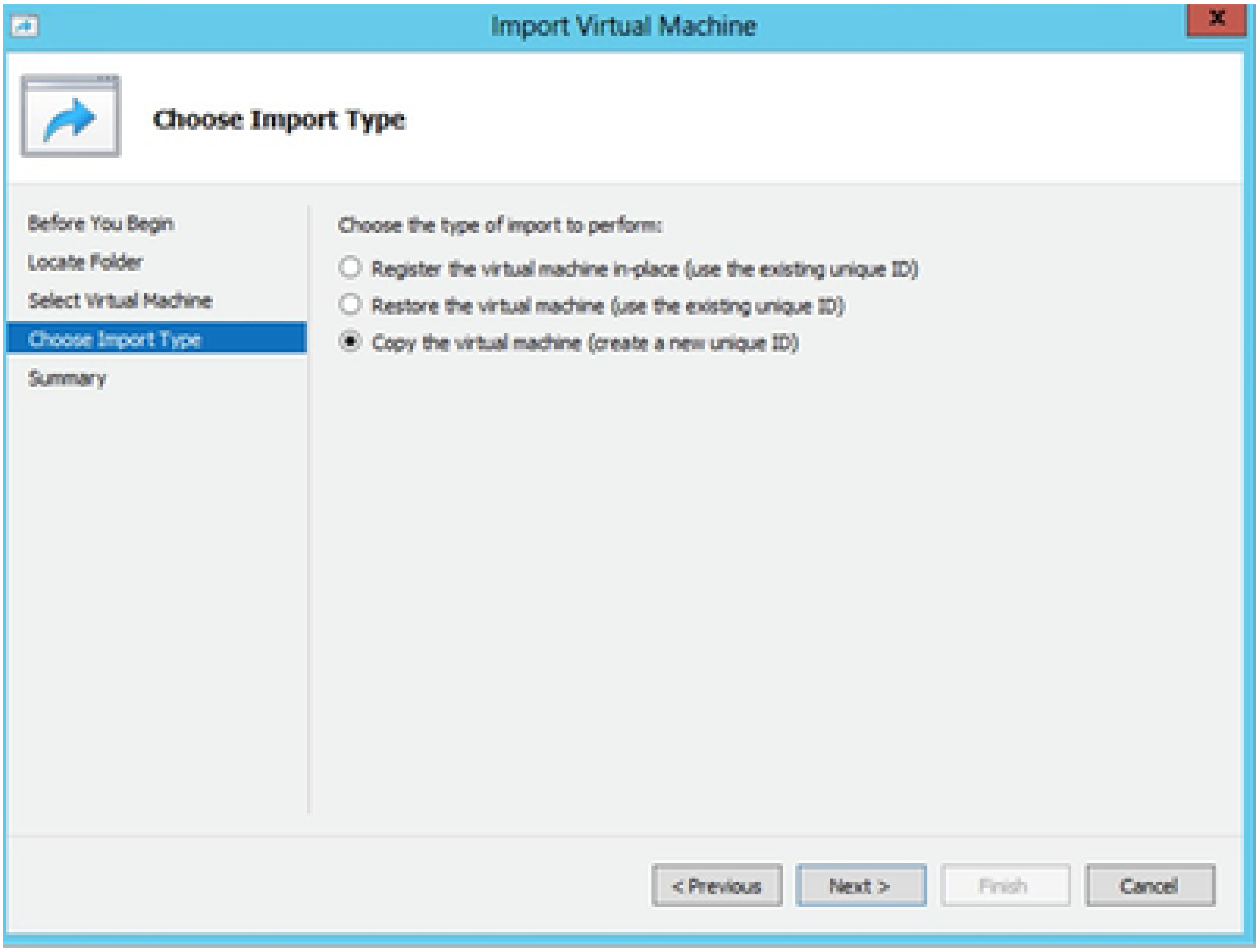


Select the virtual machine to import:

Name	Date Created
CXCloudAgent_2.0_Build-144	3/3/2022 9:29:22 PM

Select VM

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



Import Virtual Machine

Choose Import Type

Choose the type of import to perform:

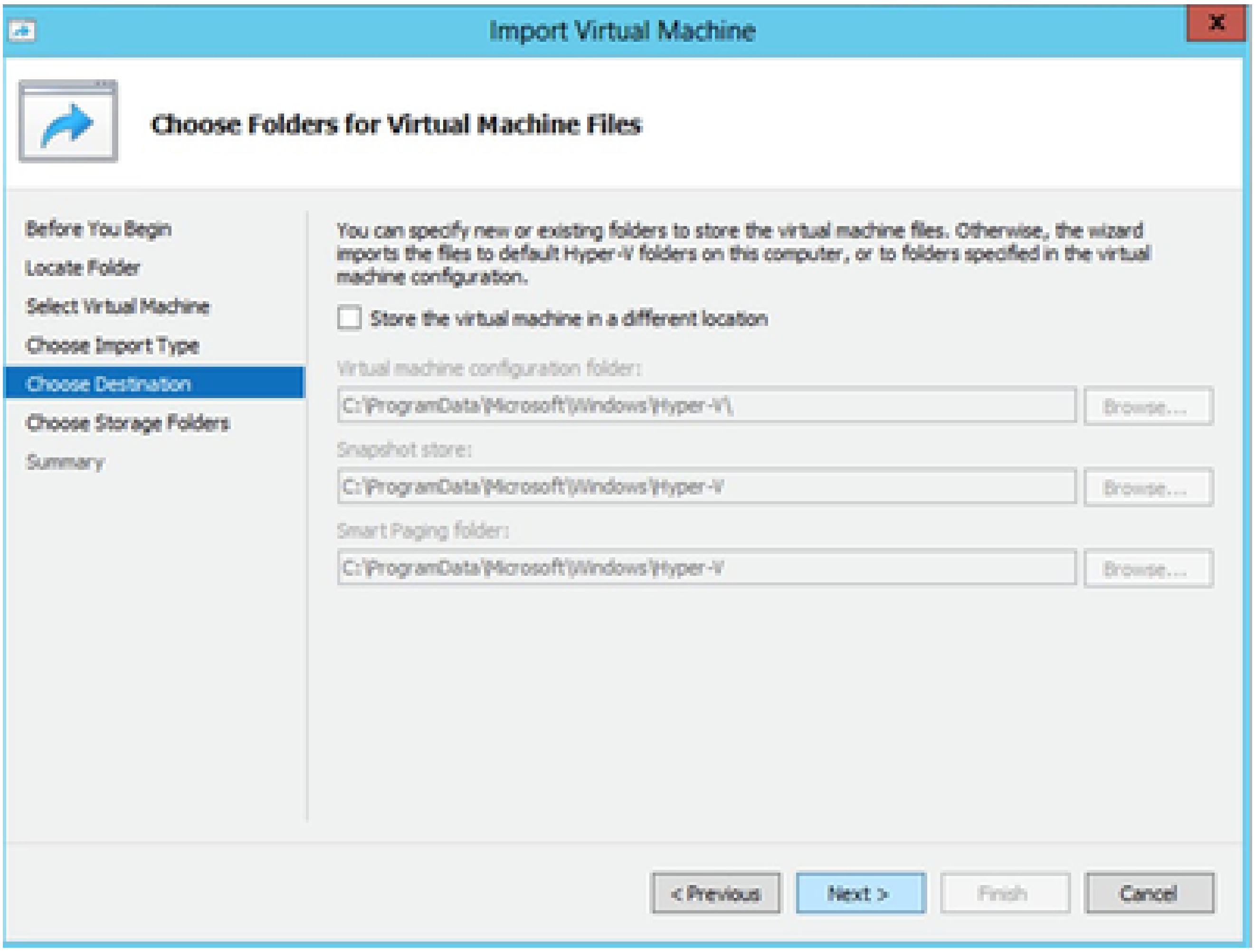
○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

Import Type

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



You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

□ Store the virtual machine in a different location

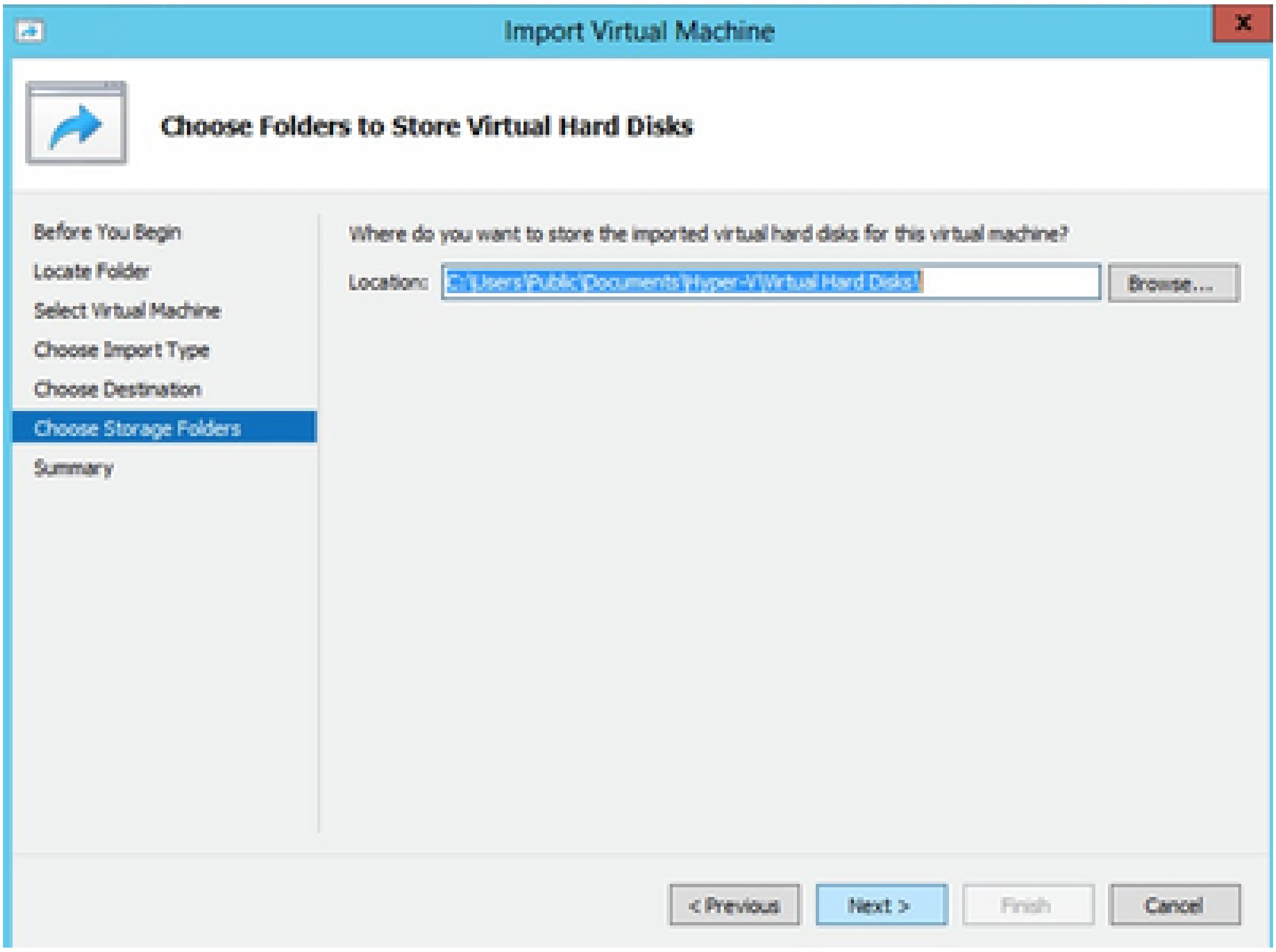
Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Snapshot store: C:\ProgramData\Microsoft\Windows\Hyper-V

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V

Choose Folders for Virtual Machine Files

6. Browse to select the folder for VM files. Cisco recommends using the default paths.
7. Click **Next**.



Import Virtual Machine

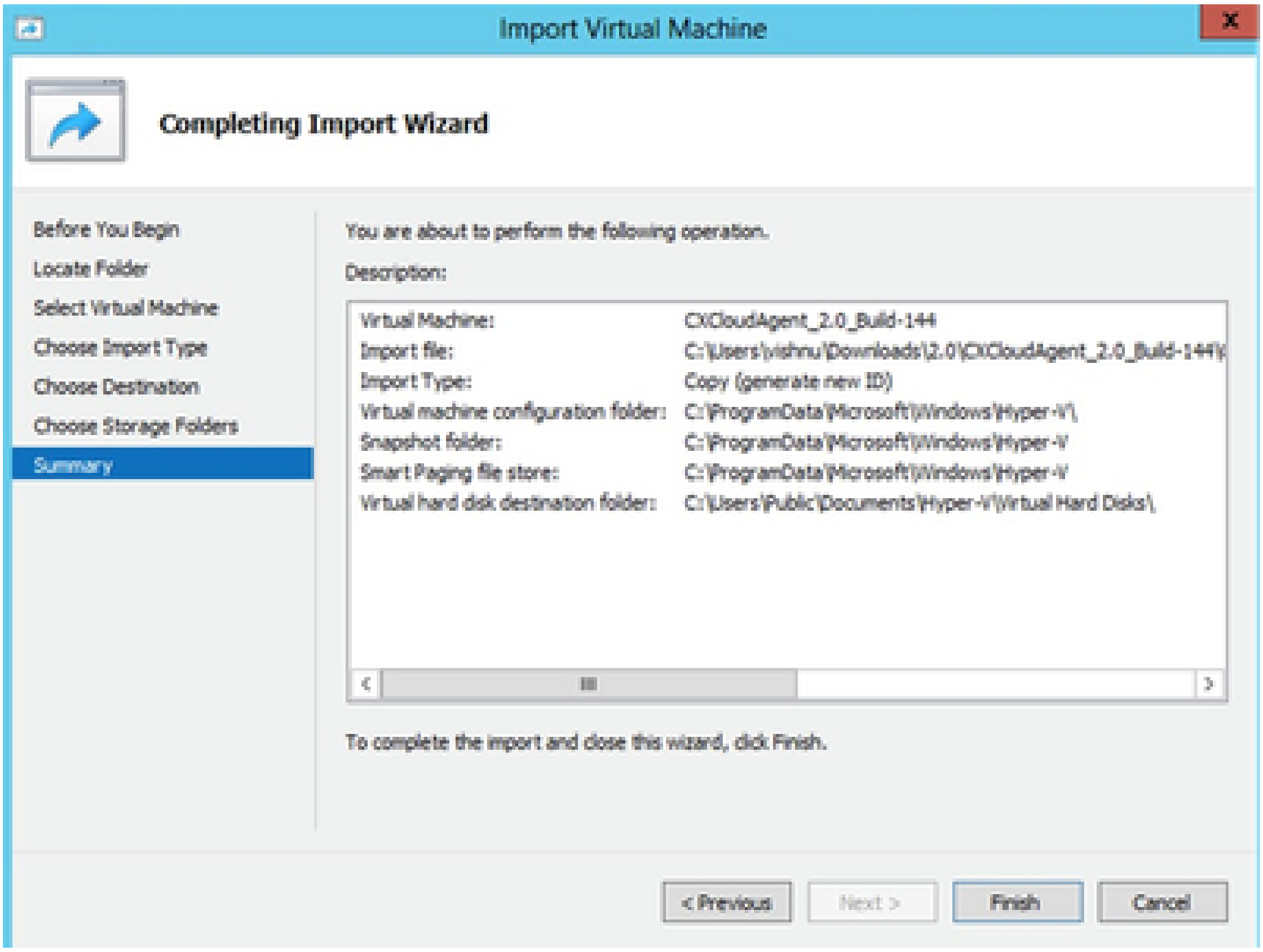
Choose Folders to Store Virtual Hard Disks

Where do you want to store the imported virtual hard disks for this virtual machine?

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Folder to Store the Virtual Hard Disks

8. Browse and select the folder to store the VM hard disks. Cisco recommends using the default paths.
9. Click **Next**. The VM summary displays.



You are about to perform the following operation.

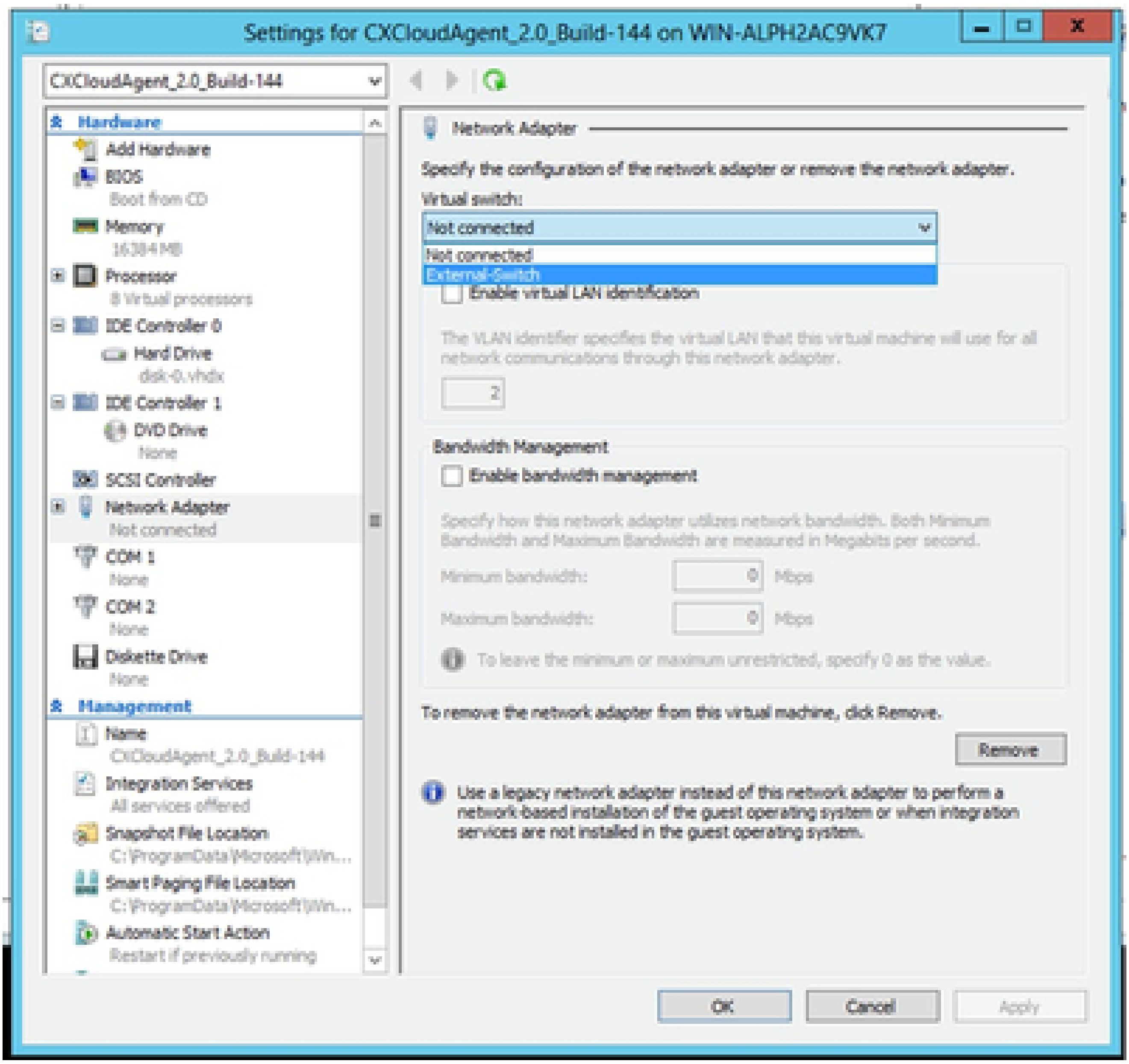
Description:

Virtual Machine:	CXCloudAgent_2.0_Build-144
Import file:	C:\Users\vishnu\Downloads\2.0\CXCloudAgent_2.0_Build-144\
Import Type:	Copy (generate new ID)
Virtual machine configuration folder:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Snapshot folder:	C:\ProgramData\Microsoft\Windows\Hyper-V
Smart Paging file store:	C:\ProgramData\Microsoft\Windows\Hyper-V
Virtual hard disk destination folder:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

To complete the import and close this wizard, click Finish.

Summary

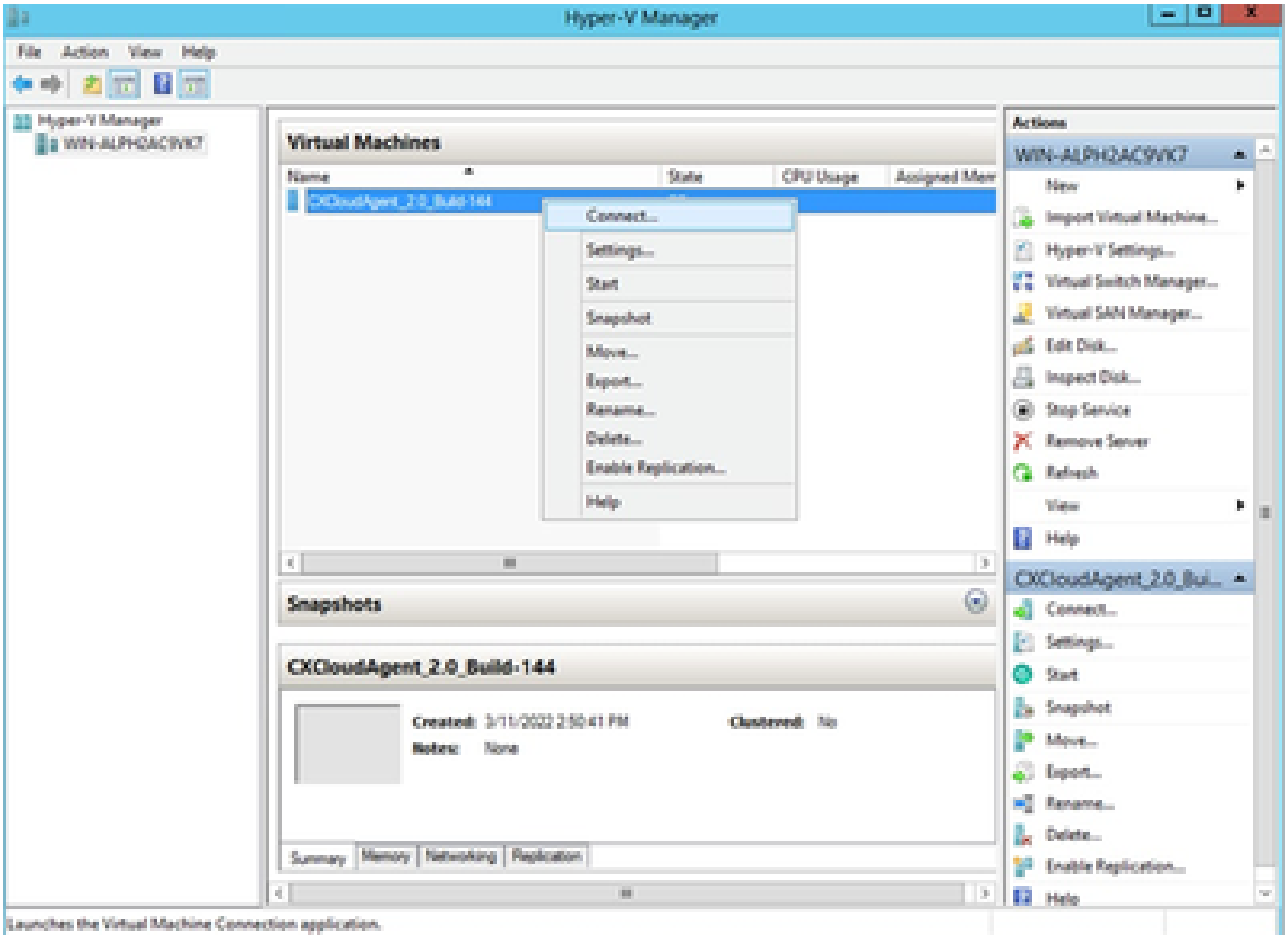
10. Verify all inputs and click **Finish**.
11. Once the import is successfully complete, a new VM is created on Hyper-V. Open the VM settings.



Settings for CXCloudAgent_2.0_Build-144 on WIN-ALPH2AC9VK7
CXCloudAgent_2.0_Build-144
Hardware
Add Hardware
BIOS
Boot from CD
Memory
16384 MB
Processor
8 Virtual processors
IDE Controller 0
Hard Drive
disk-0.vhdx
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
Not connected
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
CXCloudAgent_2.0_Build-144
Integration Services
All services offered
Snapshot File Location
C:\ProgramData\Microsoft\Win...
Smart Paging File Location
C:\ProgramData\Microsoft\Win...
Automatic Start Action
Restart if previously running
Network Adapter
Specify the configuration of the network adapter or remove the network adapter.
Virtual switch:
Not connected
Not connected
External-Switch
Enable virtual LAN identification
The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.
2
Bandwidth Management
Enable bandwidth management
Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.
Minimum bandwidth:
0
Mbps
Maximum bandwidth:
0
Mbps
To leave the minimum or maximum unrestricted, specify 0 as the value.
To remove the network adapter from this virtual machine, click Remove.
Remove
Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.
OK
Cancel
Apply

Virtual Switch

12. Select the **Network Adaptor** from the left panel and select the available **Virtual Switch** from the drop-down list.

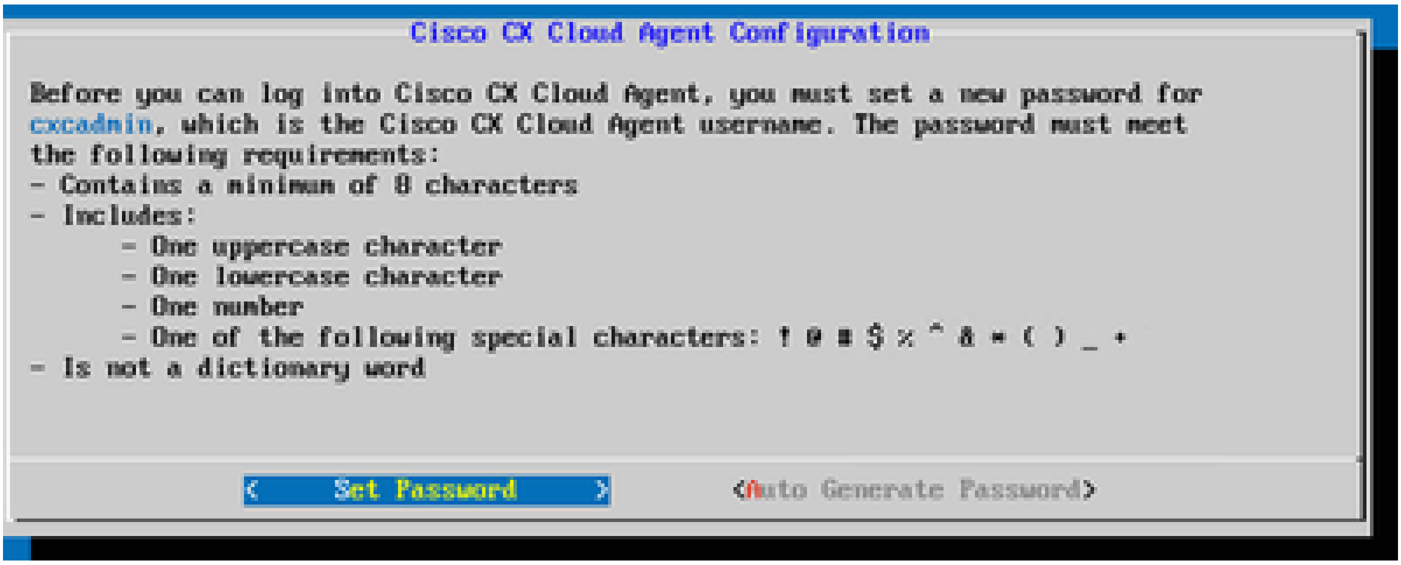


Starting VM

13. Select **Connect** to start the VM.
14. Navigate to Network Configuration to proceed with the next steps.

Network Configuration

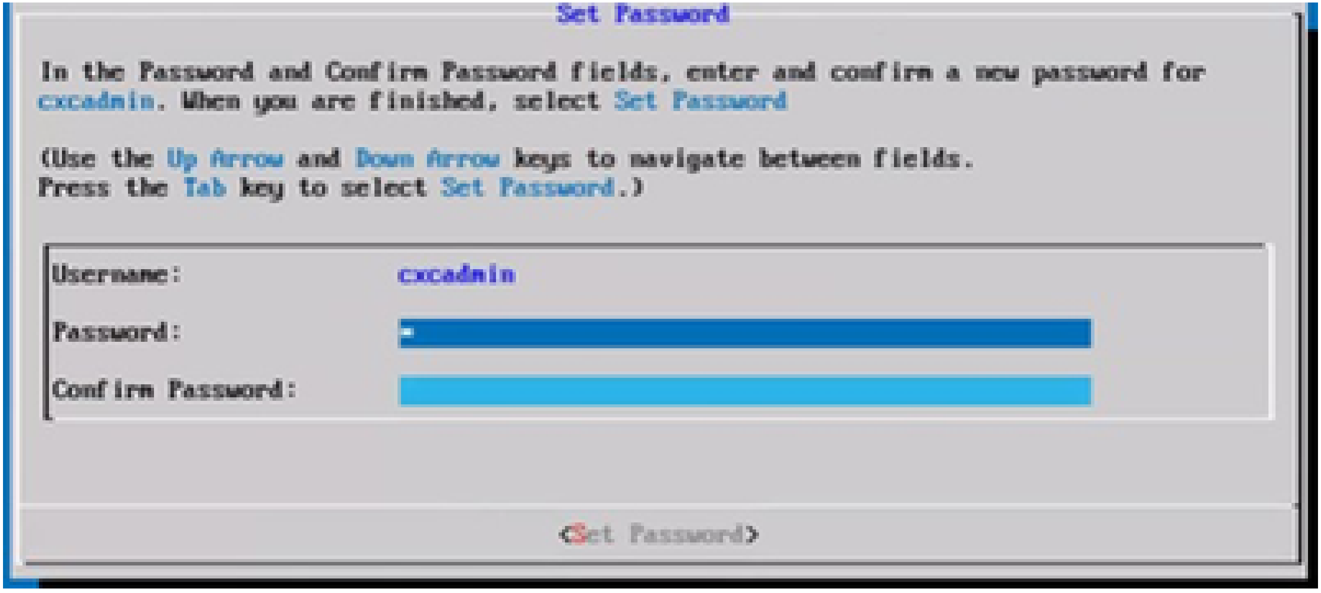
To set the CX Cloud Agent password for the *cxcadmin* username:



```
Cisco CX Cloud Agent Configuration

Before you can log into Cisco CX Cloud Agent, you must set a new password for
cxcadmin, which is the Cisco CX Cloud Agent username. The password must meet
the following requirements:
- Contains a minimum of 8 characters
- Includes:
      - One uppercase character
      - One lowercase character
      - One number
      - One of the following special characters: ! @ # $ % ^ & * ( ) _ +
- Is not a dictionary word
```

Set Password

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



Set Password

In the Password and Confirm Password fields, enter and confirm a new password for cxcadmin. When you are finished, select Set Password

(Use the Up Arrow and Down Arrow keys to navigate between fields.
Press the Tab key to select Set Password.)

Username: cxcadmin

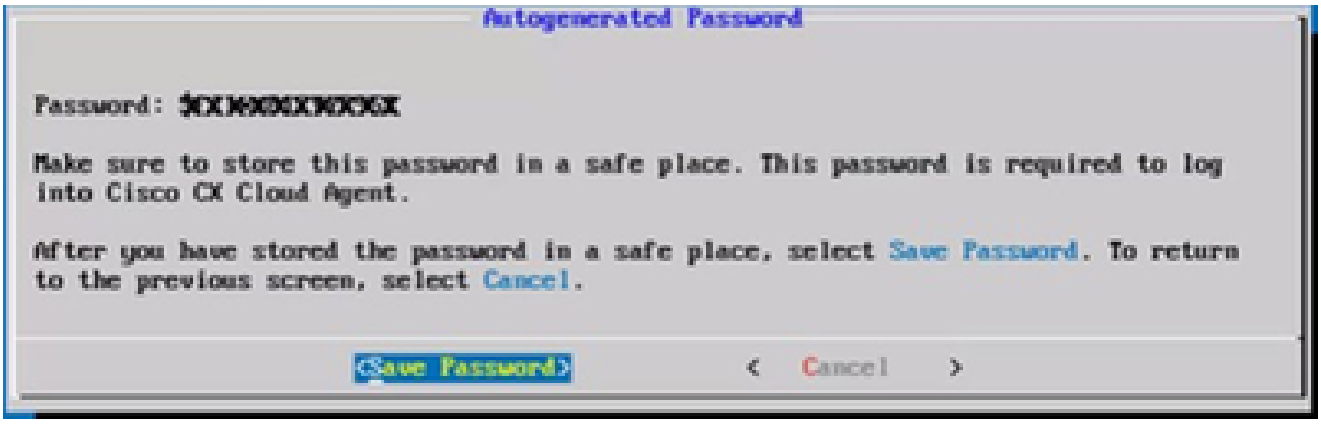
Password:

Confirm Password:

New Password

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



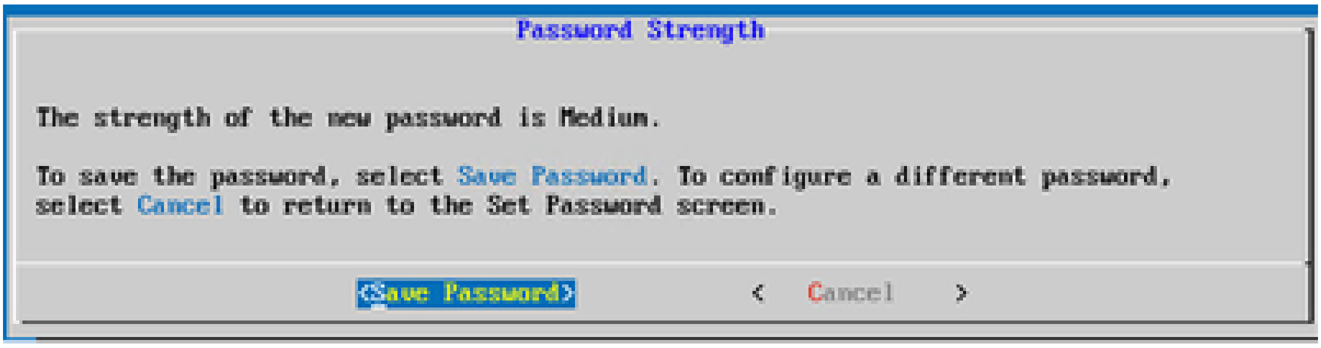
Autogenerated Password

Password: XXXXXXXXXX

Make sure to store this password in a safe place. This password is required to log into Cisco CX Cloud Agent.

After you have stored the password in a safe place, select Save Password. To return to the previous screen, select Cancel.

Auto Generated Password



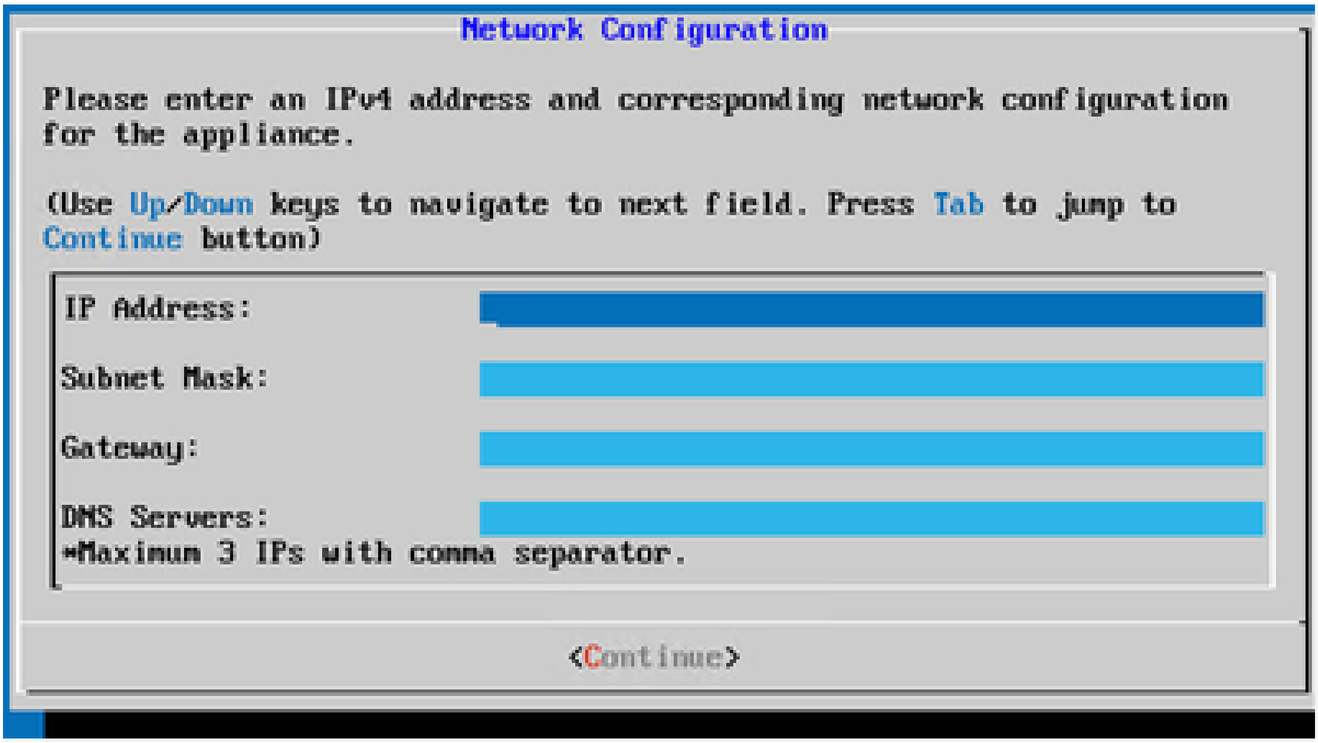
Password Strength

The strength of the new password is Medium.

To save the password, select Save Password. To configure a different password, select Cancel to return to the Set Password screen.

Save Password

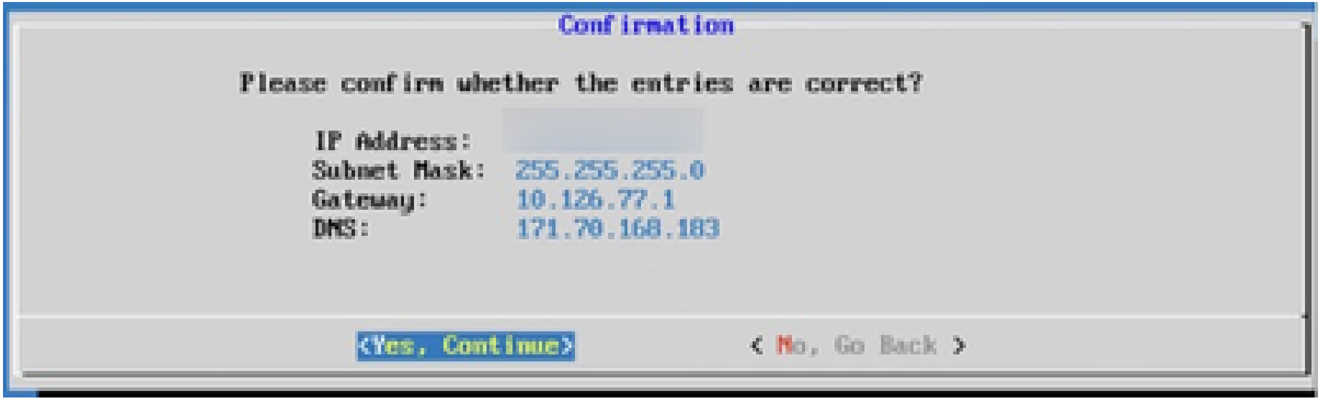
3. Click **Save Password** to use it for authentication.



```
                    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:
Subnet Mask:
Gateway:
DNS Servers:
*Maximum 3 IPs with comma separator.

                         <Continue>
```

Network Configuration

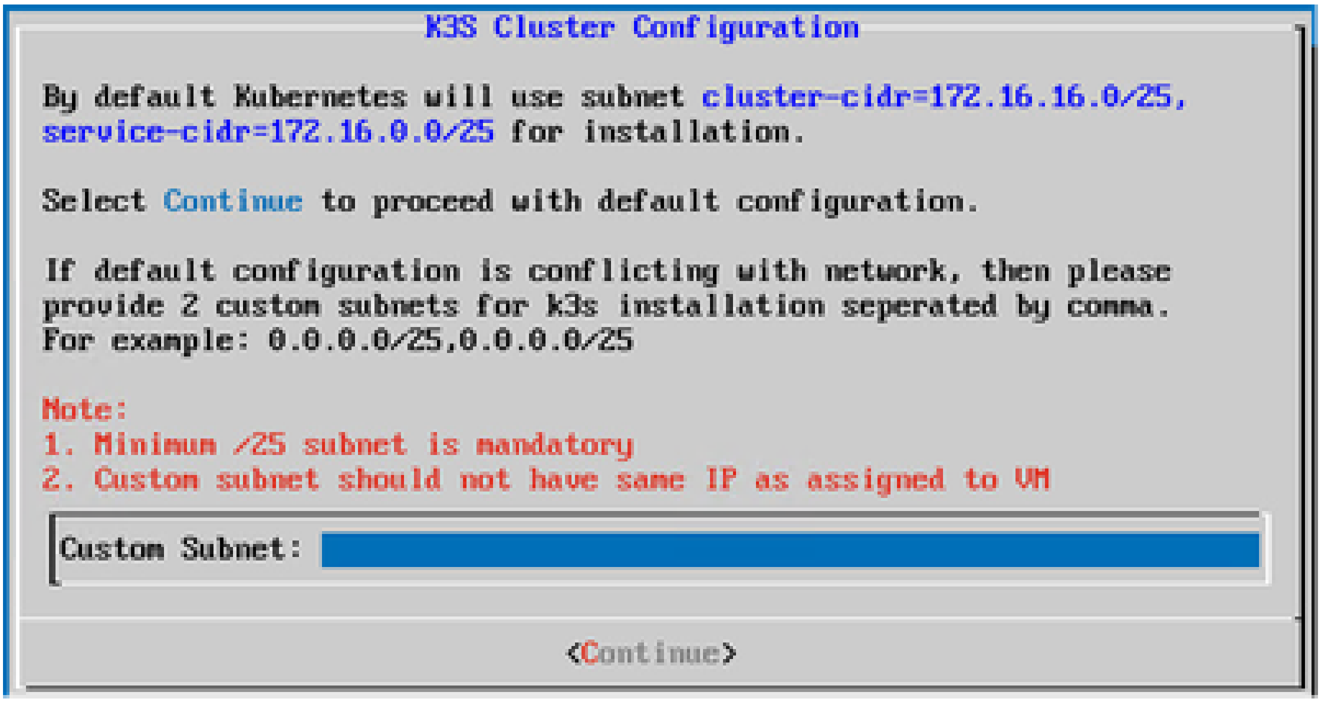
4. Enter the **IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server** and click **Continue**.



```
                        Confirmation

        Please confirm whether the entries are correct?

              IP Address:    [redacted]
              Subnet Mask:   255.255.255.0
              Gateway:       10.126.77.1
              DNS:           171.70.168.183

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

Confirmation

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



K3S Cluster Configuration

By default Kubernetes will use subnet cluster-cidr=172.16.16.0/25, service-cidr=172.16.0.0/25 for installation.

Select Continue to proceed with default configuration.

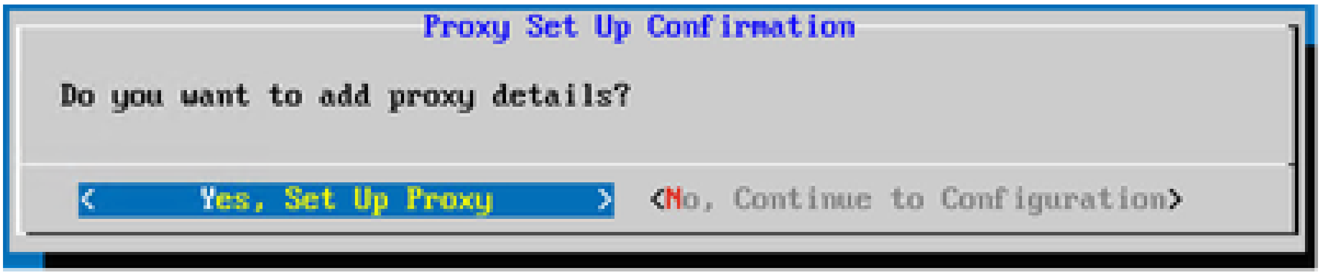
If default configuration is conflicting with network, then please provide 2 custom subnets for k3s installation seperated by comma. For example: 0.0.0.0/25,0.0.0.0/25

Note:
1. Minimum /25 subnet is mandatory
2. Custom subnet should not have same IP as assigned to VM

Custom Subnet:

Custom Subnet

6. Enter the **Custom Subnet** IP for the K3S cluster configuration (if a customer's default subnet conflicts with their devices network, select another custom subnet).
7. Click **Continue**.

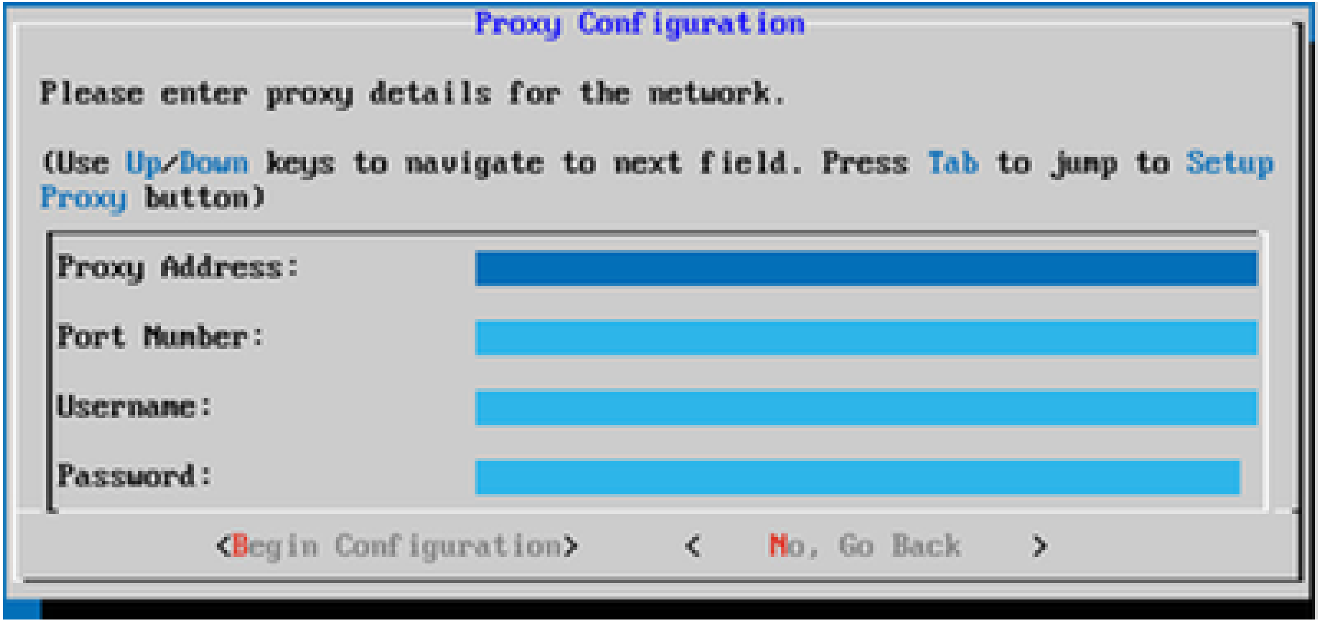


Proxy Set Up Confirmation

Do you want to add proxy details?

Proxy Set Up

8. Click **Yes, Set Up Proxy** to set the proxy details or click **No, Continue to Configuration** to directly proceed to Step 11.



Proxy Configuration

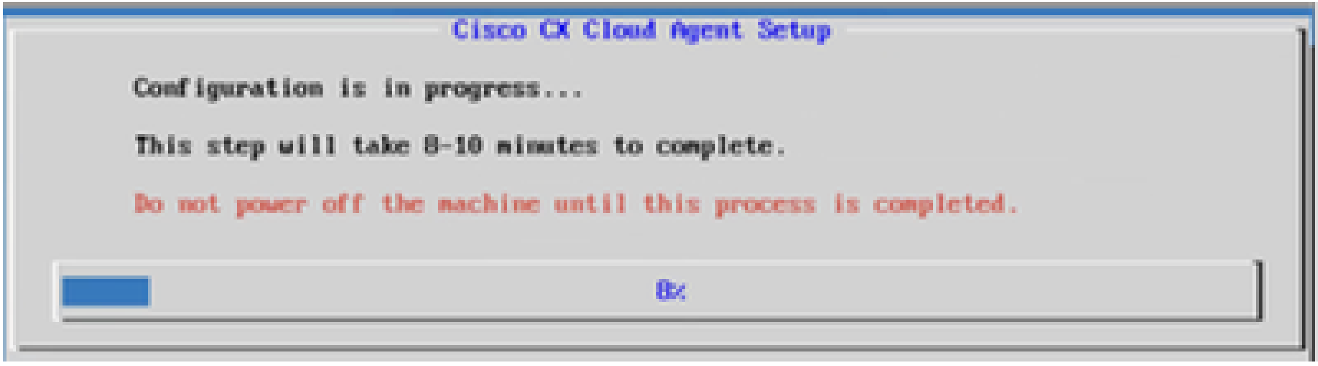
Please enter proxy details for the network.

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

Proxy Address:
Port Number:
Username:
Password:

Proxy Configuration

9. Enter the **Proxy Address**, **Port Number**, **Username**, and **Password**.
10. Click **Begin Configuration**.



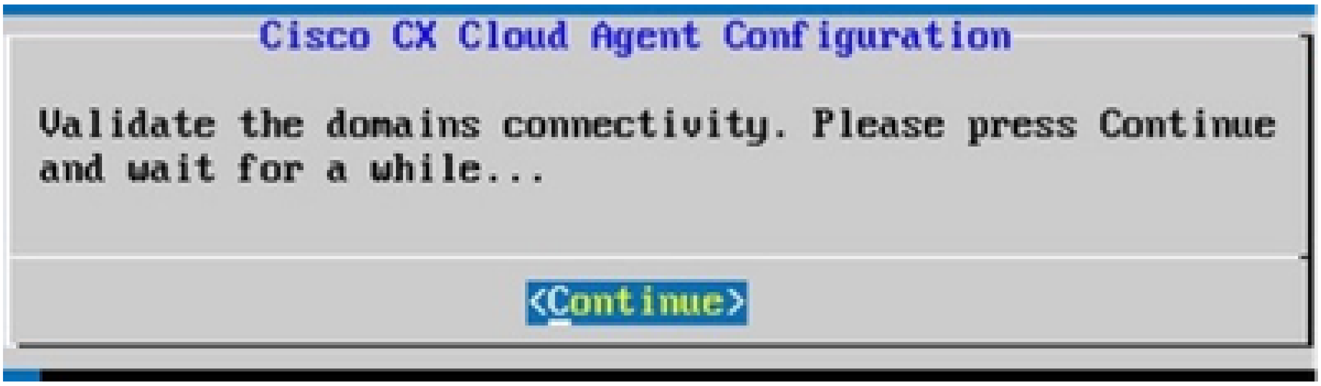
Cisco CX Cloud Agent Setup

Configuration is in progress...

This step will take 8-10 minutes to complete.

Do not power off the machine until this process is completed.

CX Cloud Agent Set Up

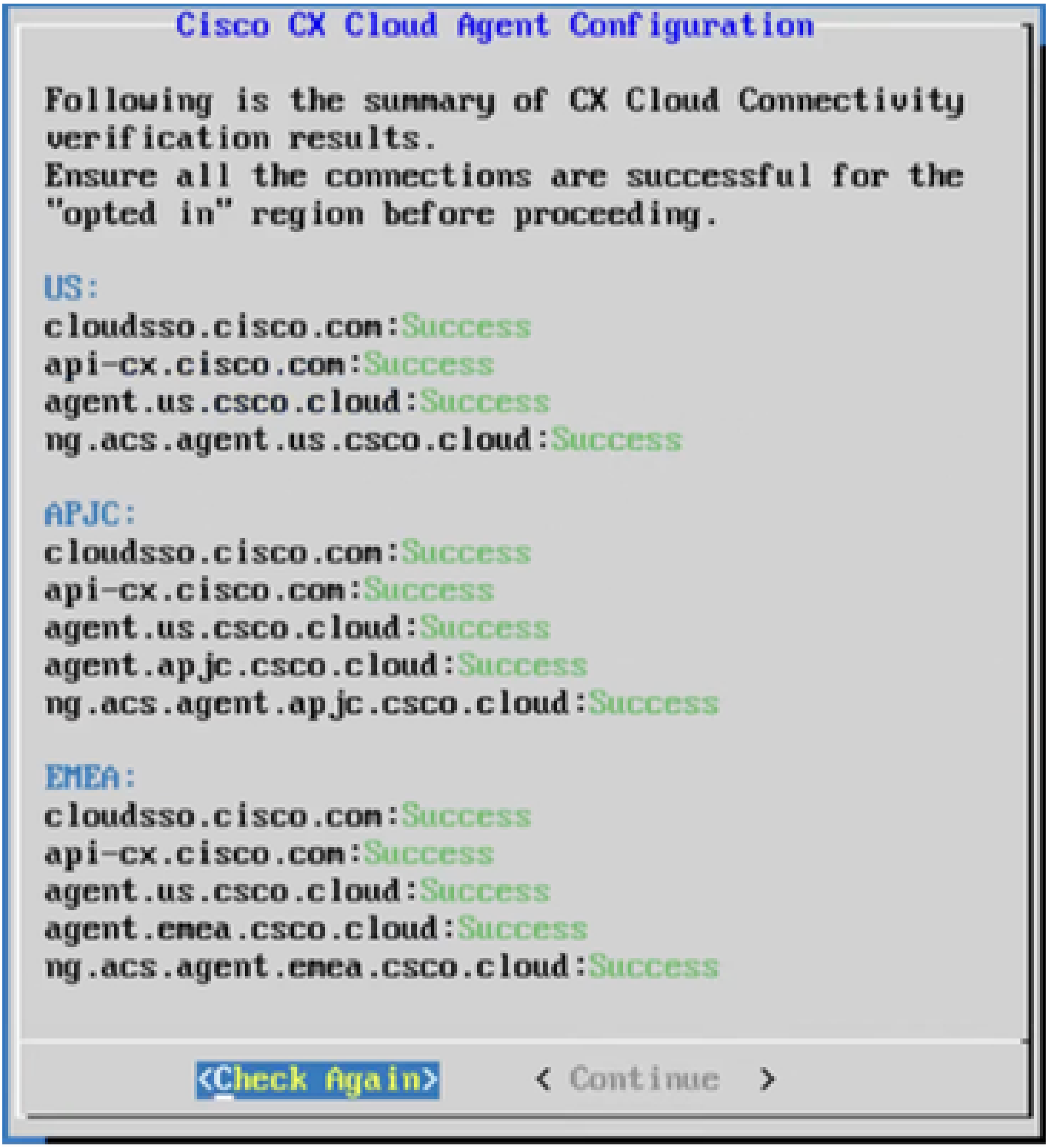


Cisco CX Cloud Agent Configuration

Validate the domains connectivity. Please press Continue and wait for a while...

CX Cloud Agent Configuration

11. Click **Continue.**

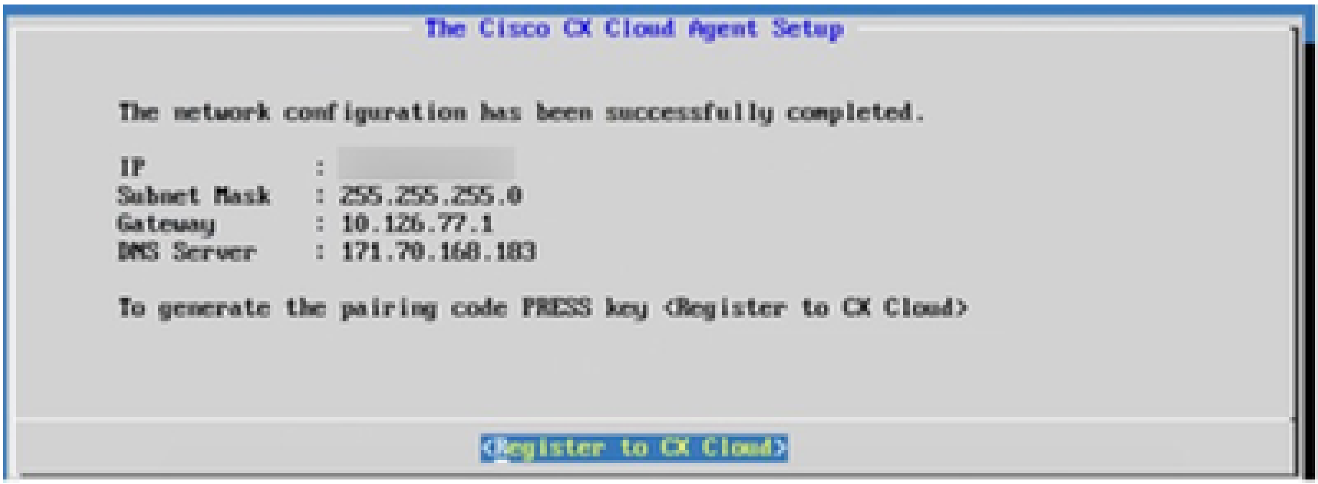


```
Cisco CX Cloud Agent Configuration

Following is the summary of CX Cloud Connectivity
verification results.
Ensure all the connections are successful for the
"opted in" region before proceeding.

US:
cloudsso.cisco.com:Success
api-cx.cisco.com:Success
agent.us.csco.cloud:Success
ng.acs.agent.us.csco.cloud:Success

APJC:
cloudsso.cisco.com:Success
api-cx.cisco.com:Success
agent.us.csco.cloud:Success
agent.apjc.csco.cloud:Success
ng.acs.agent.apjc.csco.cloud:Success

EMEA:
cloudsso.cisco.com:Success
api-cx.cisco.com:Success
agent.us.csco.cloud:Success
agent.emea.csco.cloud:Success
ng.acs.agent.emea.csco.cloud:Success
```

Configuration Continues

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

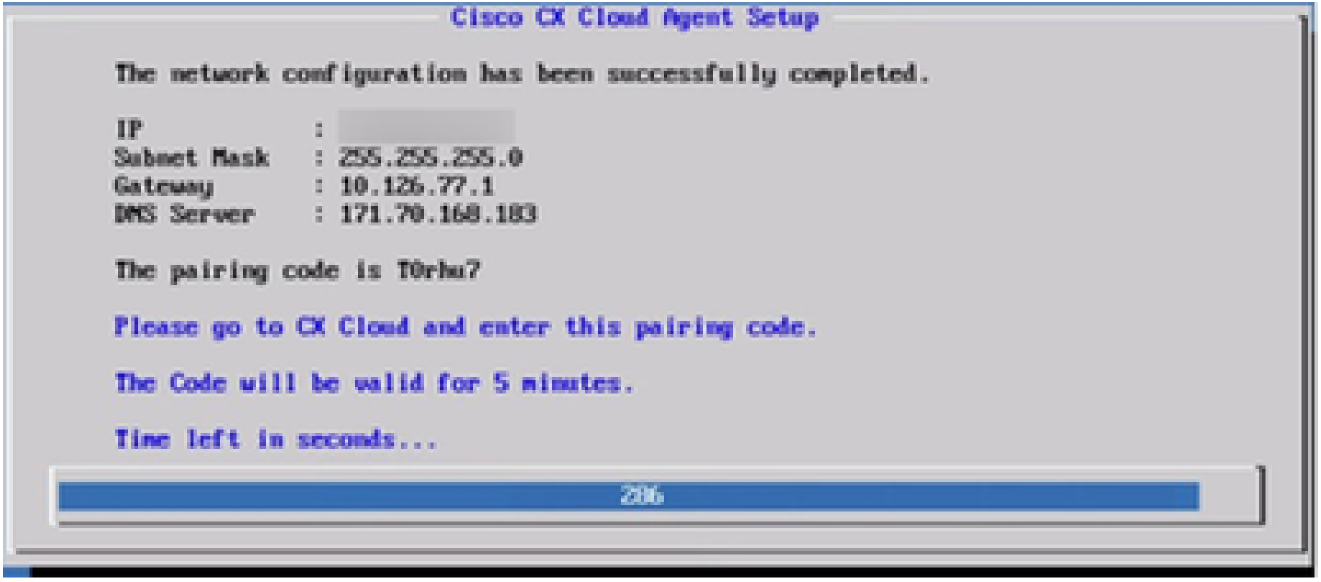
> **Note**: If the domains cannot be reached successfully, the customer must fix domain reachability by making changes in their firewall to ensure that domains are reachable. Click **Check Again** once the domains reachability issue is resolved.



```
The Cisco CX Cloud Agent Setup

The network configuration has been successfully completed.

IP            : [redacted]
Subnet Mask   : 255.255.255.0
Gateway       : 10.126.77.1
DNS Server    : 171.70.168.183

To generate the pairing code PRESS key <Register to CX Cloud>

<Register to CX Cloud>
```

Register to CX Cloud

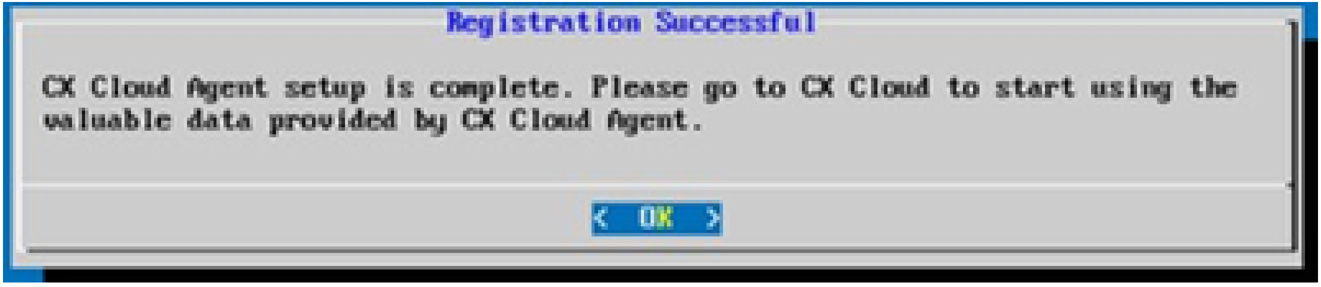
13. Click **Register to CX Cloud** to obtain pairing code.



```
Cisco CX Cloud Agent Setup

The network configuration has been successfully completed.

IP            : [redacted]
Subnet Mask   : 255.255.255.0
Gateway       : 10.126.77.1
DNS Server    : 171.70.168.183

The pairing code is T0rhu7

Please go to CX Cloud and enter this pairing code.

The Code will be valid for 5 minutes.

Time left in seconds...

286
```

Pairing Code

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



```
Registration Successful

CX Cloud Agent setup is complete. Please go to CX Cloud to start using the
valuable data provided by CX Cloud Agent.

< OK >
```

Registration Successful

✎ **Note**: If the pairing code expires, click **Register to CX Cloud** to generate new pairing code (Step 13).

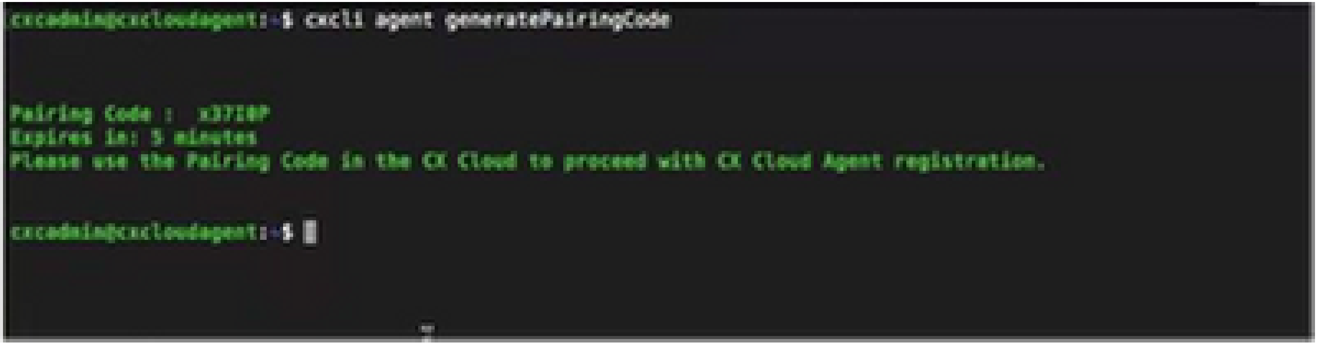
15. Click **OK**.

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 :  x37I0P
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.

Configuring Devices To Forward Syslog to CX Cloud Agent

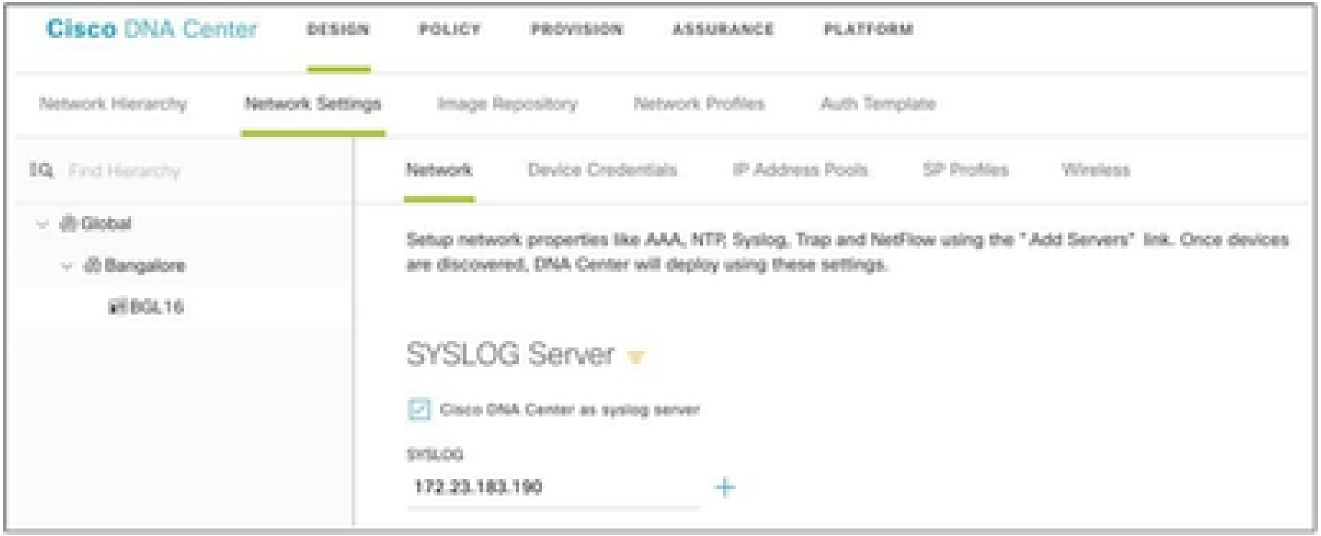
Prerequisites

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 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 Agent IP as the Syslog Server.



Setup network properties like AAA, NTP, Syslog, Trap and NetFlow using the " Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings.

SYSLOG Server

☑ Cisco DNA Center as syslog server

SYSLOG: 172.23.183.190

Syslog Server

Note: Once configured, all devices associated with that site are configured to send syslog with level critical to CX 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.

Configuring Other Assets (Direct Device Collection) to Forward Syslog to CX Agent

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

Note: The CX Agent only reports syslog information from Campus Success Track Level 2 assets to CX Cloud. Other assets are prevented from having their syslog configured to CX Agent and do not have their syslog data reported in CX Cloud.

Existing Syslog Servers with Forward Capability

Perform the configuration instructions for the syslog server software and add the CX 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 Agent IP Address. Refer to this documentation for specific configuration steps.

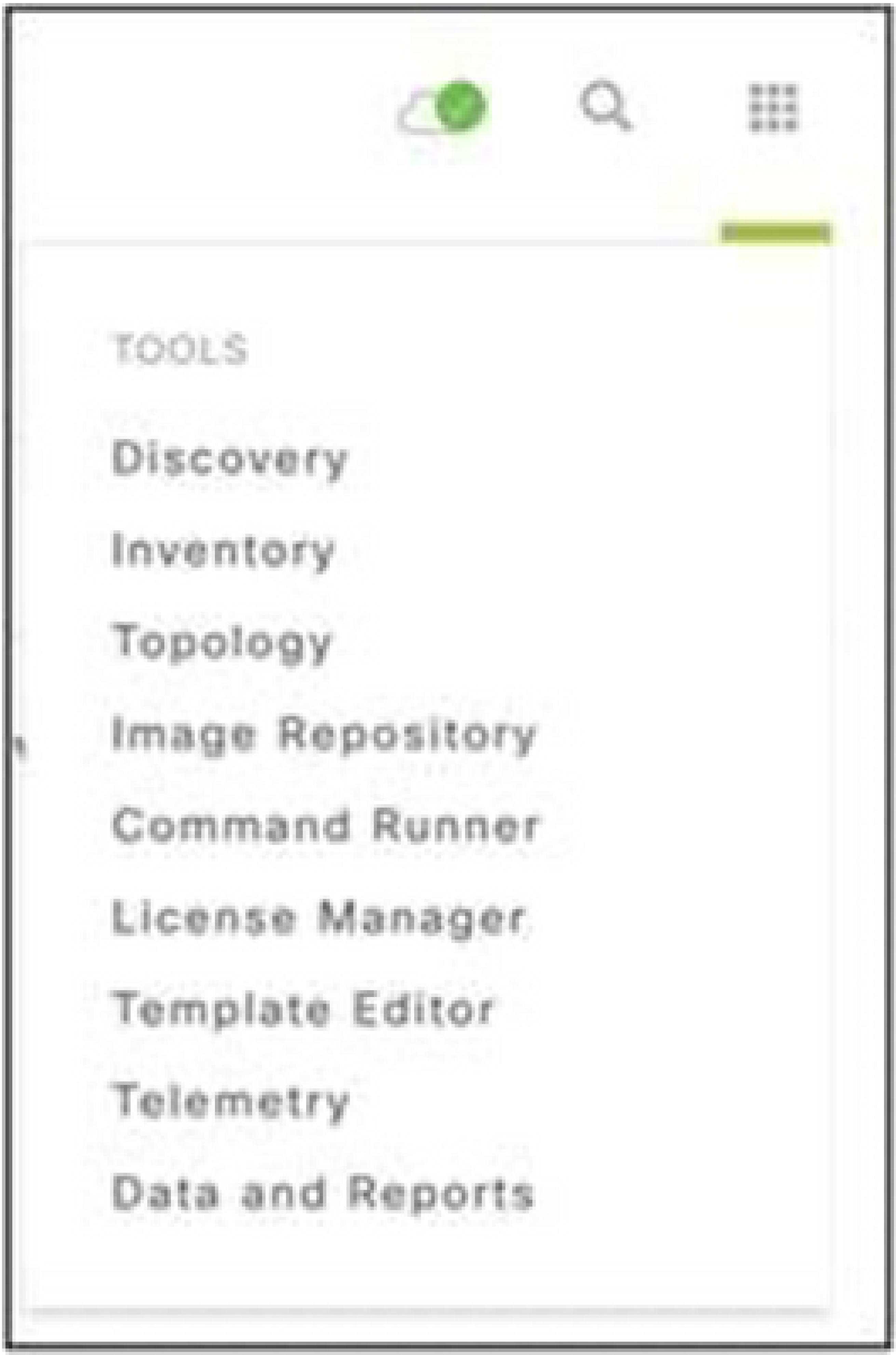
Cisco IOS® XE Configuration Guide

AireOS Wireless Controller Configuration Guide

Enabling Information Level Syslog Settings for Cisco Catalyst Center

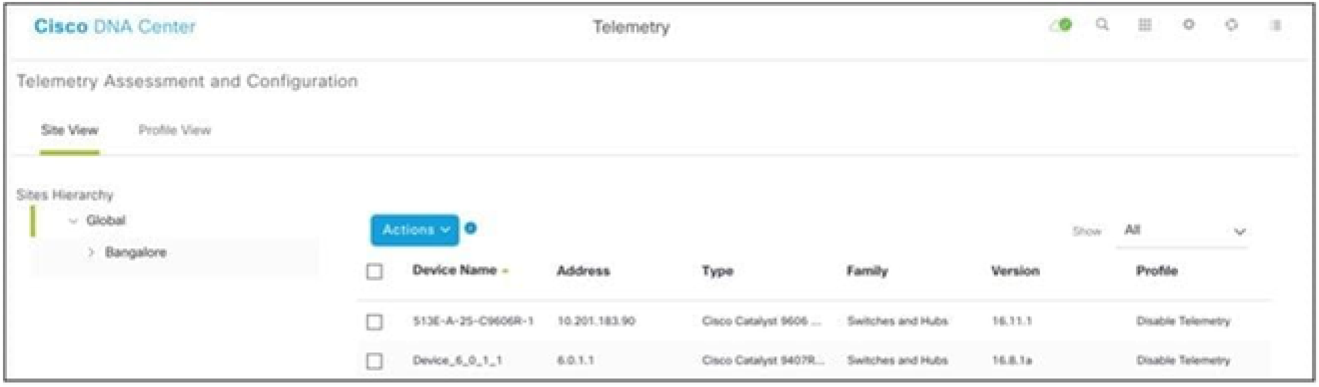
To make Syslog Information level visible, perform these steps:

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


TOOLS
Discovery
Inventory
Topology
Image Repository
Command Runner
License Manager
Template Editor
Telemetry
Data and Reports

Tools Menu

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



Cisco DNA Center — Telemetry

Telemetry Assessment and Configuration

Site View | Profile View

Sites Hierarchy
- Global
  - Bangalore

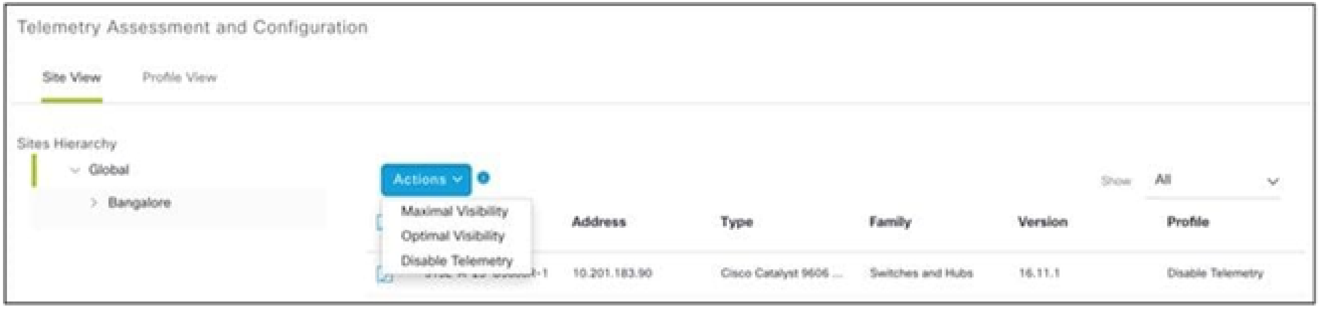
Actions ▾   Show: All

☐	Device Name	Address	Type	Family	Version	Profile
☐	513E-A-25-C9606R-1	10.201.183.90	Cisco Catalyst 9606 ...	Switches and Hubs	16.11.1	Disable Telemetry
☐	Device_6_0_1_1	6.0.1.1	Cisco Catalyst 9407R...	Switches and Hubs	16.8.1a	Disable Telemetry

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.



Telemetry Assessment and Configuration

Site View | Profile View

Sites Hierarchy
- Global
  - Bangalore

Actions ▾   Show: All

☑		Address	Type	Family	Version	Profile
☑	[illegible]-1	10.201.183.90	Cisco Catalyst 9606 ...	Switches and Hubs	16.11.1	Disable Telemetry

Actions

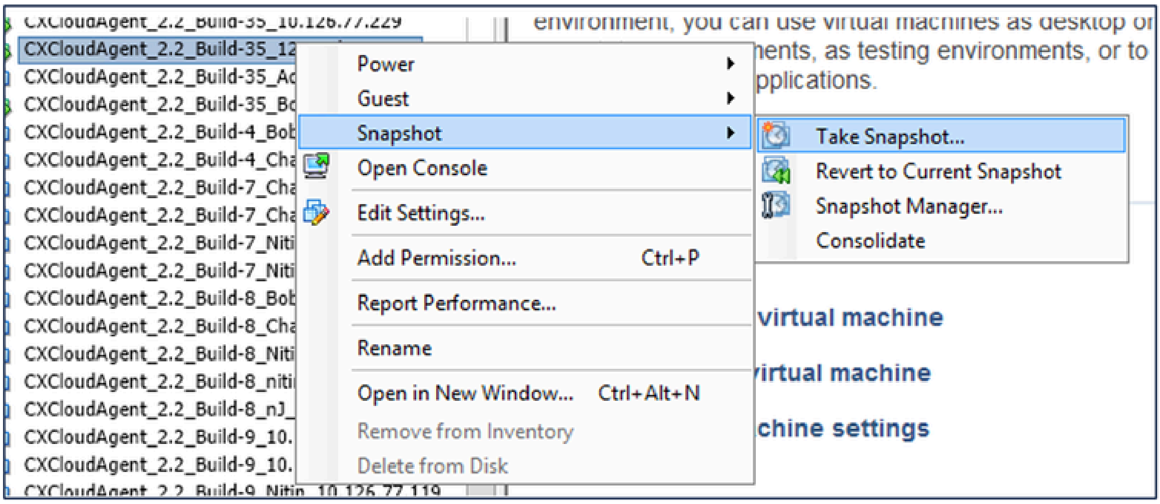
Backing Up and Restoring the CX Cloud VM

It is recommended to preserve the state and data of a CX 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.

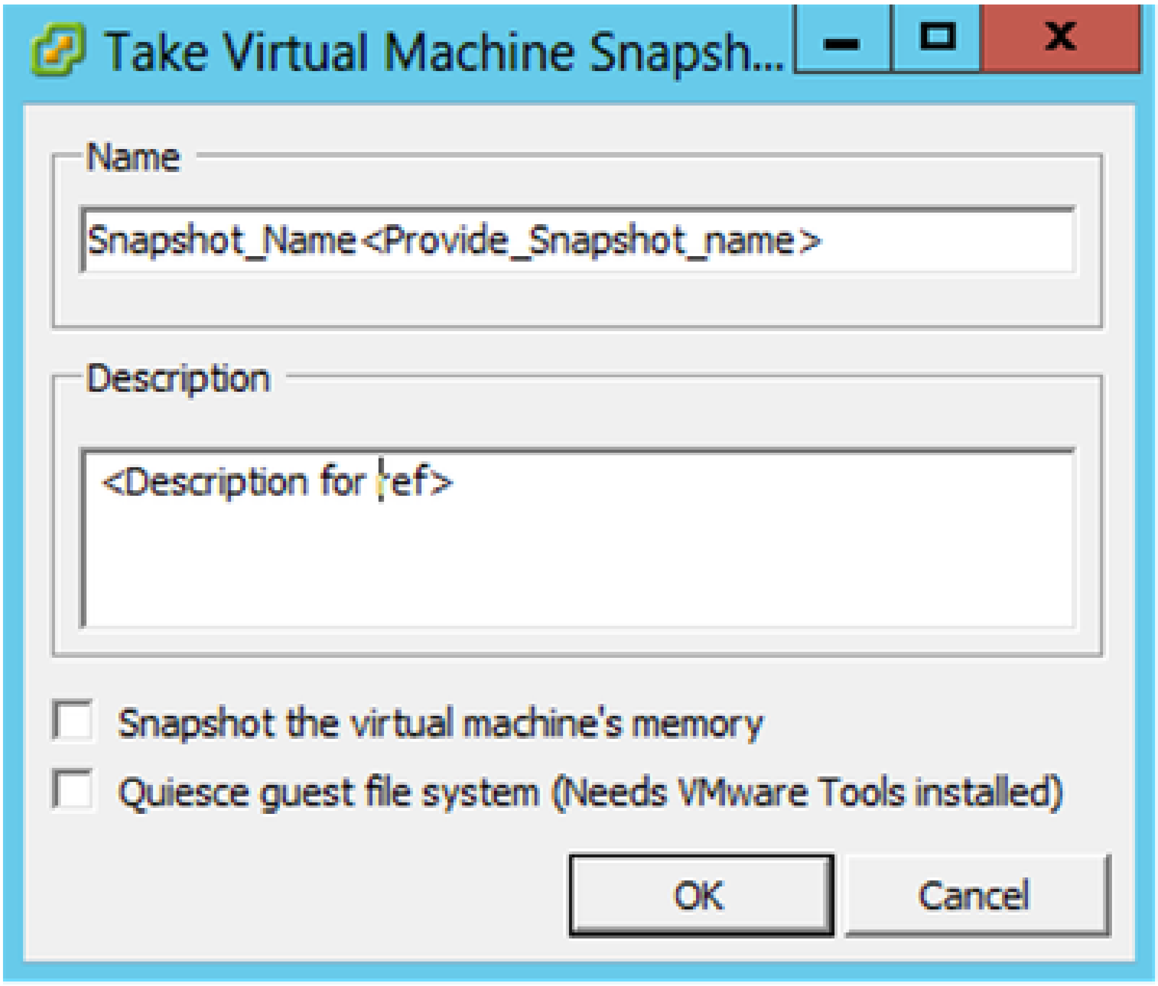
Backing Up the CX Cloud VM

To back up the CX Cloud VM:

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


CXCloudAgent_2.2_Build-35_10.126.77.229
CXCloudAgent_2.2_Build-35_12
CXCloudAgent_2.2_Build-35_Ad
CXCloudAgent_2.2_Build-35_Bo
CXCloudAgent_2.2_Build-4_Bob
CXCloudAgent_2.2_Build-4_Cha
CXCloudAgent_2.2_Build-7_Cha
CXCloudAgent_2.2_Build-7_Cha
CXCloudAgent_2.2_Build-7_Niti
CXCloudAgent_2.2_Build-7_Niti
CXCloudAgent_2.2_Build-8_Bob
CXCloudAgent_2.2_Build-8_Cha
CXCloudAgent_2.2_Build-8_Niti
CXCloudAgent_2.2_Build-8_niti
CXCloudAgent_2.2_Build-8_nJ_
CXCloudAgent_2.2_Build-9_10.
CXCloudAgent_2.2_Build-9_10.
CXCloudAgent_2.2_Build-9_Nitin_10.126.77.119
Power
Guest
Snapshot
Open Console
Edit Settings...
Add Permission... Ctrl+P
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk
Take Snapshot...
Revert to Current Snapshot
Snapshot Manager...
Consolidate
environment, you can use virtual machines as desktop or
nents, as testing environments, or to
pplications.
virtual machine
irtual machine
chine settings

Select VM



Name

Snapshot_Name<Provide_Snapshot_name>

Description

<Description for ¦ef>

□ Snapshot the virtual machine's memory

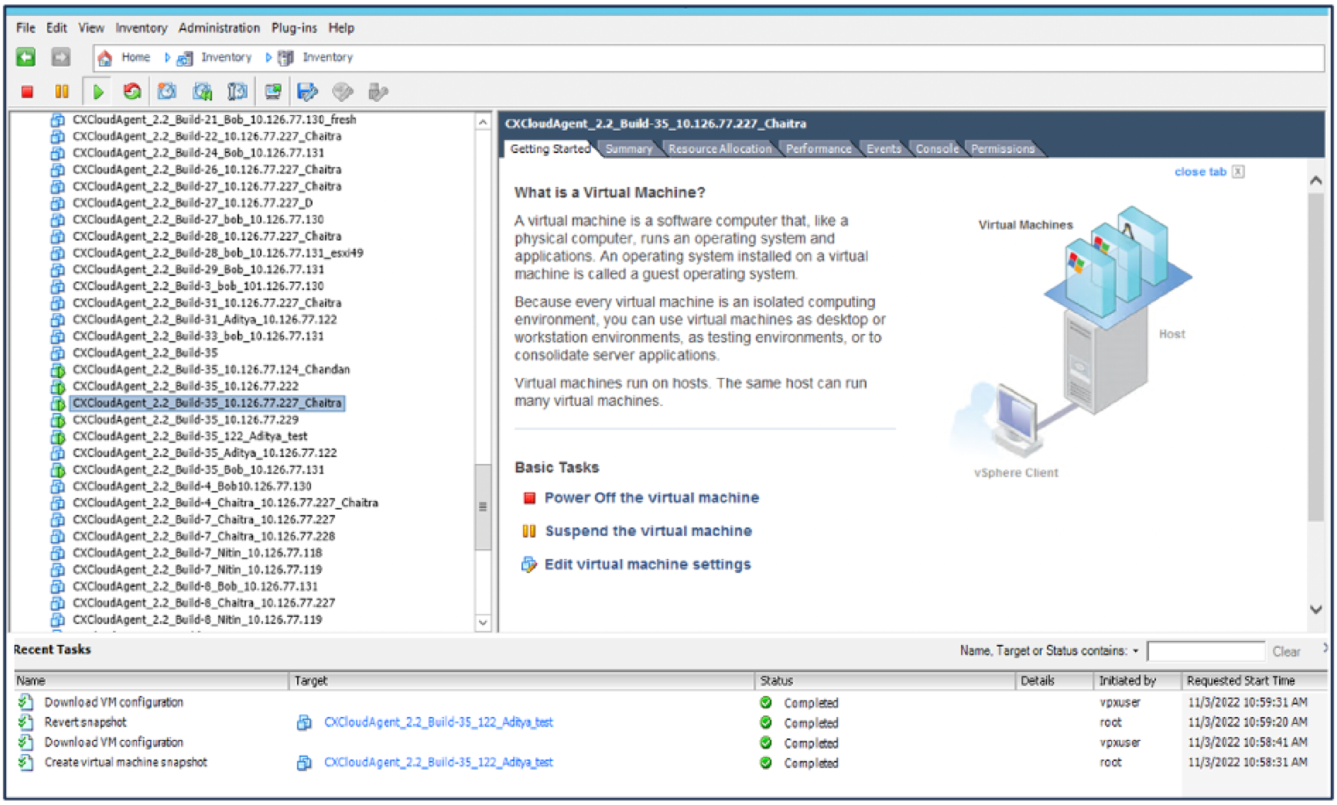
□ Quiesce guest file system (Needs VMware Tools installed)

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.


File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
CXCloudAgent_2.2_Build-21_Bob_10.126.77.130_fresh
CXCloudAgent_2.2_Build-22_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-24_Bob_10.126.77.131
CXCloudAgent_2.2_Build-26_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-27_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-27_10.126.77.227_D
CXCloudAgent_2.2_Build-27_bob_10.126.77.130
CXCloudAgent_2.2_Build-28_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-28_bob_10.126.77.131_esxi49
CXCloudAgent_2.2_Build-29_Bob_10.126.77.131
CXCloudAgent_2.2_Build-3_bob_101.126.77.130
CXCloudAgent_2.2_Build-31_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-31_Aditya_10.126.77.122
CXCloudAgent_2.2_Build-33_bob_10.126.77.131
CXCloudAgent_2.2_Build-35
CXCloudAgent_2.2_Build-35_10.126.77.124_Chandan
CXCloudAgent_2.2_Build-35_10.126.77.222
CXCloudAgent_2.2_Build-35_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-35_10.126.77.229
CXCloudAgent_2.2_Build-35_122_Aditya_test
CXCloudAgent_2.2_Build-35_Aditya_10.126.77.122
CXCloudAgent_2.2_Build-35_Bob_10.126.77.131
CXCloudAgent_2.2_Build-4_Bob10.126.77.130
CXCloudAgent_2.2_Build-4_Chaitra_10.126.77.227_Chaitra
CXCloudAgent_2.2_Build-7_Chaitra_10.126.77.227
CXCloudAgent_2.2_Build-7_Chaitra_10.126.77.228
CXCloudAgent_2.2_Build-7_Nitin_10.126.77.118
CXCloudAgent_2.2_Build-7_Nitin_10.126.77.119
CXCloudAgent_2.2_Build-8_Bob_10.126.77.131
CXCloudAgent_2.2_Build-8_Chaitra_10.126.77.227
CXCloudAgent_2.2_Build-8_Nitin_10.126.77.119
CXCloudAgent_2.2_Build-35_10.126.77.227_Chaitra
Getting Started
Summary
Resource Allocation
Performance
Events
Console
Permissions
close tab
Virtual Machines
Host
vSphere Client

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.

Basic Tasks

- Power Off the virtual machine
- Suspend the virtual machine
- Edit virtual machine settings

Recent Tasks

Name, Target or Status contains: Clear

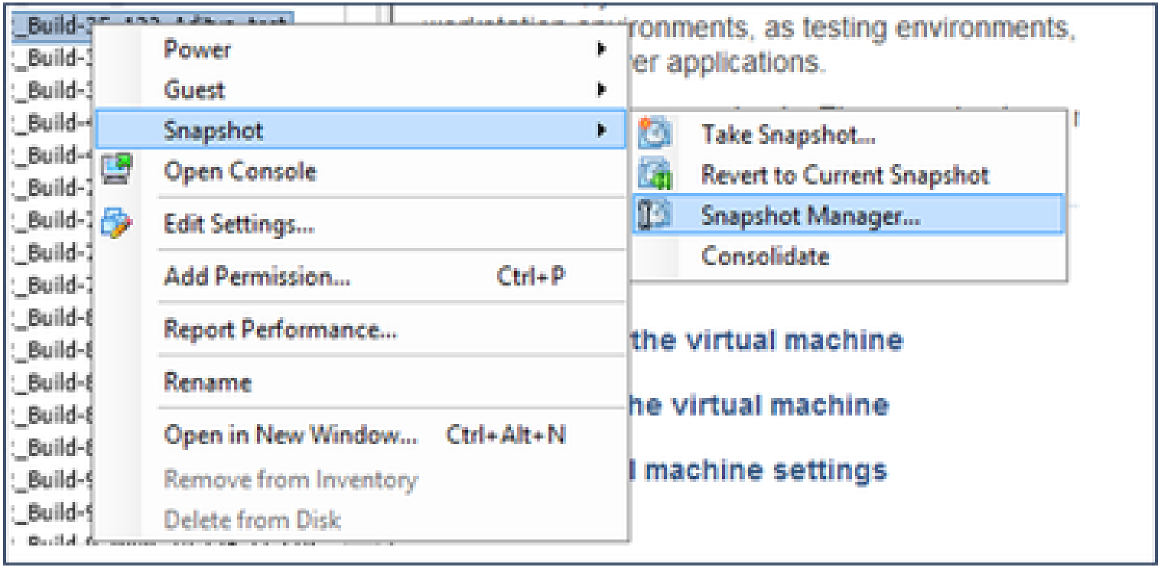
Name	Target	Status	Details	Initiated by	Requested Start Time
Download VM configuration		Completed		vpxuser	11/3/2022 10:59:31 AM
Revert snapshot	CXCloudAgent_2.2_Build-35_122_Aditya_test	Completed		root	11/3/2022 10:59:20 AM
Download VM configuration		Completed		vpxuser	11/3/2022 10:58:41 AM
Create virtual machine snapshot	CXCloudAgent_2.2_Build-35_122_Aditya_test	Completed		root	11/3/2022 10:58:31 AM

Recent Tasks

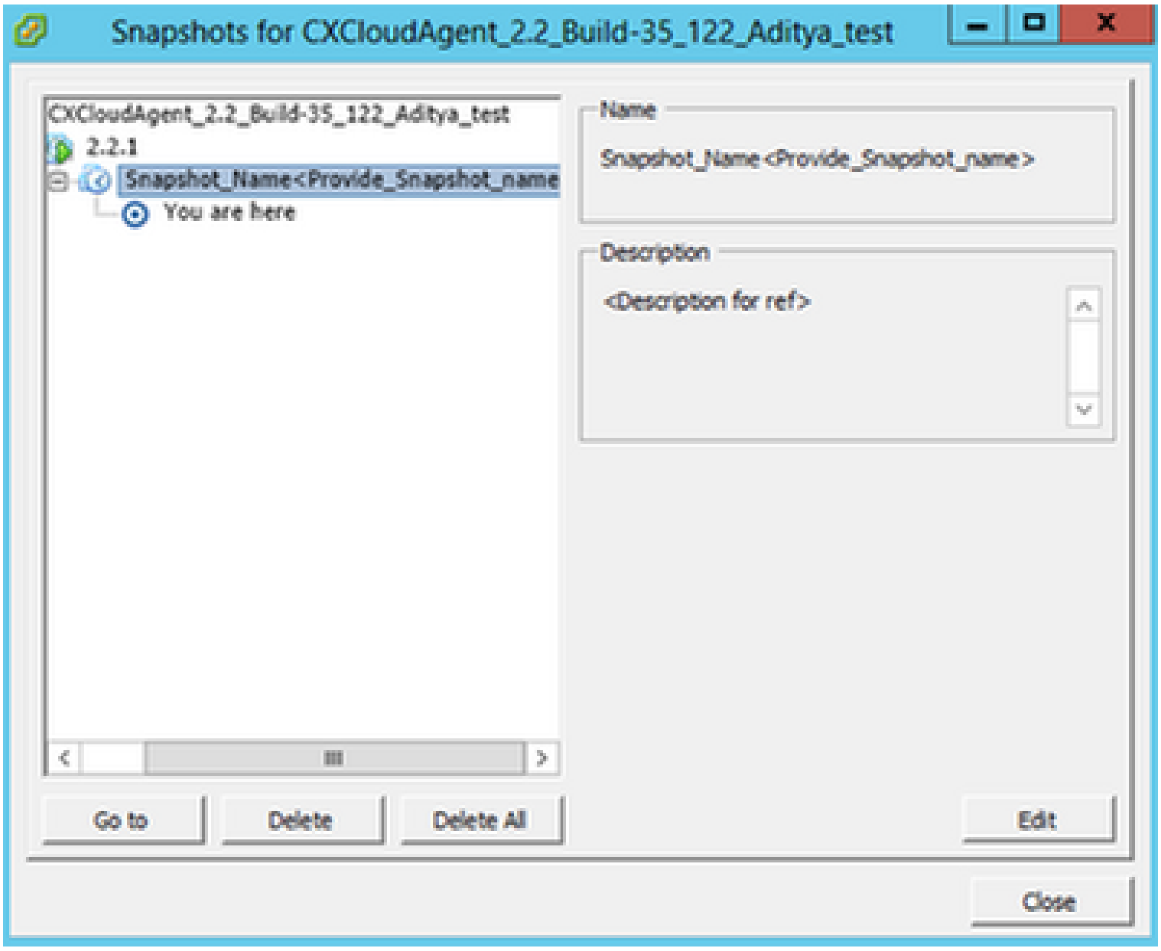
Restoring the CX Cloud VM

To restore the CX Cloud VM:

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

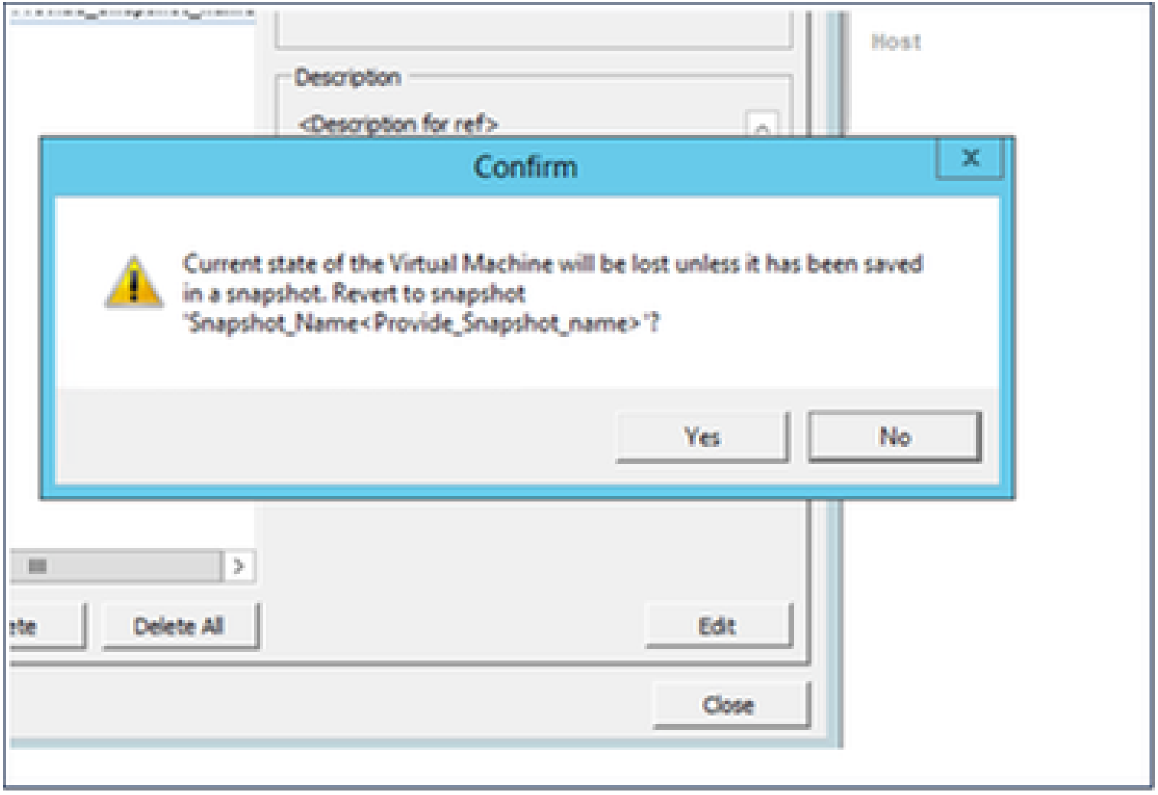


Select VM window


Snapshots for CXCloudAgent_2.2_Build-35_122_Aditya_test
CXCloudAgent_2.2_Build-35_122_Aditya_test
2.2.1
Snapshot_Name<Provide_Snapshot_name
You are here
Name
Snapshot_Name<Provide_Snapshot_name>
Description
<Description for ref>
Go to
Delete
Delete All
Edit
Close

Snapshots Window

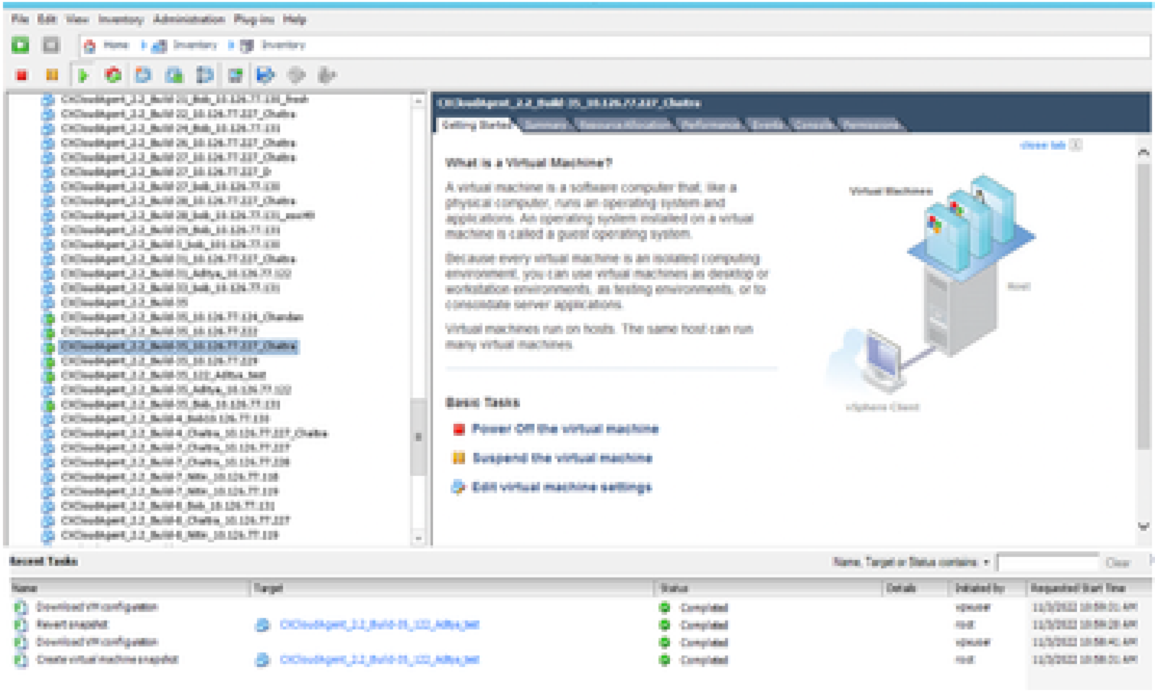
2. Click **Go to**. The **Confirm** window opens.



Current state of the Virtual Machine will be lost unless it has been saved in a snapshot. Revert to snapshot 'Snapshot_Name<Provide_Snapshot_name>'?

Confirm Window

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



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.

Basic Tasks

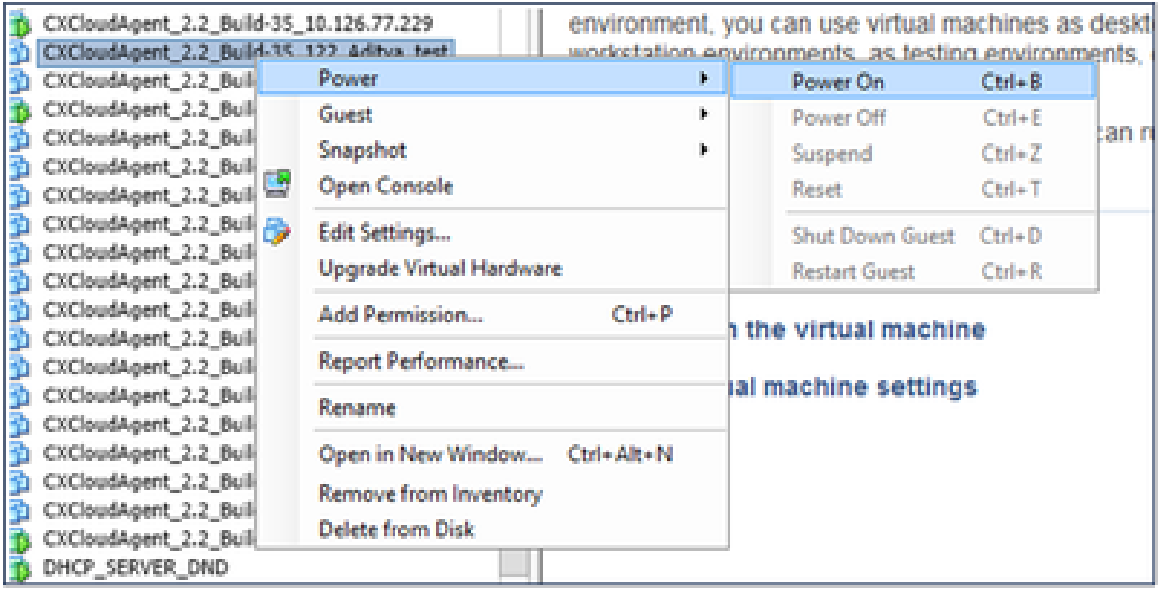
- Power Off the virtual machine
- Suspend the virtual machine
- Edit virtual machine settings

Recent Tasks

Name	Target	Status	Details	Initiated by	Requested Start Time
Download VM configuration		Completed		vpxuser	[illegible]
Revert snapshot	CXCloudAgent_2.2_Build-35_122_Aditya_test	Completed		root	[illegible]
Download VM configuration		Completed		vpxuser	[illegible]
Create virtual machine snapshot	CXCloudAgent_2.2_Build-35_122_Aditya_test	Completed		root	[illegible]

Recent Tasks

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



Security

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

Physical Security

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

Data Security

CX 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 Agent.

Sensitive information within asset telemetry is masked before being transmitted to the cloud. The CX Agent masks sensitive data for all the collected assets that send telemetry directly to the CX 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 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 Agent).

Security Summary

Security Features	**Description**
Bootloader Password	Bootloader (Single user mode) password is set with a randomly unique password. Users must refer to FAQ to set his bootloader (single user mode) password.
User Access	SSH: · Access to appliance using cxcadmin user requires credentials created during installation. · Access to appliance using cxcroot user requires credentials to be decrypted using SWIM portal by authorized personnel.
User Accounts	· cxcadmin: default user account created; User can execute CX Agent application commands using cxcli and has least privileges on the appliance; cxcroot user and its encrypted password is generated using cxcadmin user. · cxcroot: cxcadmin can create this user using the utility remoteaccount; User can gain root privileges with this account.
cxcadmin password policy	· Password is one-way hashed using SHA-256 and stored securely. · Minimum eight (8) characters, containing three of these categories: uppercase, lowercase, numbers, and special characters.
cxcroot password policy	· cxcroot password is RSA/ECB/PKCS1v1_5 encrypted · The passphrase generated needs to be decrypted in SWIM portal. · The cxcroot user and password is valid for two days and can be regenerated using cxcadmin user.

ssh login password policy	· Minimum of eight characters that contains three of these 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	· No Customer information stored. · No Device data stored. · Cisco Catalyst Center server credentials encrypted and stored in the database.