# CX Agent Overview Guide v3.1

## Contents


- **Introduction**
  - Prerequisites
  - Accessing Critical Domains
  - Domains Specific to the CX Cloud Portal
  - Domains Specific to CX Agent VM
  - Catalyst Center Supported Versions
  - Supported Browsers
  - Supported Product List
  - Upgrading/Installing CX Agent v3.1.5
  - Upgrading Existing VMs to Large and Medium Configuration
- **Upgrading to CX Agent v3.1.5**
  - Automatic Upgrades
  - Manual Upgrades
- **Adding CX Agent**
- **Configuring CX Agent for BCS/LCS**
  - Prerequisites
  - Configuring CX Agent
- **Configuring RADKit Capabilities**
  - Integrating RADKit Client Through CLI
- **Configuring Vault for Existing CX Agents**
  - Integrating CX Agent with HashiCorp Vault Through CLI
    - Prerequisites
    - Integrating with HashiCorp Vault
  - Enabling HashiCorp Vault Integration
  - Disabling HashiCorp Vault Integration
  - HashiCorp Vault Device Credentials Schema
  - Configuring Device Credentials in HashiCorp Vault (First Time)
  - Adding More Credentials to HashiCorp Vault
  - CX Cloud Seed File with Default Credentials
- **Adding Catalyst Center as Data Source**
- **Adding BCS/LCS Data Sources**
  - Adding SolarWinds®
  - Adding EPNM
  - Adding APIC
- **Adding Other Assets as Data Sources**
  - Discovery Protocols
  - Connectivity Protocols
  - Telemetry Processing Limitations for Devices
- **Adding Other Assets Using a Seed File**

- Adding Other Assets Using a New Seed File
- Adding Other Assets Using a Modified Seed File
- Default Credentials for the Seed File

## Adding Other Assets Using IP Ranges

- Adding Other Assets by IP Ranges
- Editing IP Ranges
- Deleting IP Ranges
- AboutDevices Discovered from Multiple Controllers

## Adding Other Assets Using CDP or LLDP

- Editing CDP or LLDP Details

## Scheduling Diagnostics Scans

## Upgrading CX Agent VMs to Medium and Large Configurations

- Reconfiguring Using VMware vSphere Thick Client
- Reconfiguring Using Web Client ESXi v6.0
- Reconfiguring Using Web Client vCenter

## Deployment and Network Configuration

- OVA Deployment
  - ThickClient ESXi 5.5/6.0 Installation
  - WebClient ESXi 6.0 Installation
  - WebClient vCenter Installation
  - OracleVirtual Box 7.0.12 Installation
  - MicrosoftHyper-V Installation
  - Processor Settings
  - Microsoft Hyper-V Image Signature Validation
- Network Configuration
- Alternative Approach to Generate Pairing Code Using CLI
- Configuring Devices To Forward Syslog to CX Cloud Agent
  - Prerequisites
  - Configure Syslog Forward Setting
- Configuring Other Assets (Direct Device Collection) to Forward Syslog to CX Agent
  - Existing Syslog Servers with Forward Capability
  - ExistingSyslog Servers without Forward Capability OR without Syslog Server
- Enabling Information Level Syslog Settings for Cisco Catalyst Center

## Backing Up and Restoring the CX Cloud VM

- Backing Upthe CX Cloud VM
- Restoring the CX Cloud VM

## Security

- Physical Security
- Account Security
- Network Security
- Authentication
- Hardening
- Data Security
- Data Transmission
- Logs and Monitoring
- Cisco Telemetry Commands

# 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).

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 v3.1.5 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, Windows Hyper-V |
| Large OVA | 32C | 64GB | 1200GB | 50,000 | VMware ESXi, Windows Hyper-V |

*In addition to connecting 20 Cisco Catalyst Center (Catalyst Center) non-clusters or 10 Catalyst Center

clusters for each CX Cloud Agent instance.

- 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
- 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
- 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
- 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:

| Source | Destination | Protocol | Port | Purpose | Type |
|---|---|---|---|---|---|
| CX Cloud Agent | **All Regions:**<br>◦ agent.us.csco.cloud<br>◦ Catalyst Center<br>**AMER Region:**<br>◦ ng.acs.agent.us.csco.cloud<br>◦ radkit.us.csco.cloud*<br>**EMEA Region:**<br>◦ agent.emea.csco.cloud<br>◦ ng.acs.agent.emea.csco.cloud<br>◦ radkit.emea.csco.cloud*<br>**APJC Region:** | HTTPS | TCP/443 | ◦ Initial configuration<br>◦ Upgrades<br>◦ Inventory and telemetry transfers<br>◦ Access to RADKit Cloud | Outbound to Cisco AWS regional data centers and Catalyst Center |

| | | | | | |
|---|---|---|---|---|---|
| | ◦ agent.apjc.csco.cloud<br>◦ ng.acs.agent.apjc.csco.cloud<br>◦ radkit.apjc.csco.cloud* | | | | |
| CX Cloud Agent | Network Devices | SNMP | UDP/161 | ◦ Initial discovery<br>◦ Ongoing inventory collections | Outbound to LAN |
| CX Cloud Agent | Network Devices | SSH | TCP/22 | Collection of telemetry data 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 |

*Not mandatory unless RADKit is being used.

---

**Notes**:
- An IP is automatically detected if the Dynamic Host Configuration Protocol (DHCP) is enabled in the VM environment; otherwise, a free IPv4 address, Subnet mask, Default Gateway IP address, and Domain Name Service (DNS) server IP address must be available.
- Only IPv4 is supported.
- The certified single node and High Availability (HA) Cluster 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.
- 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 should not be used.

---

## Accessing Critical Domains

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

## Domains Specific to the CX Cloud 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 VM

| **AMERICAS** | **EMEA** | **APJC** |
|---|---|---|
| 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 v3.1.5

- Existing customers upgrading to the new version should refer to Upgrading CX Agent v3.1.5

- 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 v3.1.5

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

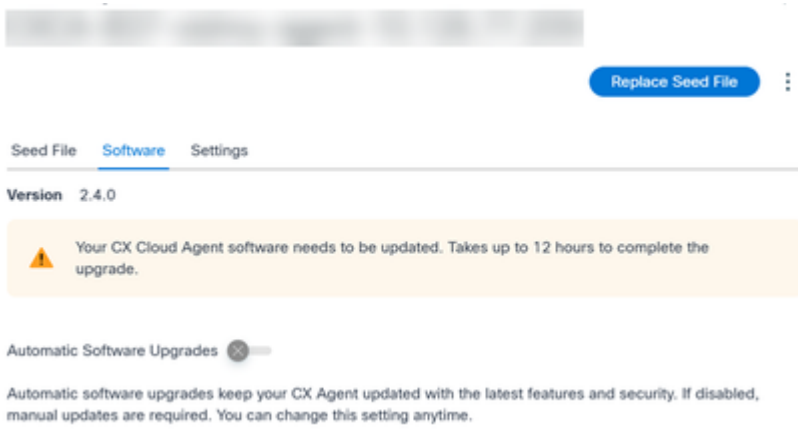
---

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

---

### Automatic Upgrades

Customers can enable the **Automatic Software Upgrades** toggle to ensure their system is updated when 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.




---

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

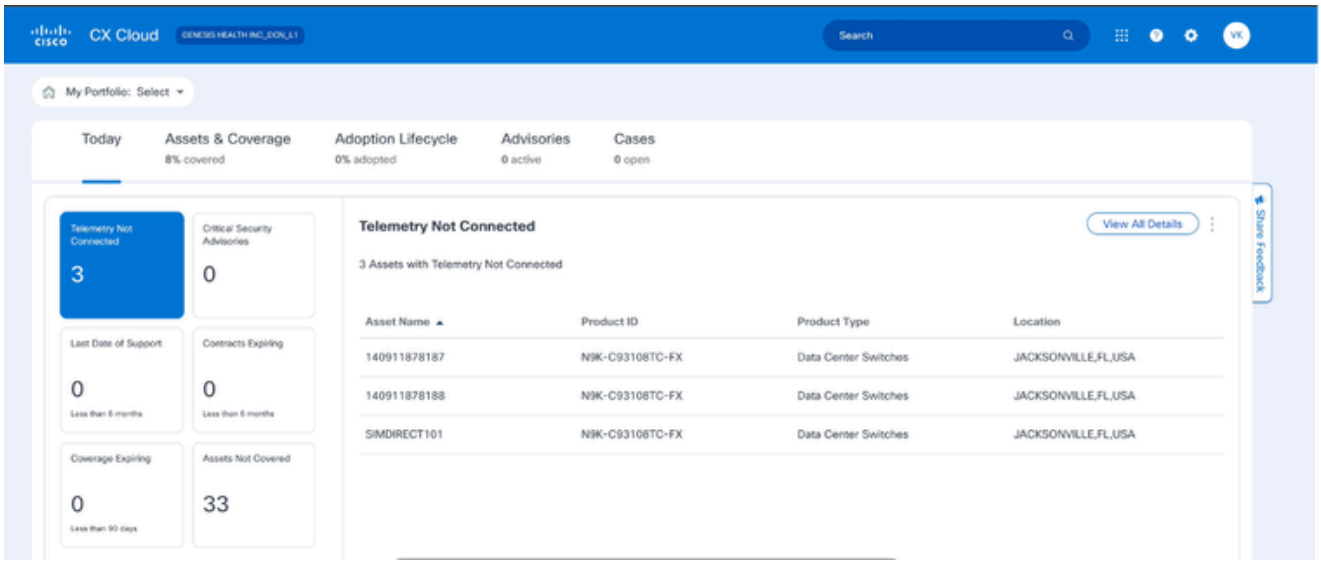
---

### Manual Upgrades

Customers who prefer not to use automatic upgrades and have not enabled **Automatic Software Upgrades** can choose to upgrade manually. CX Agent supports a direct upgrades to v3.1.5.

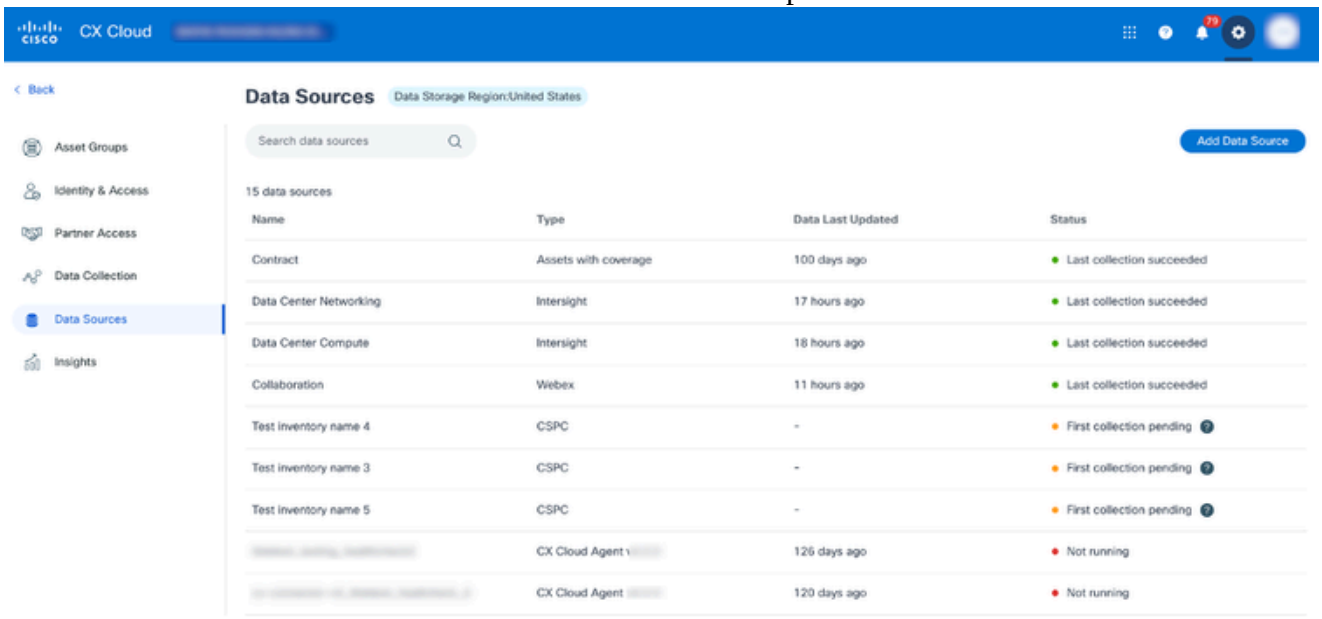
To install the CX Agent upgrade v3.1.5 from CX Cloud:

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



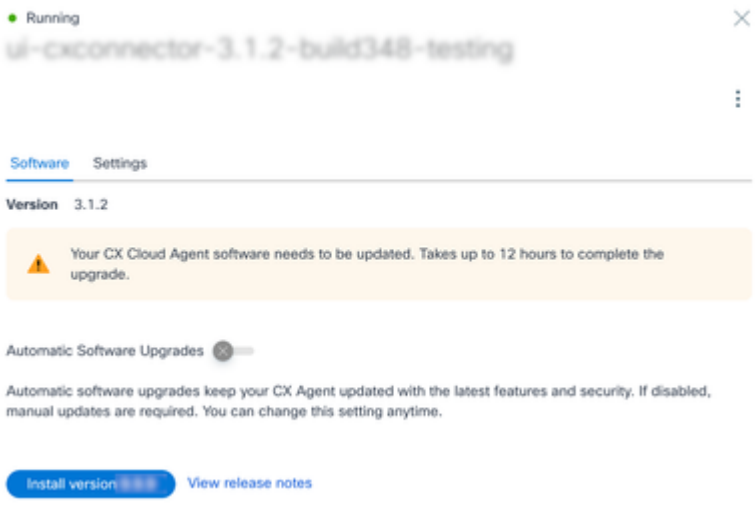

*CX Cloud Home Page*

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




*Data Sources*

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



*Install Version*

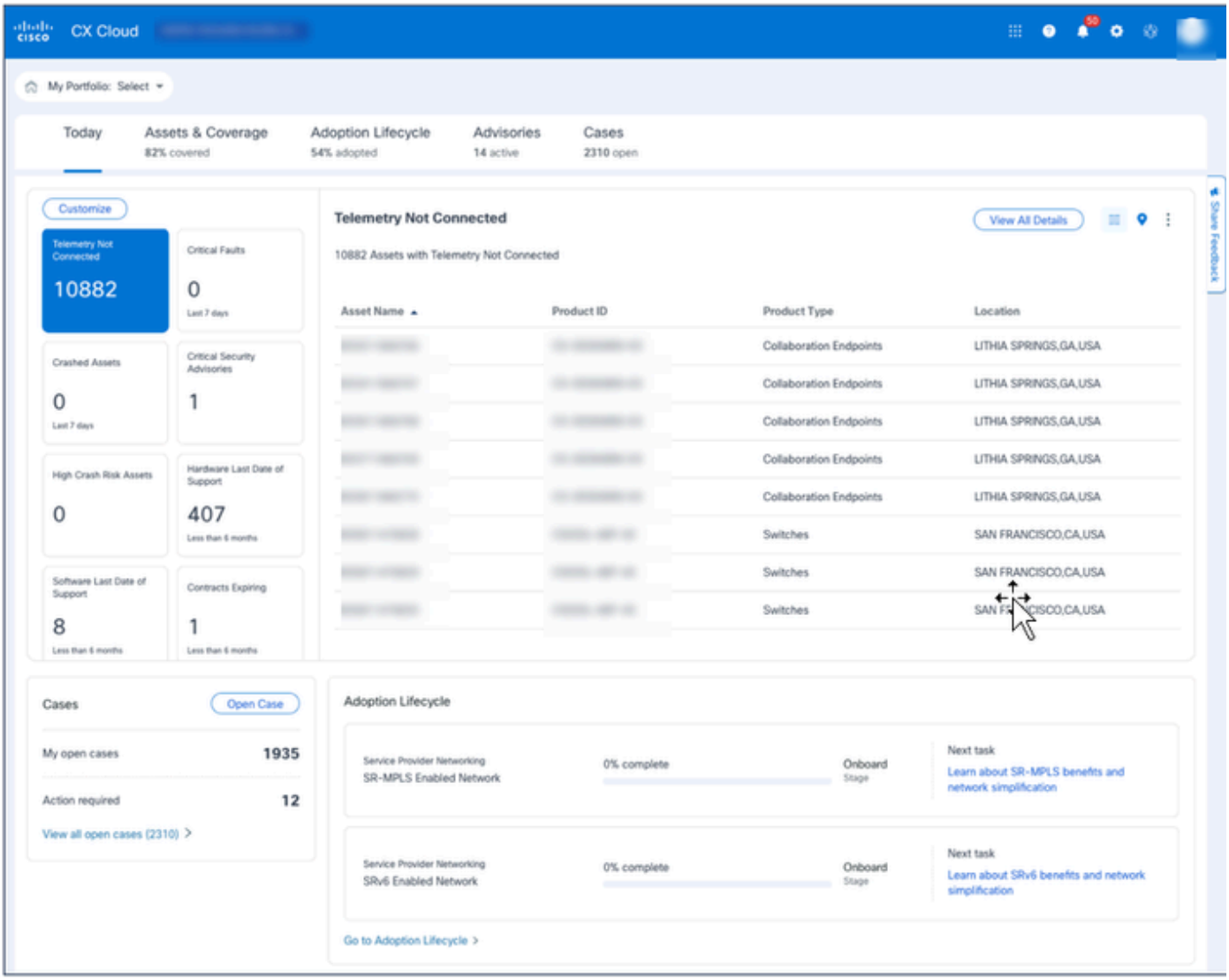
4. Click the **Software** tab.
5. Click **Install version**.

# Adding CX Agent

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

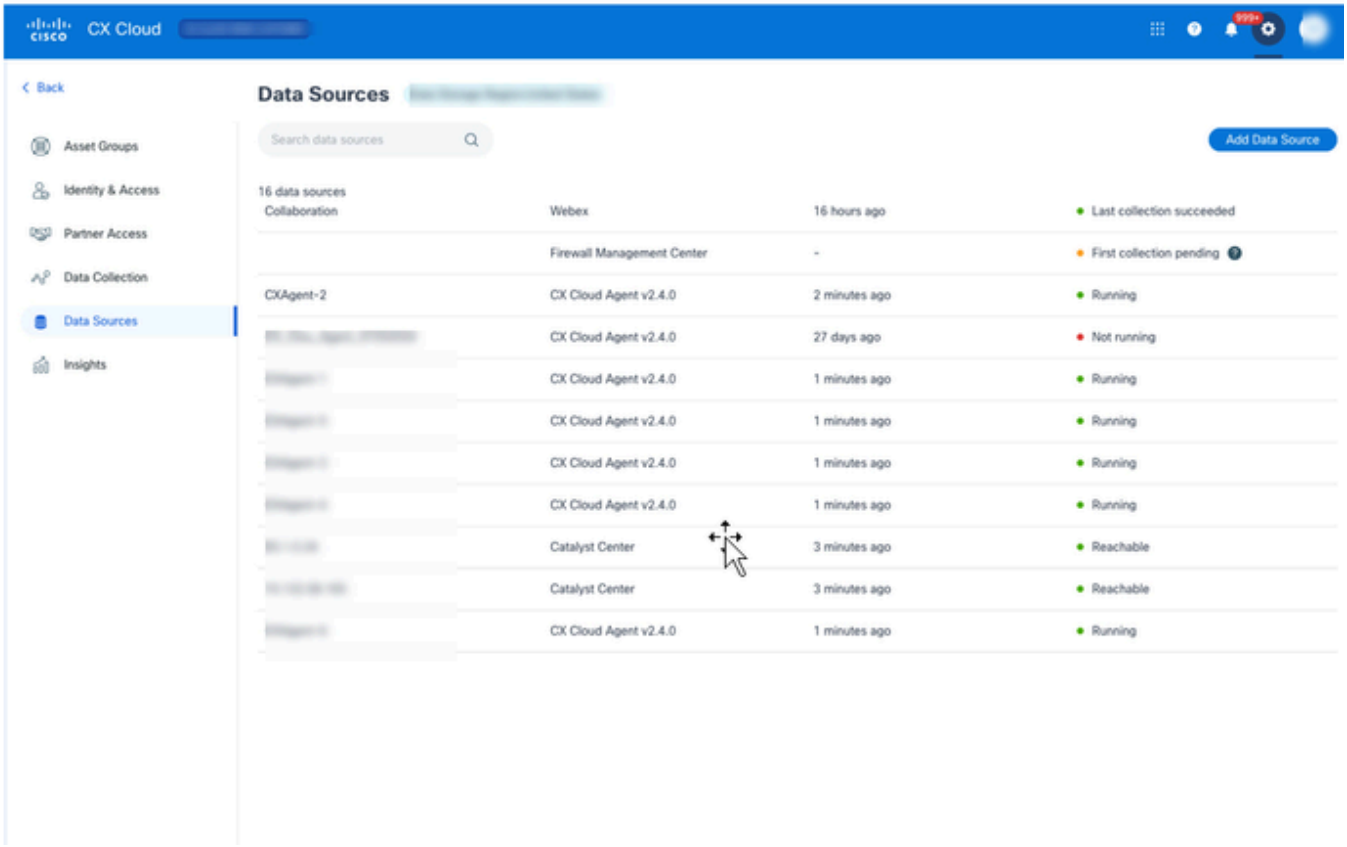
To add a CX Agent:

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



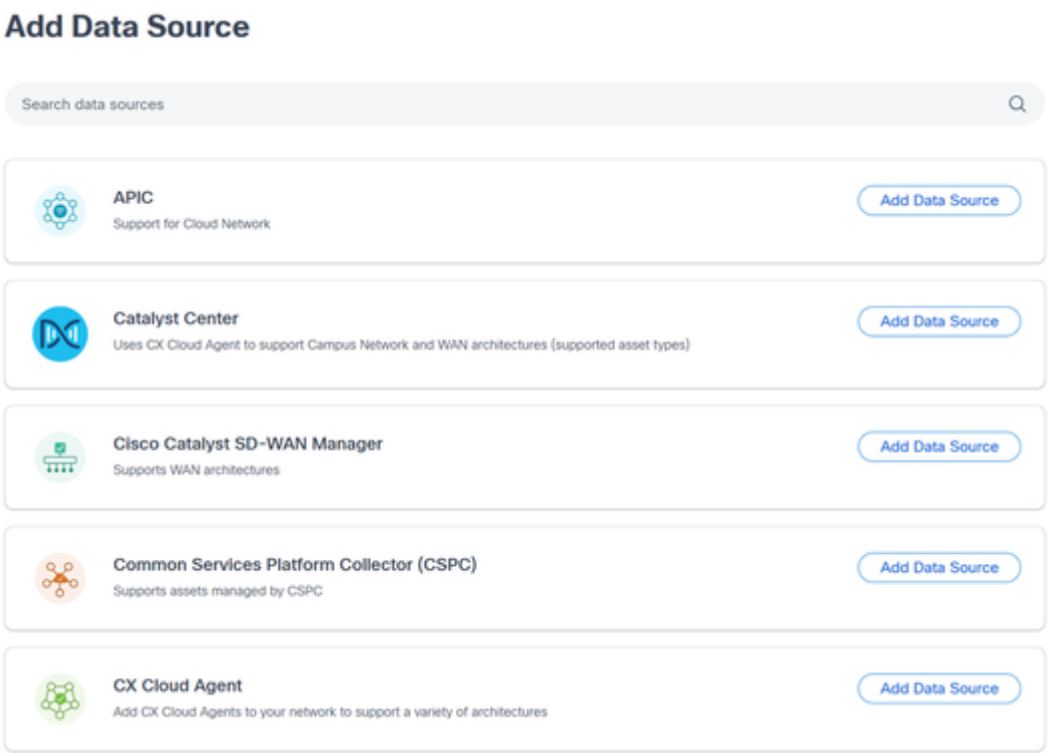

*CX Cloud Home page*

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

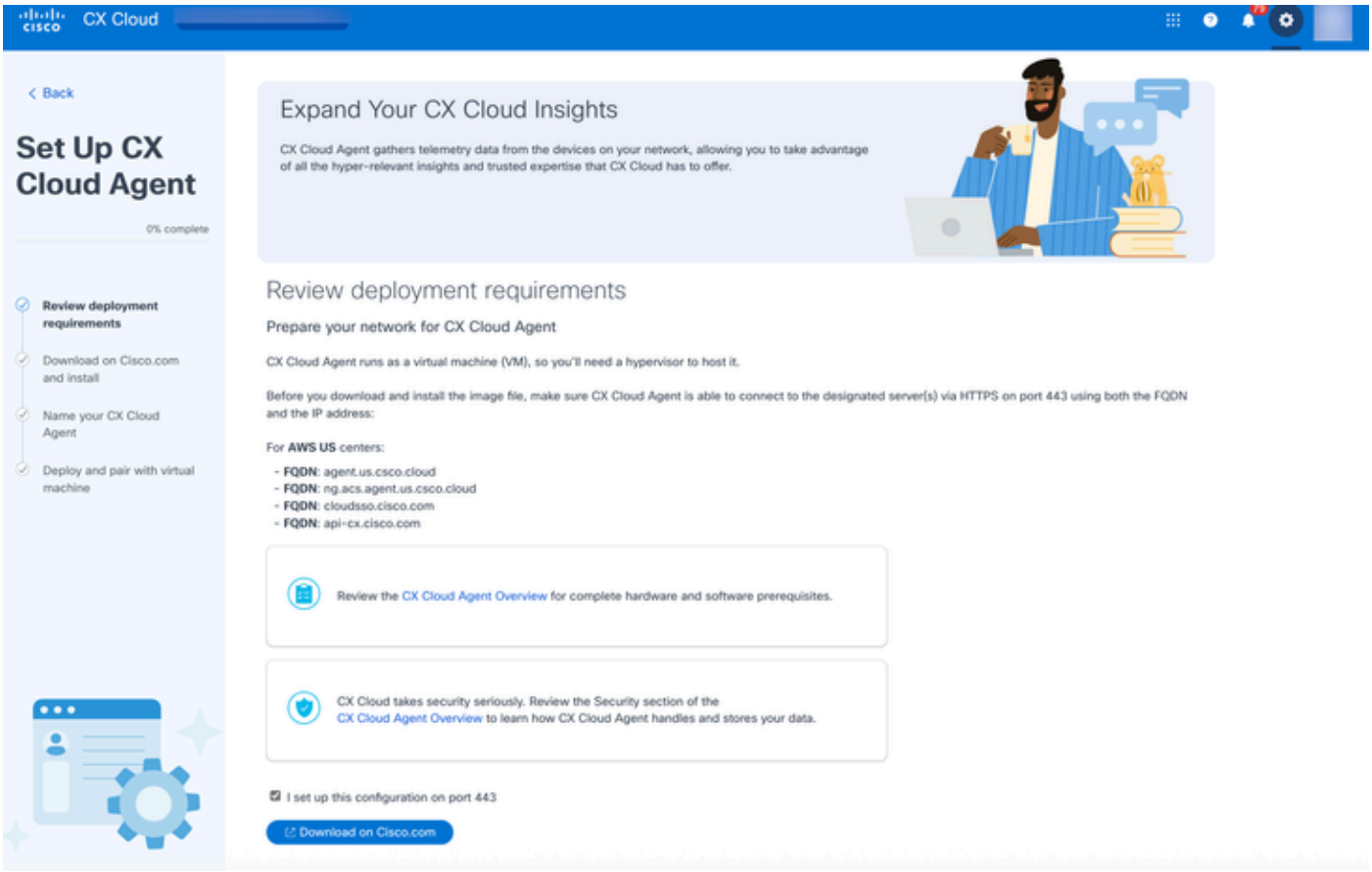



*Data Sources*

3. Click **Add Data Source**. The **Add Data Source** page opens.




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




*Adding CX Agent*

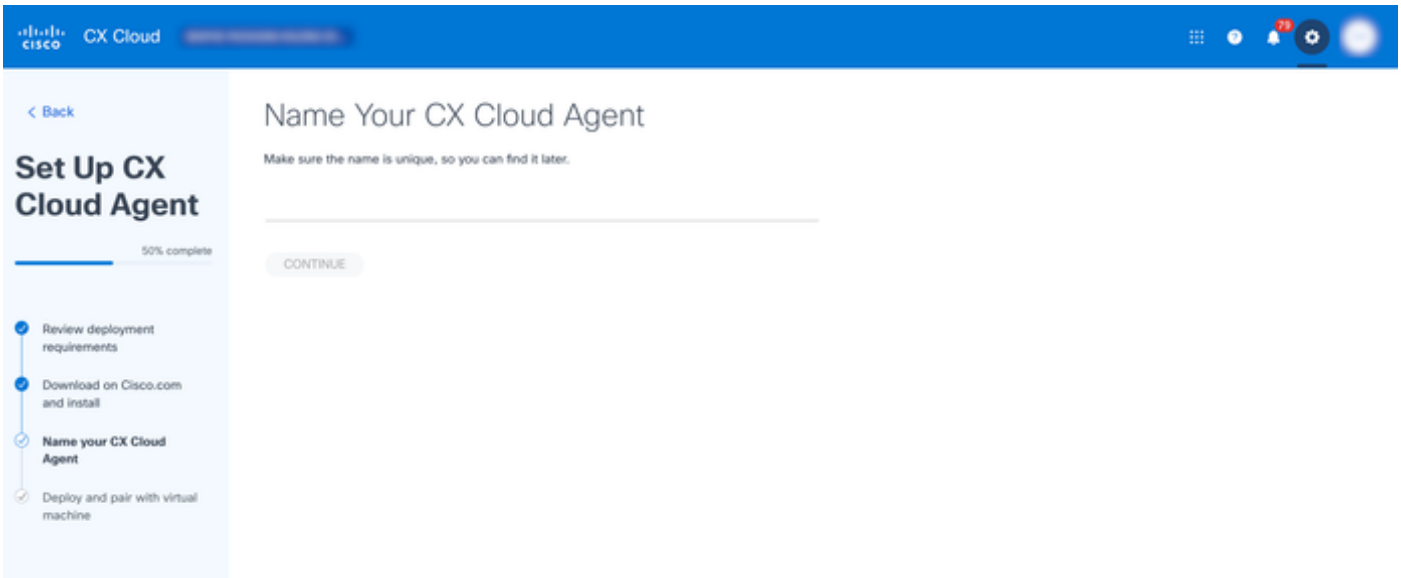
5. Review the **Review deployment requirements** section and select the **I set up this configuration on port 443** check box.
6. Click **Download on Cisco.com**. The **Software Download** window opens in another tab.
7. Download the “CX Agent v3.1.5 OVA” file.

---

**Note**: A Pairing Code required to complete the CX Agent setup is generated after deploying the VM.

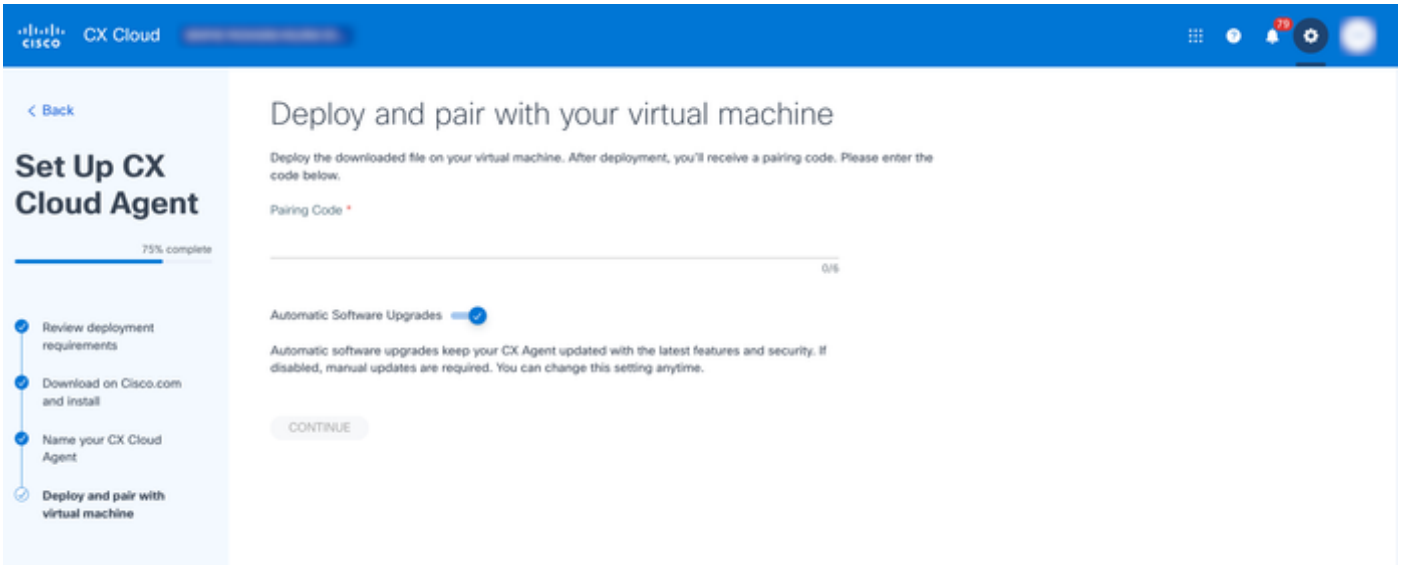
---

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




*Name CX Agent*

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




*Pairing Code*

10. Enter the **Pairing Code** received after deployment of the VM.

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.

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

---

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

---

## 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 your assigned BCS/LCS Technical Consulting Engineer.

# Configuring RADKit Capabilities

CX Agent v3.1.5 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 initial 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 inital login, users are prompted to change the password. Follow the on-screen 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 through CLI.

## 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

---



**Note**: A support case must be opened to access the cxroot and root users.

---

- 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, refer to the "Vault credentials schema" file..

**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": "*******"
}
}
}
```

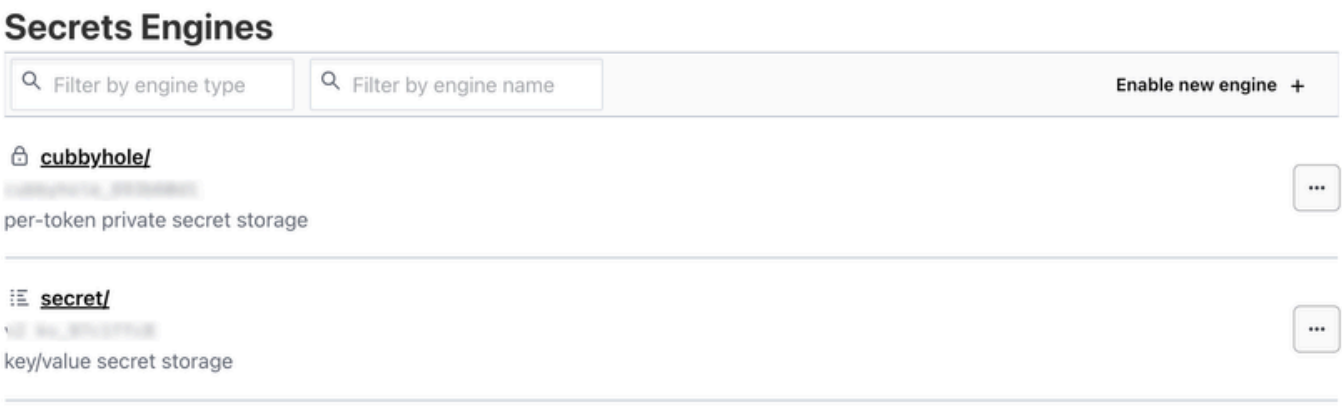
---

**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).

---

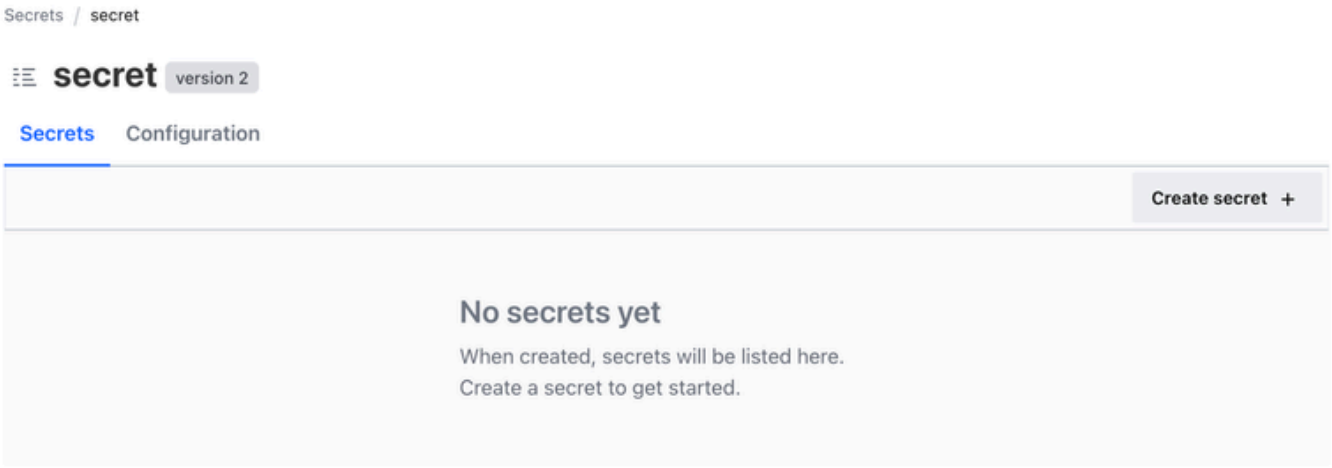
## Configuring Device Credentials in HashiCorp Vault (First Time)

1. Log in to a Vault instance.



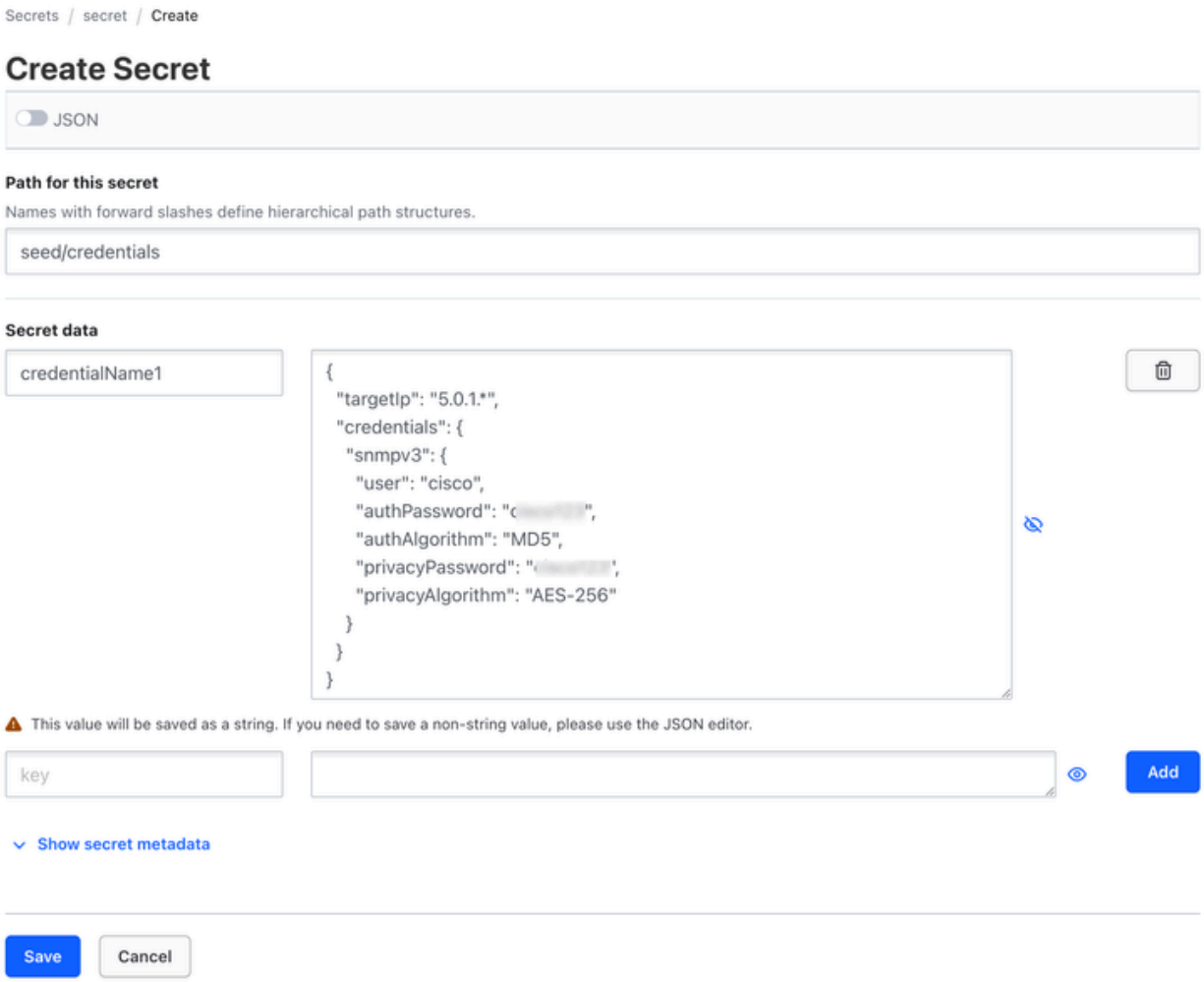

*Secret*

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




*Key value secret*

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

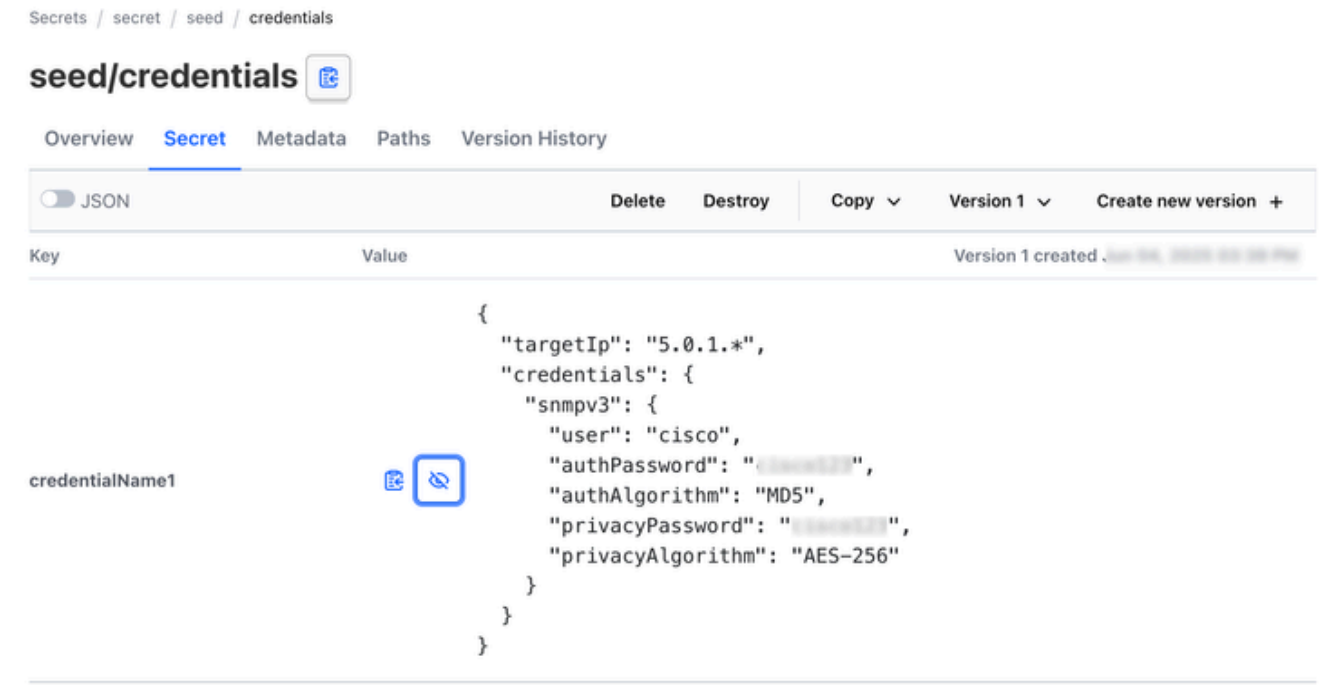



*Client Secret*

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

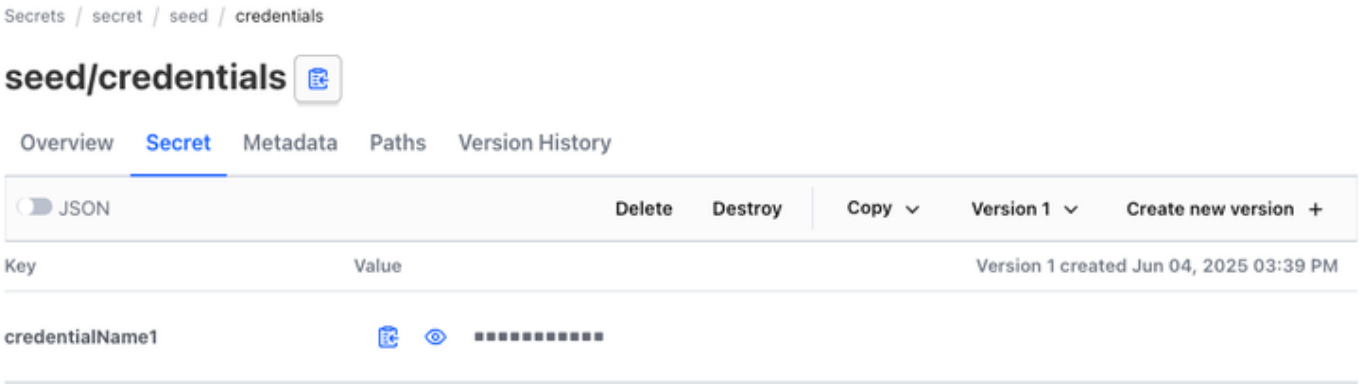
6. Click **Save**. The secret should now be stored in the HashiCorp Vault.




*Credentials*

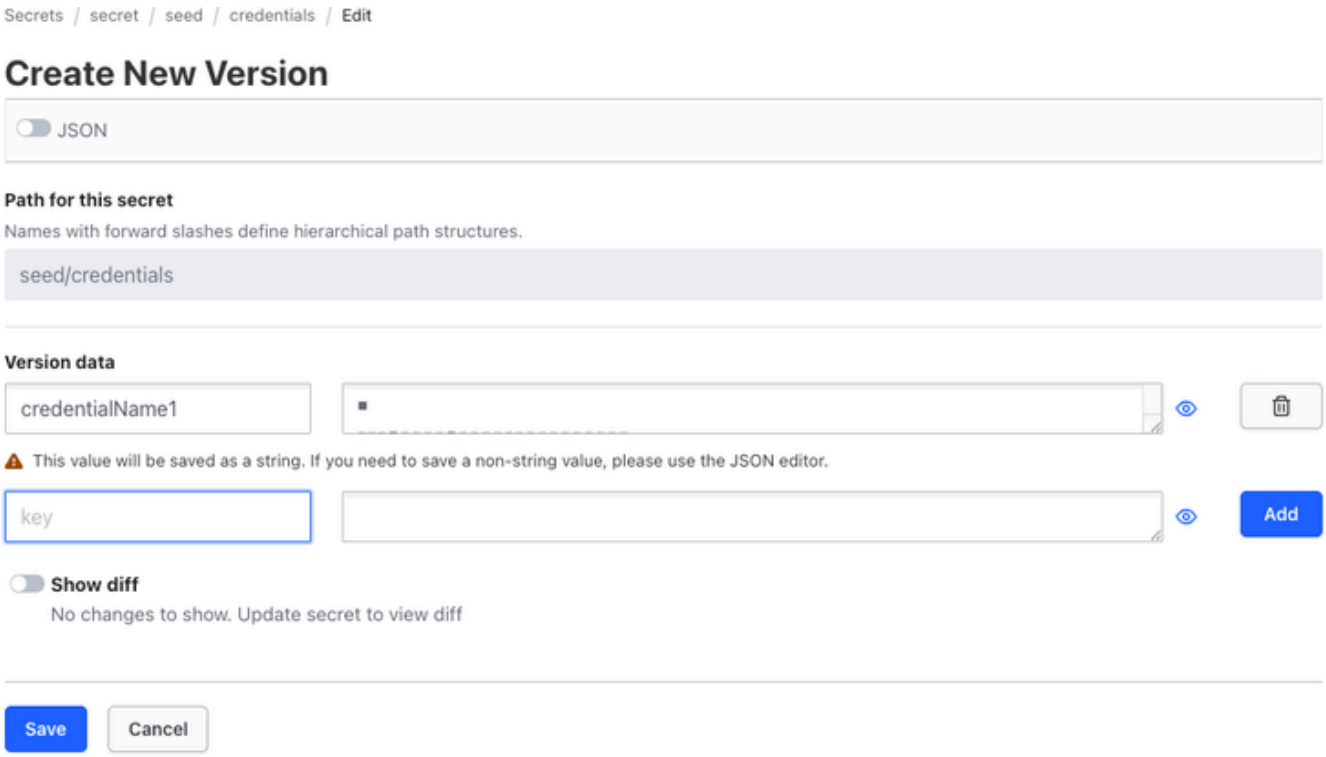
## Adding More Credentials to HashiCorp Vault

1. Log in to a HashiCorp vault instance.




*Add Credentials*

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




*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,,,,,,,,,,,,,,,,,,
```

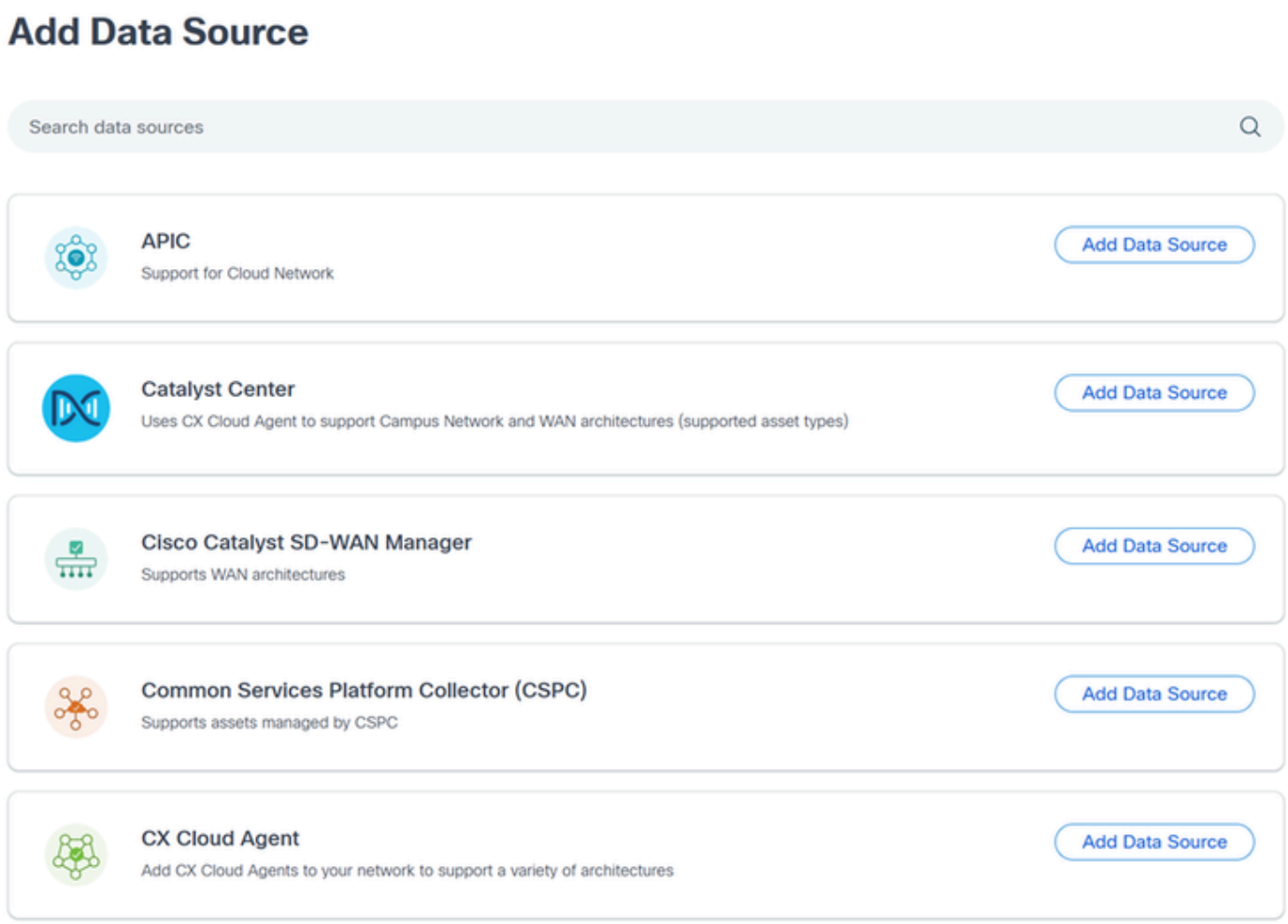
*IP or Hostname*

# Adding Catalyst Center as Data Source

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

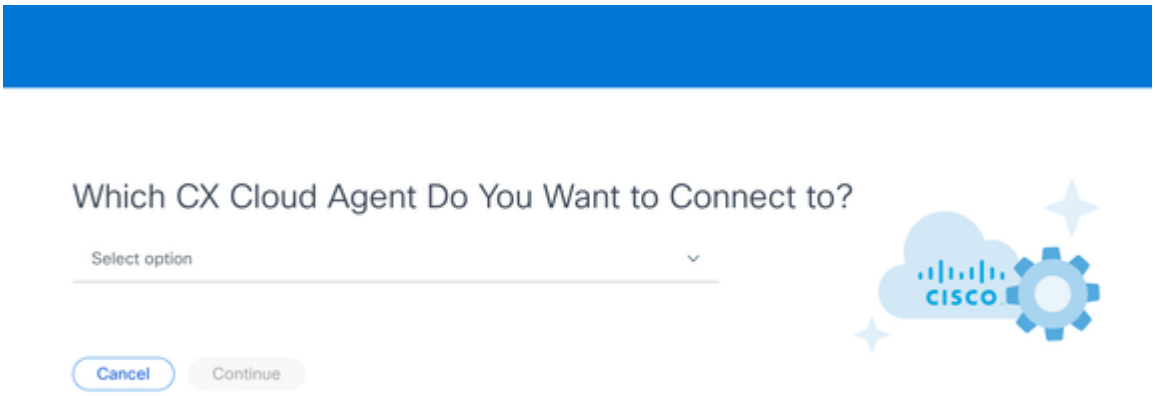
To add Catalyst Center as a Data Source:

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



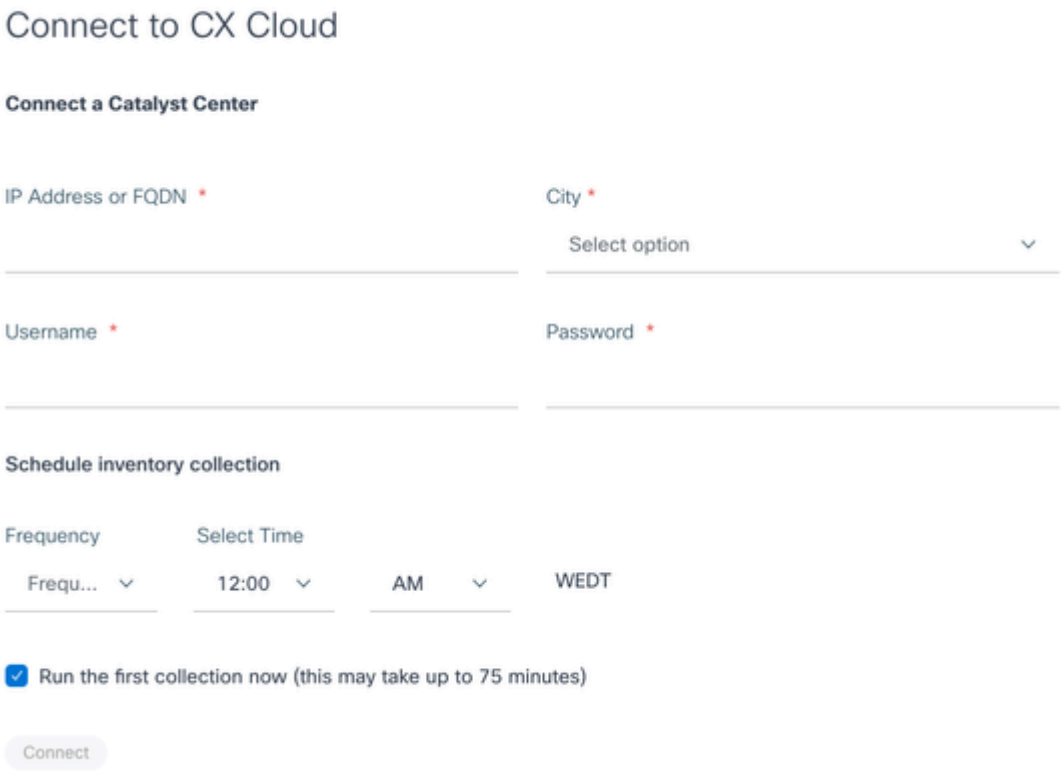

*Catalyst Center*

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




*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 BCS/LCS Data Sources

**Warning**: The following data sources are for BCS forwarding assets only.

## Adding SolarWinds®

**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®.

**Note**: 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 EPNM

BCS/LCS customers can now use the CX Agent capability to externally integrate with Evolved Programmable Network Manager (EPNM). 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 OIC.

## Adding APIC

BCS/LCS customers can now use the CX Agent capability to externally integrate with Application Policy Infrastructure Controller (APIC). 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 OIC.

# 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 v3.1.5 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. |

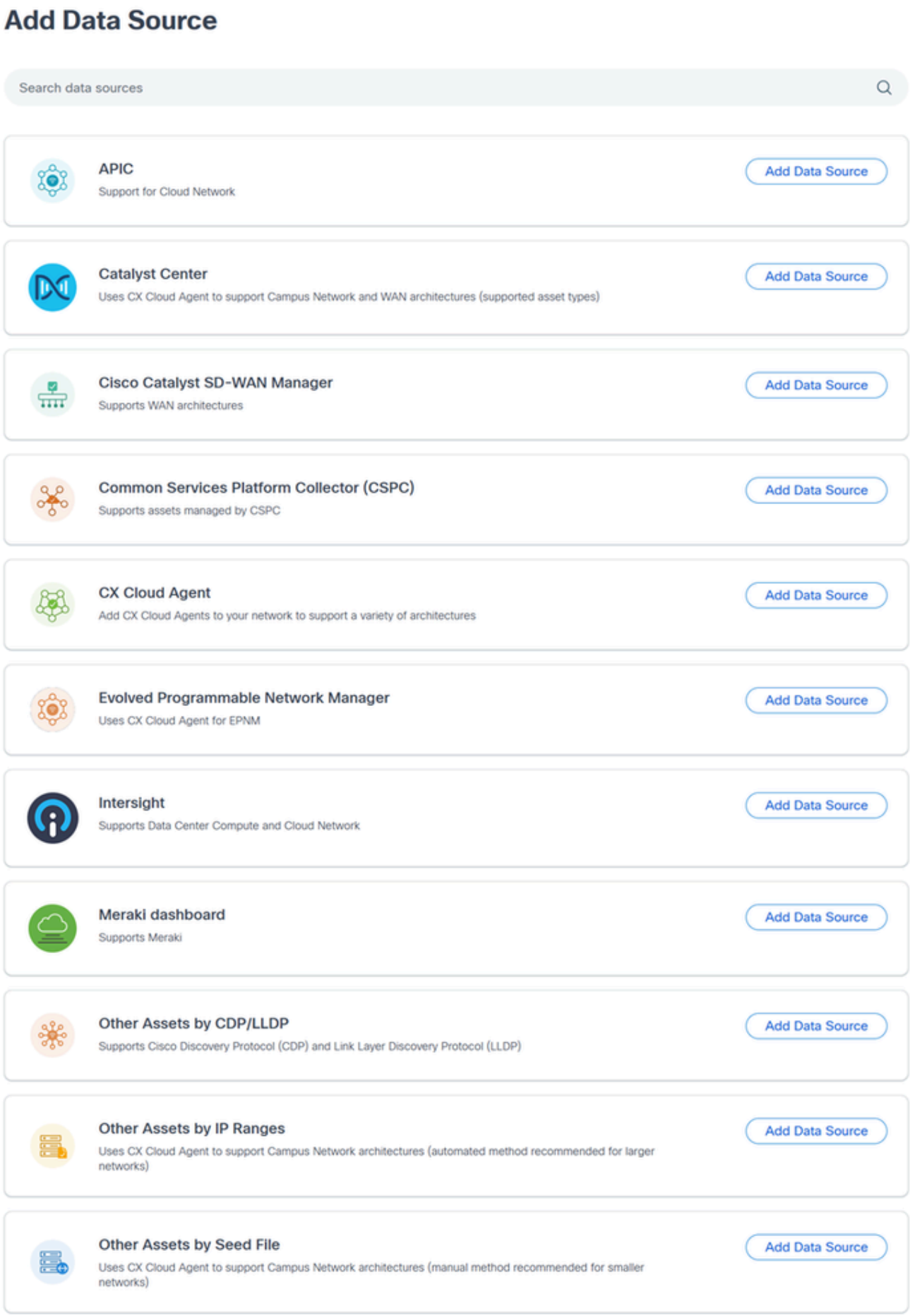
| Seed File Column | Column Header / Identifier | Purpose of the Column |
|---|---|---|
| E | snmpv3AuthAlgorithm : values can be MD5 or SHA | SNMPv3 protocol permits Authentication via either the Message Digest (MD5) or Secure Hash Algorithm (SHA). If the device is configured with secure authentication, then the respective Auth Algorithm must be provided.<br> **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, AES-128, AES-192, AES-256 | 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.<br> **Note**: 56-bit keys used by Data Encryption Standard (DES) are considered too short to provide cryptographic security, and that 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 |

| Seed File Column | Column Header / Identifier | Purpose of the Column |
|---|---|---|
| | | 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 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

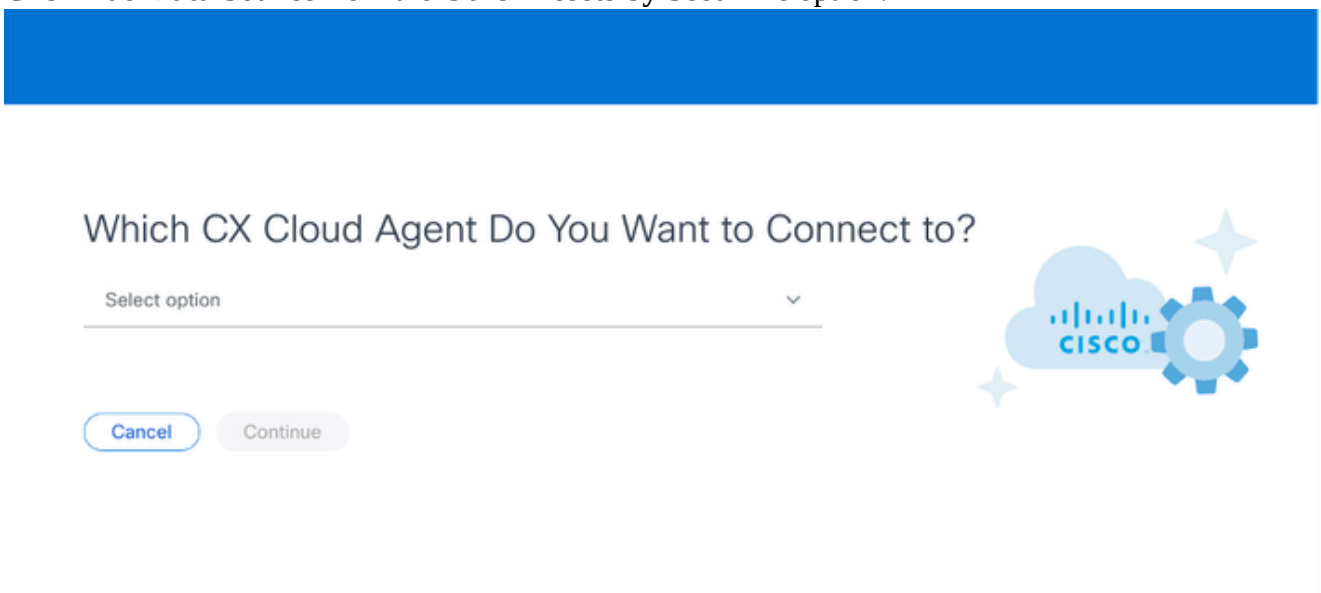
To add other assets using a new Seed File:

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



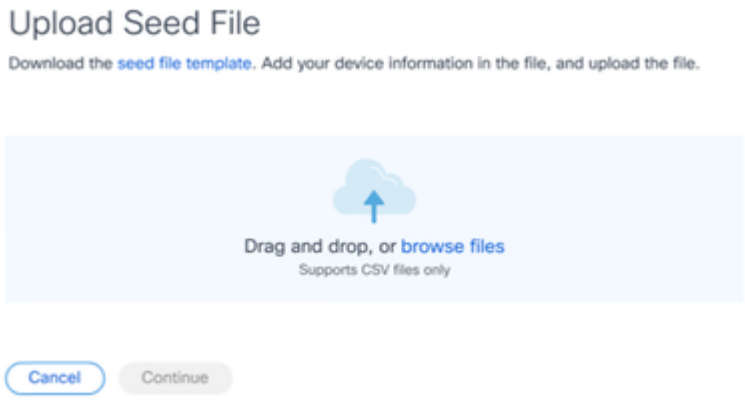

*Other Assets by Seed File*

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



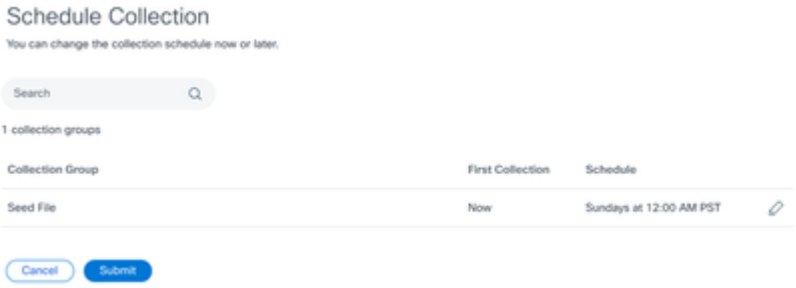

*Select CX Agent*

3. Select the CX Agent from the **Which CX Cloud Agent Do You Want to Connect to** drop-down list.
4. Click **Continue**. The **Upload Seed File** page displays.



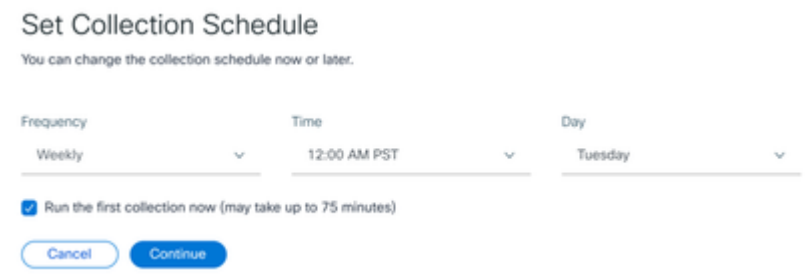

*Upload Seed File*

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. Once the file is uploaded, click **Continue**. The **Schedule Collection** page displays.




*Schedule Collection*

9. Click the **Edit** icon. The **Set Collection Schedule** page displays.




*Set Collection Schedule*

10. Select an option from the following drop-down lists:
    - **Frequency**
    - **Time**
    - **Day**
11. Select the **Run the first collection now** check box to run the collection.

> **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.

12. Click **Continue**. The **Schedule Collection** page redisplays.
13. Click **Submit**. The **Data Sources** window opens, displaying a confirmation message.

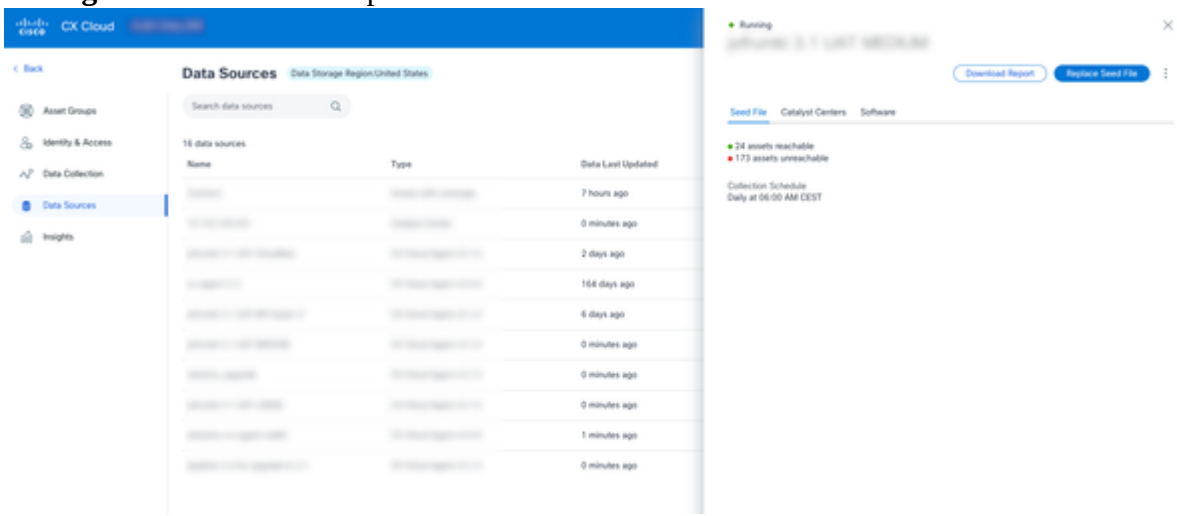
## Adding Other Assets Using a Modified Seed File

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.

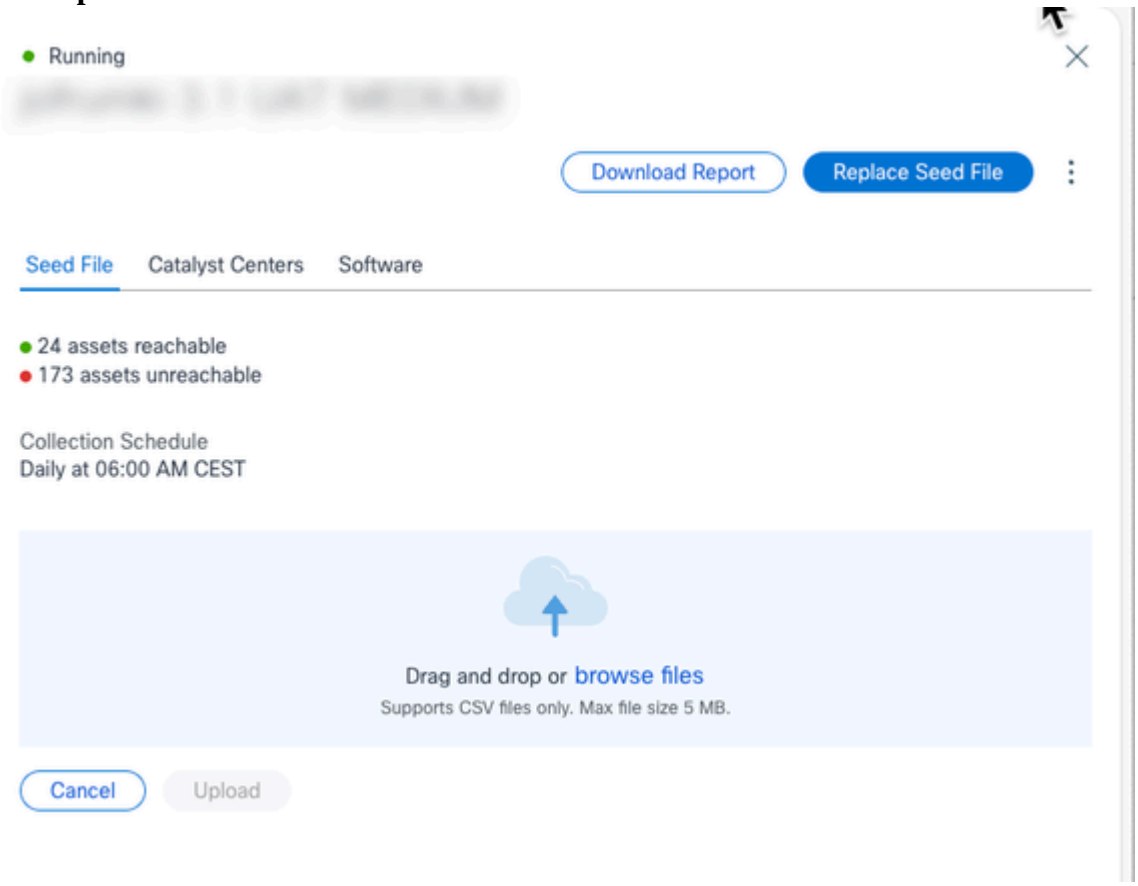
> **Note**: To add assets to the seed file, append those assets to the previously created seed file and reload the file. This is necessary since uploading a new seed file replaces the current seed file. Only the latest uploaded seed file is used for discovery and collection.

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



*Seed File*

3. Click **Replace Seed File**.




*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 eliminates 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. Refer to Configuring Vault for Existing CX Agents for information about enabling this feature.

## 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.

---

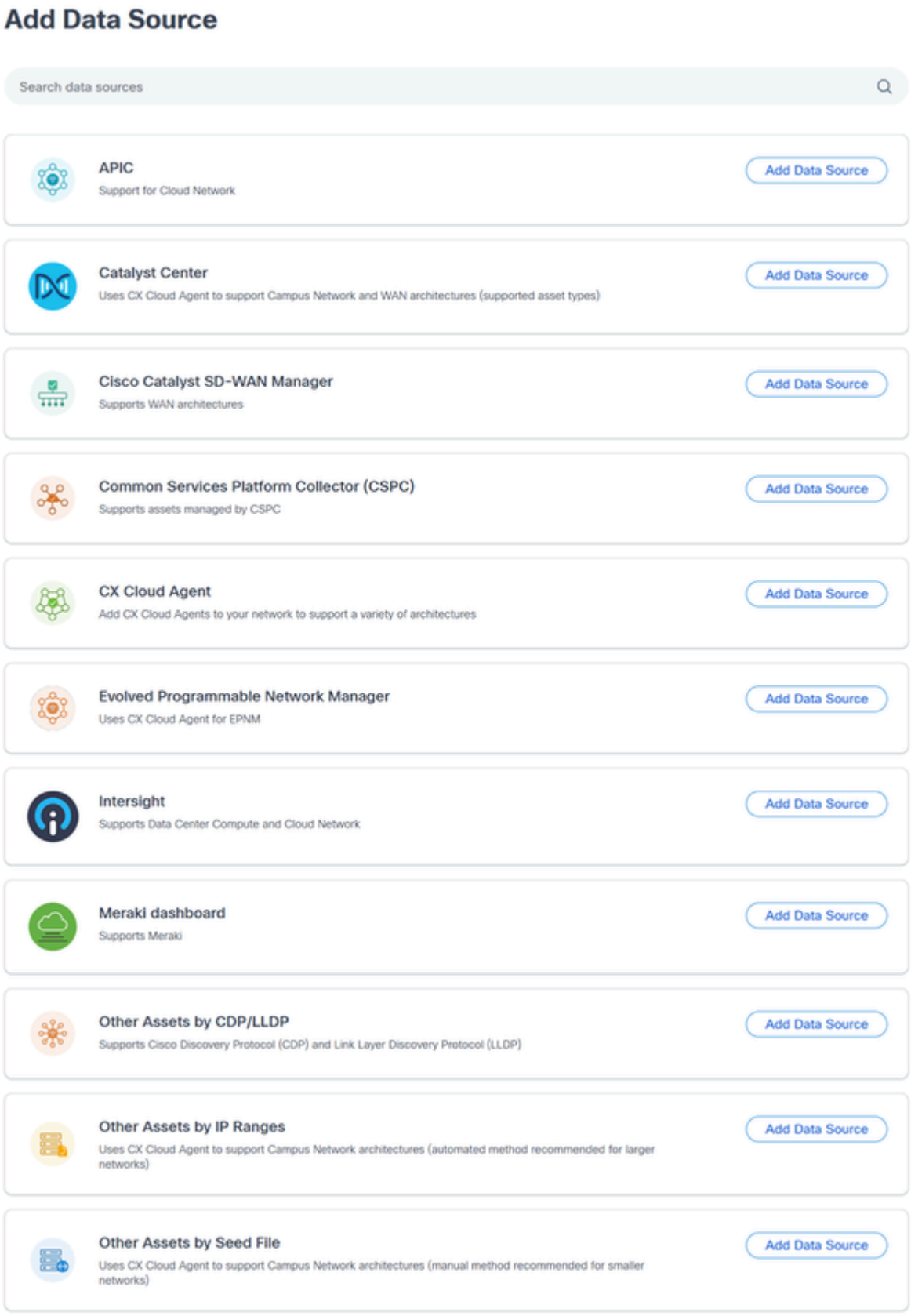
Adding devices using an IP range requires users to specify all applicable credentials through the configuration UI. The fields visible vary depending on the protocols selected on the previous windows. If multiple selections are made for the same protocol, for example, selecting both SNMPv2c and SNMPv3 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

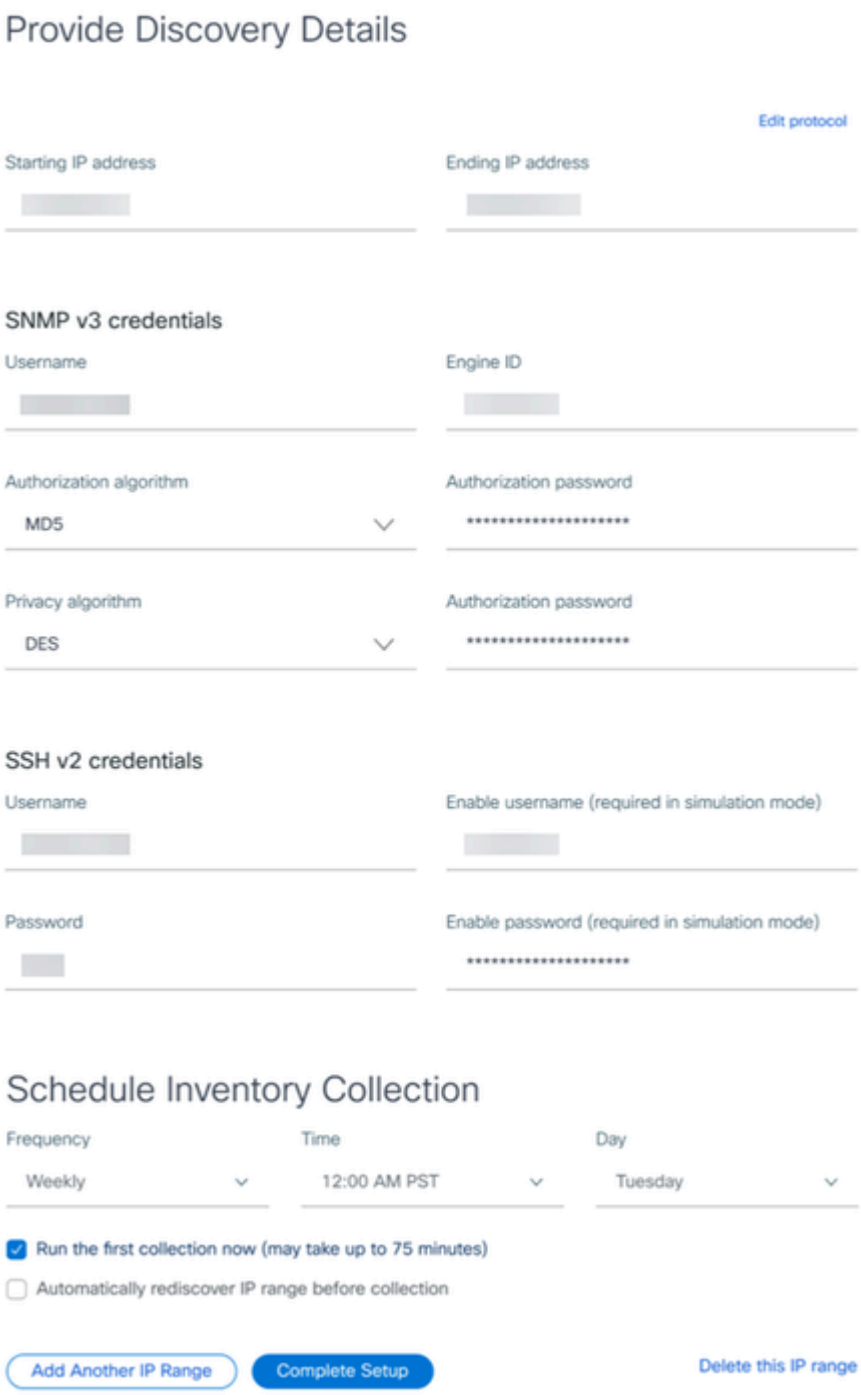
To add devices using the IP range:

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



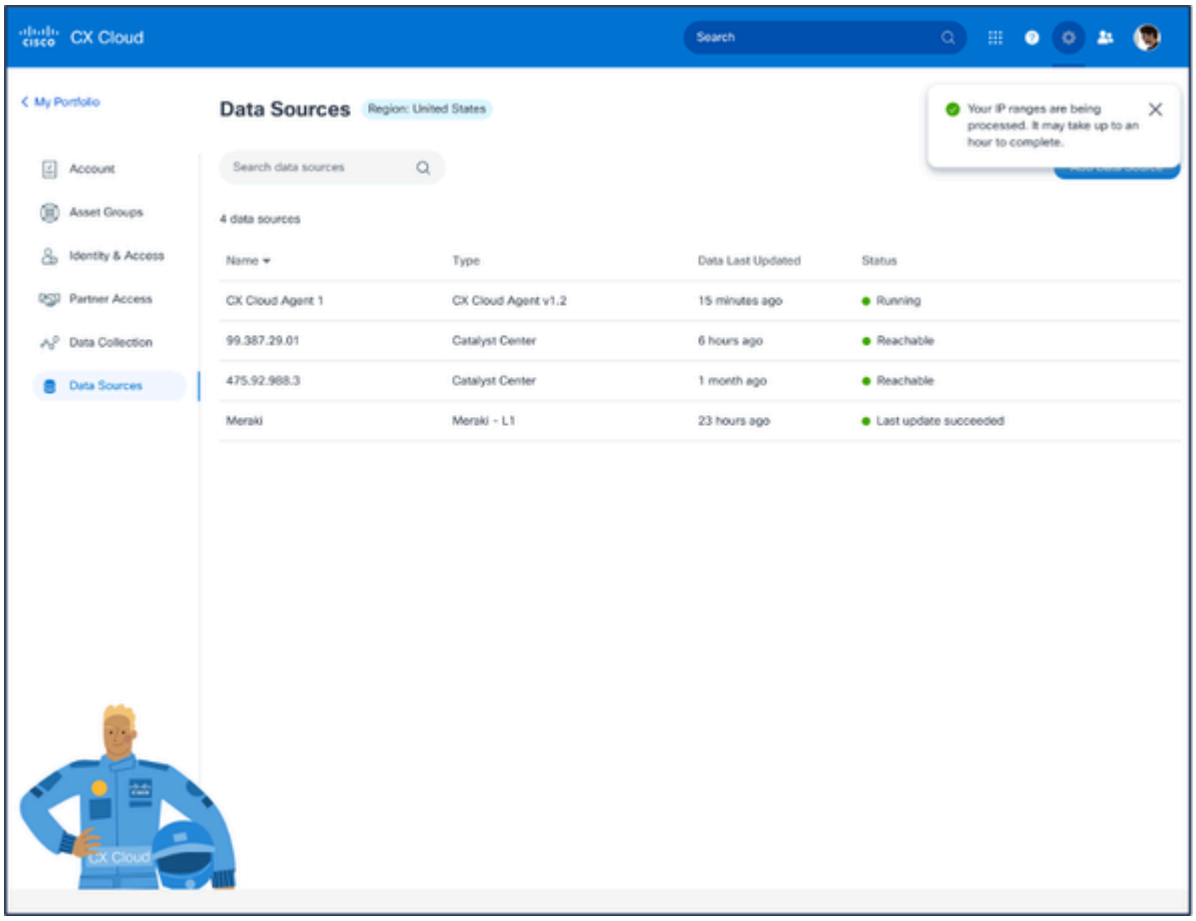

*Other Assets by IP Range*

3. Click **Add Data Source** in the **Other Assets by IP Range** option. The **Provide Discovery Details** page displays.




*Provide Discovery Details*

4. Enter a **Starting IP address** and an **Ending IP** address.
5. Enter the required details in the SNMP and CLI credentials sections.
6. In the **Schedule Inventory Collection** section, select options from the following drop-down lists.
    - **Frequency**
    - **Time**
    - **Day**
7. Select the **Run the first collection now** check box to run the collection.
8. Optionally, select the **Automatically rediscover IP range before collection** check box to enable auto-rediscovery of IP ranges.
9. Click **Complete Setup**. A confirmation displays upon successful deployment.

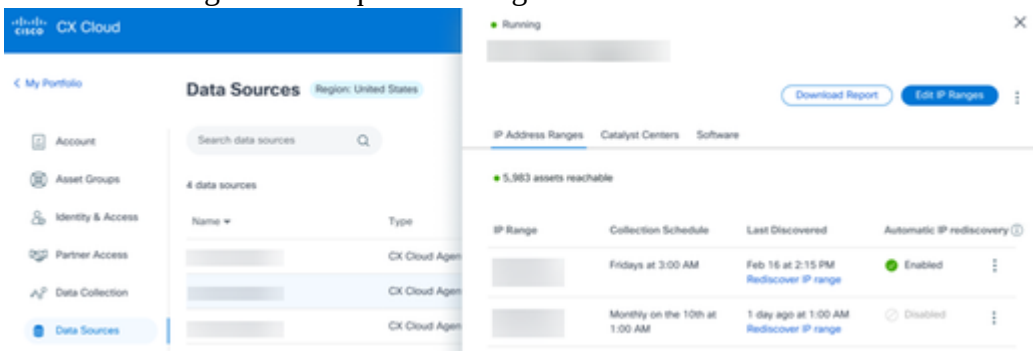



*Confirmation Message*

## Editing IP Ranges

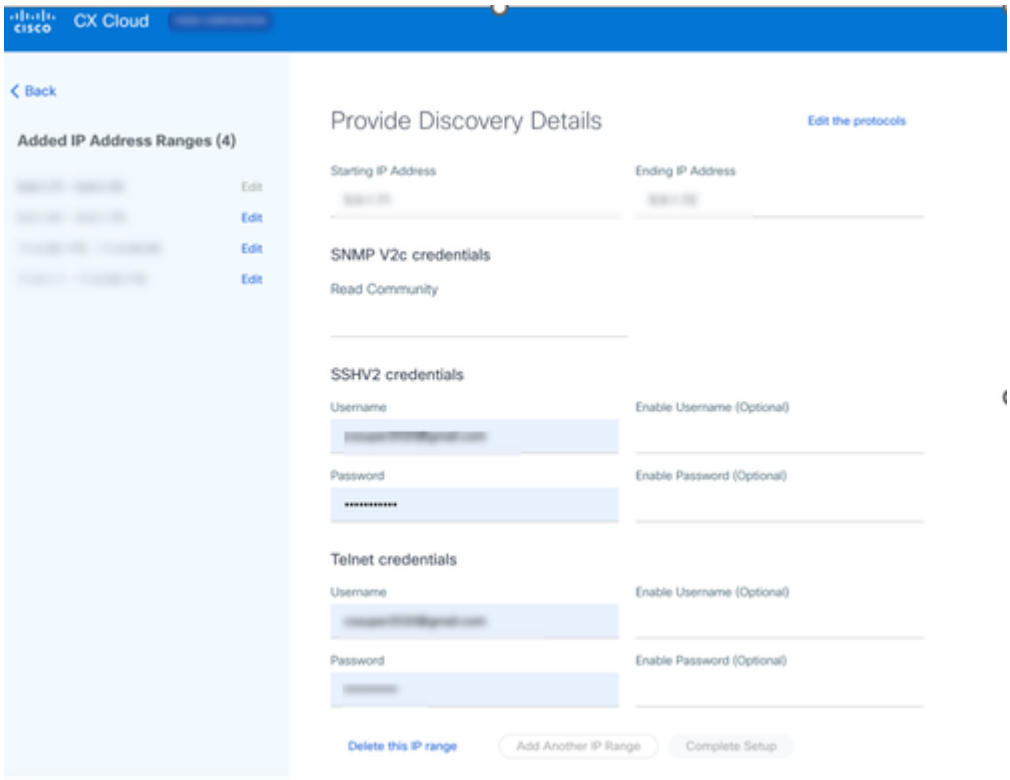
To edit an IP range:

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

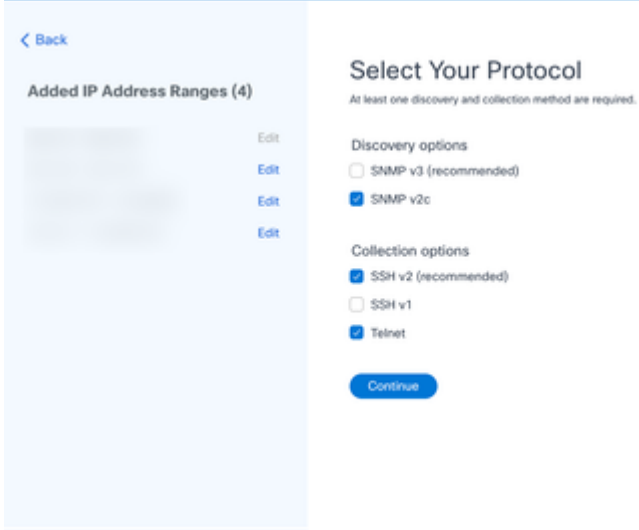



*IP Range Details Window*

3. Click **Edit IP Address Range**.

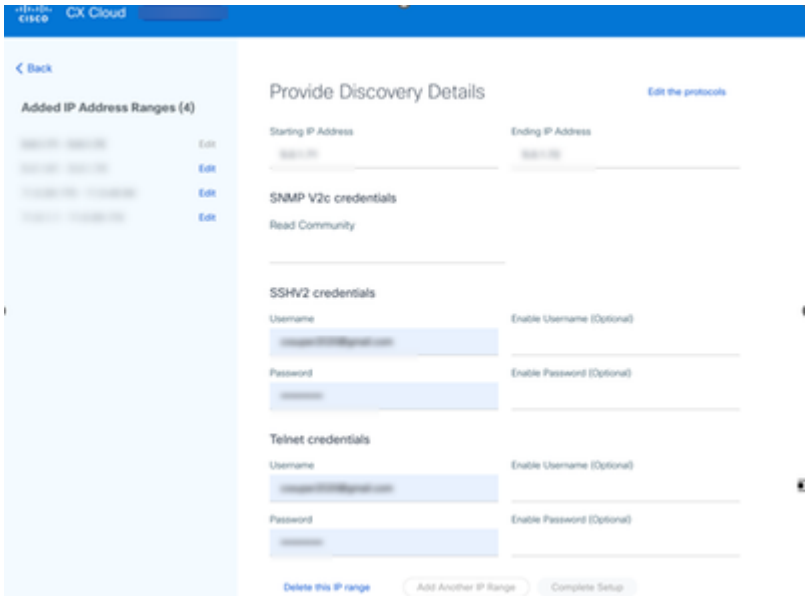



4. Click **Edit the protocols**. The **Select Your Protocol** window opens.




*Select Your Protocol*

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



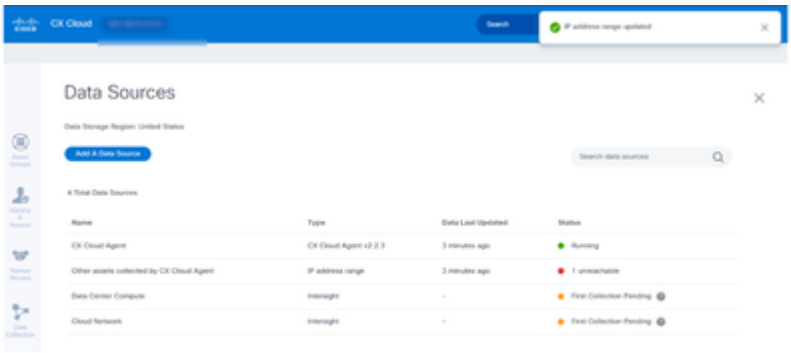

*Provide Discovery Details*

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.

---

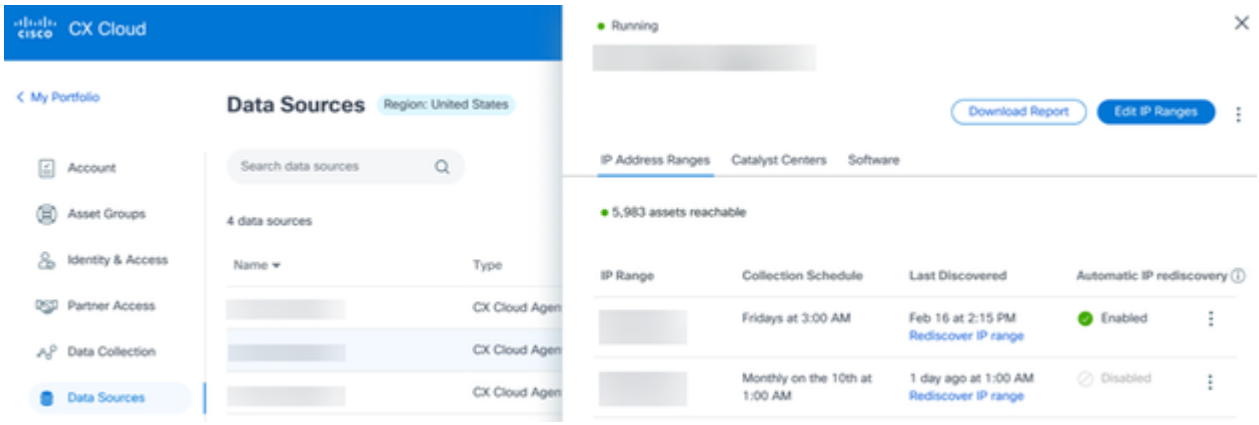



*Confirmation*

## Deleting IP Ranges

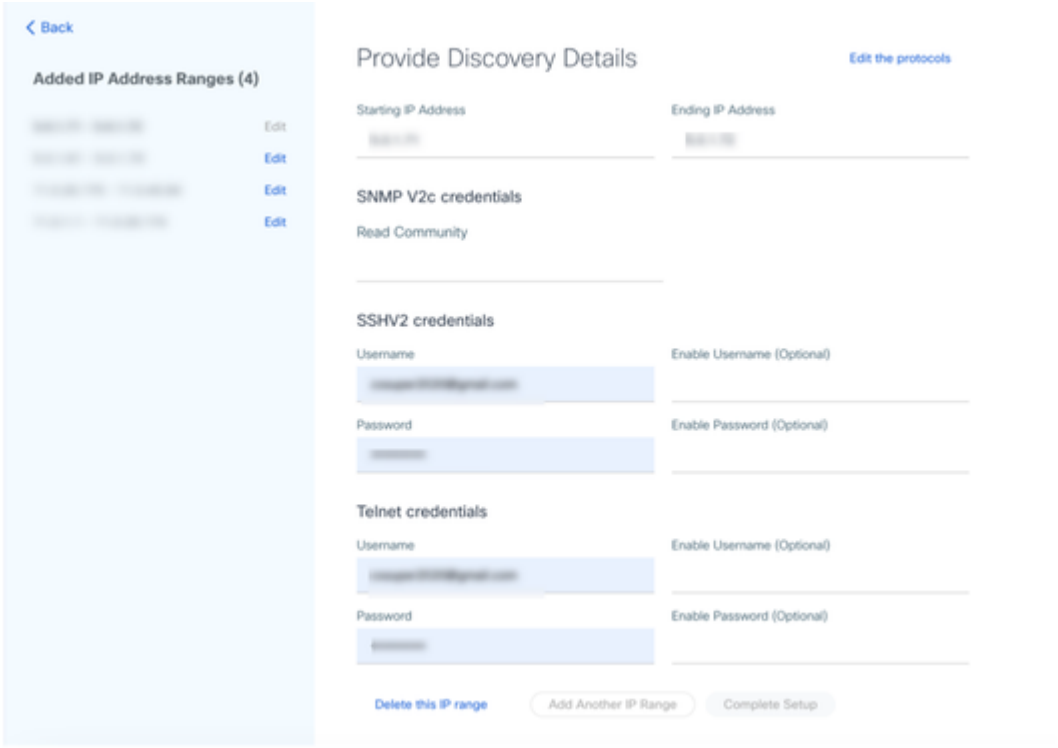
To delete an IP range:

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.



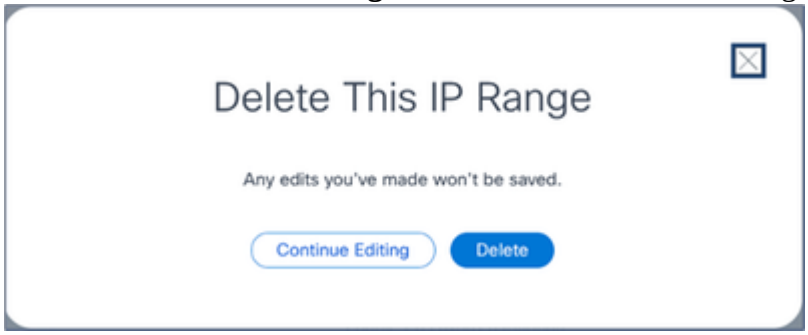

*Edit IP Ranges*

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



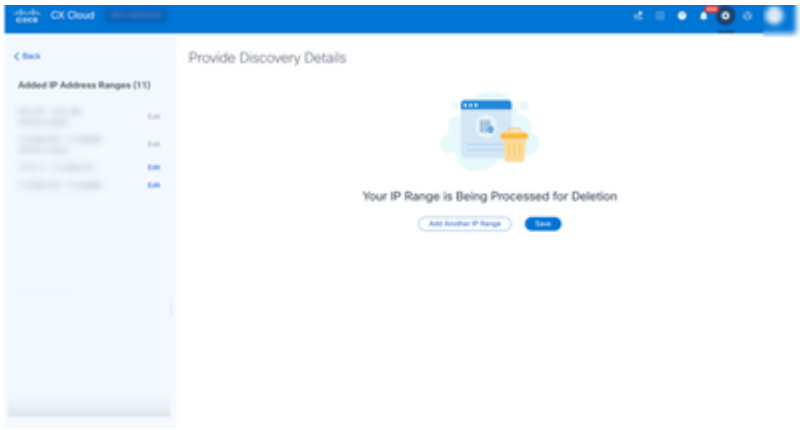

*Deleting IP Ranges*

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

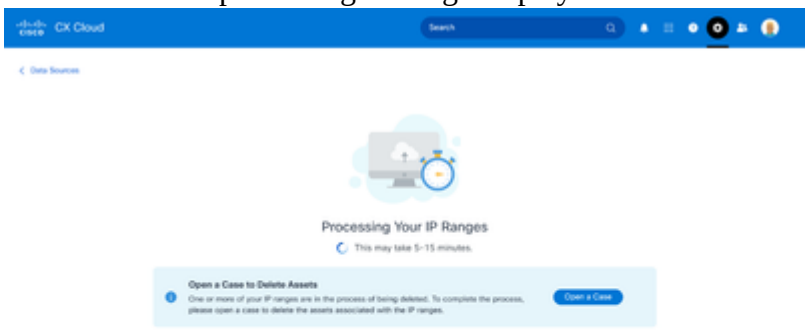



*Confirmation Delete Message*

5. Click **Delete**.




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




*Deleting IP Ranges*

Once complete, the **Data Sources** window opens and displays a confirmation message.

## About Devices Discovered from Multiple Controllers

If the Catalyst Center and IP ranges or seed files 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.

---

**Note**: CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discovery Protocol) are not included in the deduplication process.

---

- If a device is first discovered by direct device connection to CX Agent and then rediscovered by Cisco

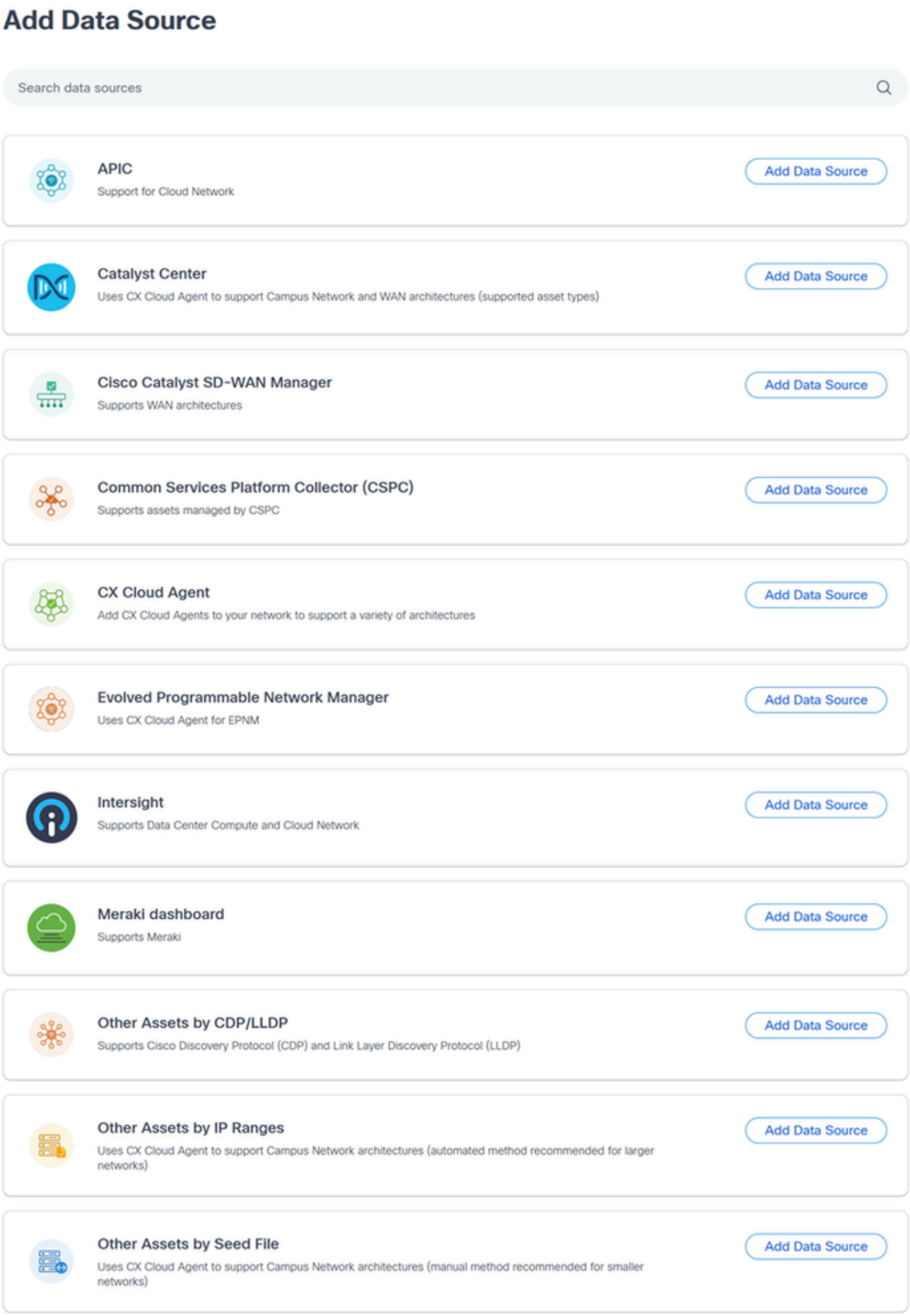
Catalyst Center, Cisco Catalyst Center takes precedence in controlling the device.

# Adding Other Assets Using CDP or LLDP

CDP and LLDP are network protocols that enable devices to automatically discover information about directly connected devices on the network. When discovery is enabled through CDP or LLDP, the CX Agent communicates with network devices to gather detailed information about neighboring devices, such as device type, IP address, and connectivity details, without requiring manual entry or pre-configuration. This automated process allows the CX Agent to dynamically identify and add new devices to the inventory as they are detected on the network, ensuring that the device list remains current even as the network evolves. Any errors or messages related to device discovery through CDP or LLDP are captured as part of the job log details in CX Cloud. Using CDP or LLDP for device discovery simplifies network management, reduces manual effort, and helps maintain an accurate and up-to-date inventory of all connected devices.

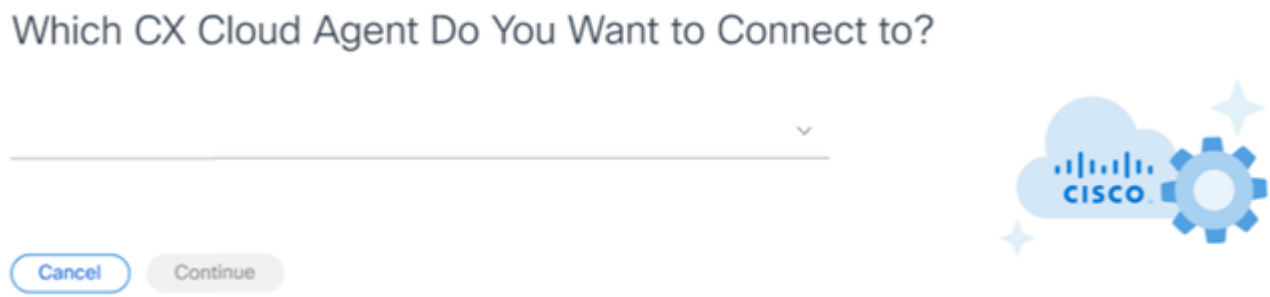
To add other assets using CDP or LLDP:

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



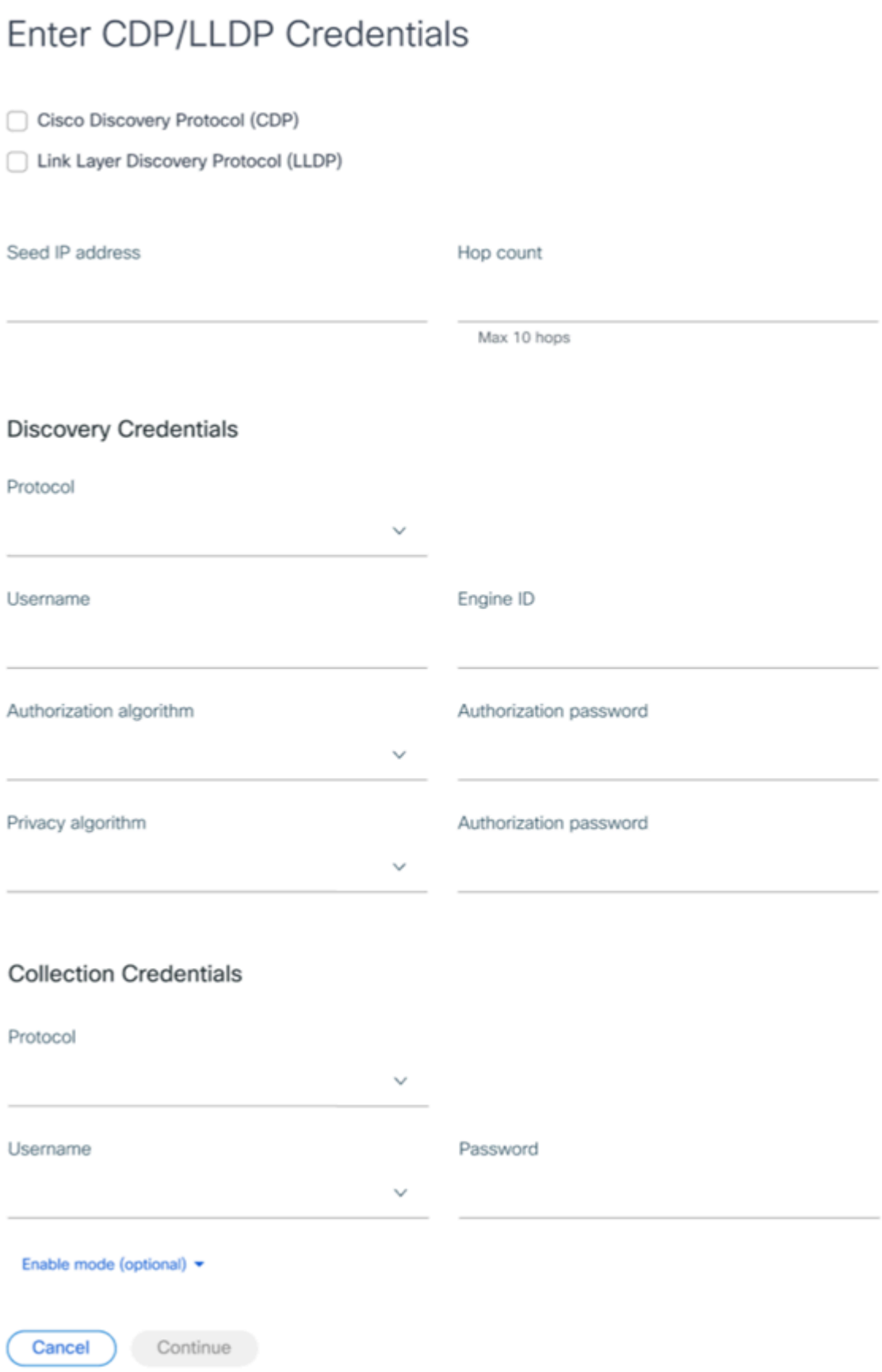

*Other Assets by CDP/LLDP*

3. Click **Add Data Source** in the **Other Assets by CDP/LLDP** option. The **Which CX Cloud Agent Do You Want to Connect to?** page displays.




*Which CX Agent Do You Want to Connect to?*

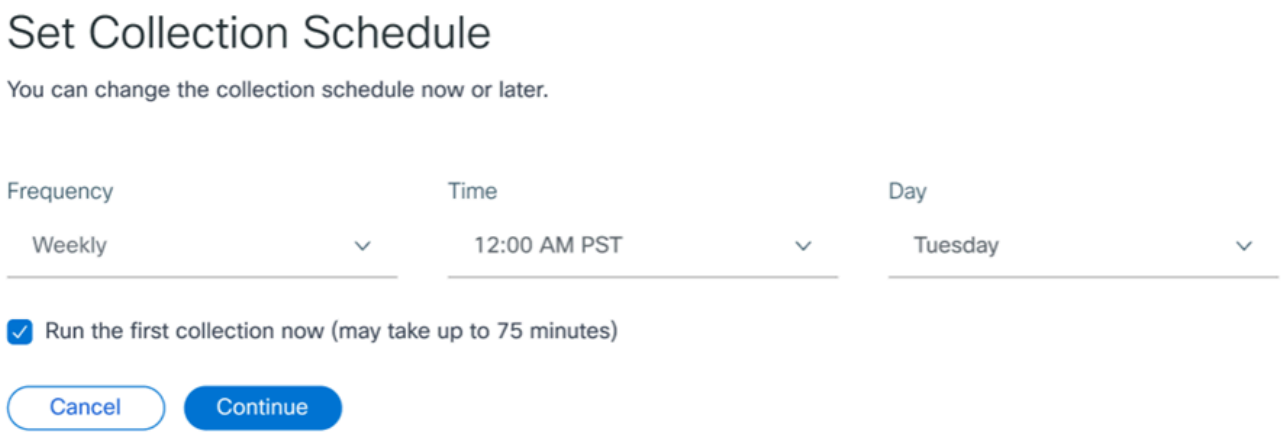
4. Select an option from the drop-down list.
5. Click **Continue**. The **Enter CDP/LLDP Credentials** page displays.




*Enter CDP/LLDP Credentials*

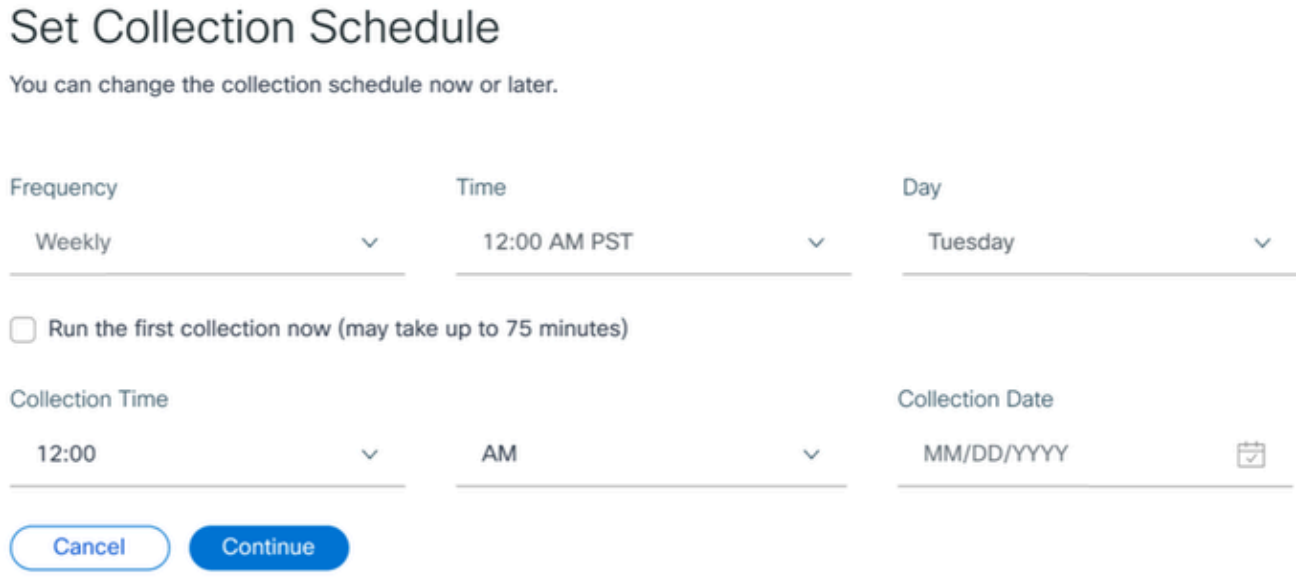
6. Select the **Cisco Discovery Protocol (CDP)** or **Link Layer Discovery Protocol (LLDP)** check box.
7. Enter a **Seed IP address** and **Hop count** (in other words, the number of hops the discovery process should traverse).
8. In the **Discovery Credentials** section, select **SNMP v3** or **SNMP v2** from the **Protocol** drop-down

list.
9. Enter SNMP credentials.
10. In the **Collection Credentials** section, select **SSH v2 (recommended)** from the **Protocol** drop-down list.
11. Enter a **Username** and **Password**.
12. Click **Continue**. The **Set Collection Schedule** page displays.




*Set Collection Schedule*

13. Select options from the following drop-down lists:
    - **Frequency**
    - **Time**
    - **Day**
14. Select the **Run the first collection now** check box.
15. Click **Continue**.



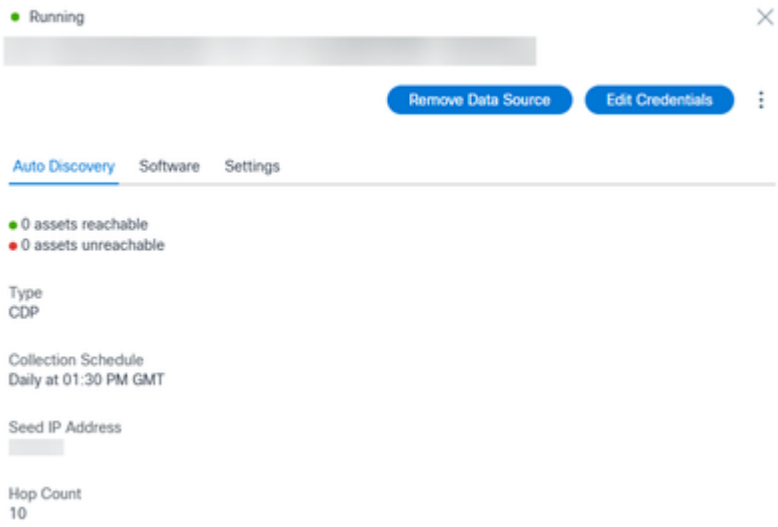

*Set Collection Schedule Continued*

16. Select options from the following drop-down lists:
    - **Collection Time**
    - **AM/PM**
    - **Collection Date**
17. Click **Continue**. Once the data source is added, a confirmation displays.

## Editing CDP or LLDP Details

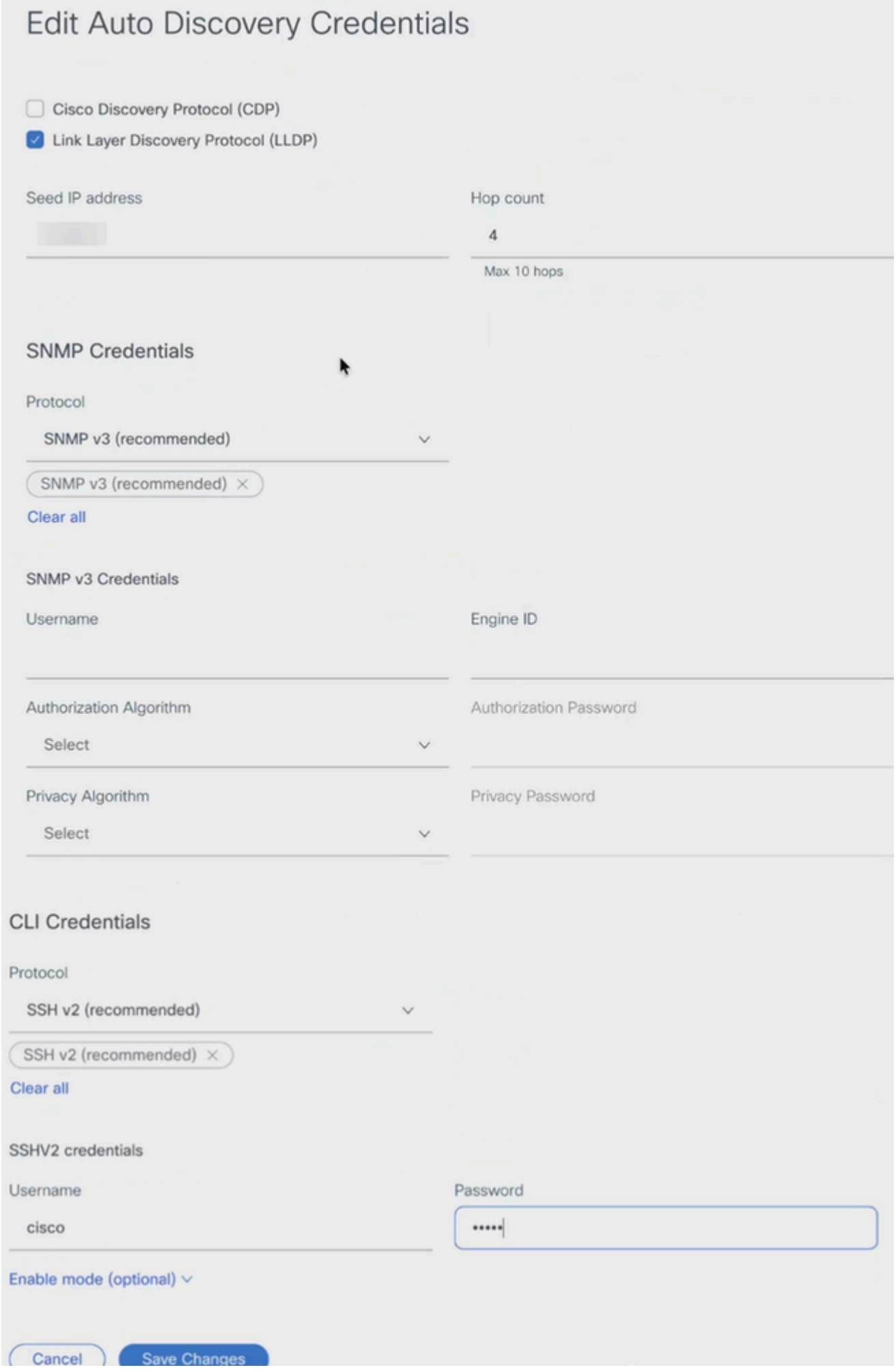
To edit CDP or LLDP details:

1. Navigate to the **Data Sources** window.
2. Click the CX Agent that requires the The CX Agent’s detail window displays.




*CX Agent Detail Window*

3. Click **Edit Credentials**. The **Edit Auto Discovery Credentials** page displays.



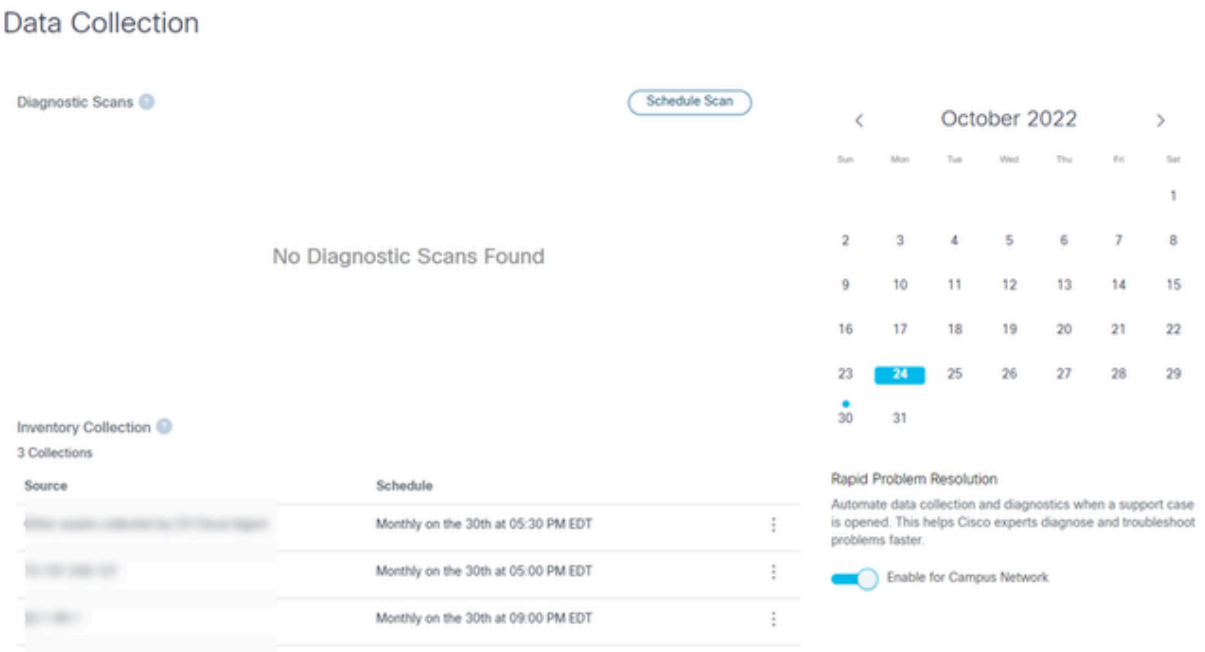

*Edit Auto Discovery Credentials*

4. Make the desired edits

: 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.

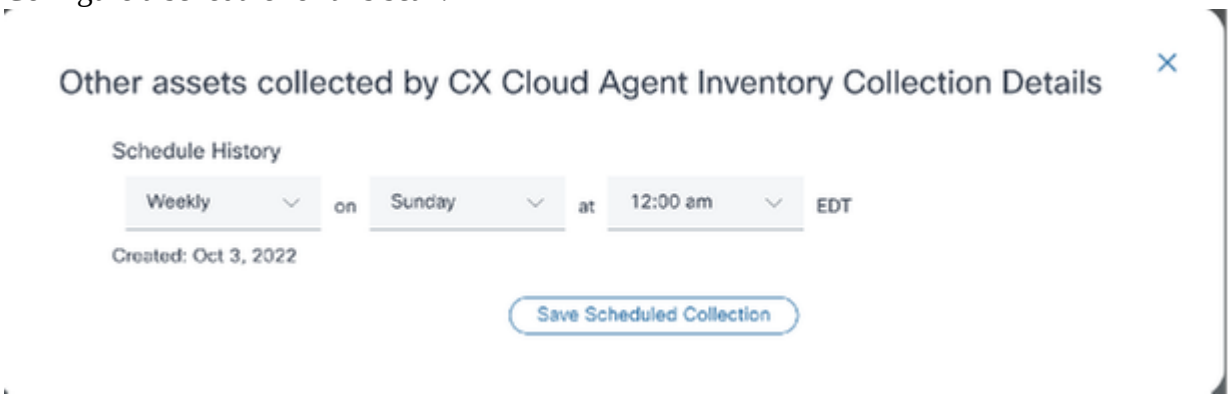
To schedule diagnostic scans:

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**.



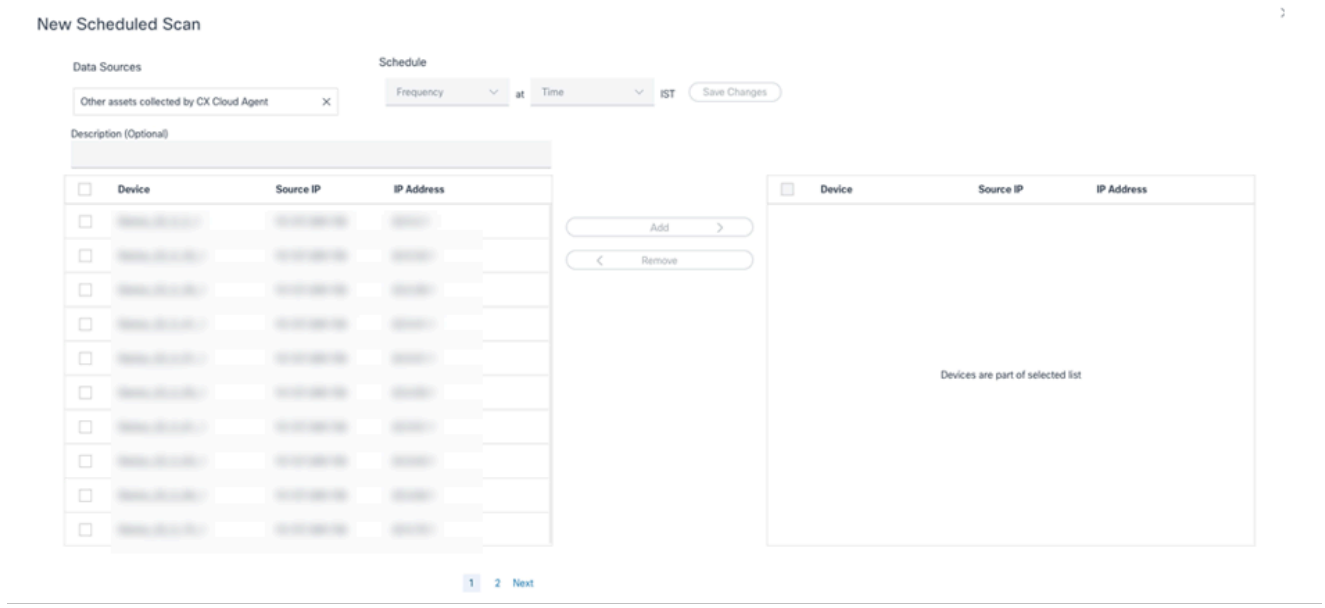

*Scheduling Scans*

4. Configure a schedule for this scan.




*Configure Scan Schedule*

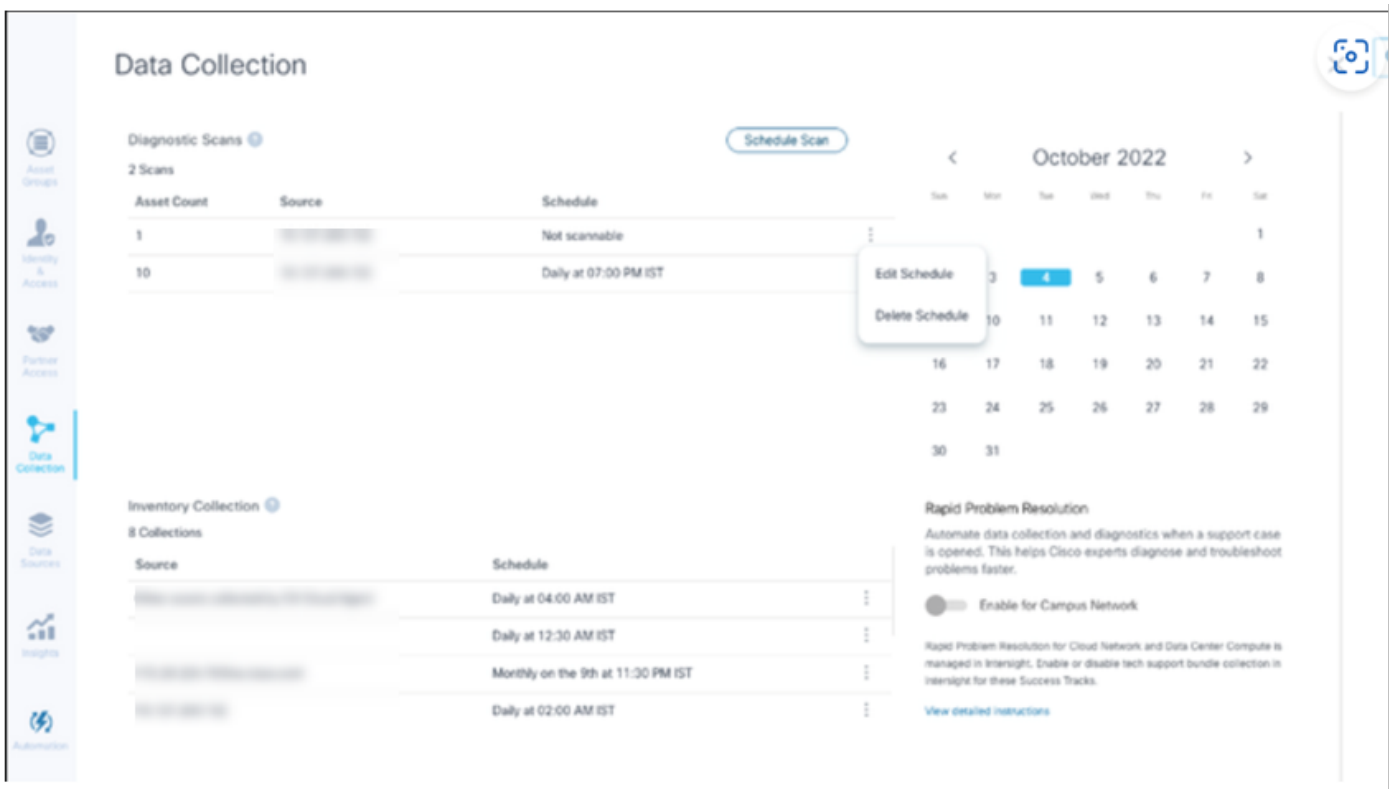
5. In the devices list, select all devices for the scan and click **Add**.




*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 with Edit and Delete Schedule options*

# Upgrading CX Agent VMs to Medium and Large Configurations

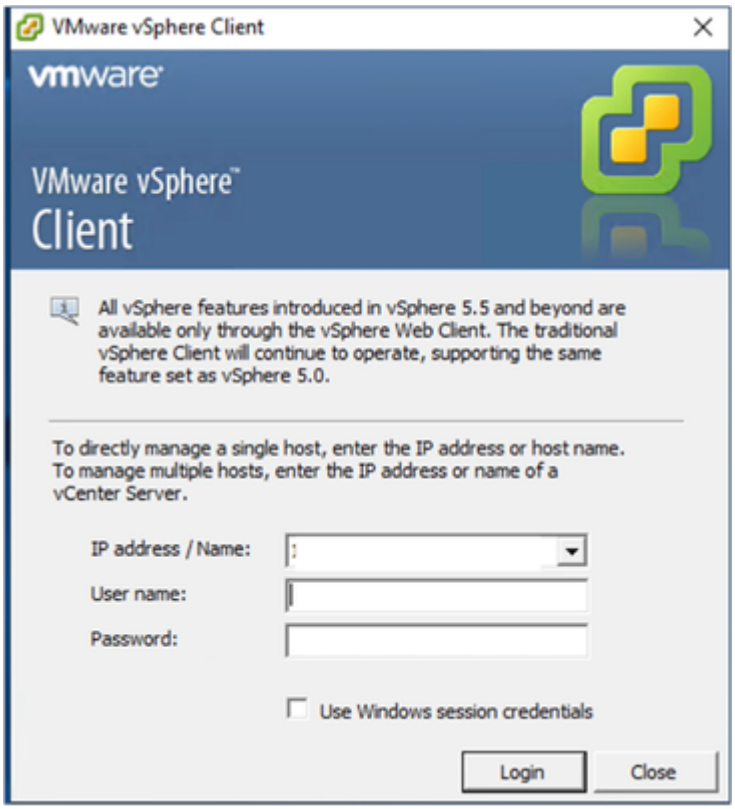
Once VMs are upgraded, it is not possible to:

- 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.

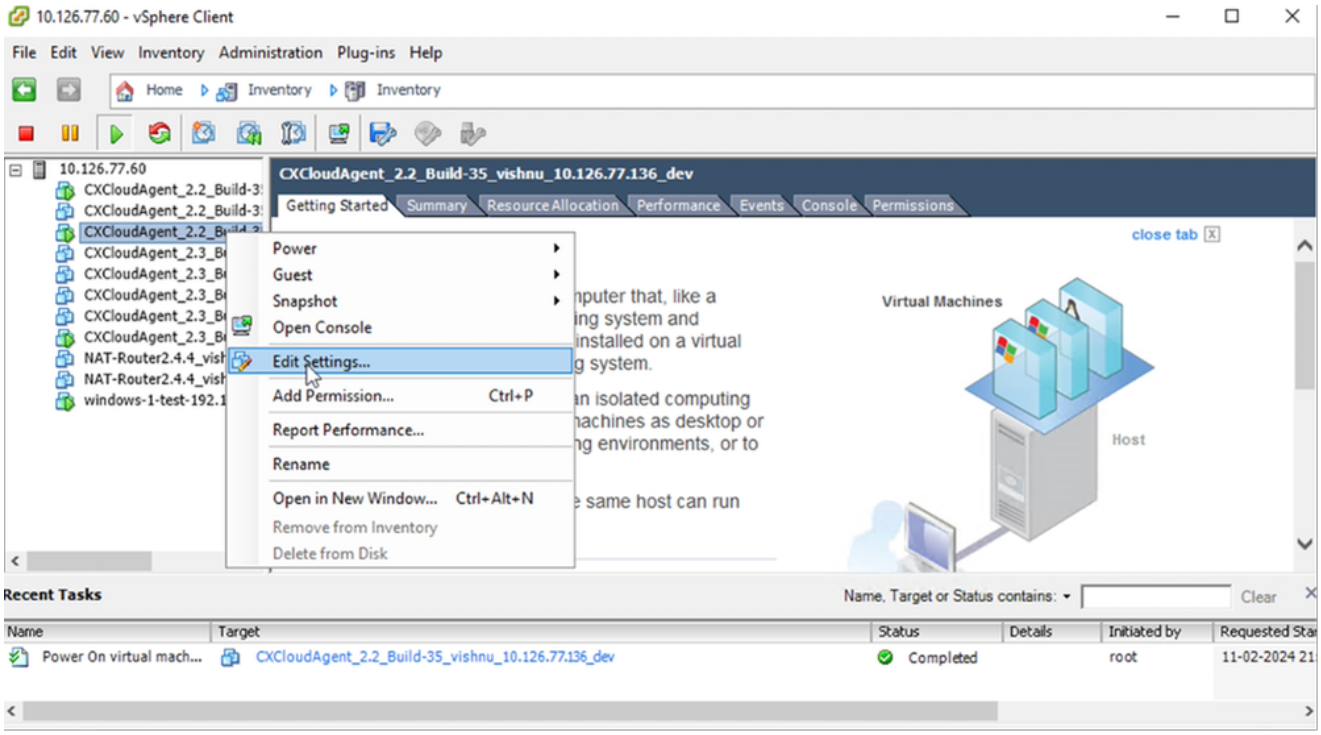
## Reconfiguring Using VMware vSphere Thick Client

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



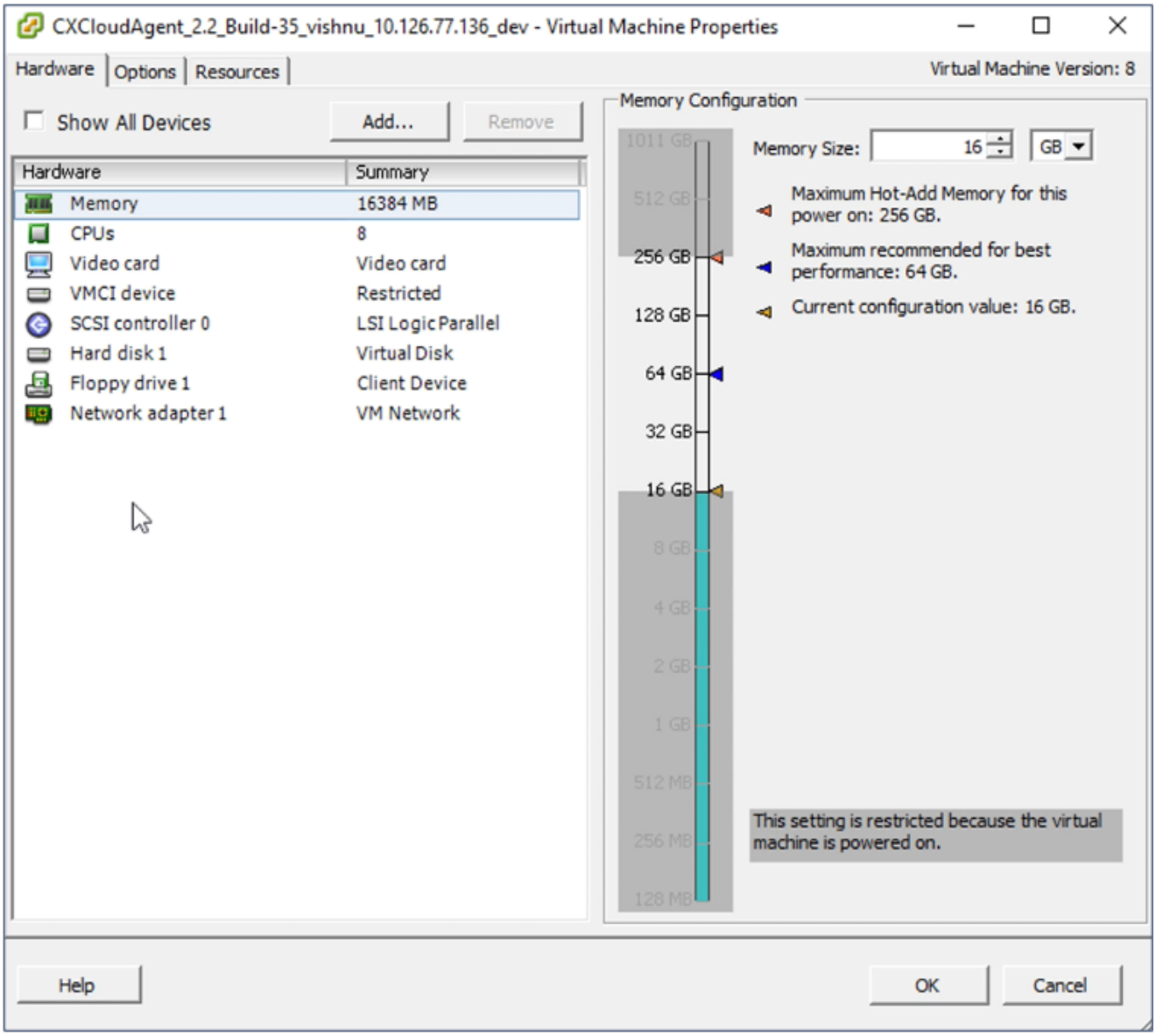

*vSphere Client*

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



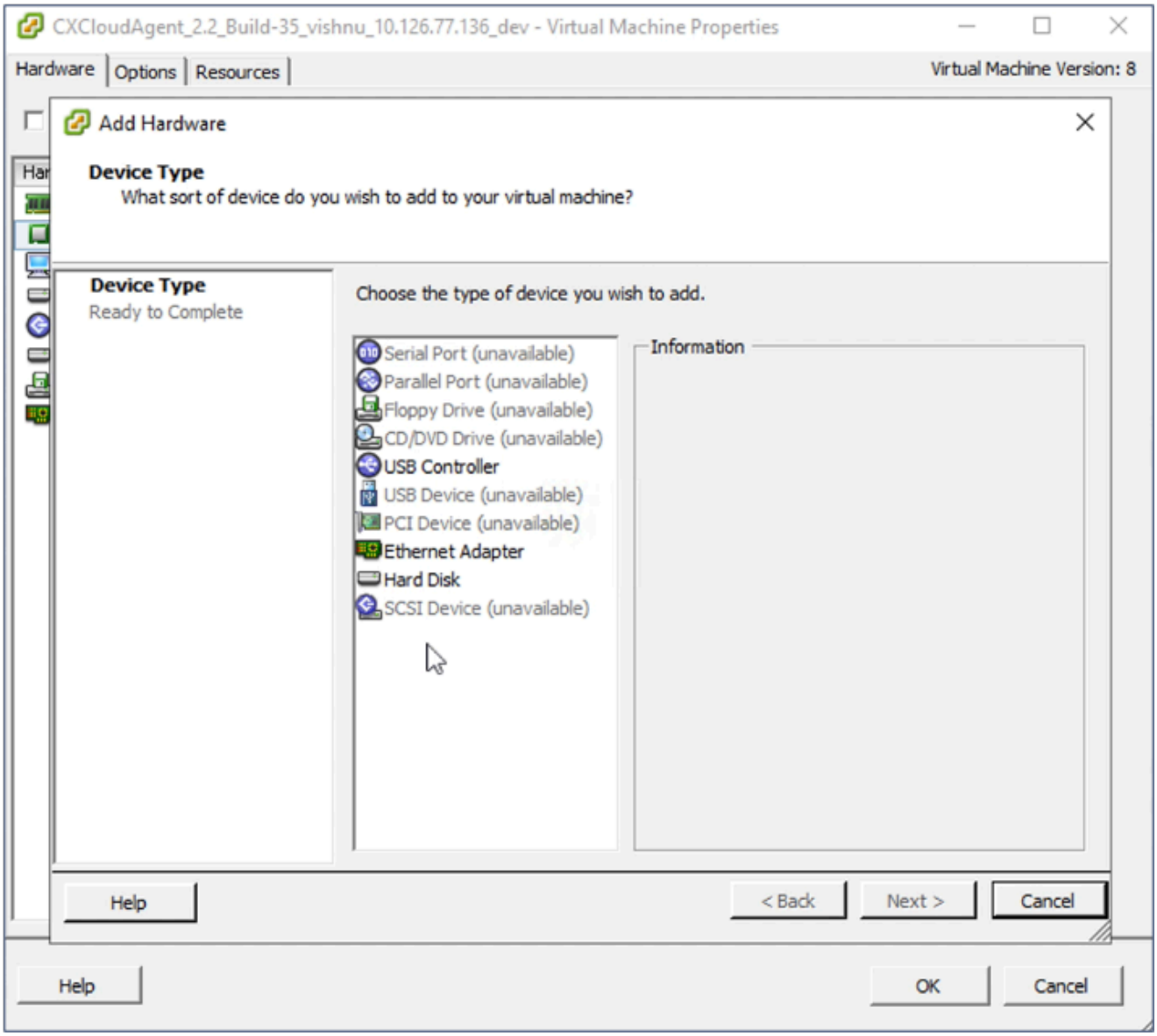

*Edit Settings*

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



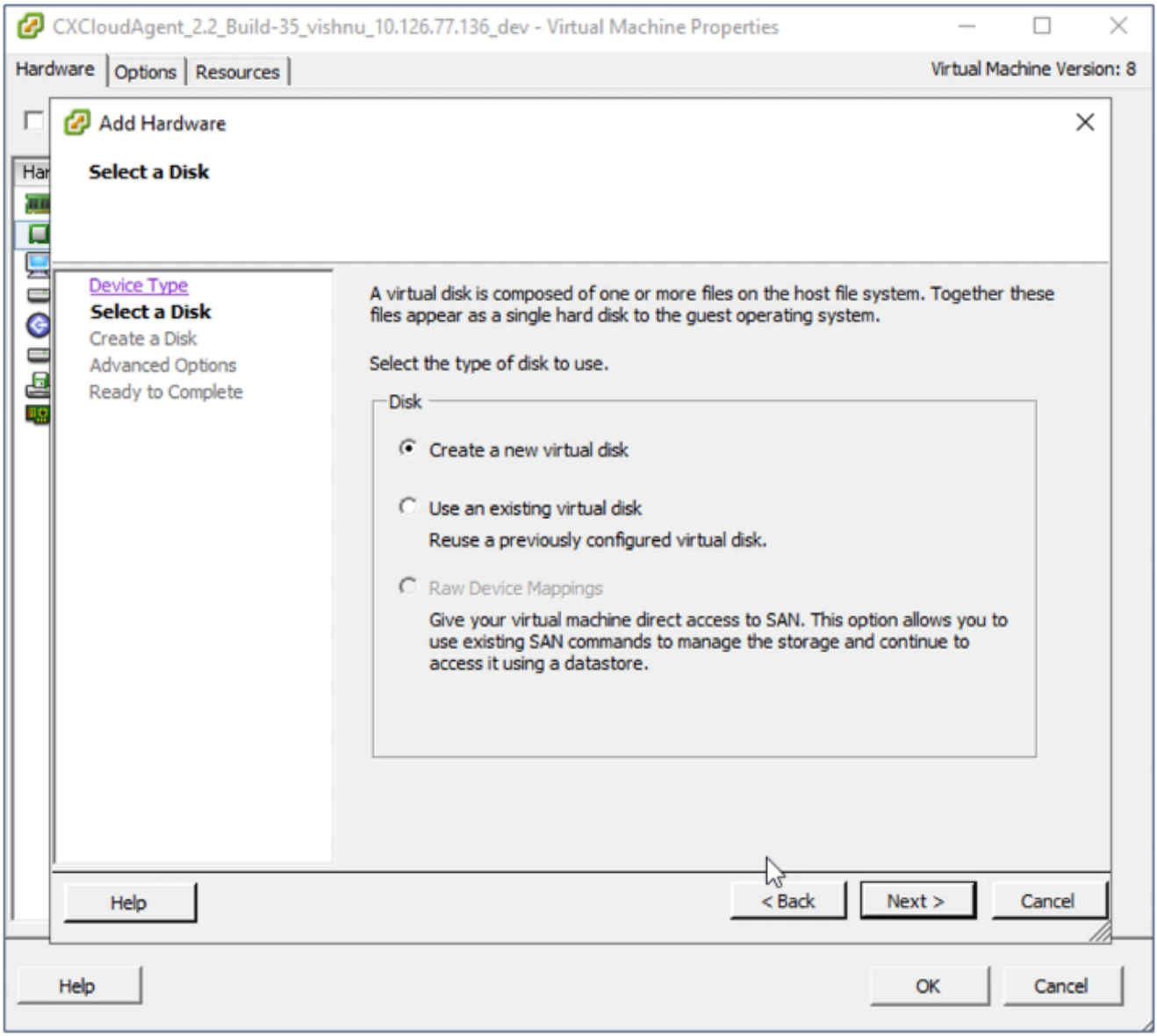

*VM Properties*

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



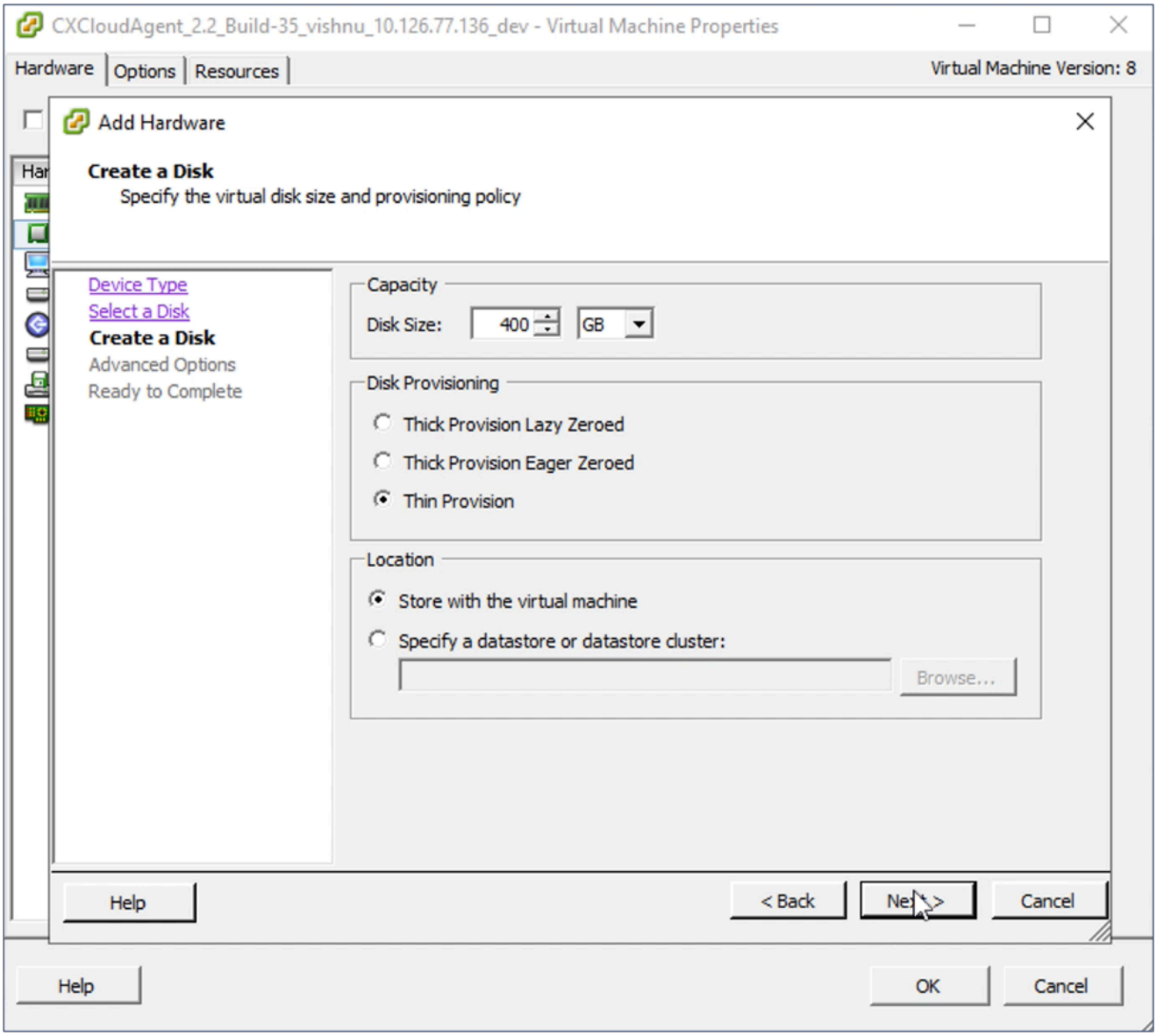

*Device Type*

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



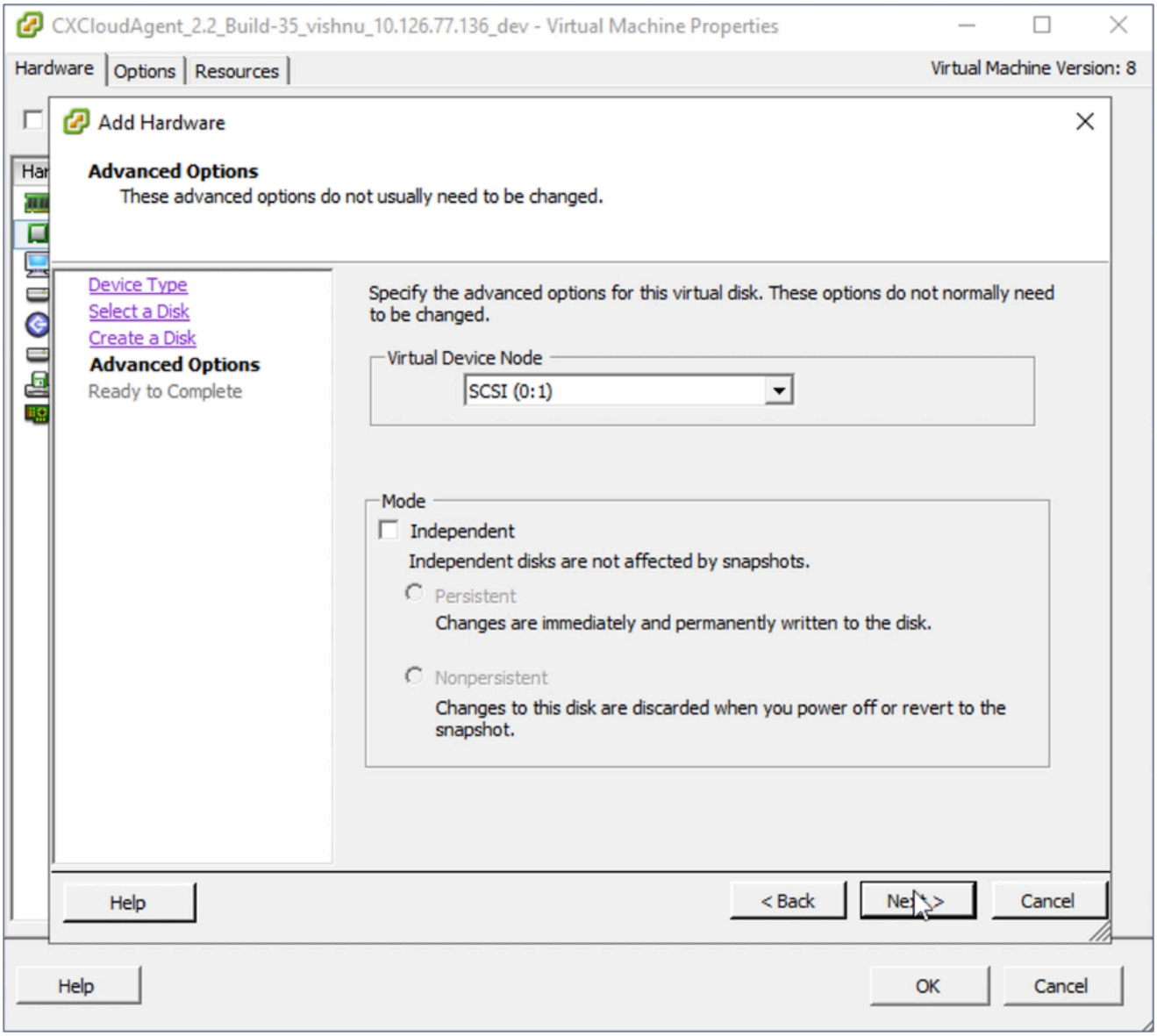

*Select Disk*

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



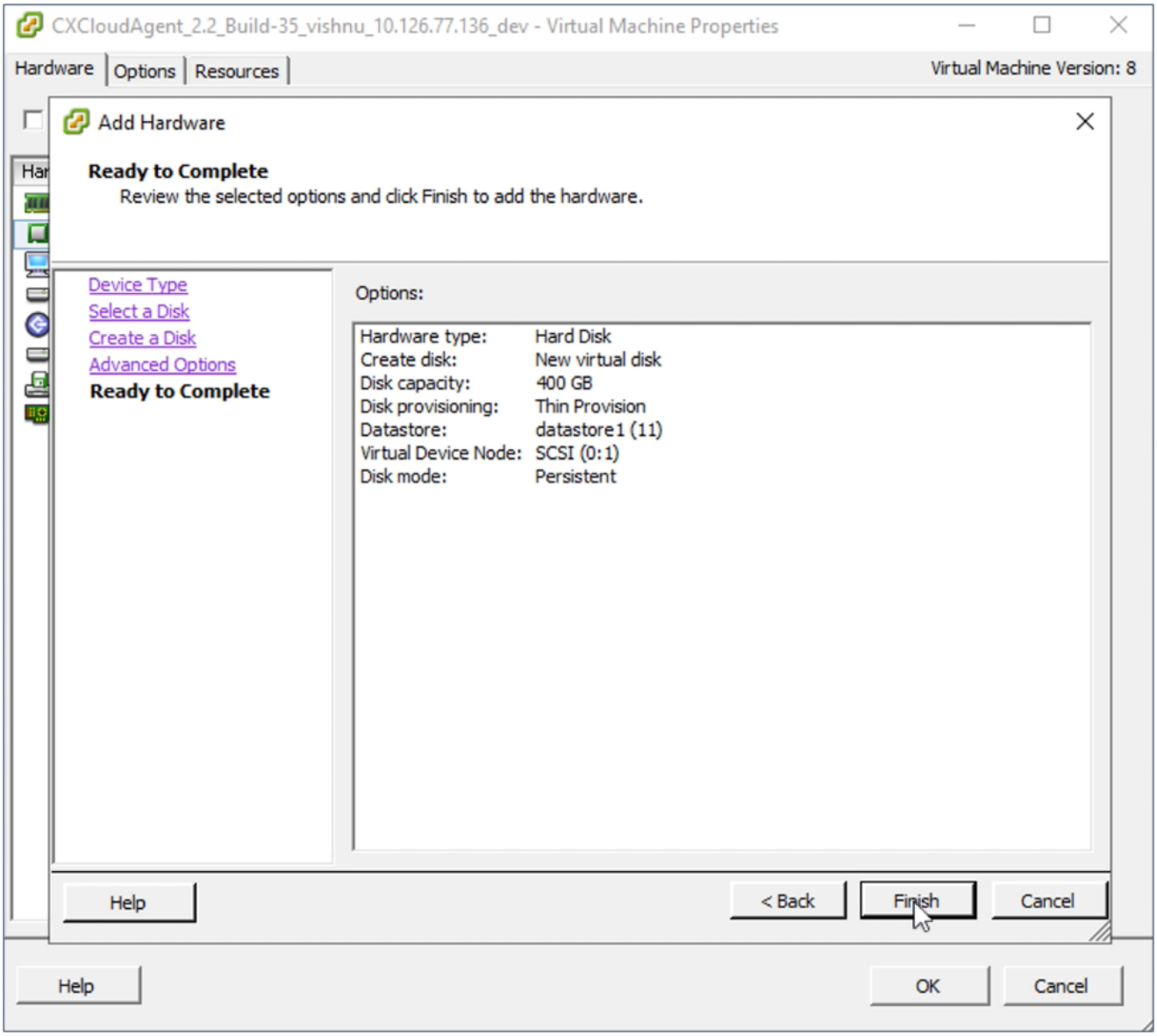

*Create Disk*

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



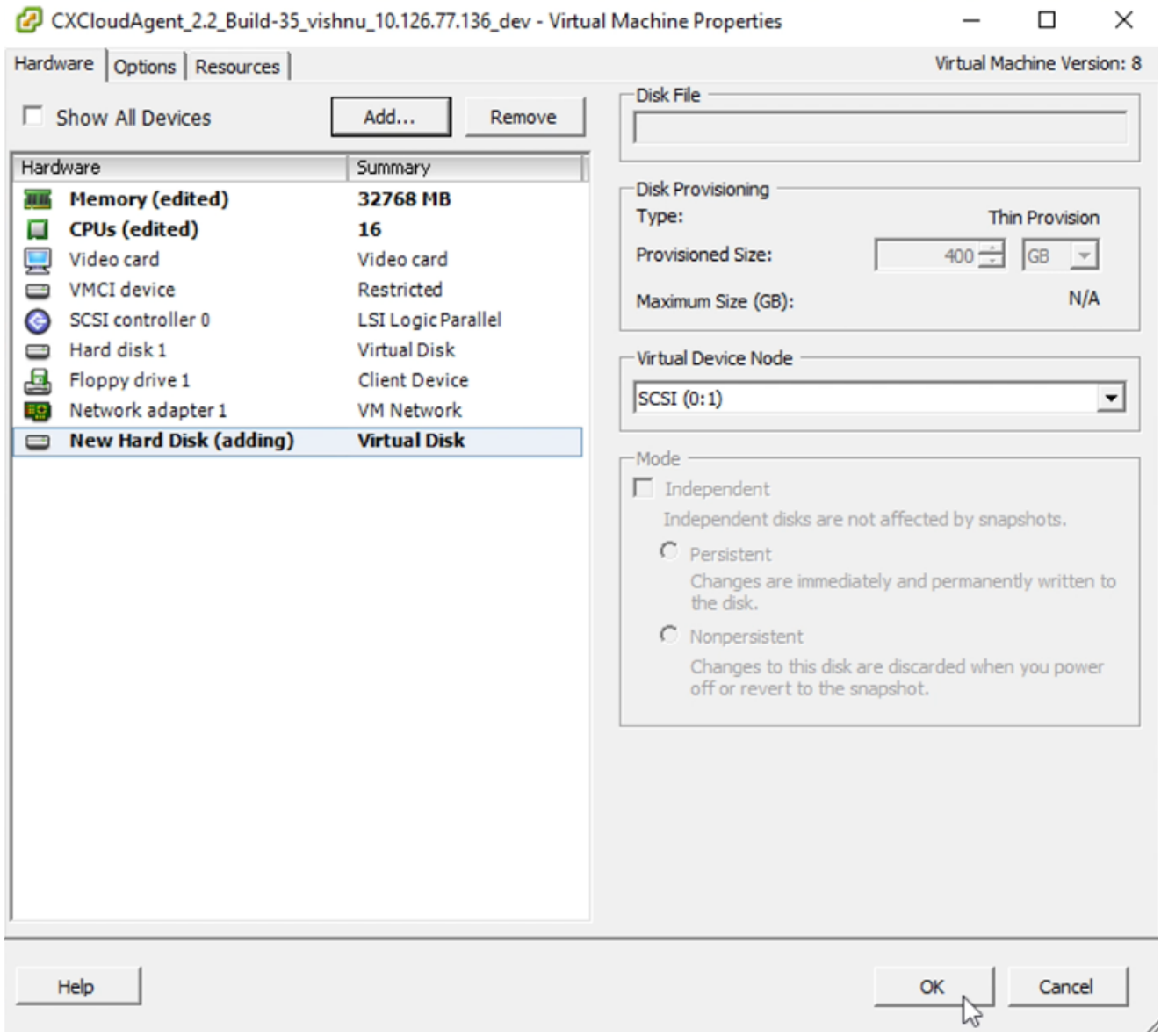

*Advanced Options*

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



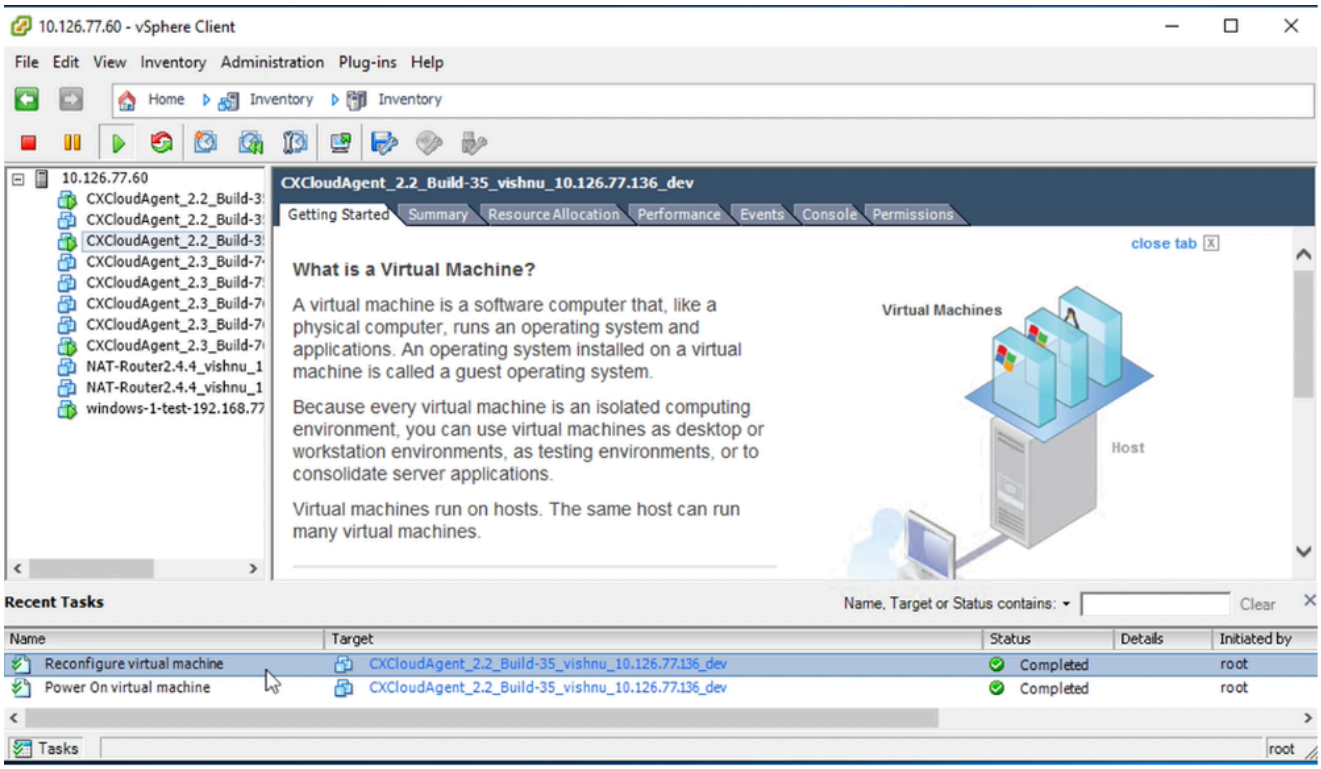

*Ready to Complete*

13. Click **Finish**.




*Hardware*

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

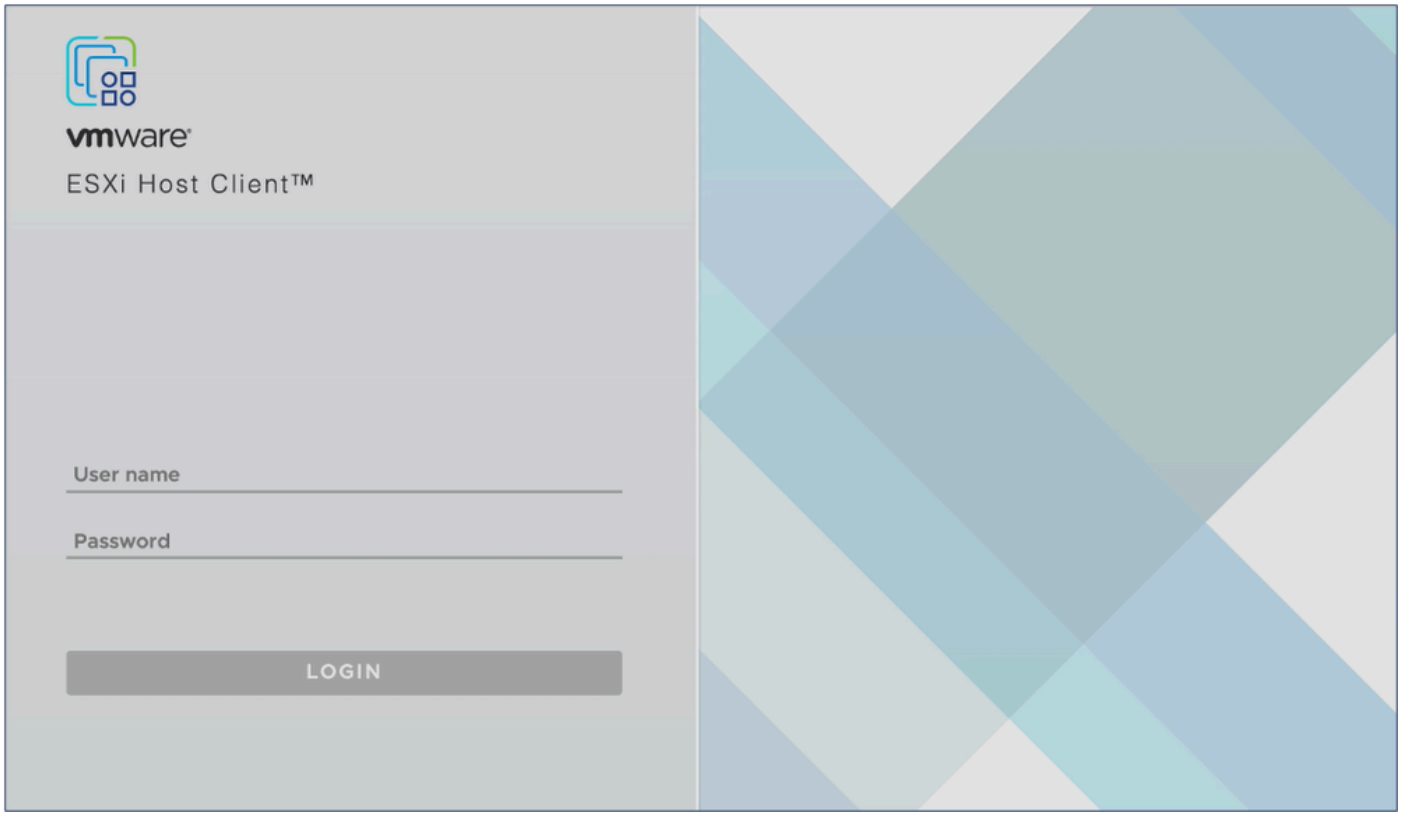



*Recent Tasks*

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

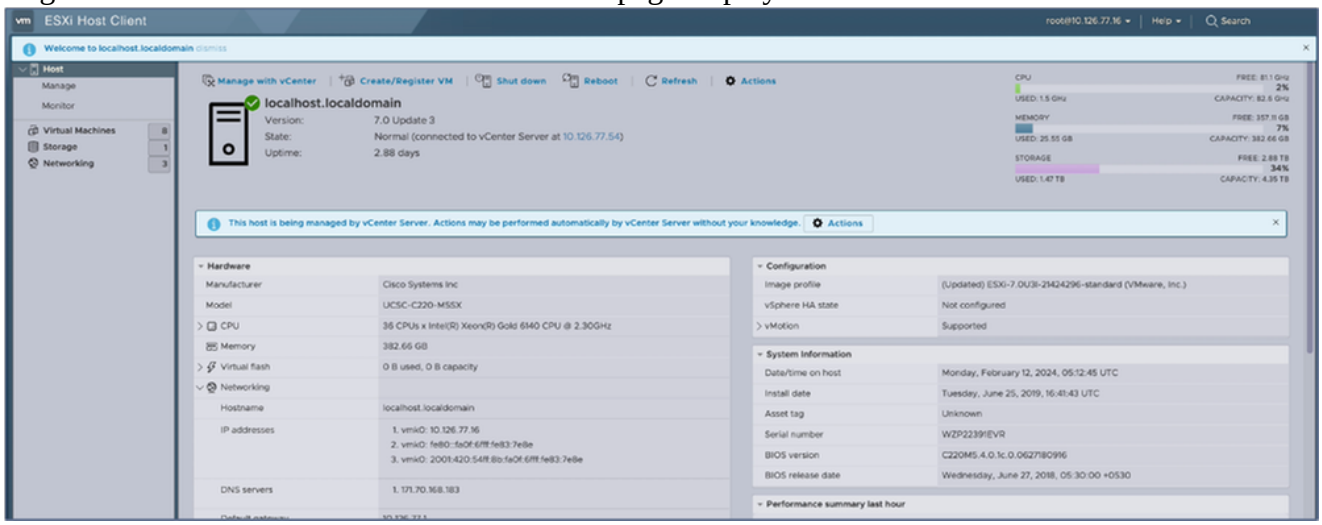
## Reconfiguring Using Web Client ESXi v6.0

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



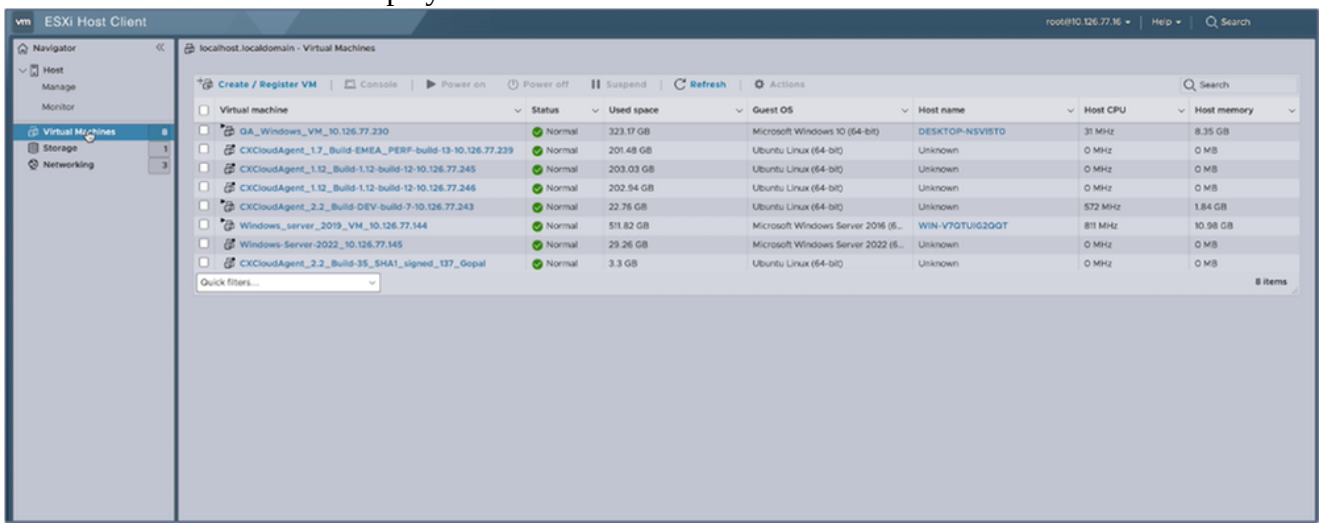
*ESXi Client*

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



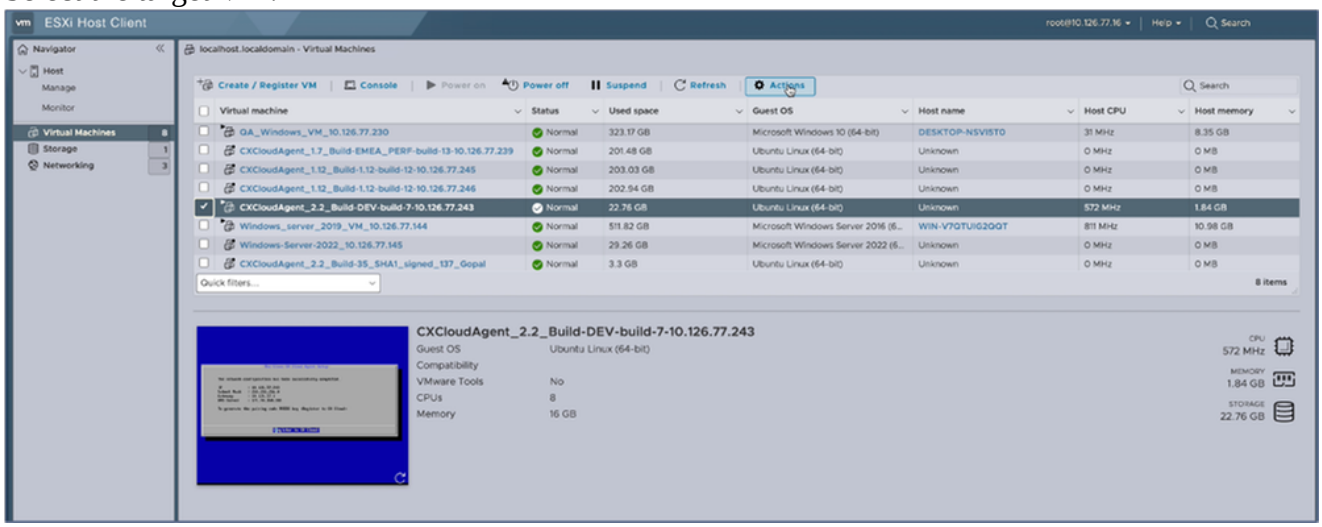

*ESXi Home Page*

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



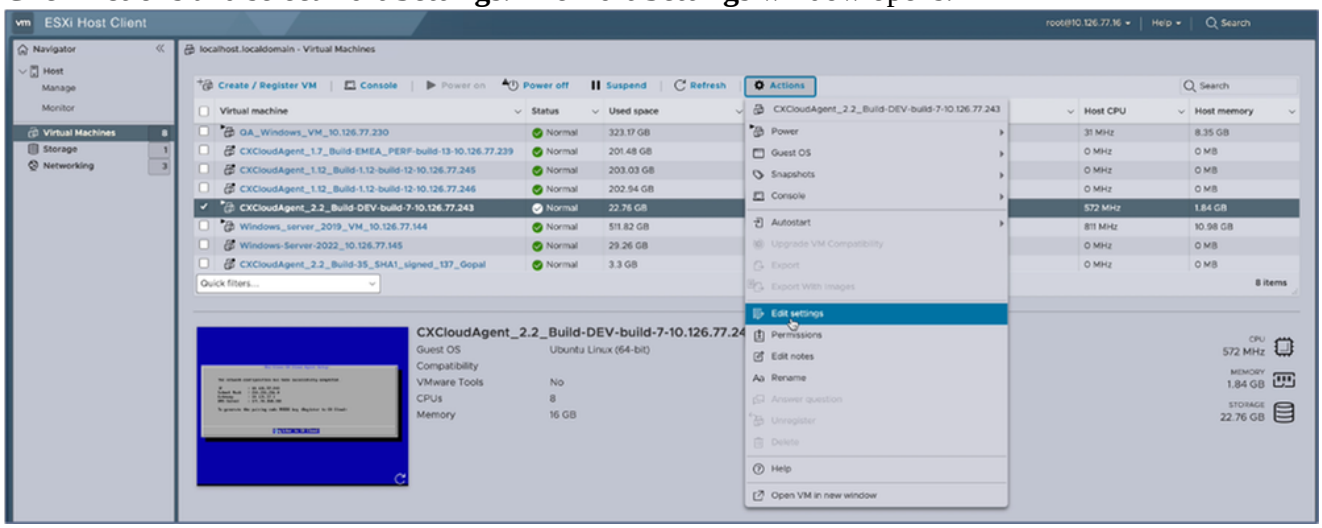

*List of VMs*

3. Select the target VM.

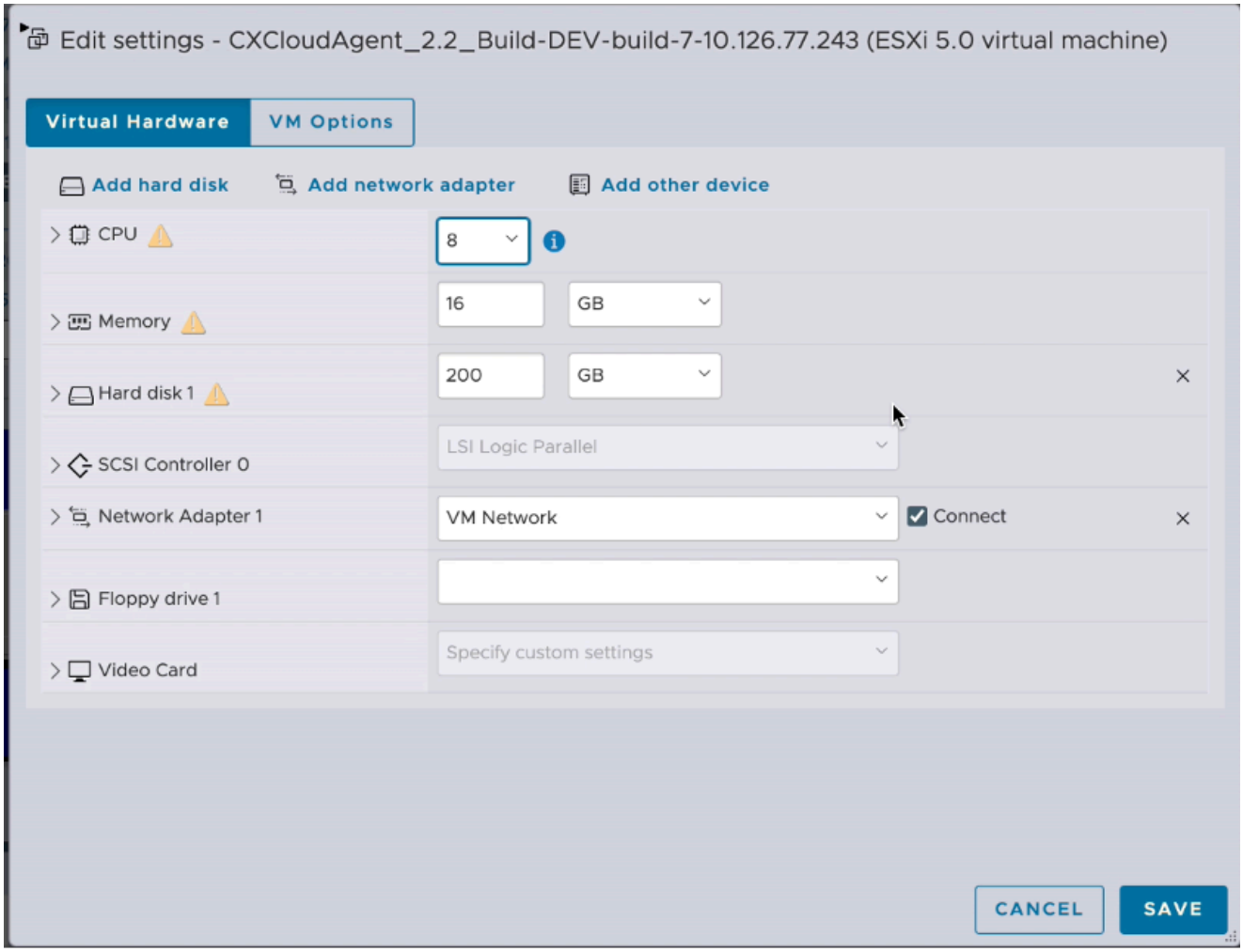



*Target VM*

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




*Actions*

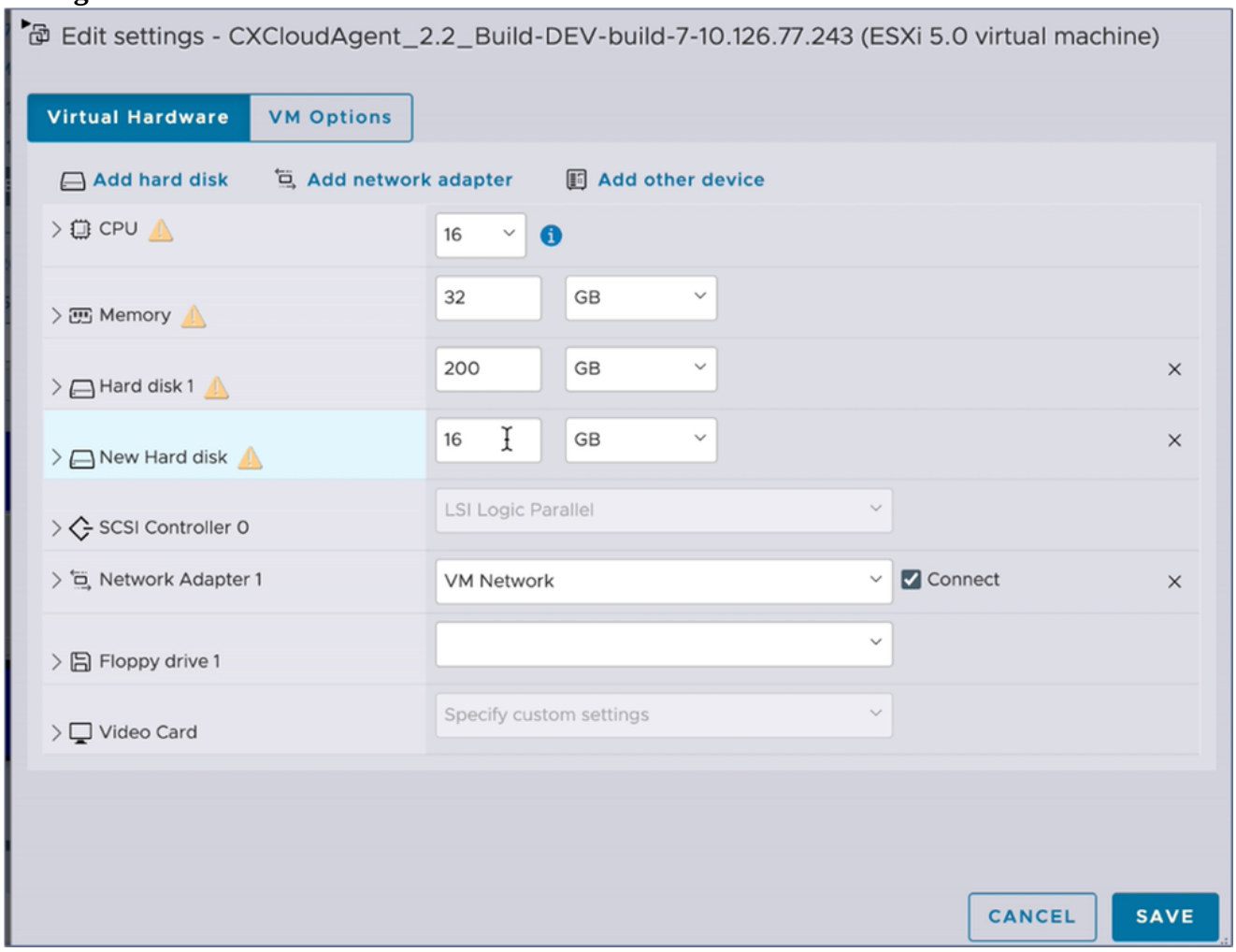



*Edit Settings*

5. Update the **CPU** value as specified:
   Medium: 16 core (8 sockets *2 core/socket)
   Large: 32 core (16 sockets *2 core/socket)
6. Update the **Memory** value as specified:

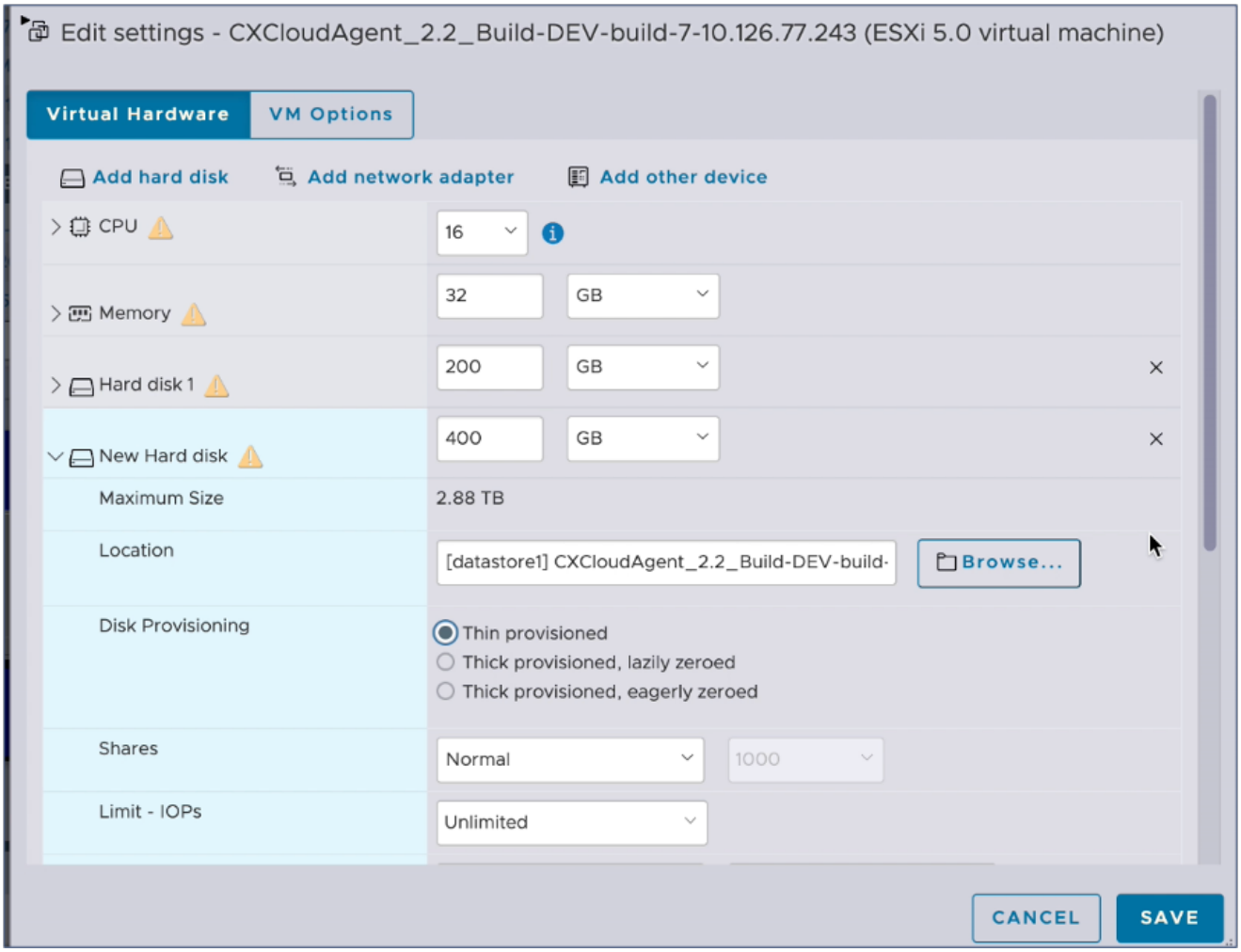
Medium: 32 GB
Large: 64 GB

7. Click **Add hard disk** > **New standard hard disk**. The new hard disk entry displays in the **Edit settings** window.



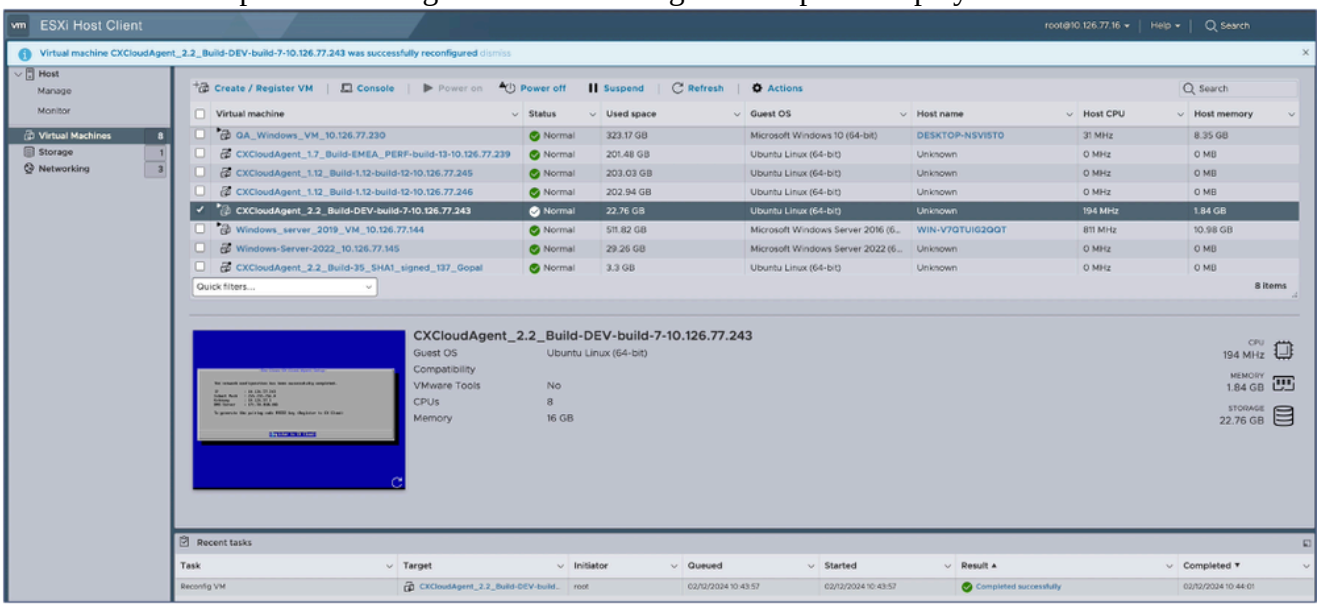

*Edit Settings*

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*

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




*Recent Tasks*

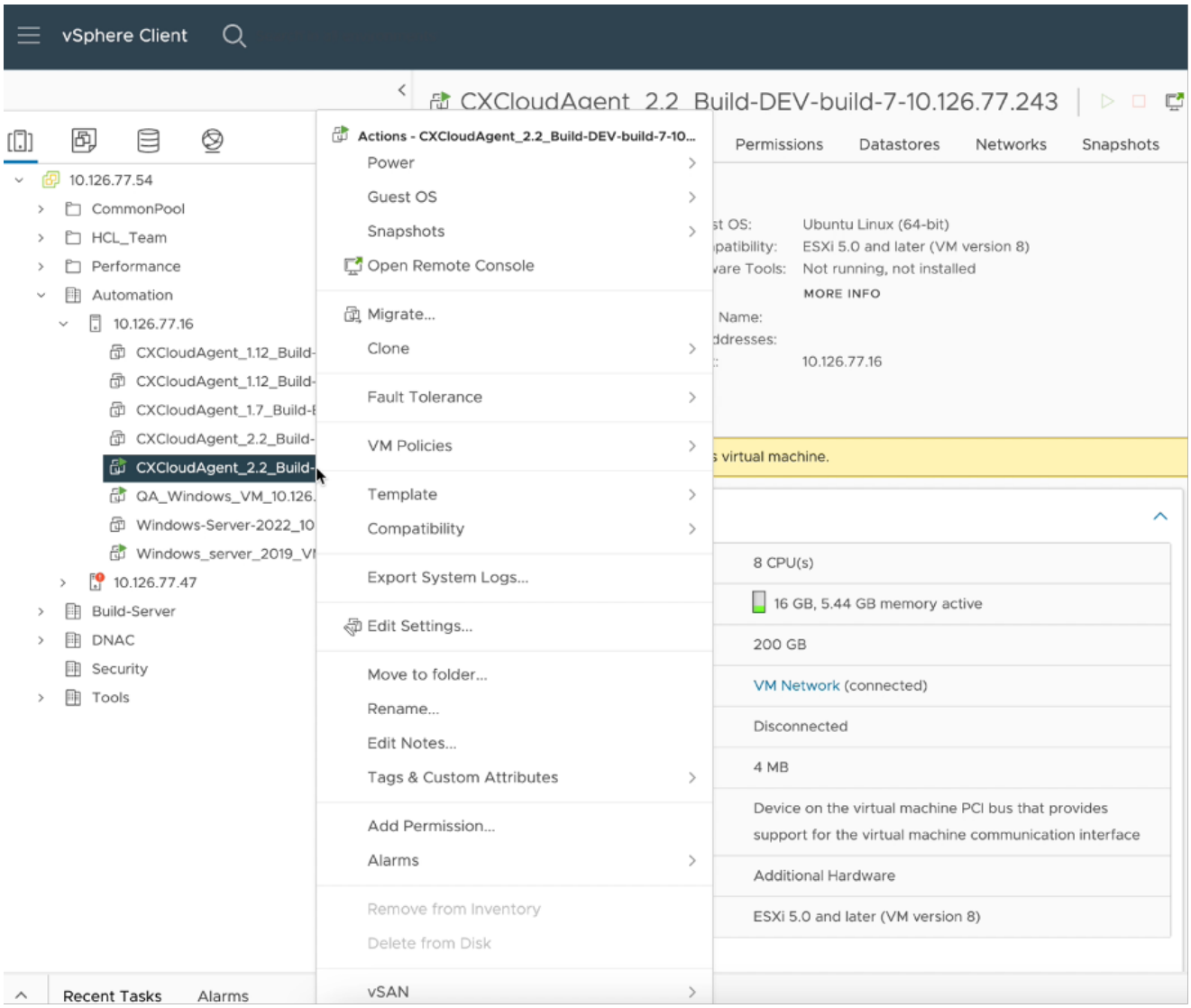
## Reconfiguring Using Web Client vCenter

To update the VM configurations using the Web Client vCenter:



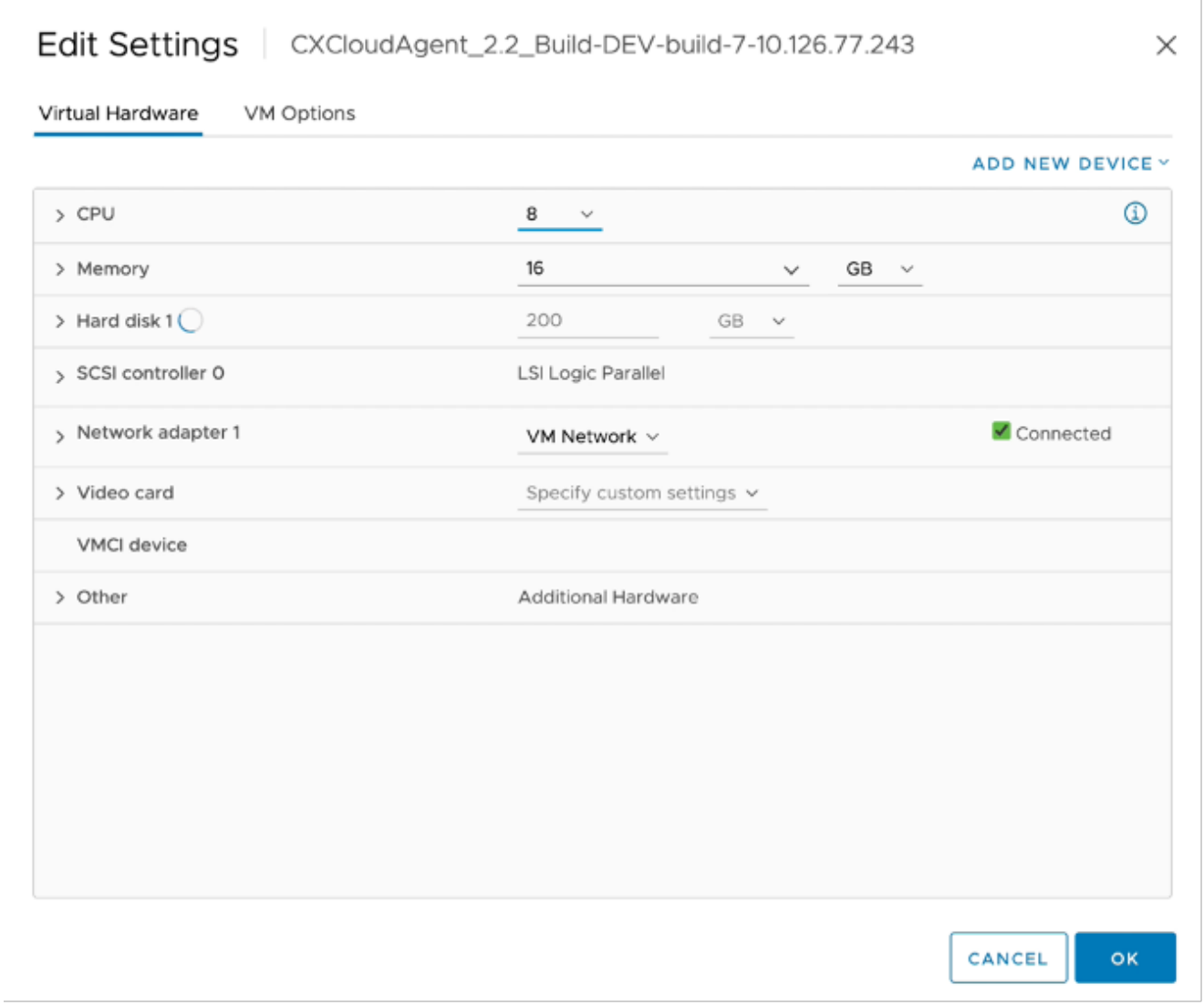

*vCenter*

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



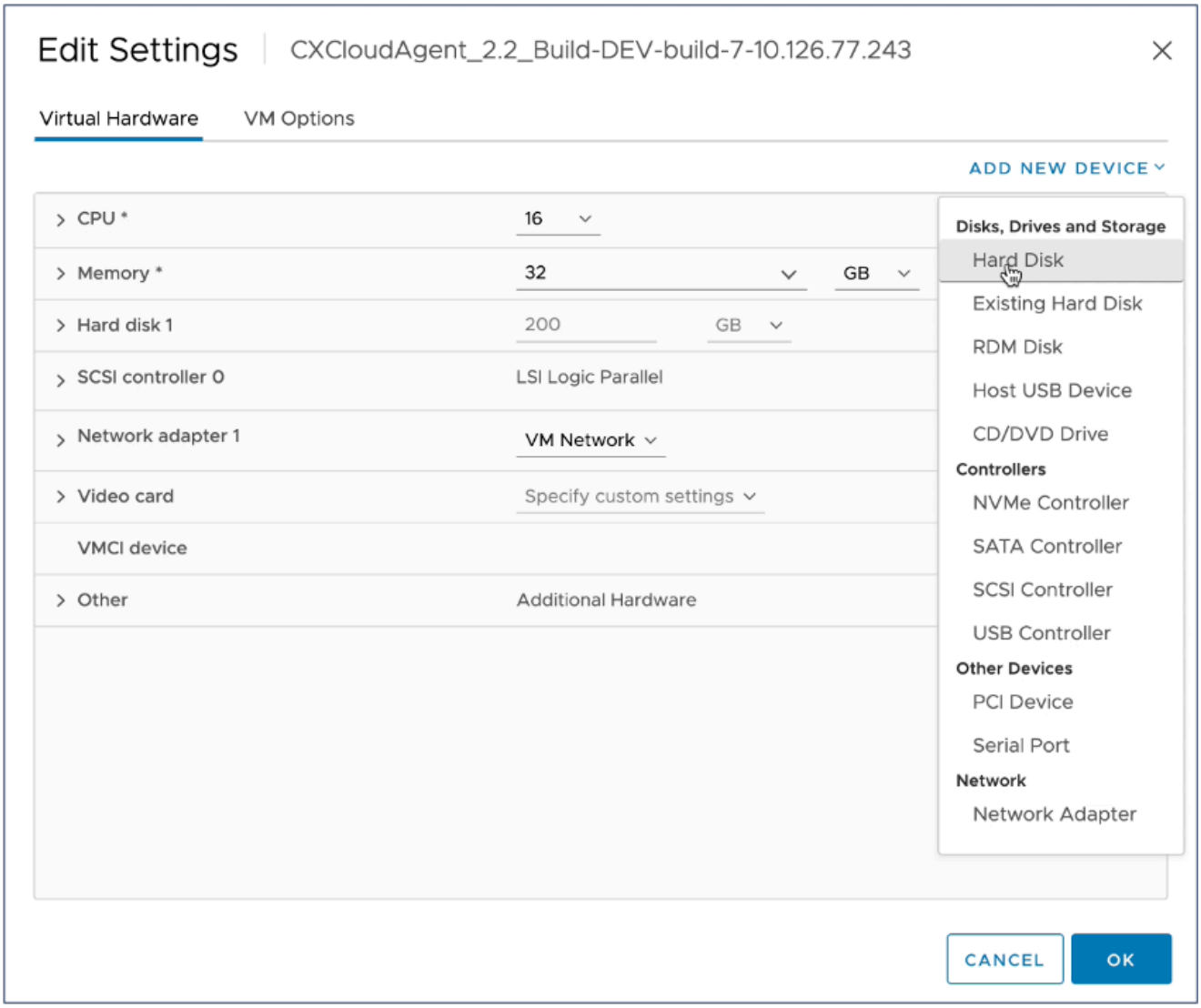

*List of VMs*

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



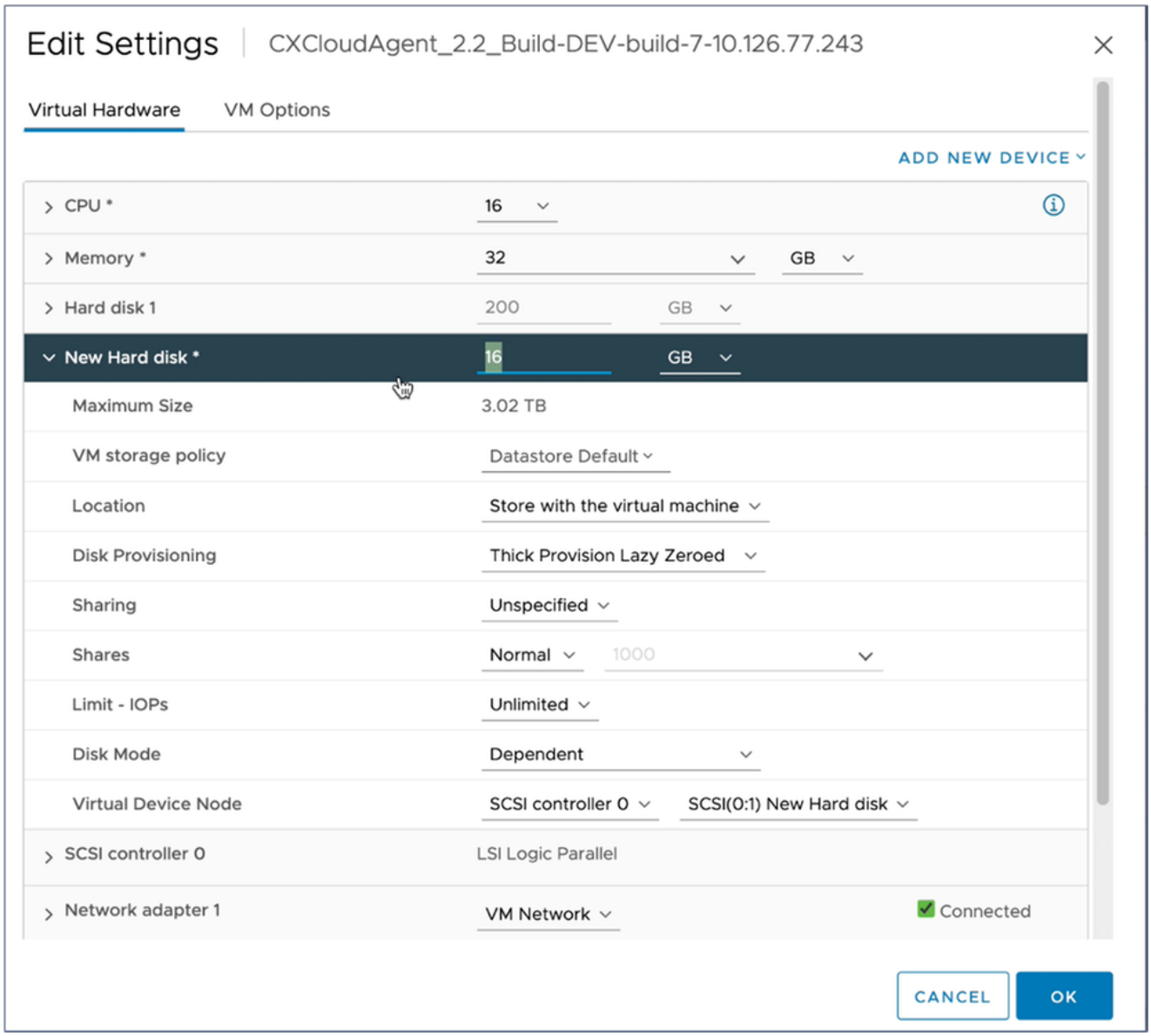

*Edit Settings*

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



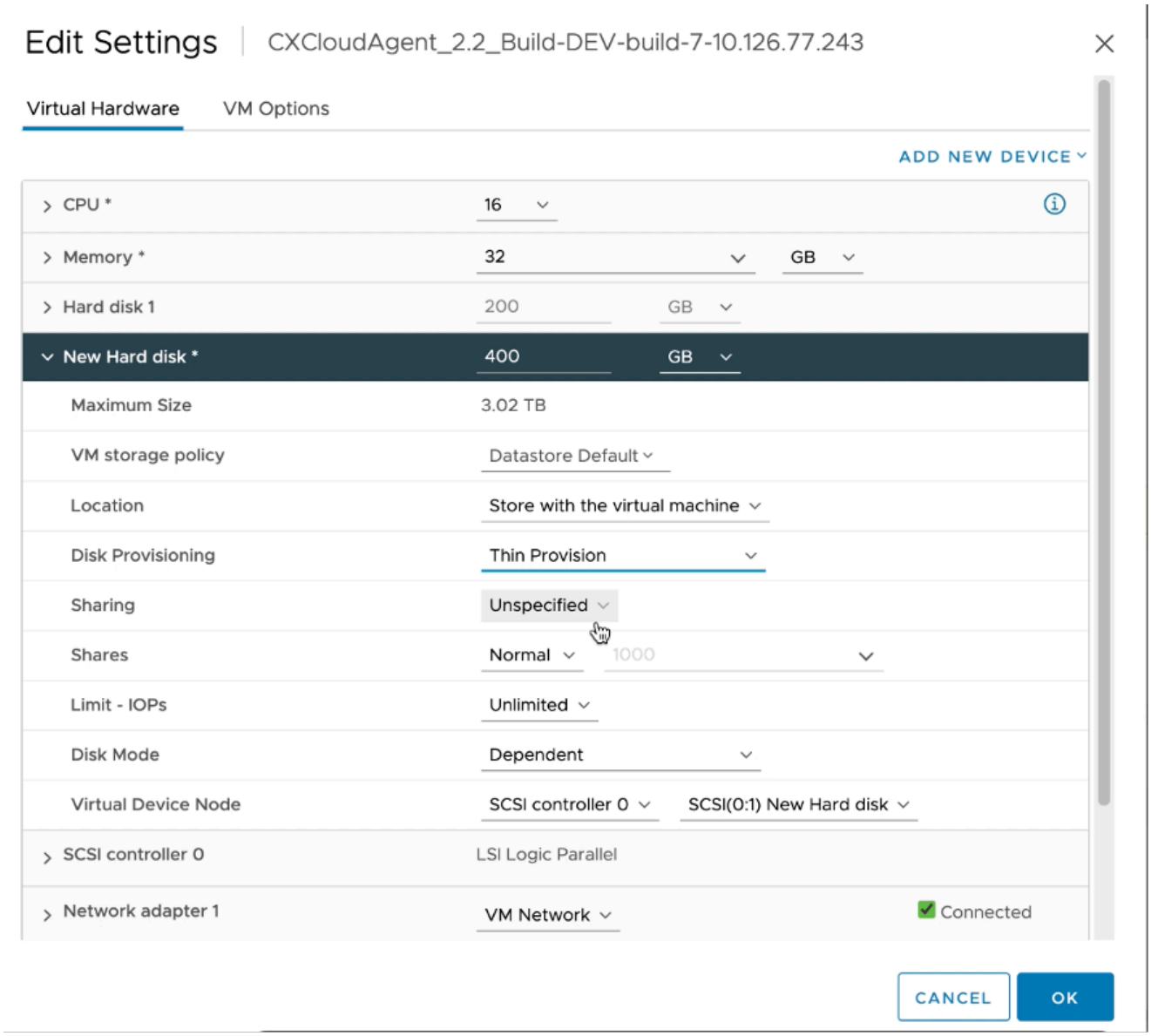

*Edit Settings*

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




*Edit Settings*

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




*Edit Settings*

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

# Deployment and Network Configuration

Select any of these options to deploy the CX 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

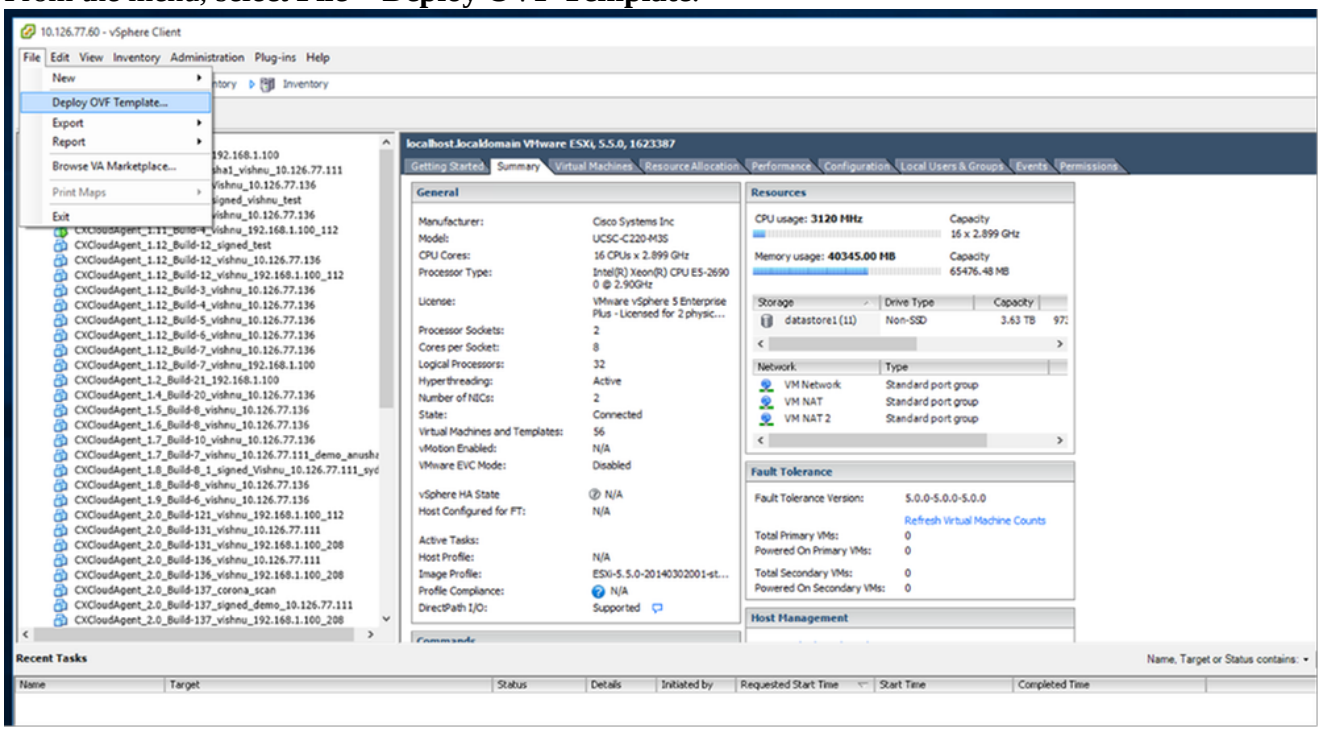
This client allows deployment of CX Agent OVA by use of the vSphere thick client.

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



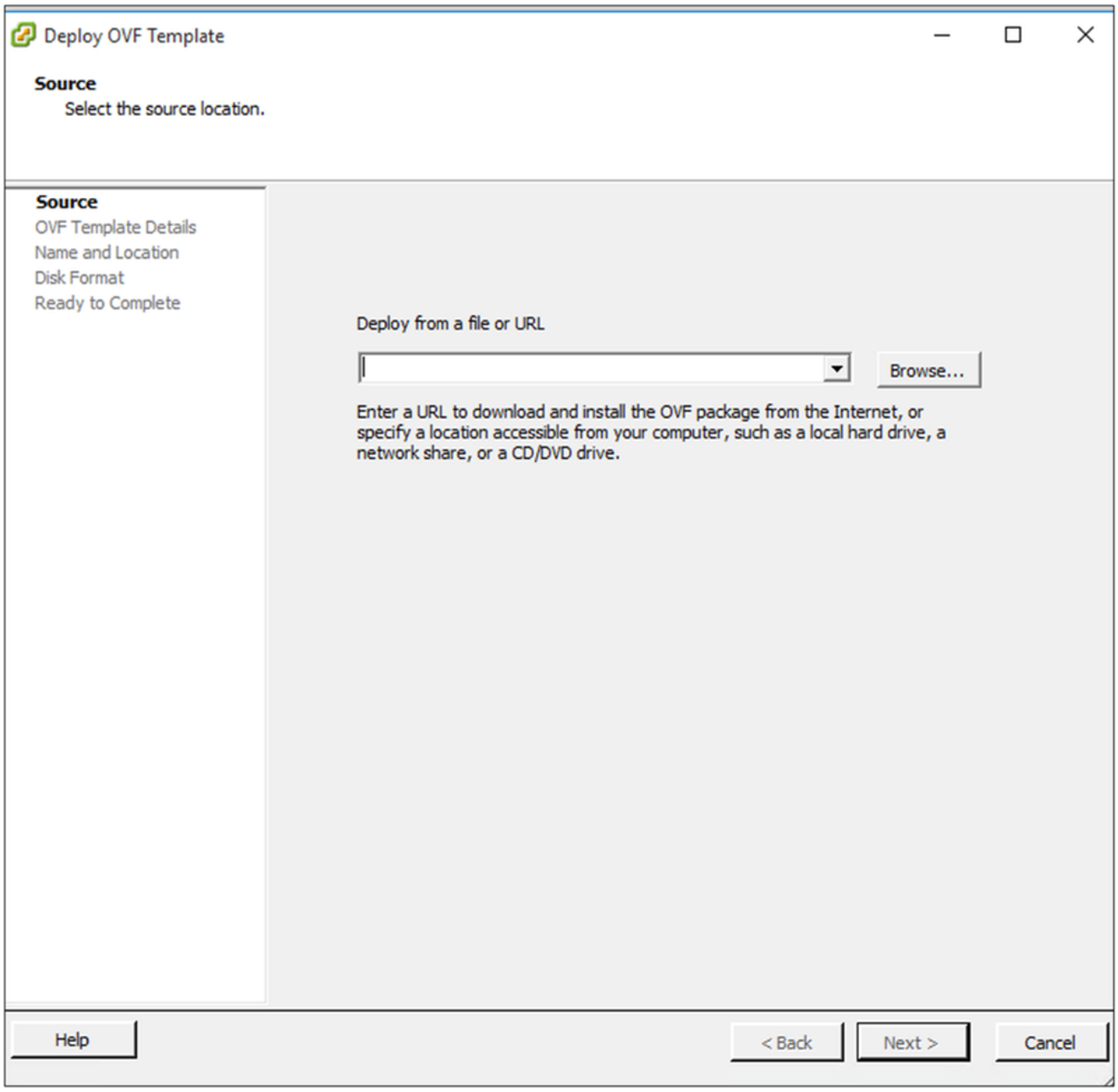

*Login*

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



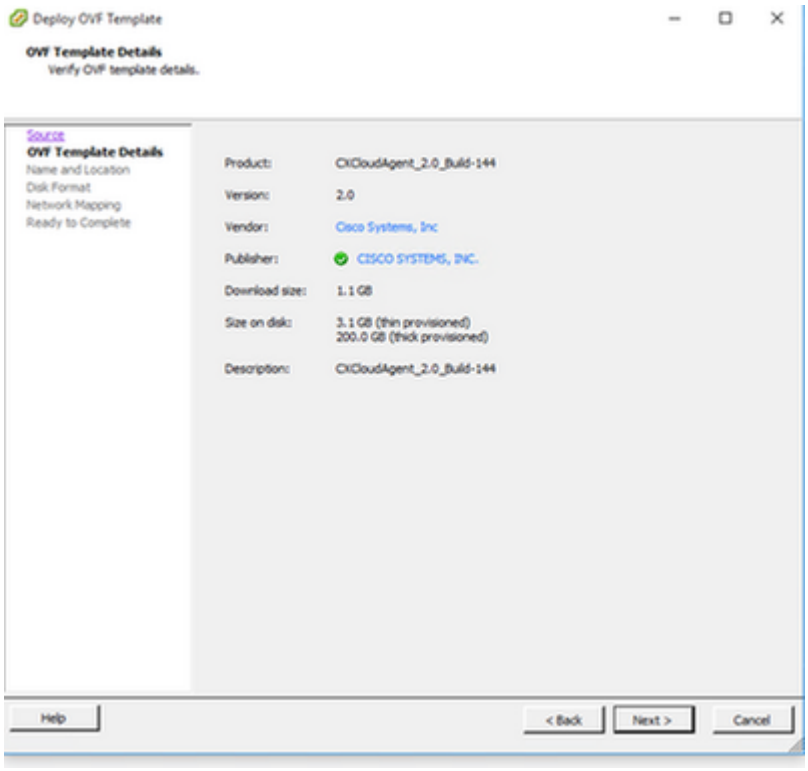

*vSphere Client*

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



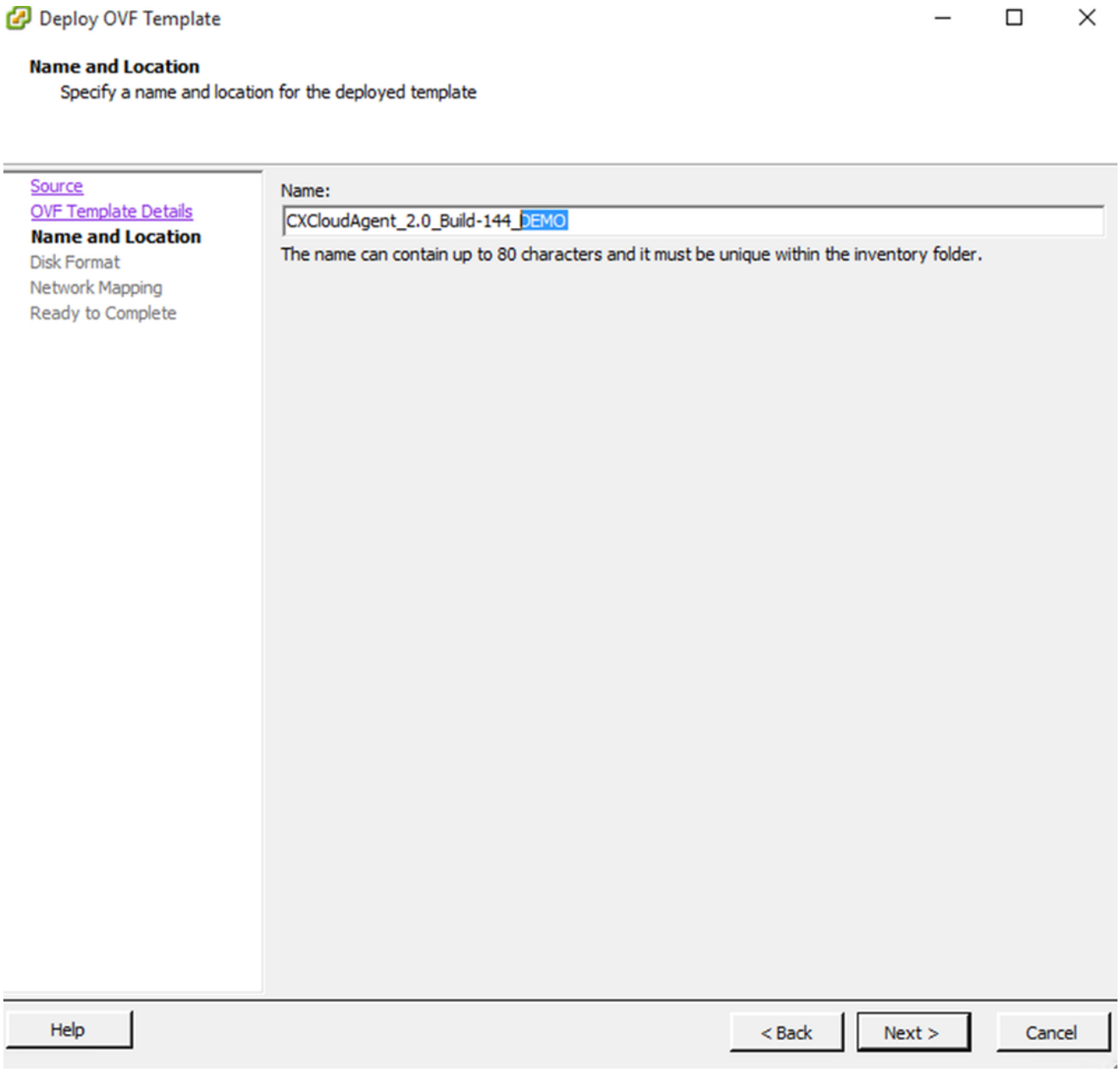

*OVA Path*

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



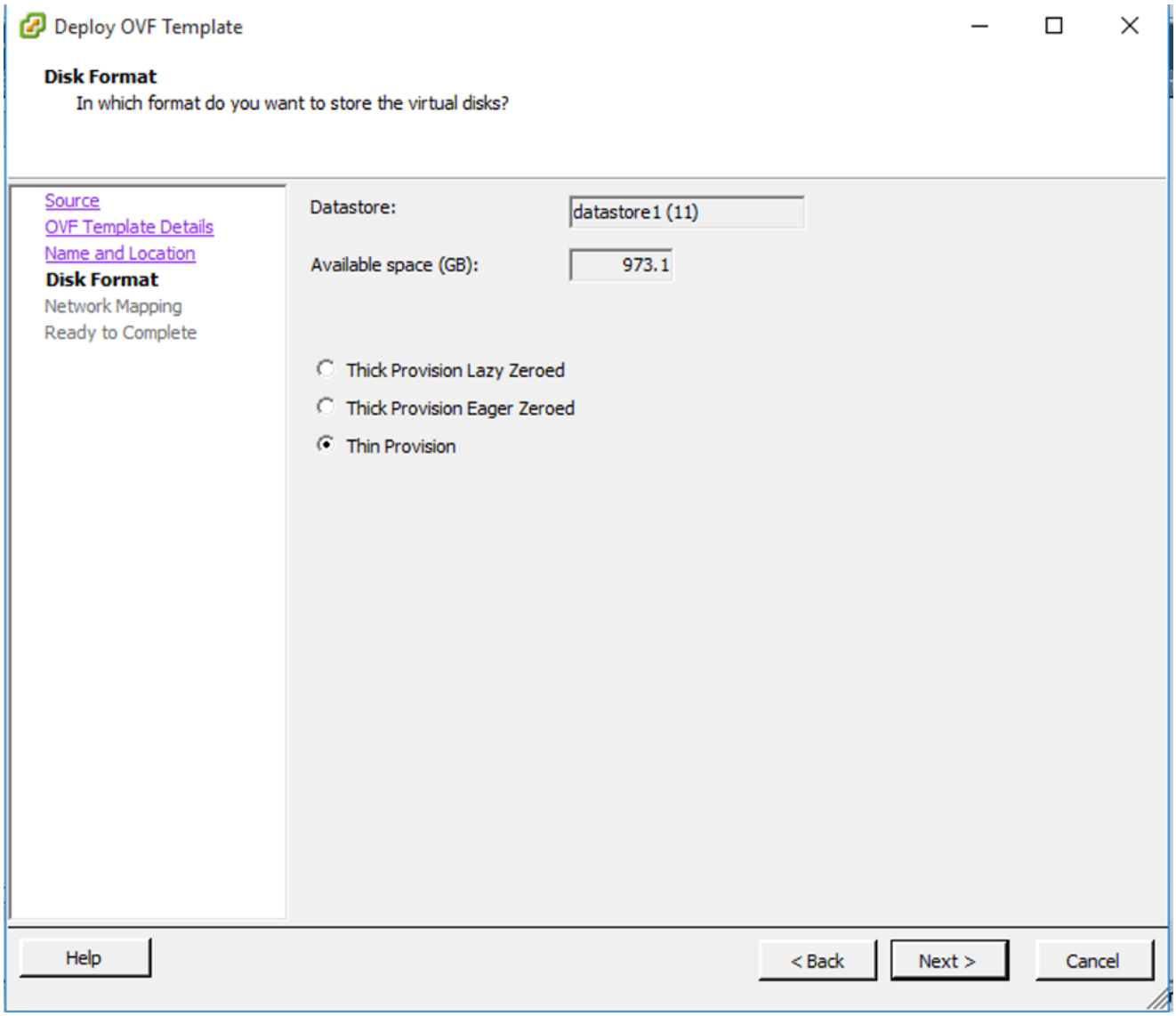

*Template Details*

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



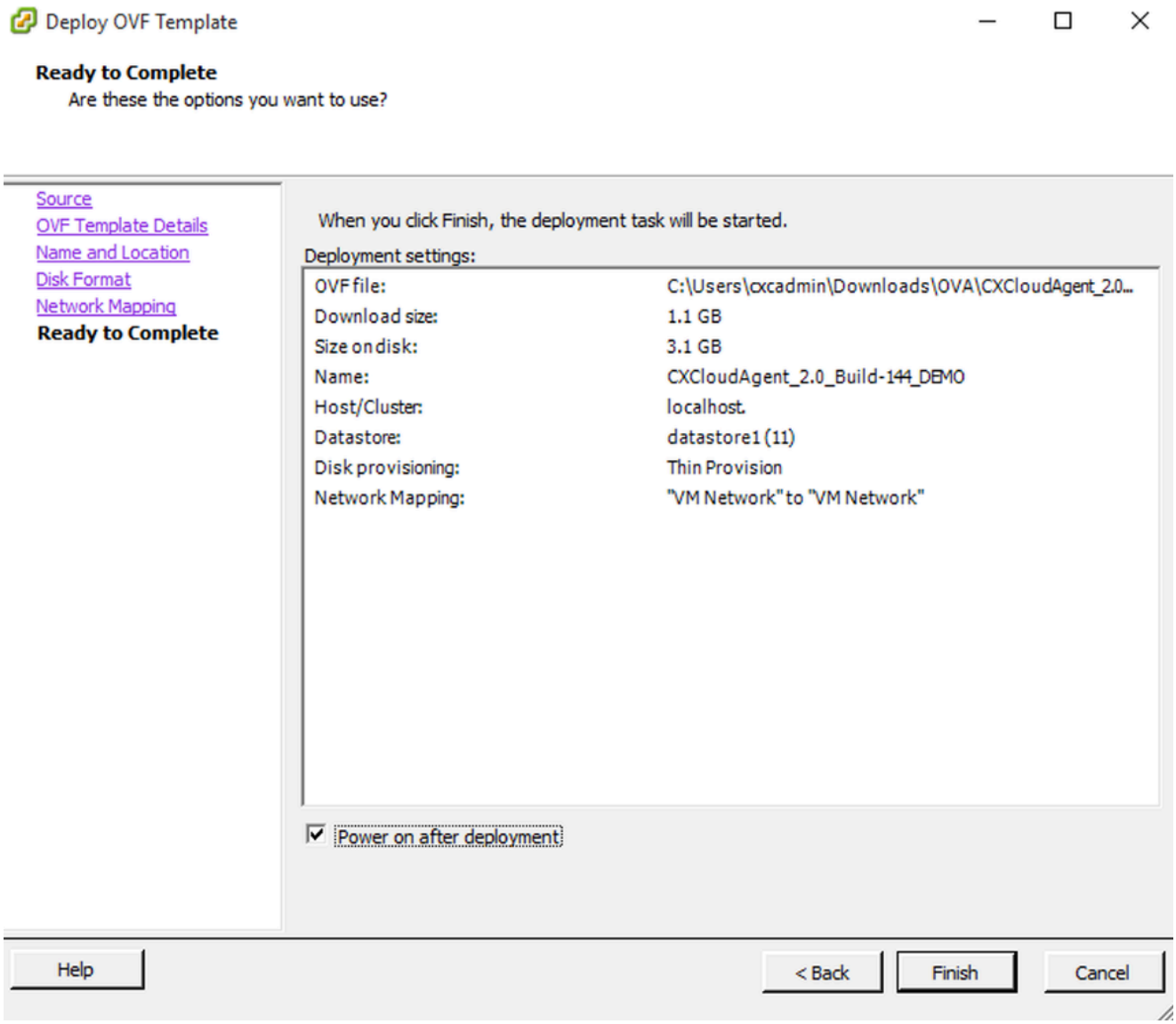

*Name and Location*

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



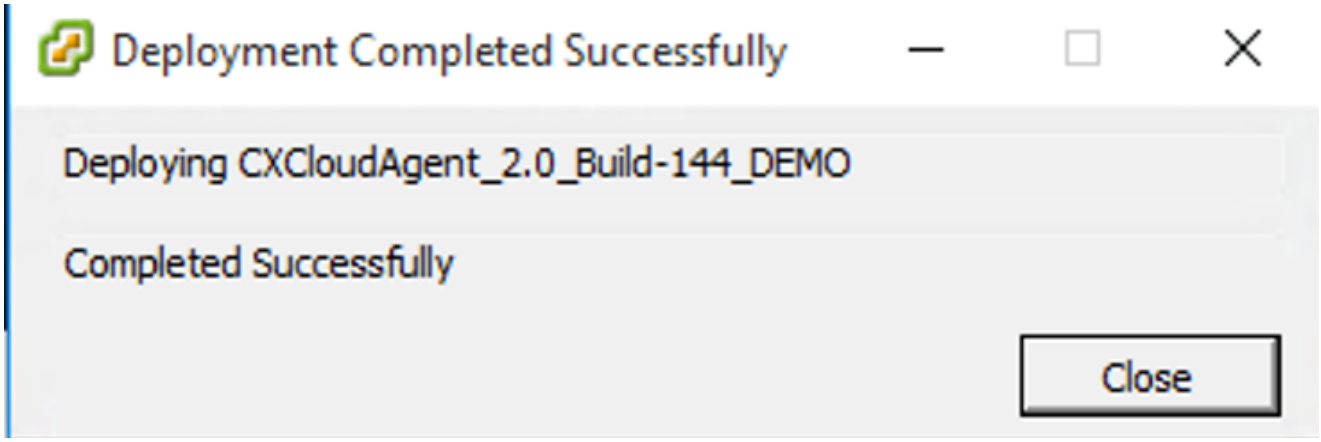

*Disk Format*

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




*Ready to Complete*

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



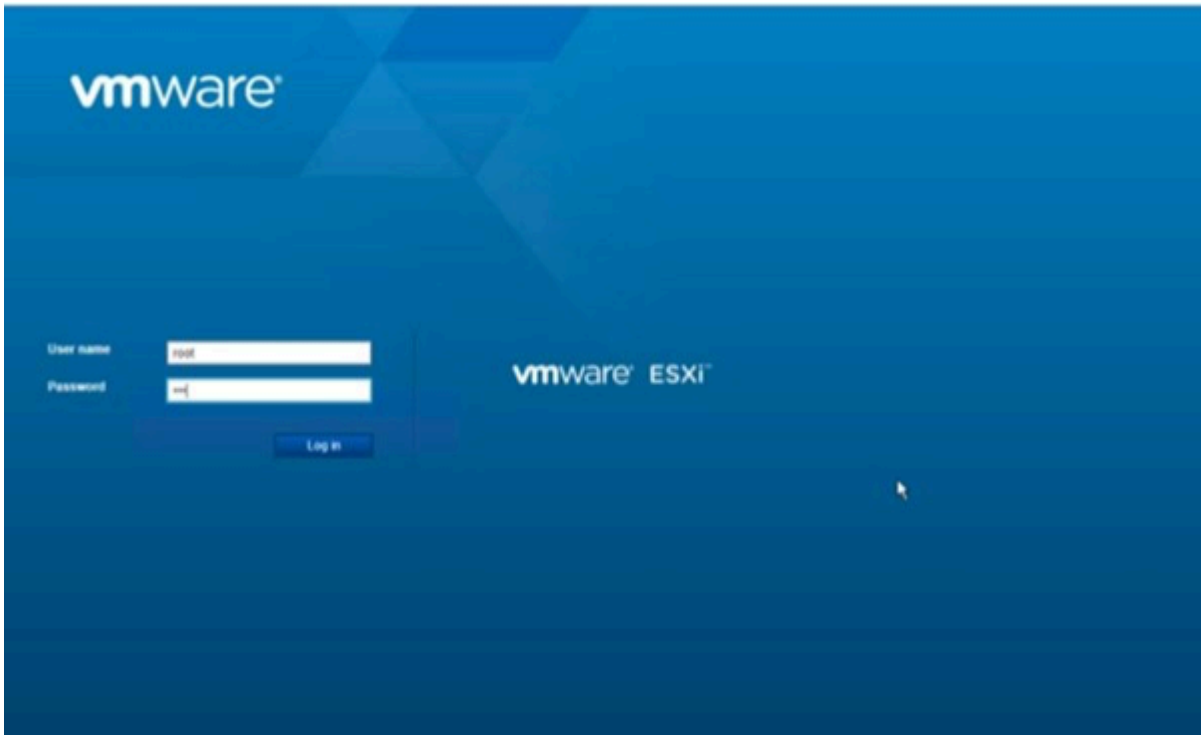

*Deployment Complete*

8. Select the deployed VM, open the console, and go to Network Configuration to proceed with the next steps.

**Web Client ESXi 6.0 Installation**

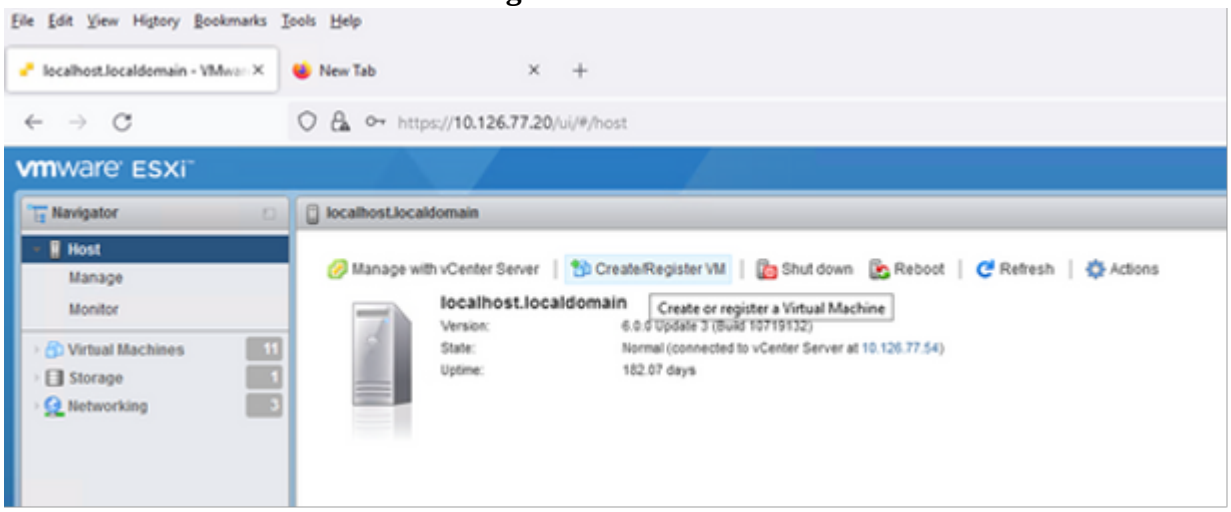
This client deploys CX Cloud OVA by use of the vSphere web.

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



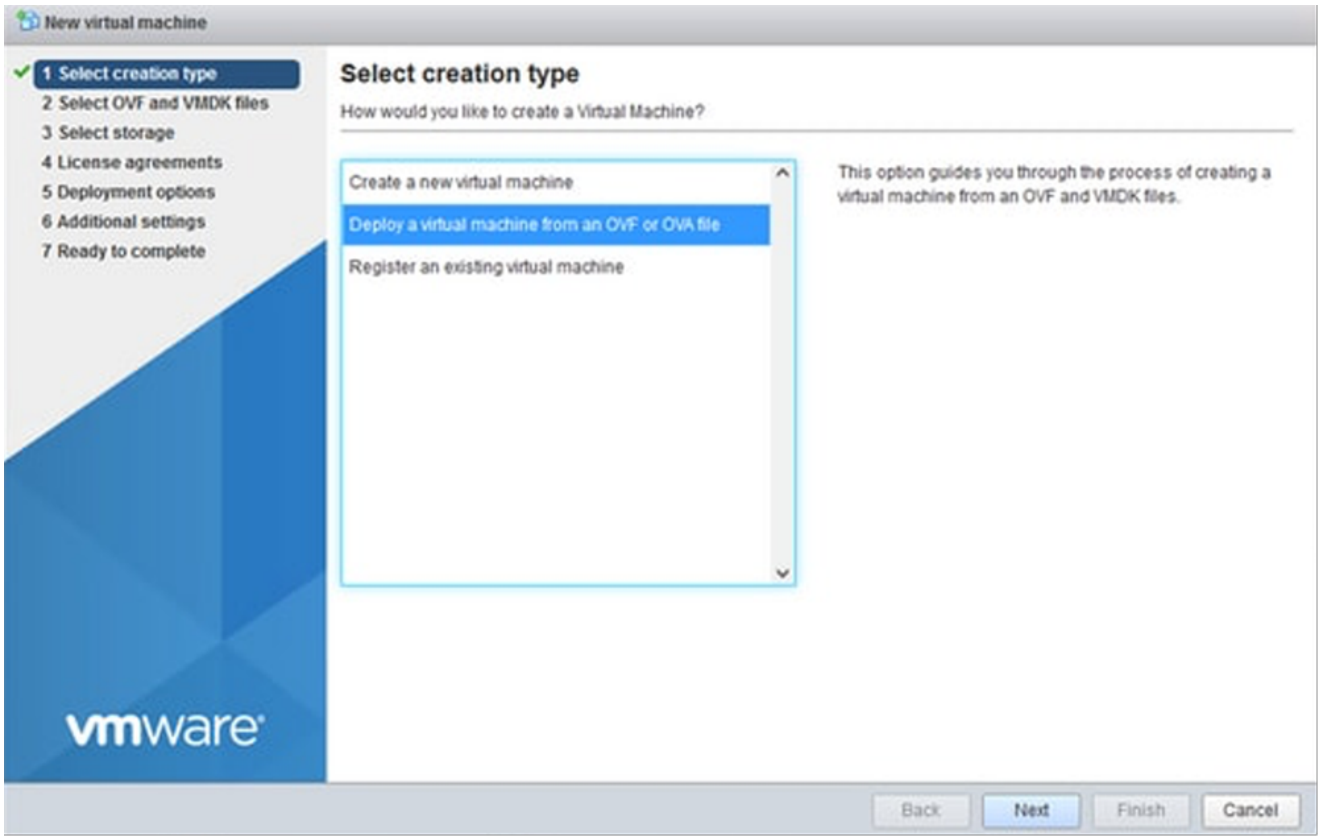

*VMWare ESXi Login*

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



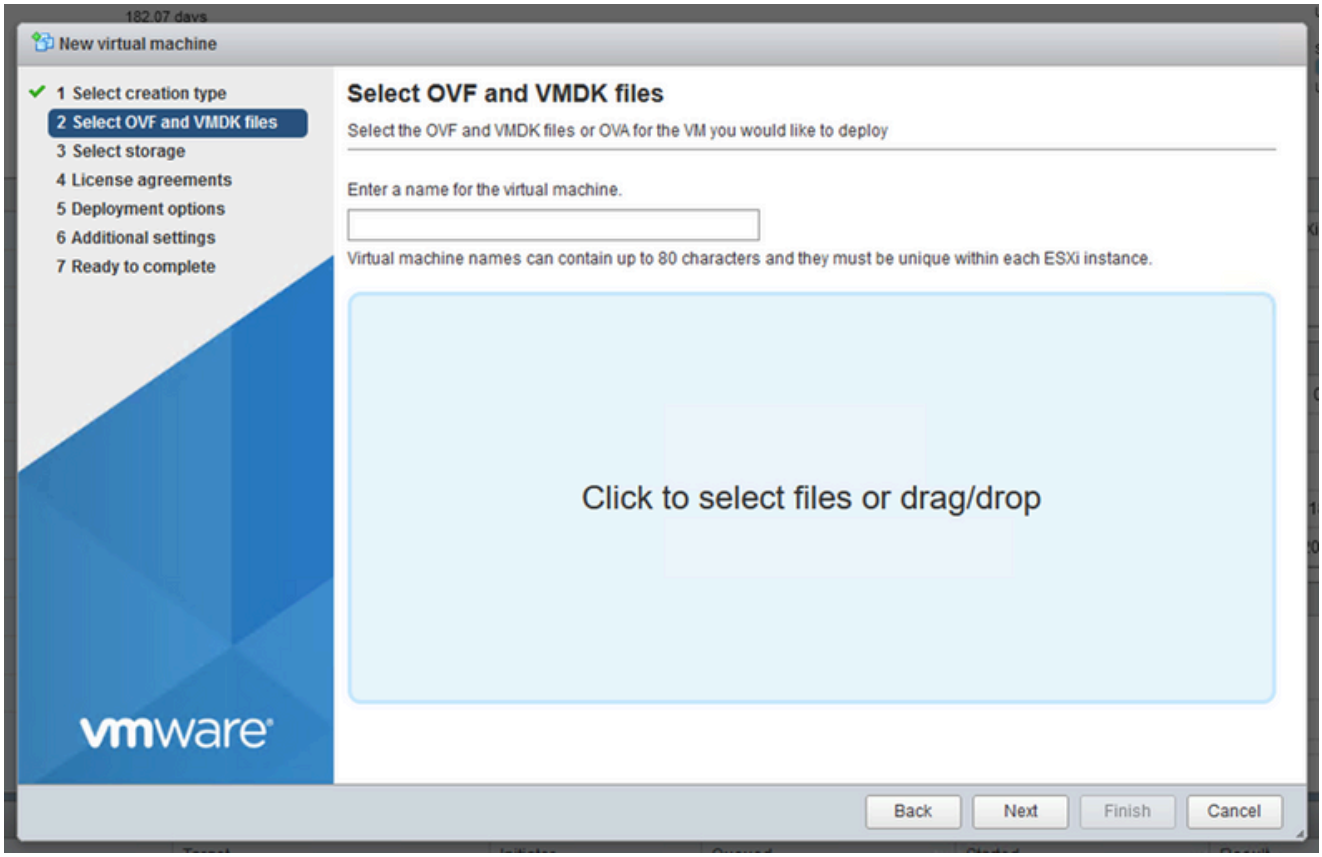

*Create VM*

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



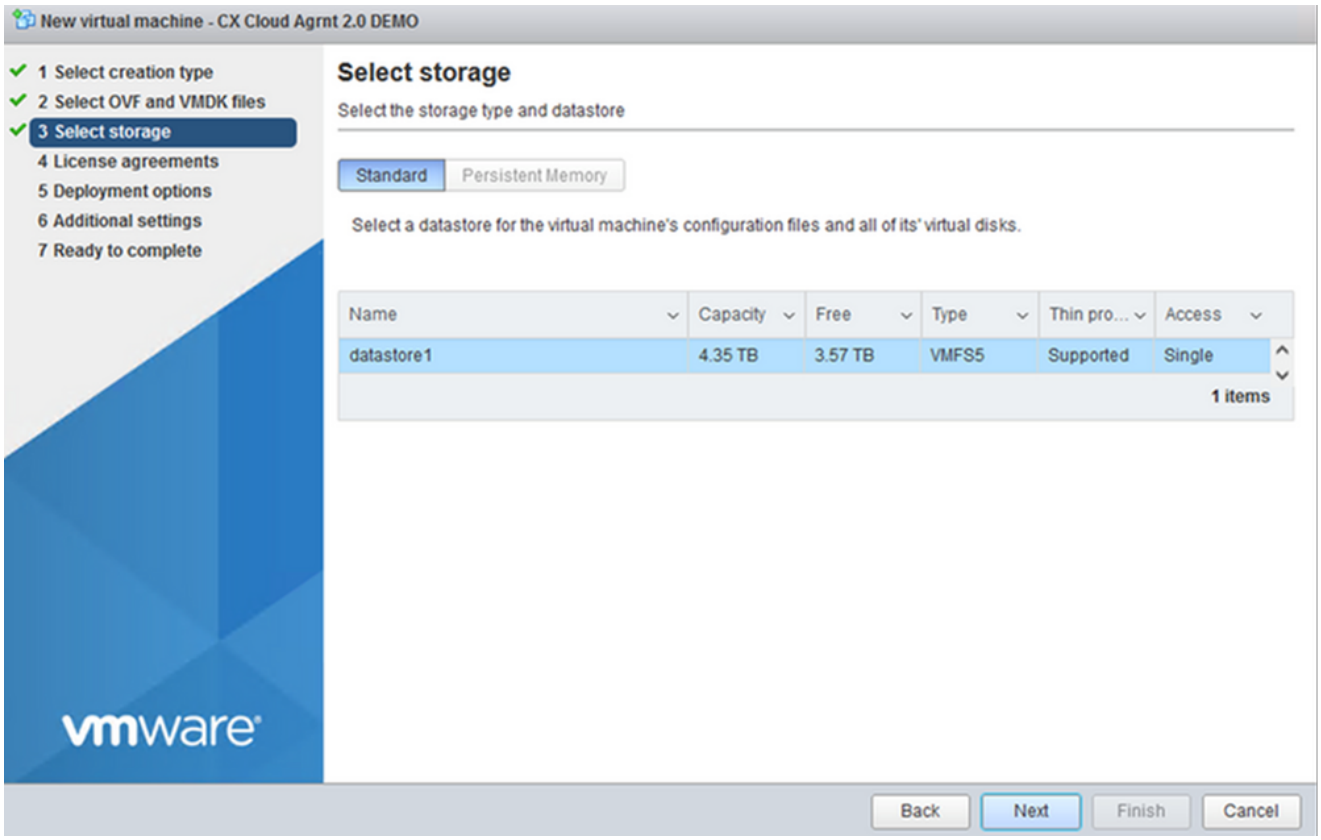

*Select Creation Type*

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



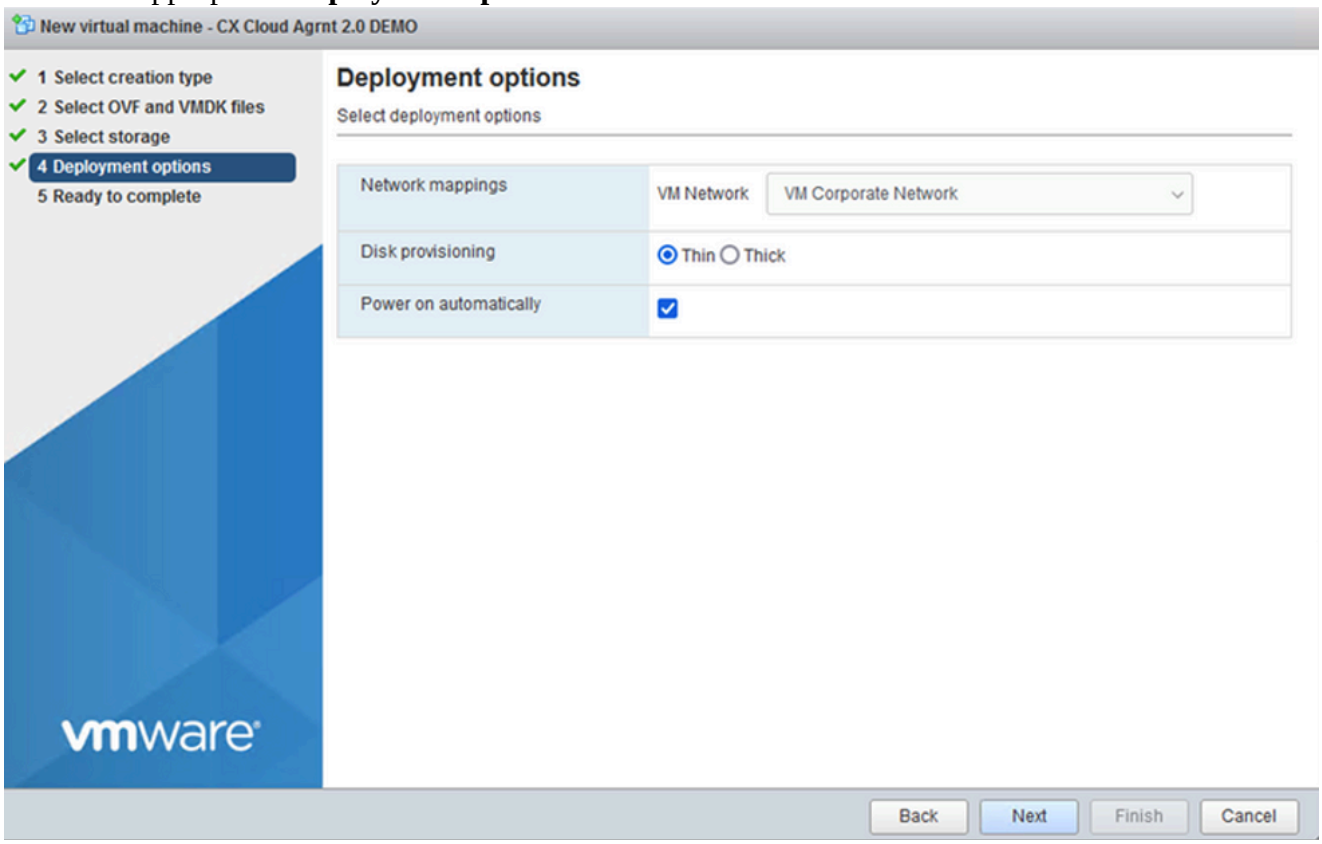

*OVA Selection*

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



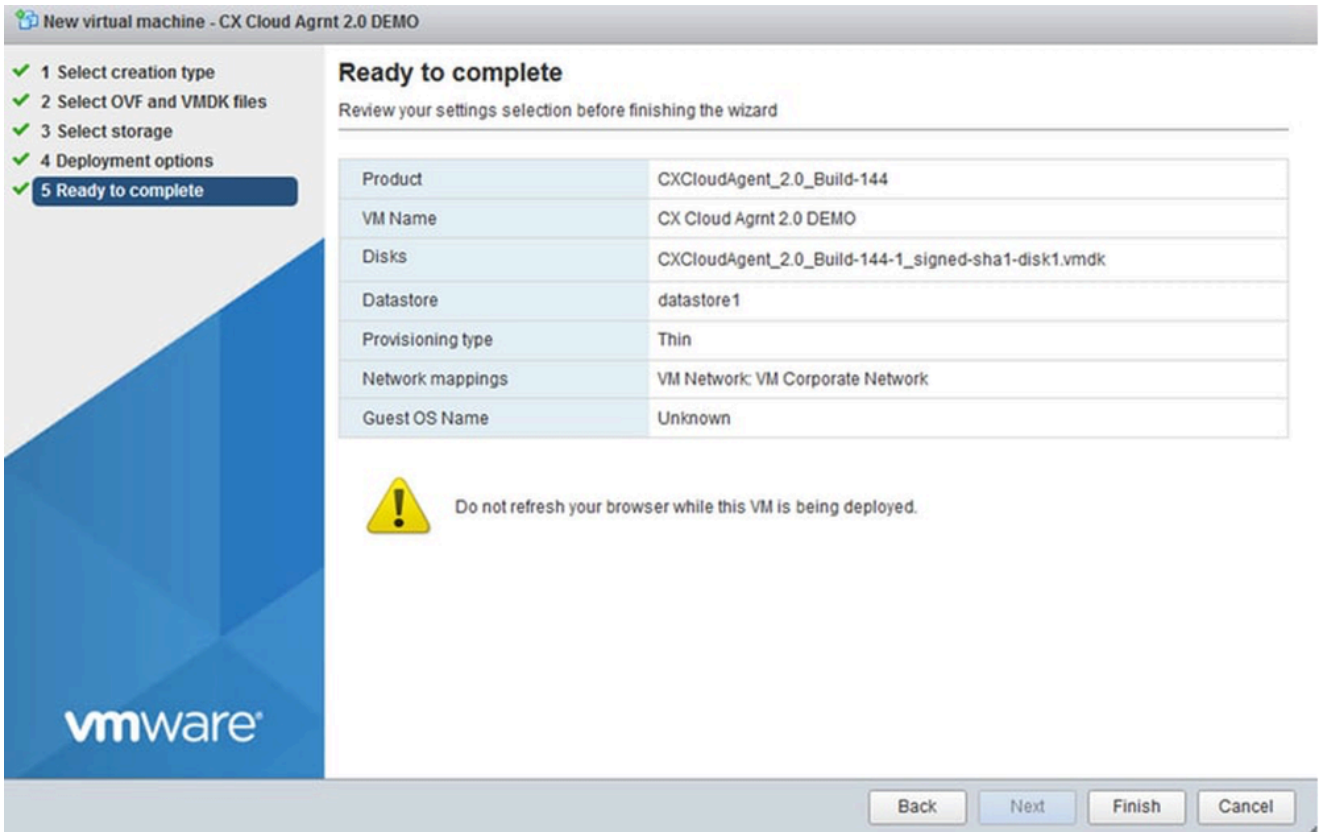

*Select Storage*

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

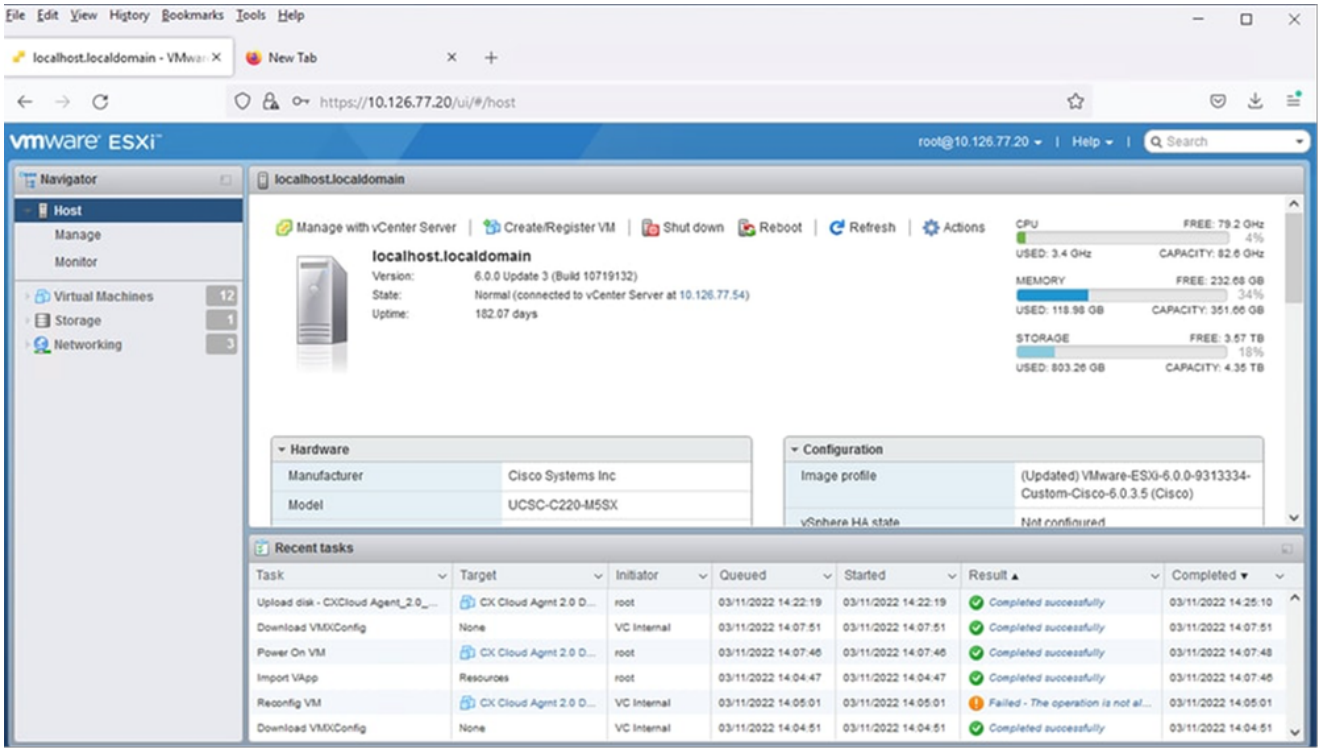



*Deployment Options*

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

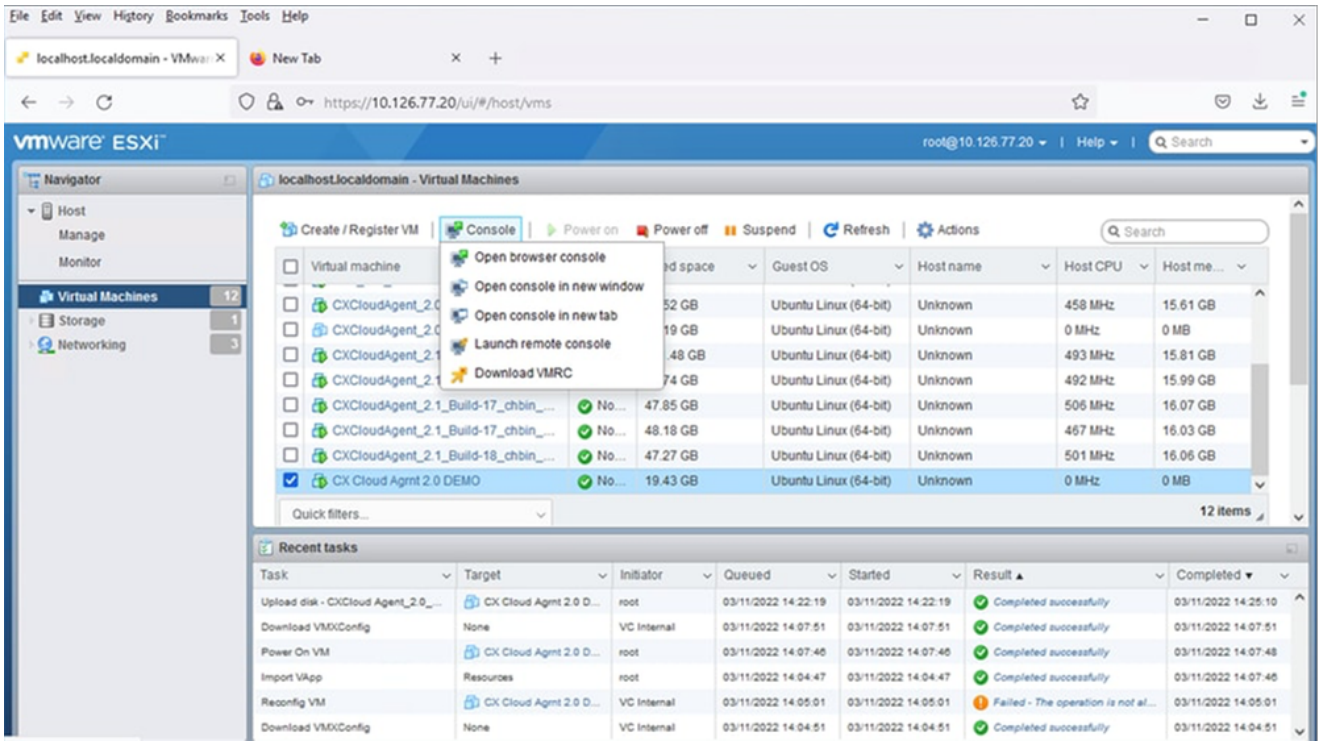



*Ready to Complete*




*Successful Completion*

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



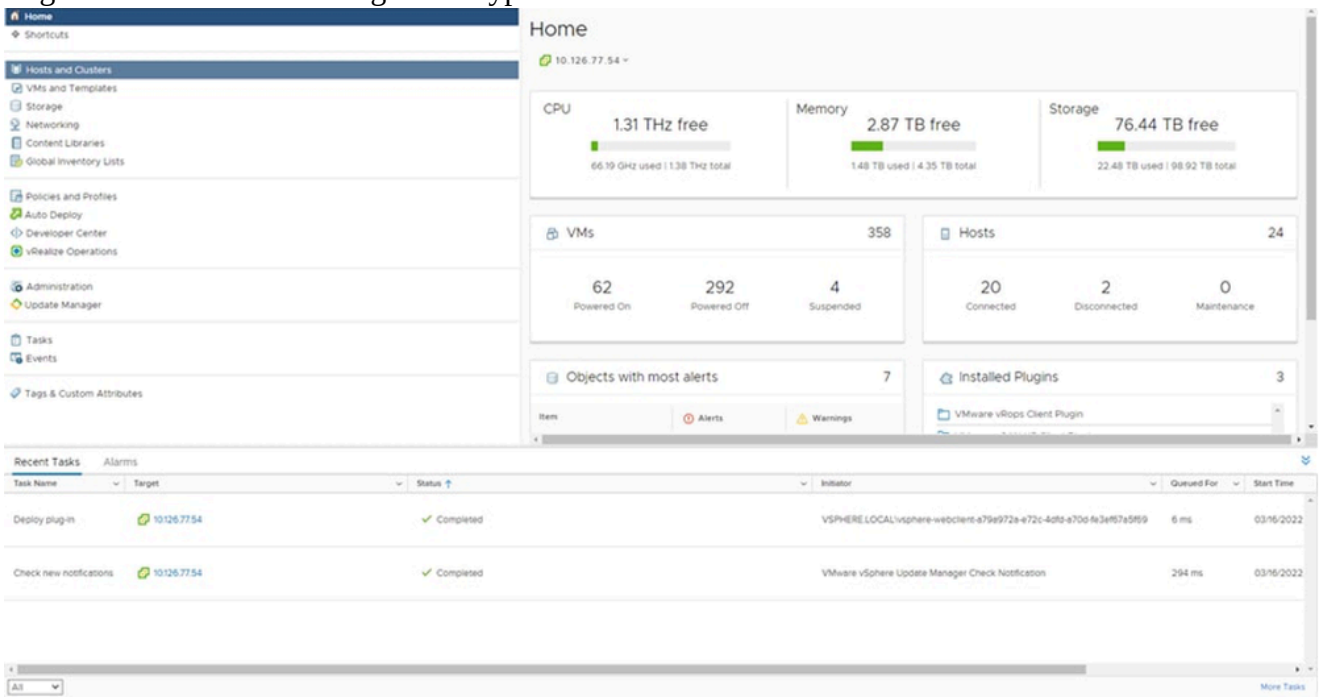

*Console*

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

### Web Client vCenter Installation

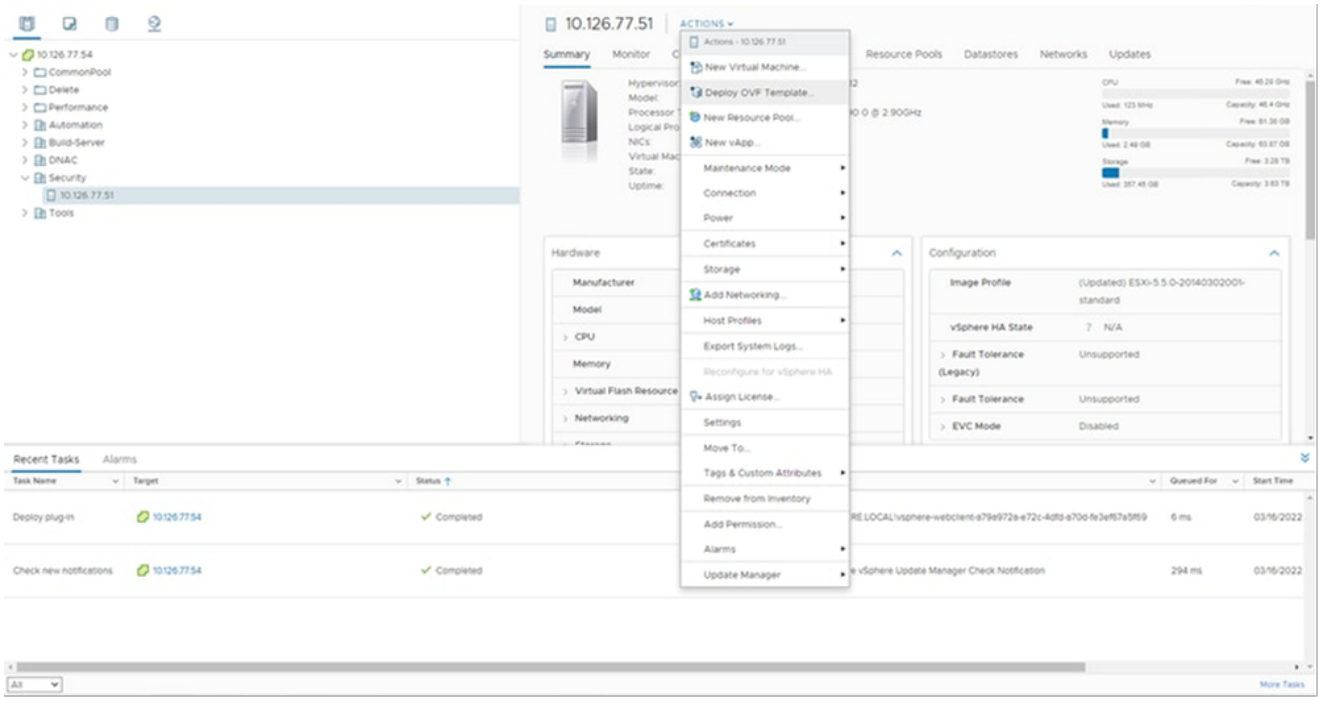
This client allows deployment of CX Agent OVA by use of the Web Client vCenter.

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



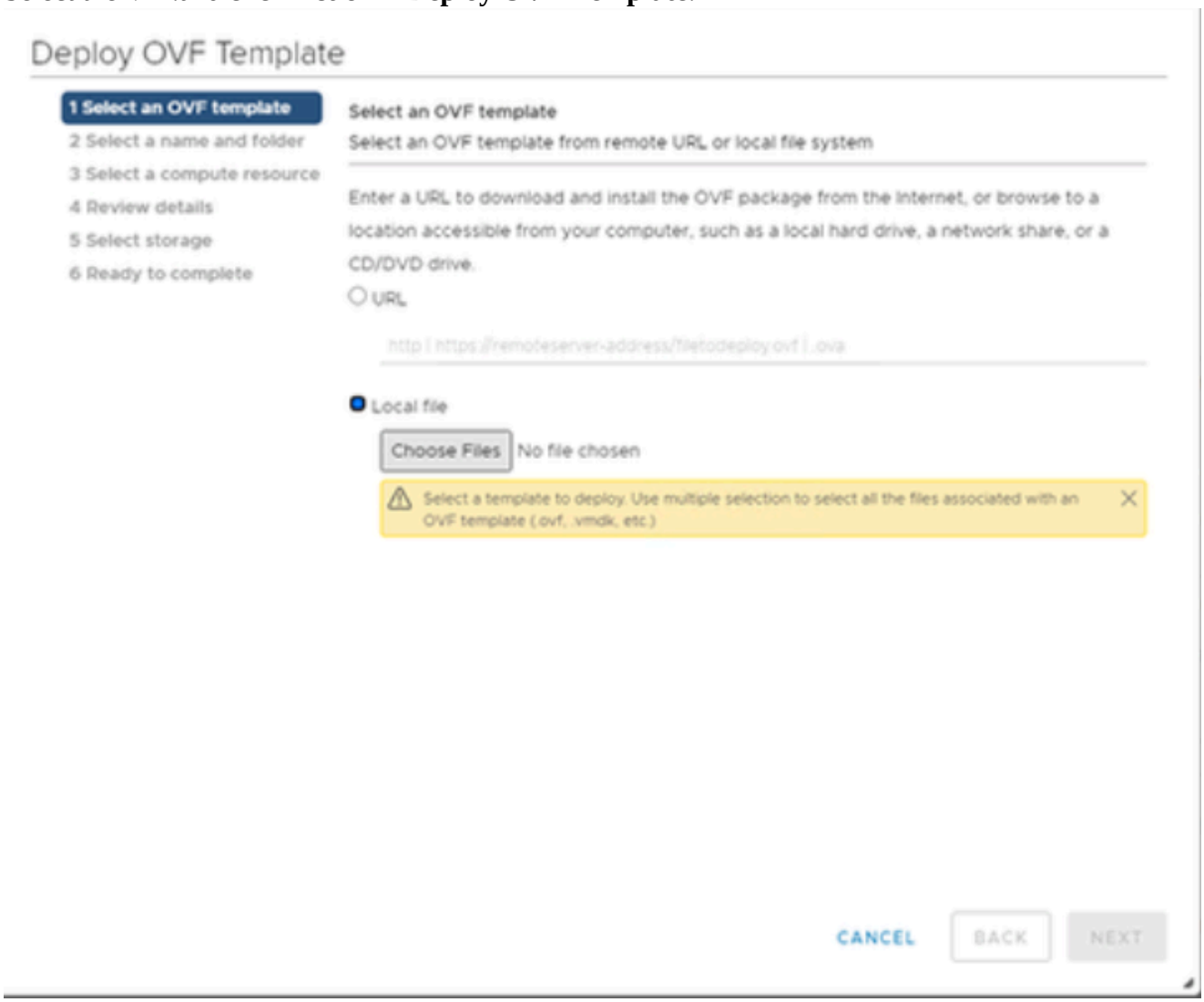

*Home Page*

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



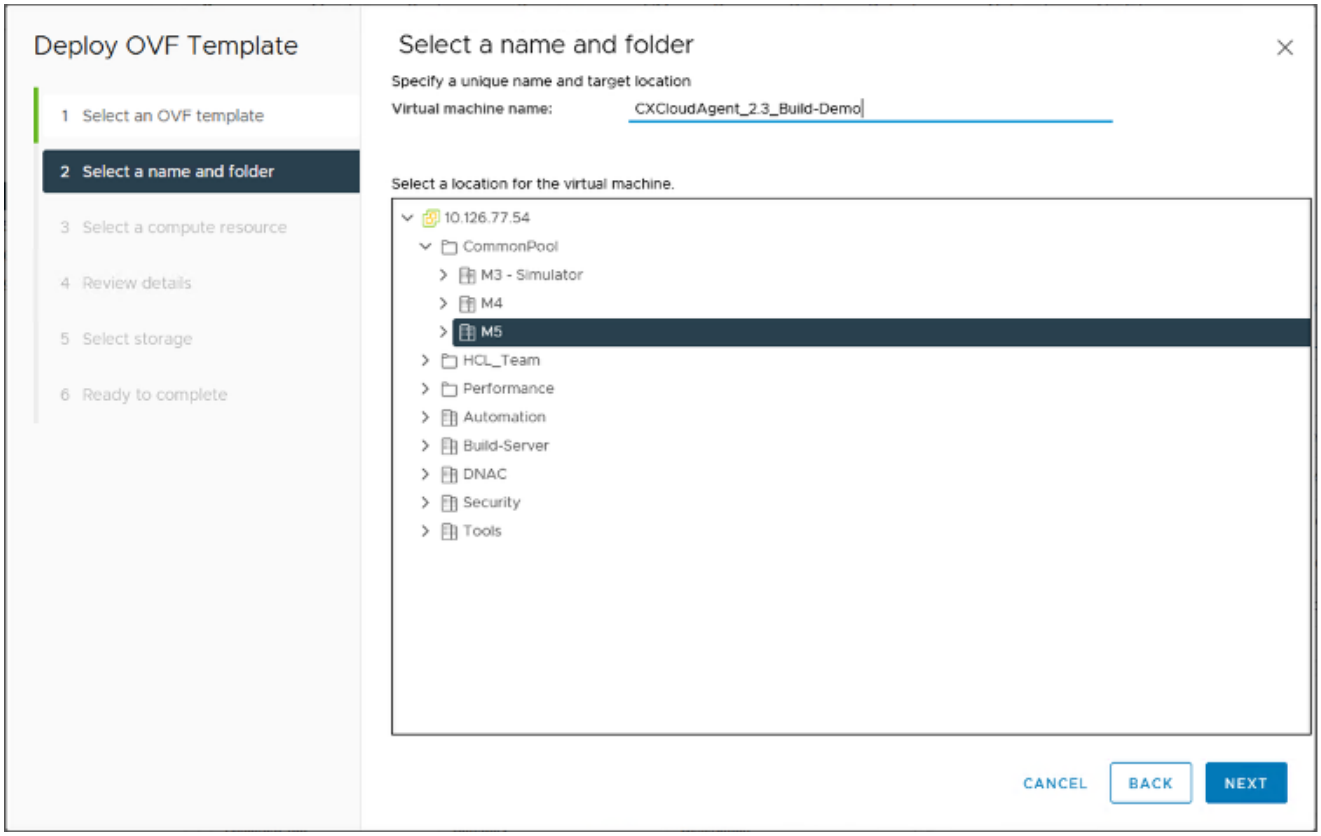

*Hosts and Clusters*

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



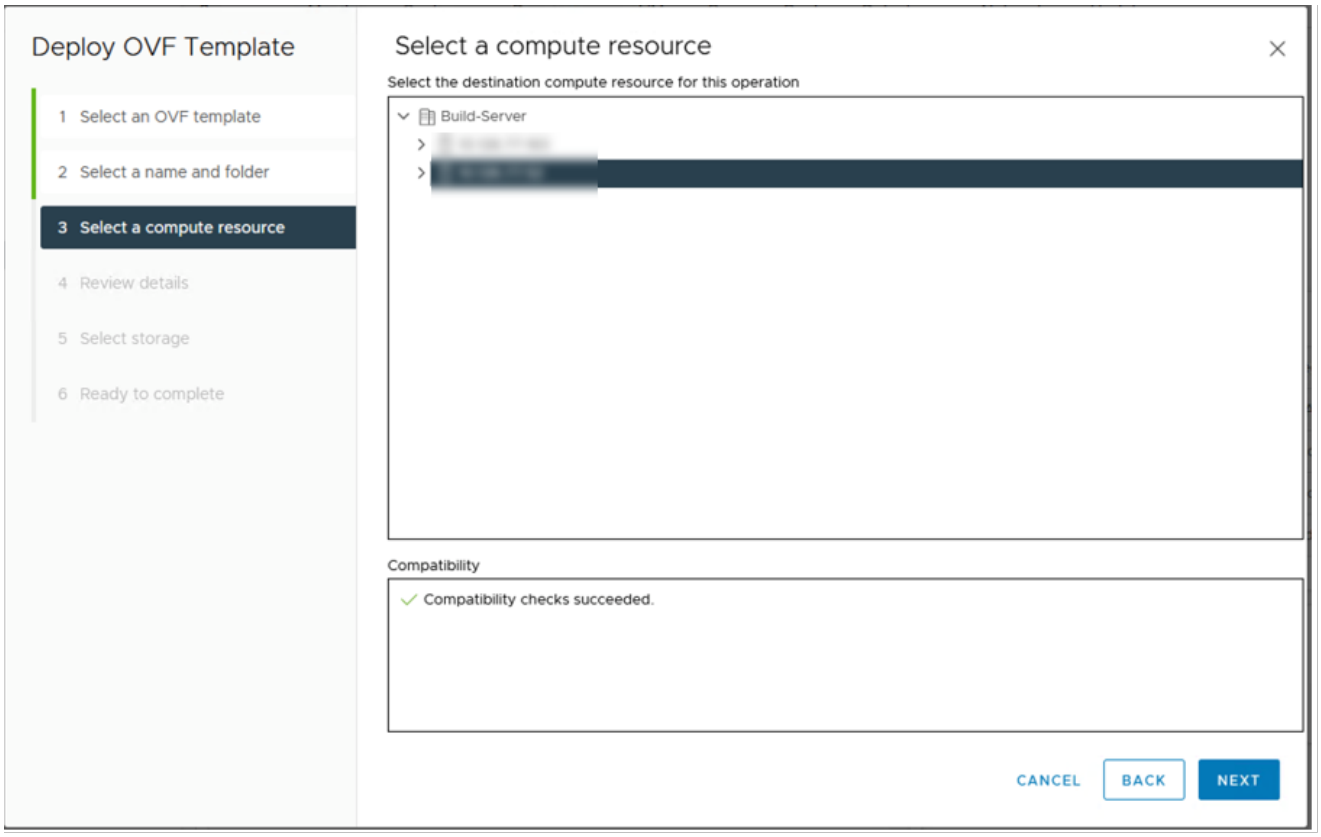

*Deploy OVF*

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



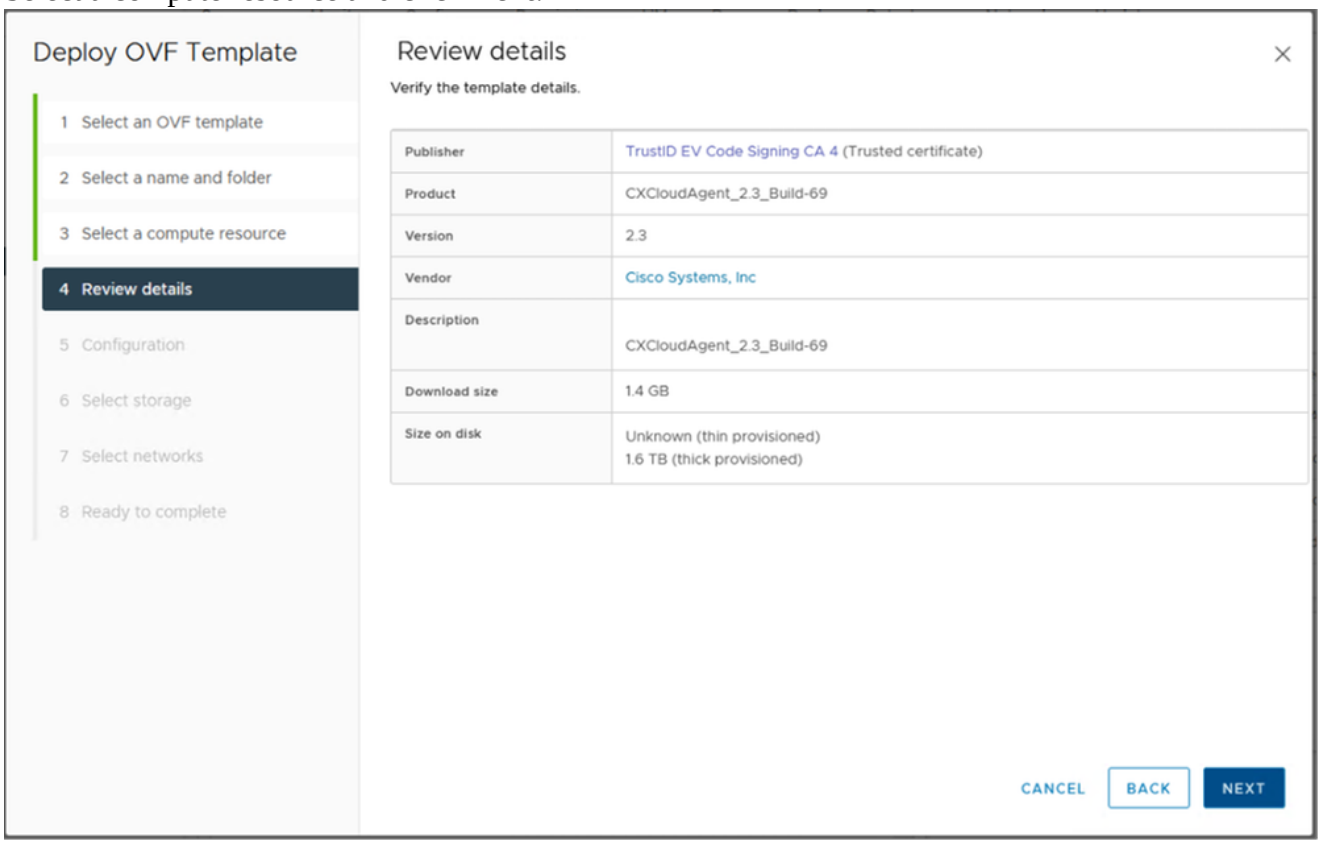

*Name and Folder*

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



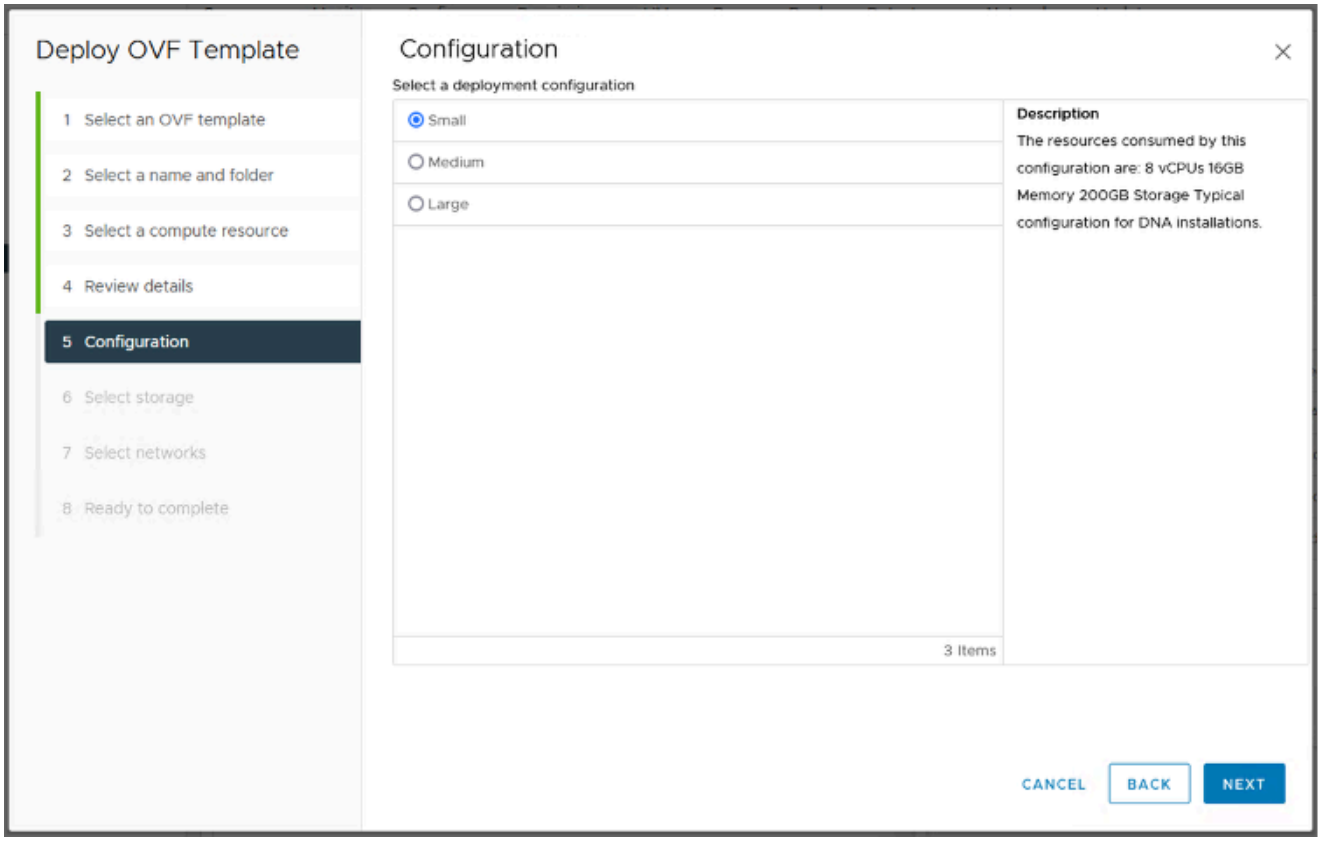

*Select compute resource*

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



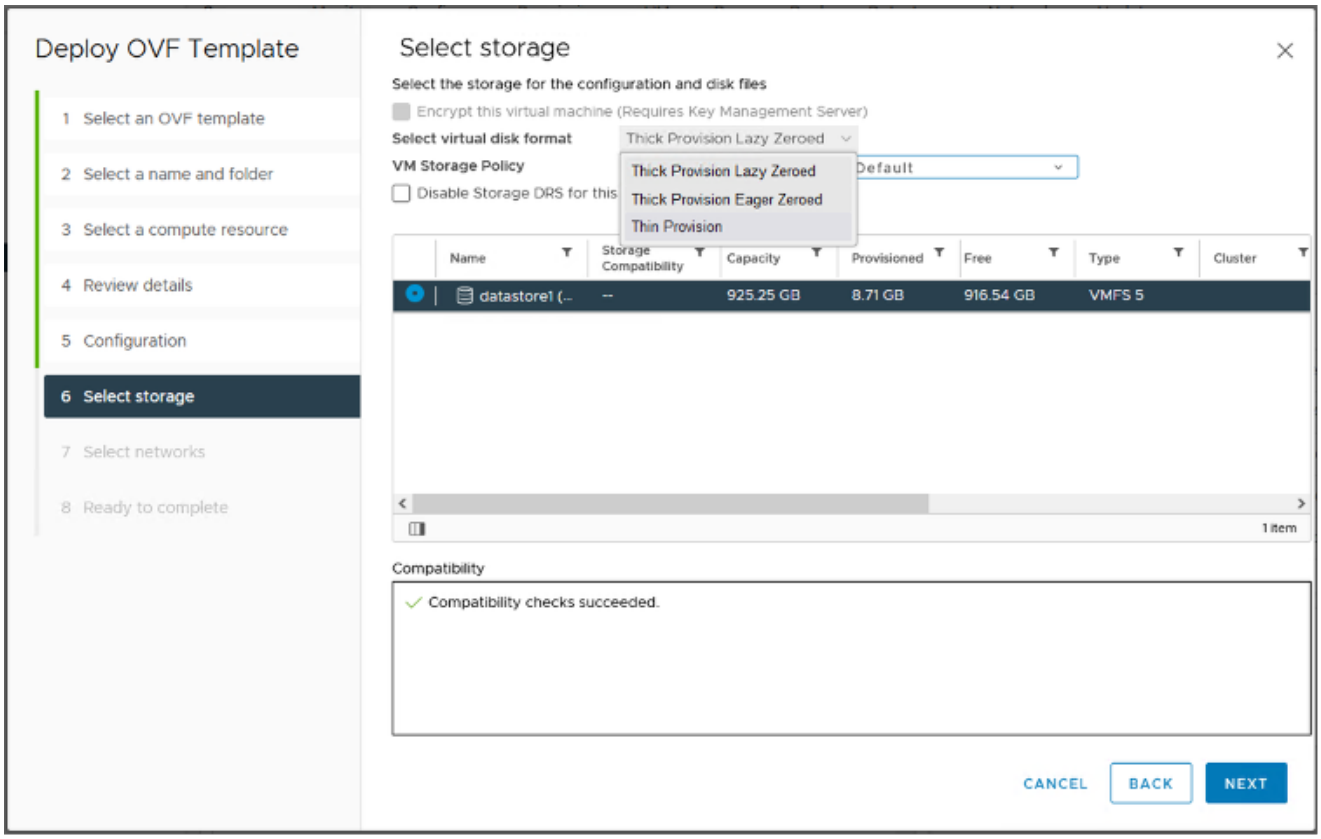

*Review details*

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



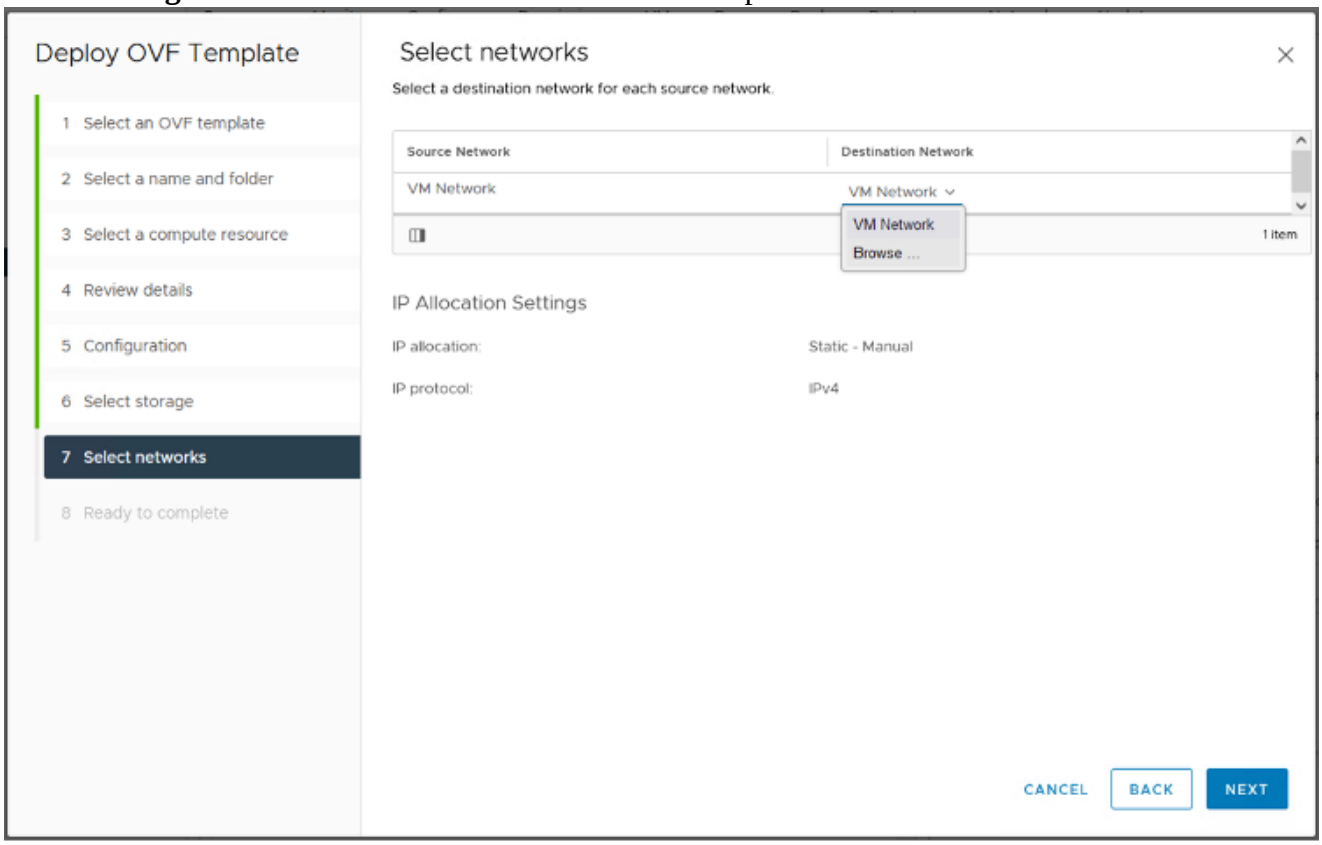

*Configuration*

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



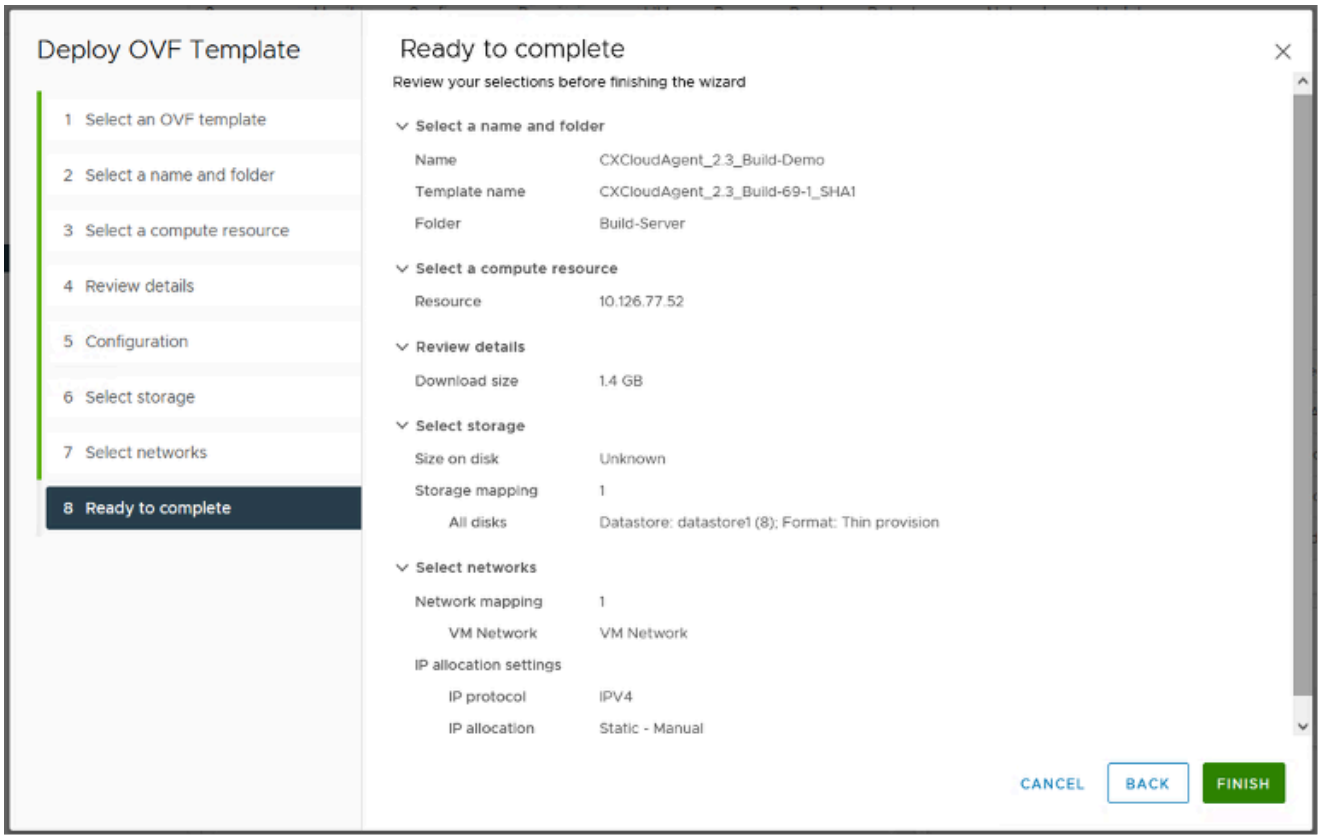

*Configuration*

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



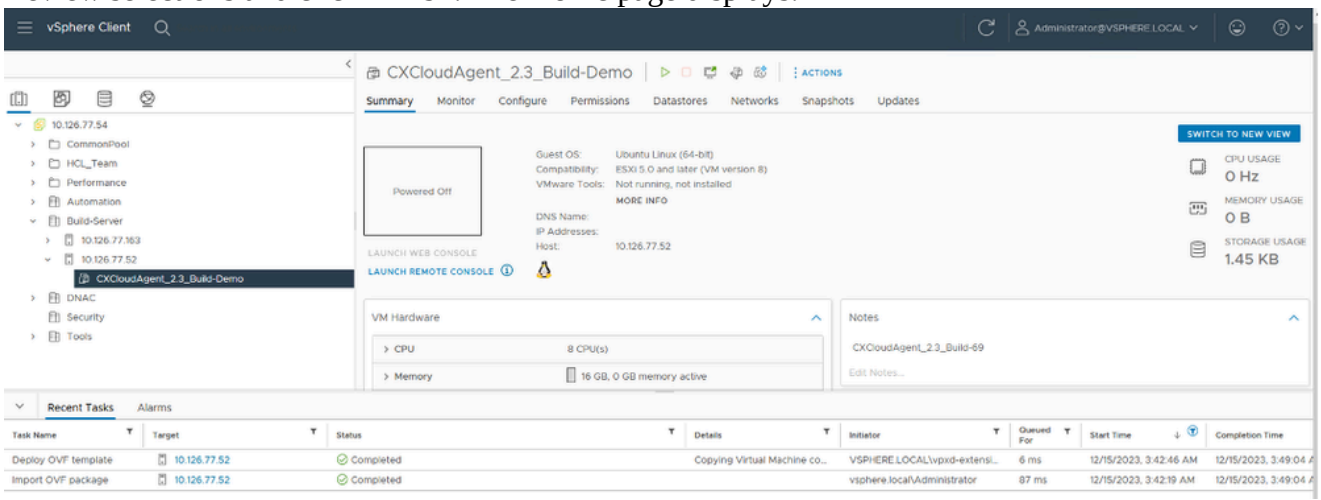

*Select Networks*

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



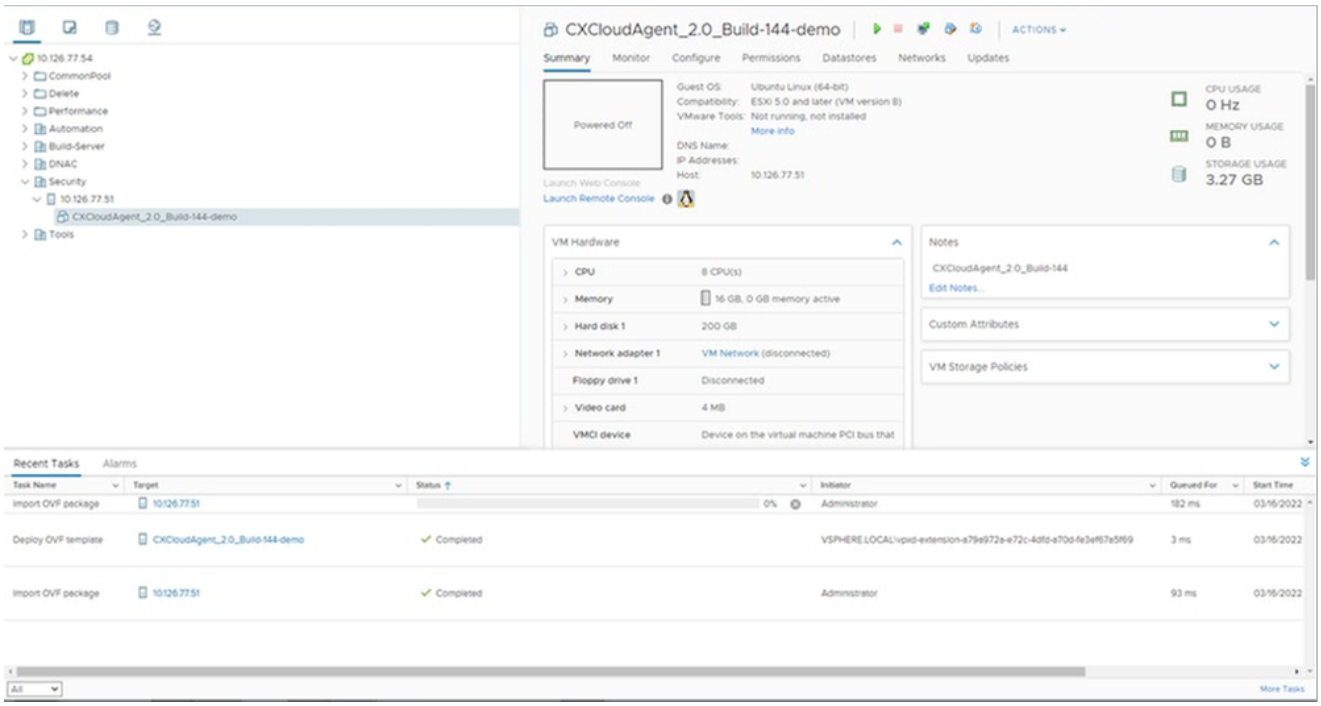

*Ready to complete*

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



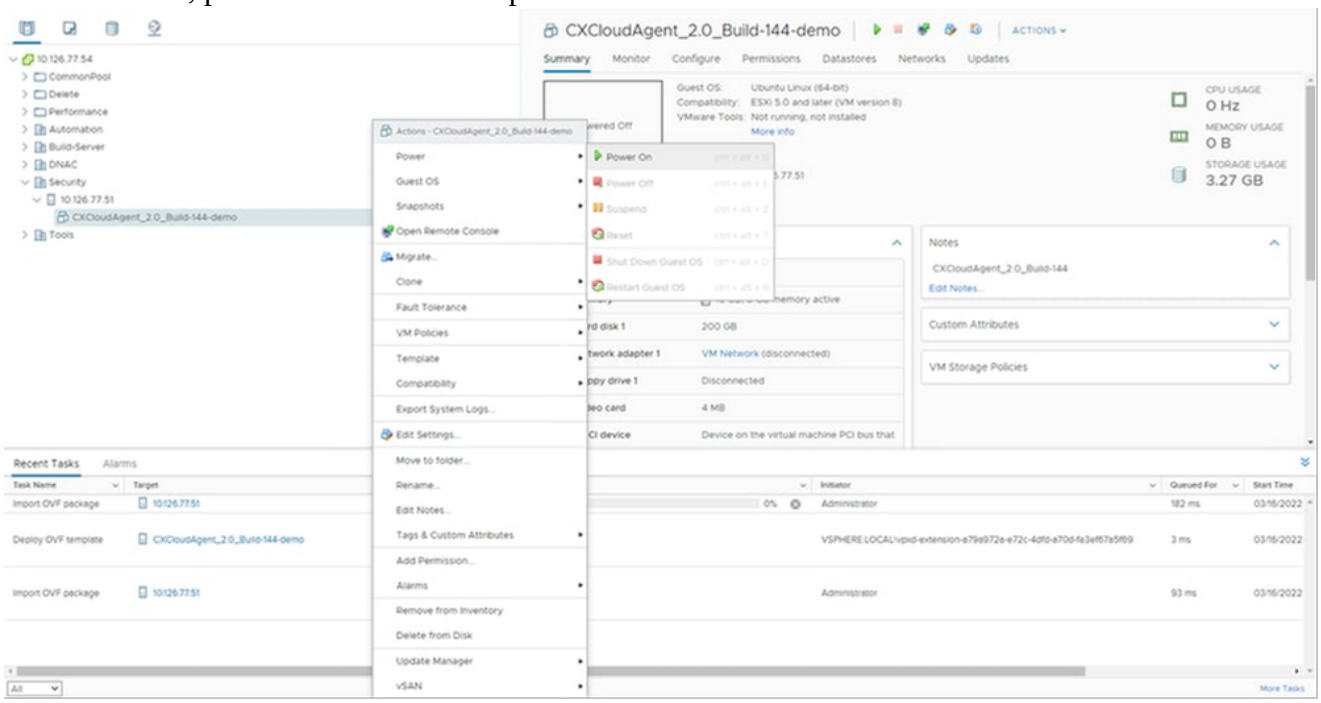

*VM added*

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*.

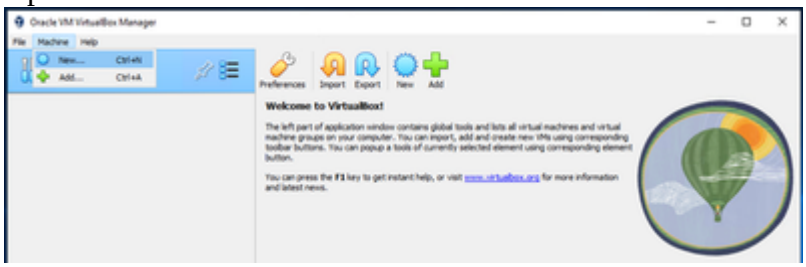
```
D:\>cd CXCAGENT

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>_
```

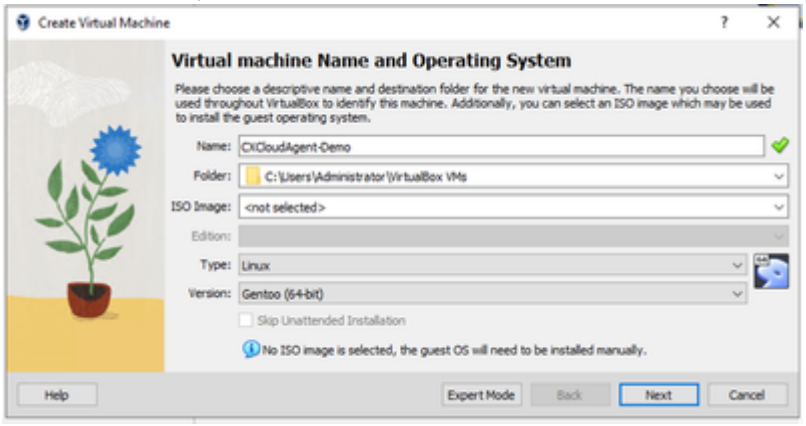
*Unzip OVA File*

4. Open the Oracle VM UI.



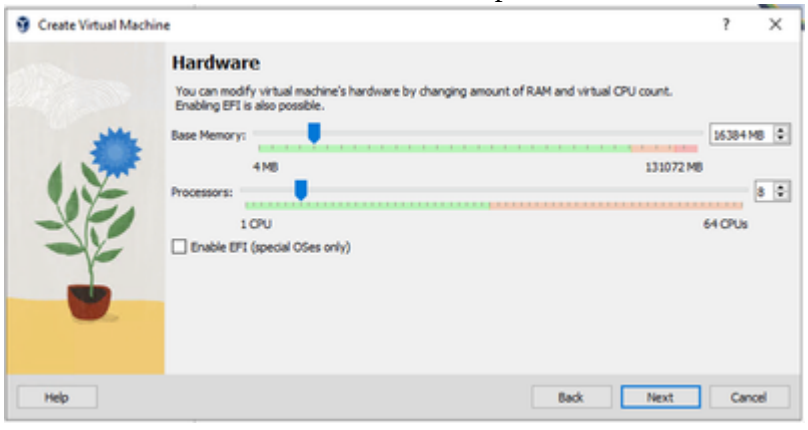

*Oracle VM*

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




*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.



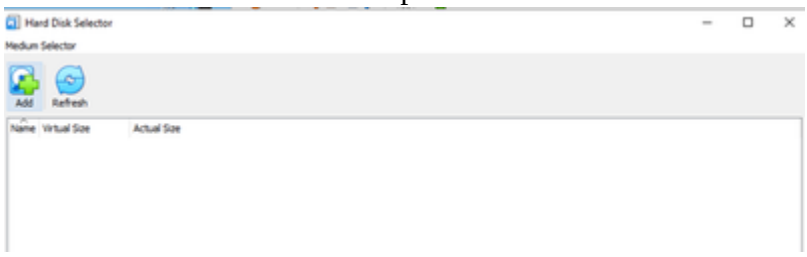
*Hardware*

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



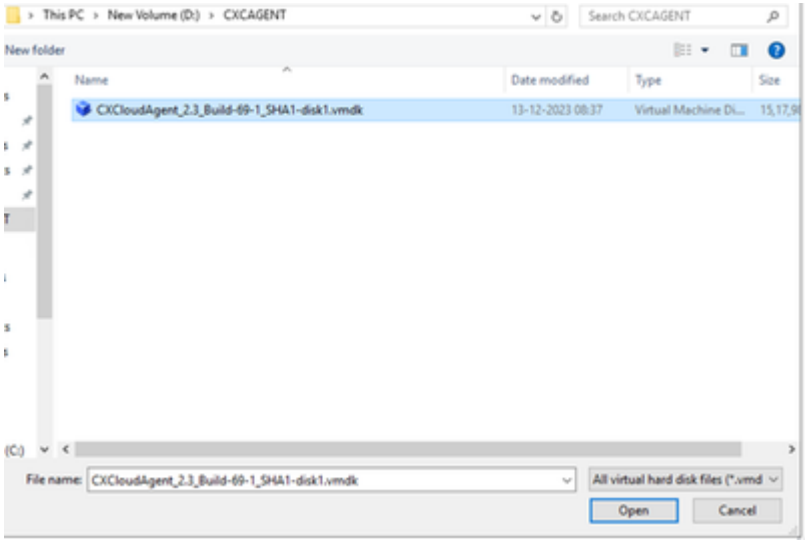

*Virtual Hard Disk*

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



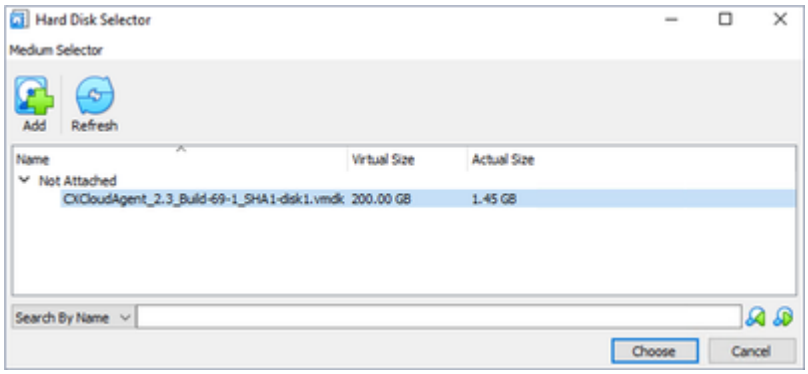

*Hard Disk Selector*

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



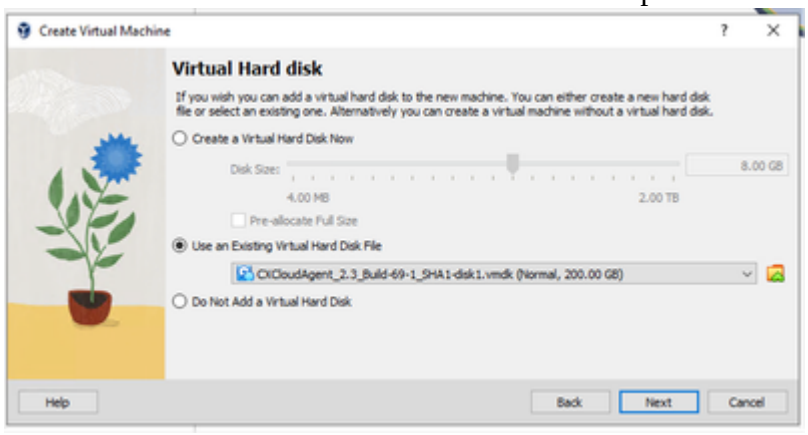

*OVA Folder*

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



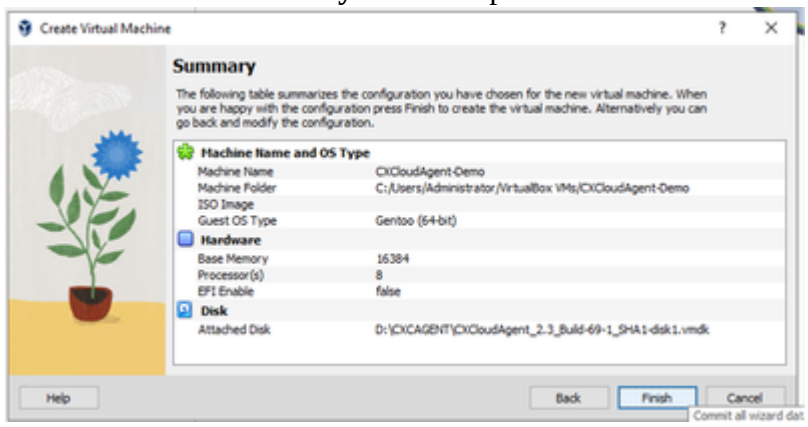

*Hard Disk Selector*

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



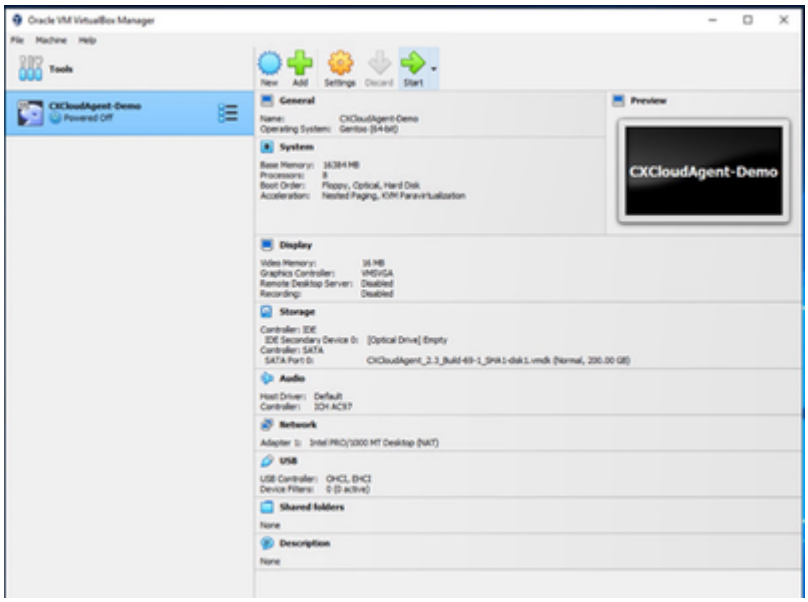

*Select file*

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




*Summary*

14. Click **Finish**.




*VM Console Startup*

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



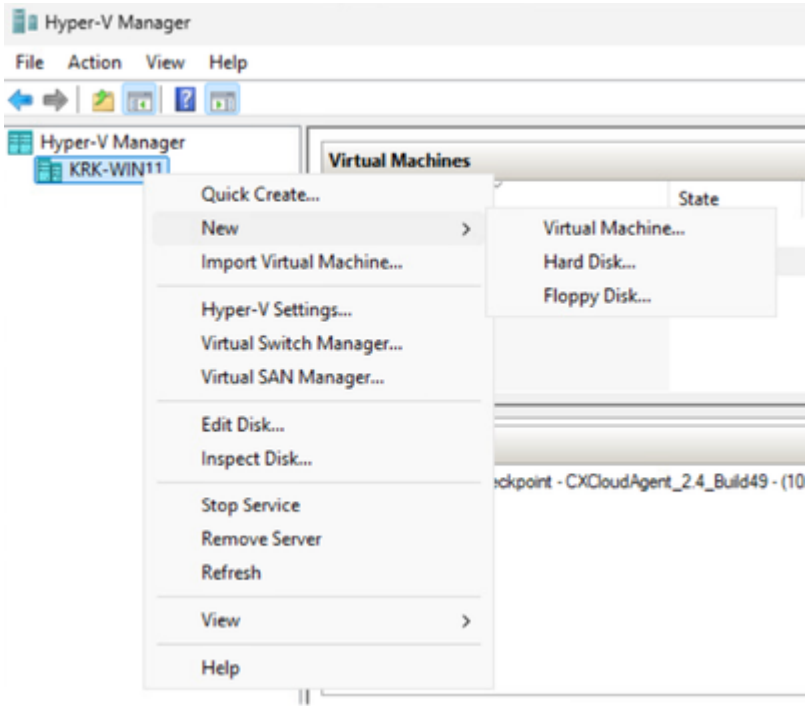

*Open the console*

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

### Microsoft Hyper-V Installation

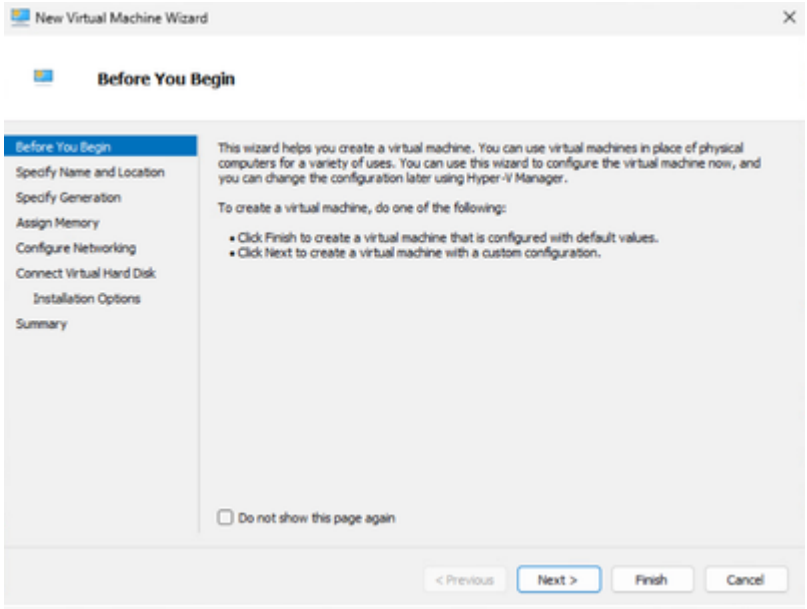
This client deploys CX Agent Virtual Disk though the Microsoft Hyper-V installation.

1. Log into the Hyper-V Manager.



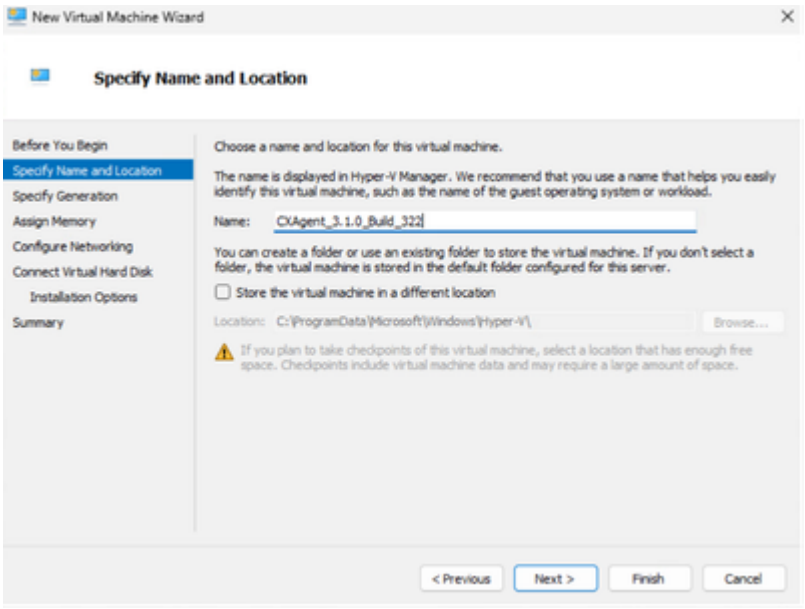

*Hyper-V Manager*

2. Right-click the target VM to open the menu.
3. Choose **New** > **Virtual Machine**. The **New Virtual Machine Wizard – Before You Begin** page displays.



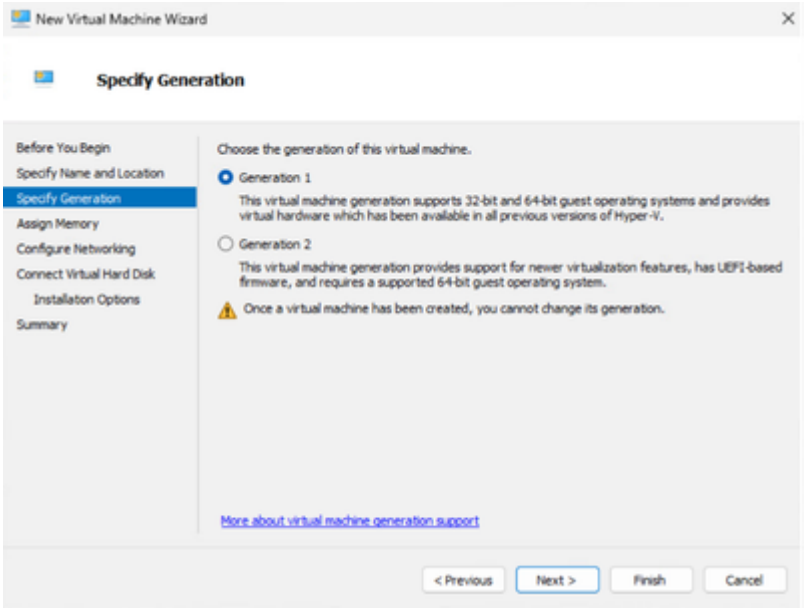

*New Virtual Machine Wizard*

4. Click **Next.** The **New Virtual Machine Wizard – Specify Name and Location** page displays.



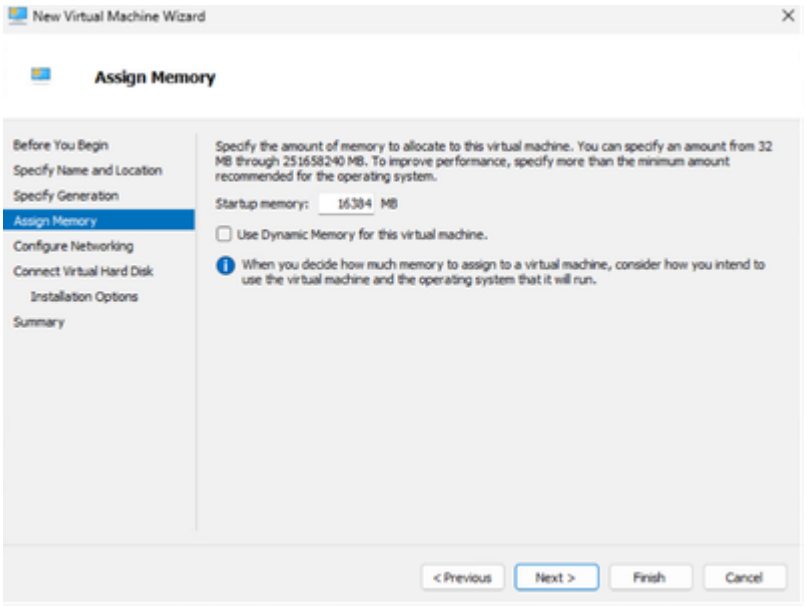

*Name and Location*

5. Enter the **Name** and **location**.
6. Click **Next**. The **New Virtual Machine Wizard – Specify Generation** page displays.




*Specify Generation*

7. Click the **Generation 1** radio button.
8. Click **Next**. The **New Virtual Machine Wizard – Assign Memory** page displays.




*Memory*

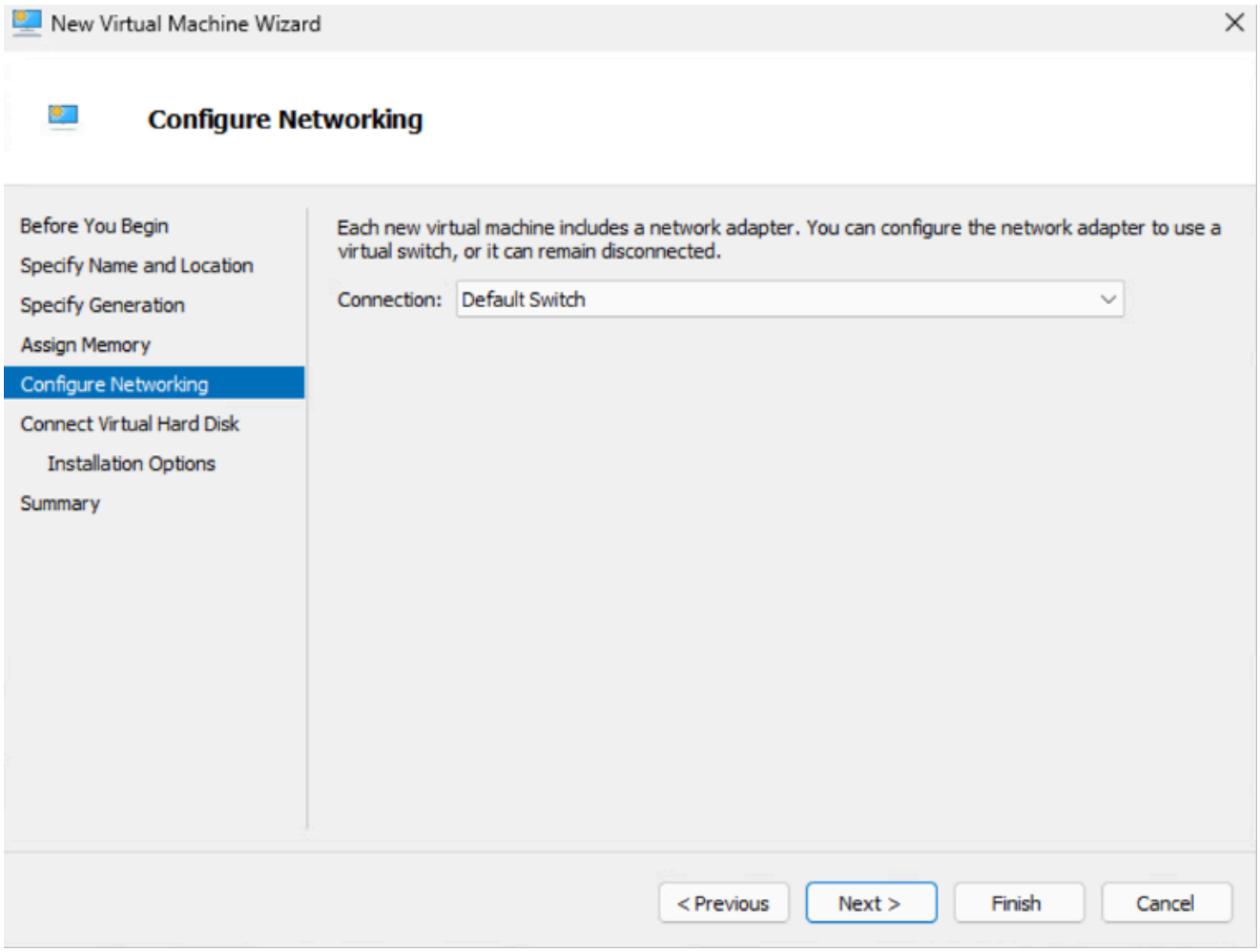
9. Enter the desired amount of RAM in the **Startup memory** field.
    - 16GB for Small deployment
    - 32GB for Medium deployment
    - 64GB for Large deployment

---

**Notes**:
- For CX Agent, the minimum allocated memory must be at least 16GB.
- The **Use Dynamic Memory for this virtual machine** check box should not be checked.

---

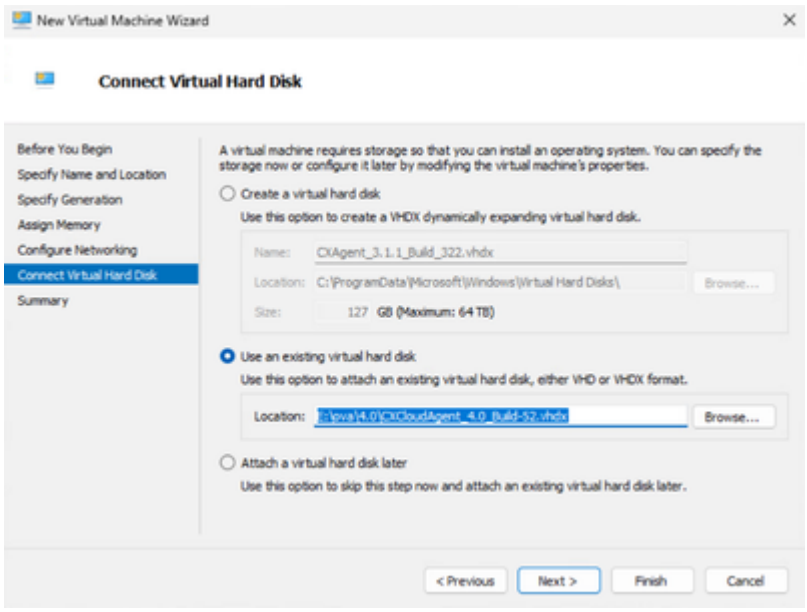
10. Click **Next**. The **New Virtual Machine Wizard – Configure Networking** page displays.




*Networking*

11. From the **Connection** drop-down list, choose a virtual switch for network connectivity.
12. Click **Next**. The **New Virtual Machine Wizard – Connect Virtual Hard Disk** page displays.

> **Note**: The "**Use an existing virtual disk**" is selected by default. Do not make any changes.



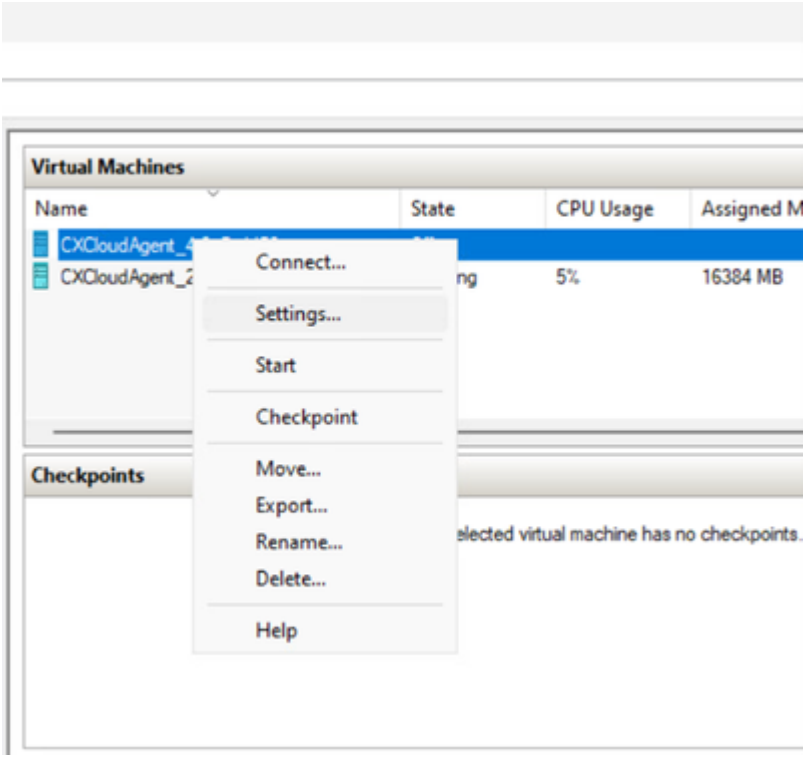

*Connect Virtual Hard Disk*

13. Review the **Summary** and click **Finish**.

### Processor Settings

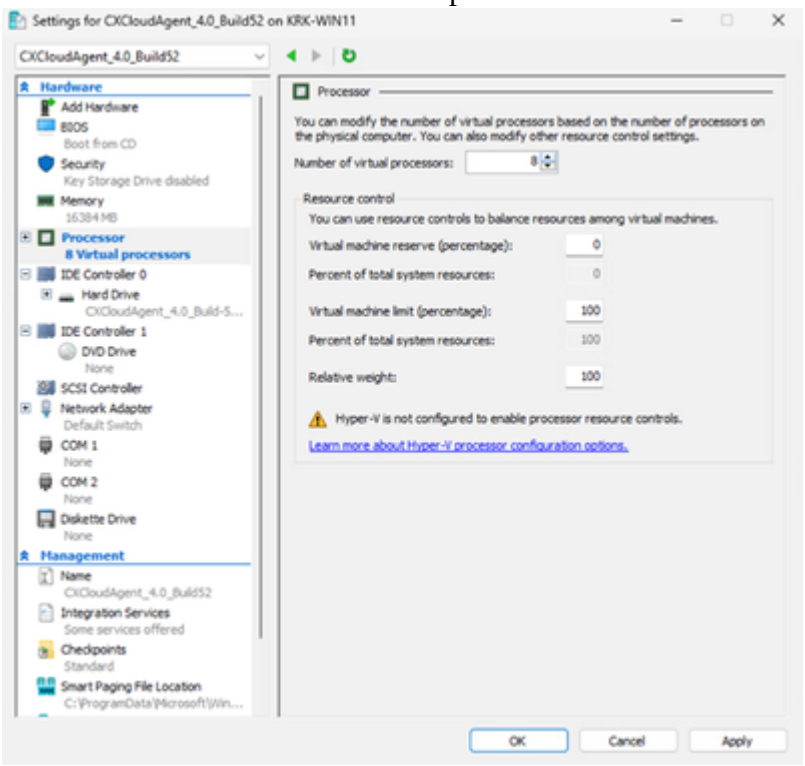
To verify Processor settings:

1. Right-click the newly created VM (as shown in the section above). The menu displays.




*VM Settings*

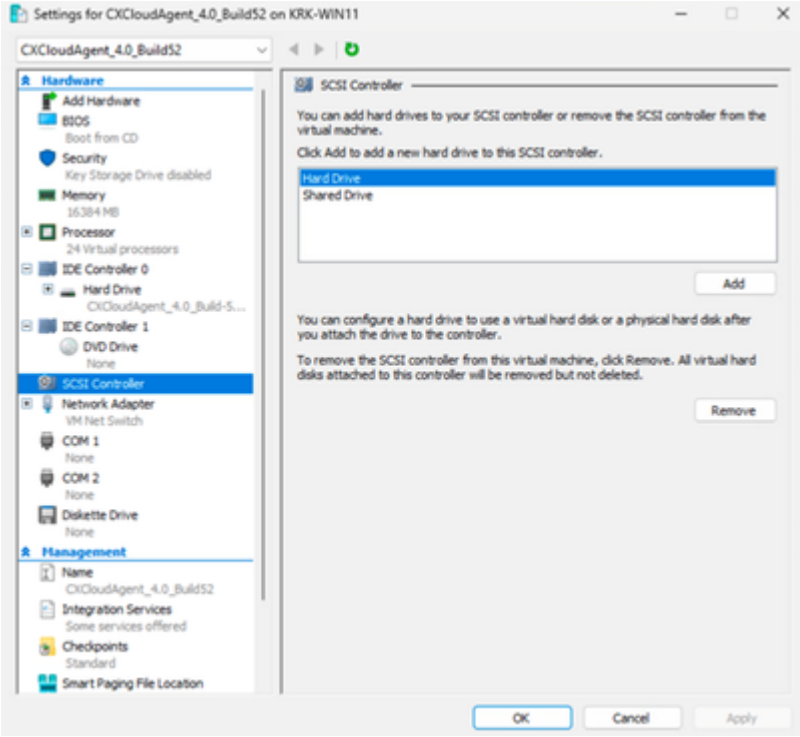
2. Choose **Settings**.
3. Click **Processor** in the **Hardware** pane.




4. Update the **Number of virtual processors** field as listed below:

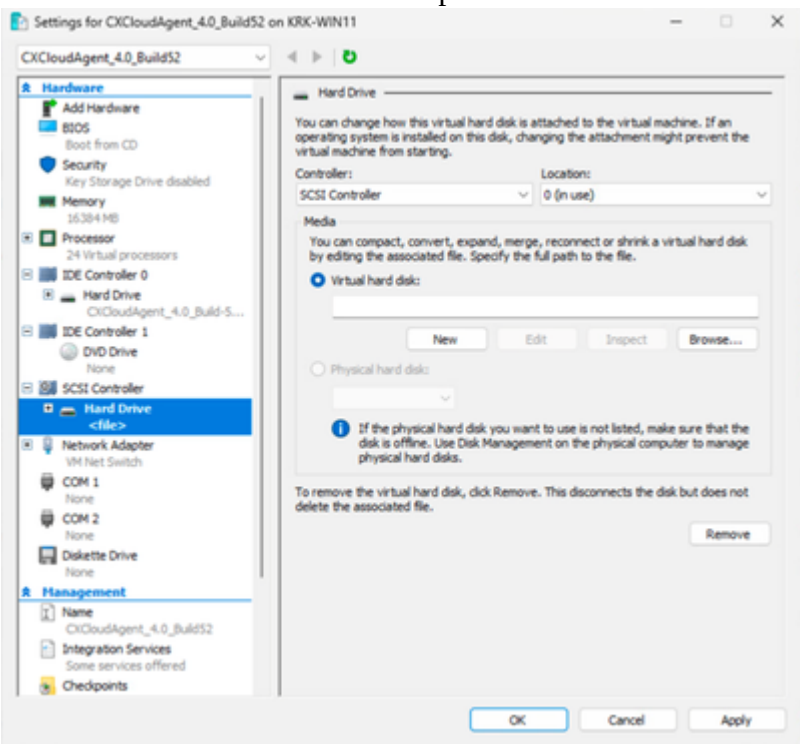
- Small Deployment: 8
- Medium Deployment: 16
- Large deployment: Minimum 32

5. Click **Apply**.
6. Click **OK**.
7. Update Storage Settings if creating a **Medium** or **Large** deployment of **CX Agent.** To update**:**
    1. Click VM **Settings**.



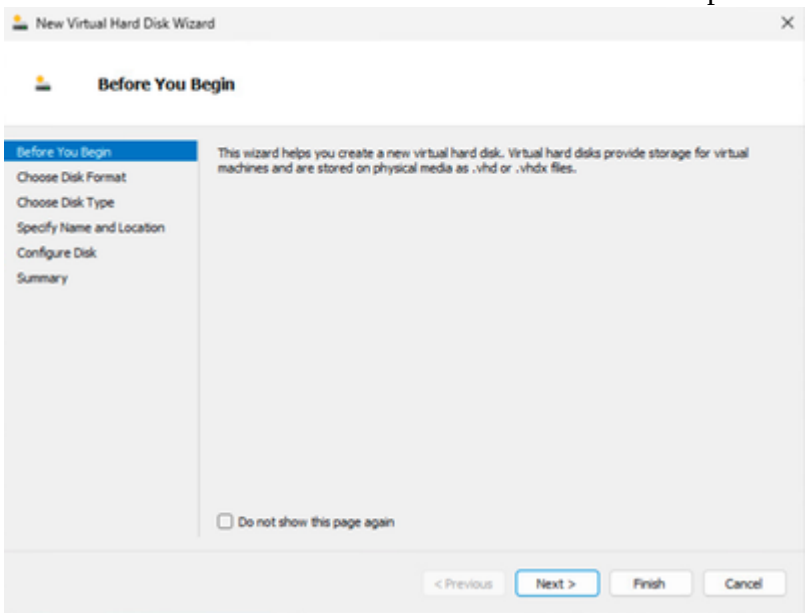

*SCSI Controller*

    2. Click **SCSI Controller** section.
    3. Click **Add** with the **Hard Drive** option selected.



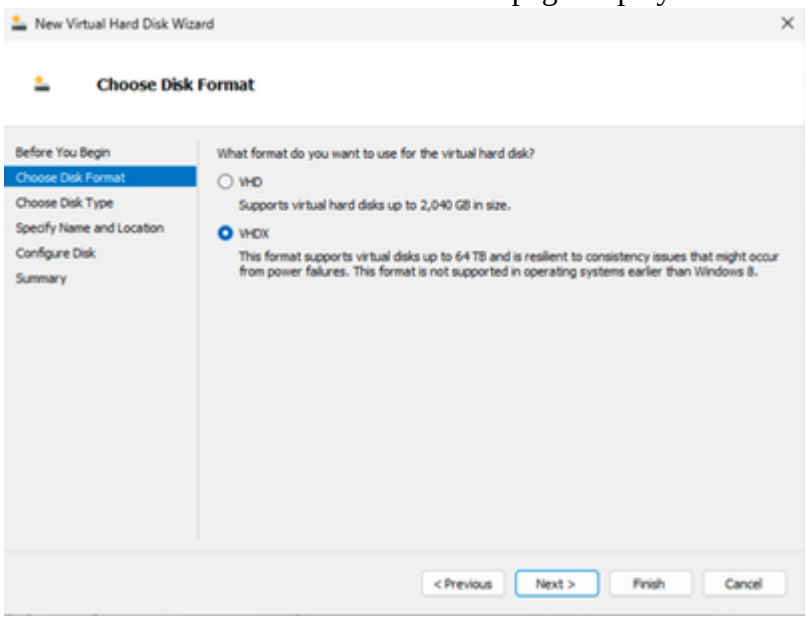

*Hard Drive*

4. Click **New** in **Media**. A new virtual hard disk wizard opens.




*New Hard Disk Wizard*

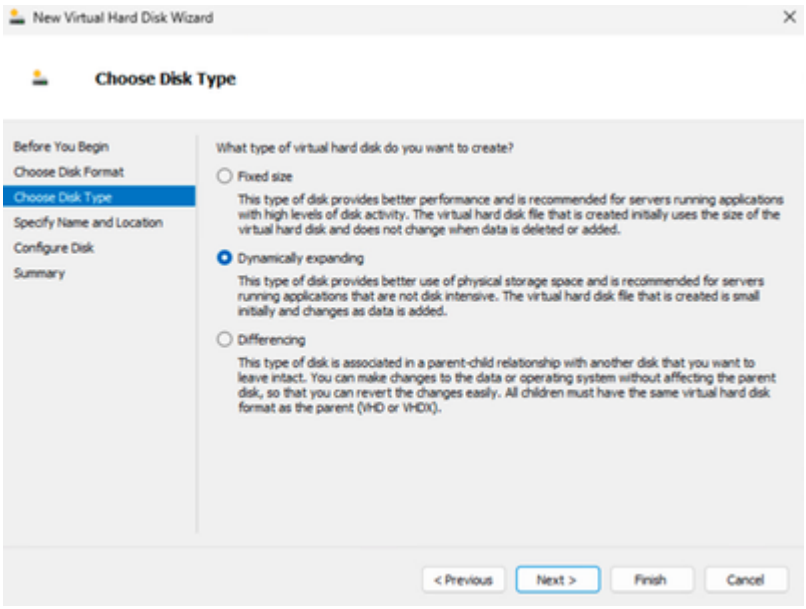
5. Click **Next. The Choose Disk Format** page displays.




*Choose Disk Format*

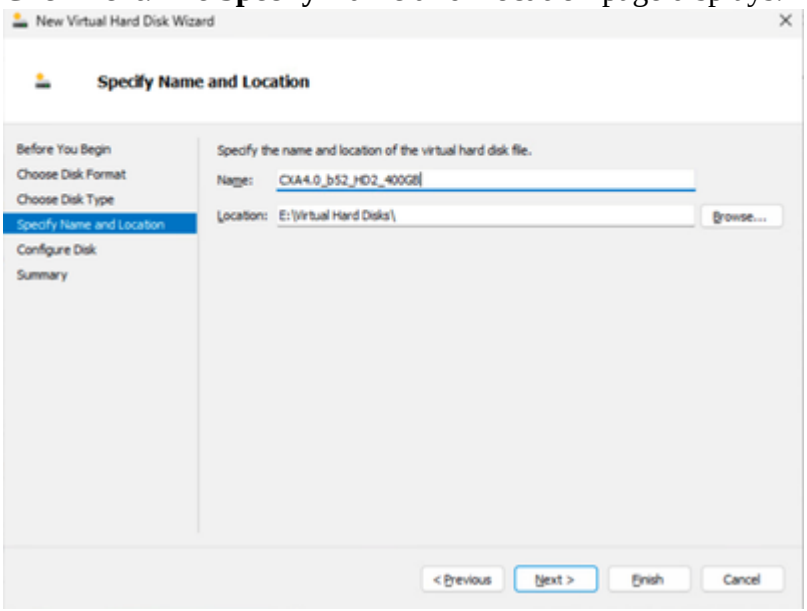
6. Click **VHDX** radio button to select disk format.
7. Click **Next**. The **Choose Disk Type** page displays.

C



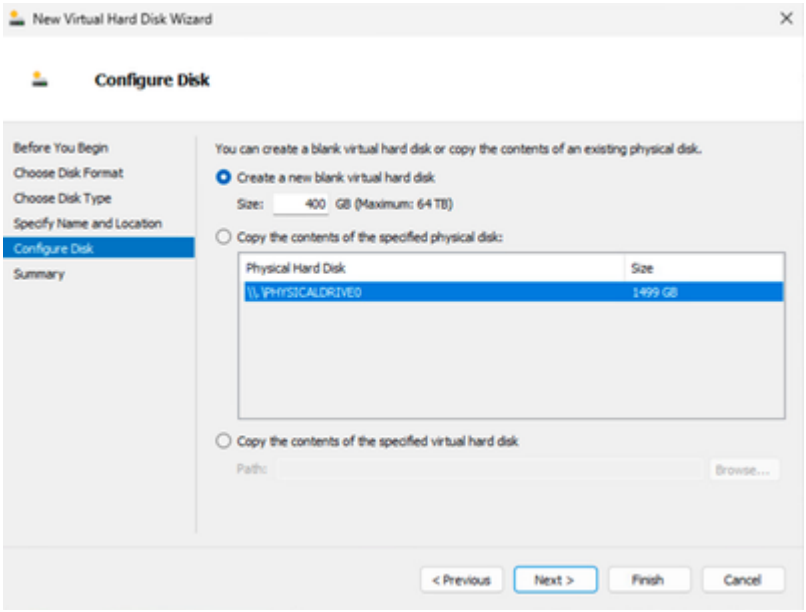

*Choose Disk Type*

8. Click **Dynamically expanding** radio button.
9. Click **Next**. The **Specify Name and Location** page displays.




*Specify Name and Location*

10. Enter disk **Name** and **Location**.
11. Click **Next**. The **Configure Disk** page displays.




*Configure Disk*

12. Enter the size of the new disk as recommended below:
    - Medium deployment: 400 GB
    - Large deployment: 1000 GB
13. Click **Finish**. Hyper-V VM is ready to use and can be started.

8. Refer to Network Configuration to proceed with the next steps.

### Microsoft Hyper-V Image Signature Validation

To ensure the integrity and authenticity of Microsoft Hyper-V images, signature validation is performed as part of the security process.

#### Prerequisites

- Ability to run OpenSSL commands via Command Line Interface
- Ability to run grep commands via Command Line Interface
- Cisco provided image for signature verification
- Cisco signed x.509 end-entity certificate containing a public key that is used for signature verification; this certificate is issued by a Cisco Subordinate CA, which is trusted by the Cisco Root CA
- Signature generated for the image
- Signature verification program required to verify the 3-tier x.509 certificate chain and signature; the certificate chain is validated first, including the end-entity certificate and well-known subCA and rootCA certificates, then the subCA and rootCA are either read from a specified local directory or downloaded from the PKI website; the authenticated end-entity certificate is used to verify the signature

#### Run Signature Verification Package

Customers can verify that the downloaded Cisco ZIP archive has been signed with a Cisco release certificate. Run the commands in the examples below to verify signatures.

---

**Note**: Ensure the correct attributes are referenced in the example commands below.

---

**Command 1 (sha512 signature, Cisco rootCA & subCA downloaded from PKI website example):**

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent__Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -v
dgst --algo sha512 --failExpiredCerts
```

*Command Output*

```
<possible error messages, some with UNSAFE_LEGACY_RENEGOTIATION_DISABLED
code word>

Retrieving rootCA certificate from
https://www.cisco.com/security/pki/certs/csirca4096.cer ...

Successfully retrieved and verified csirca4096.cer.

Retrieving subCA certificate from
https://www.cisco.com/security/pki/certs/cgsisca4096.cer ...

Successfully retrieved and verified cgsisca4096.cer.

Successfully verified root, subca and end-entity certificate chain.

Successfully fetched a public key from CX_COLLECTOR_HYPER_REL_CERT.pem.

Successfully verified the signature of CXCloudAgent_3.1_Build-
348_SHA1.vhdx_RELEASE_signed.zip using CX_COLLECTOR_HYPER_REL_CERT.pem
```

**Command 2 (sha512 signature, Cisco Virtual UEFI rootCA & subCA retrieved from Cisco PKI website example):**

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -v
dgst --algo sha512 –failExpiredCerts
```

*Command Output*

```
<possible error messages, some with UNSAFE_LEGACY_RENEGOTIATION_DISABLED
code word>

Retrieving CA certificate from
https://www.cisco.com/security/pki/certs/vuefirca.cer ...

Successfully retrieved and verified vuefirca.cer.

Retrieving SubCA certificate from
https://www.cisco.com/security/pki/certs/vuefiscav2.cer ...

Successfully retrieved and verified vuefiscav2.cer.

Successfully verified root, subca and end-entity certificate chain.

Successfully fetched a public key from CX_COLLECTOR_HYPER_REL_CERT.pem.
```

```
Successfully verified the signature of CXCloudAgent_3.1_Build-
348_SHA1.vhdx_RELEASE_signed.zip using CX_COLLECTOR_HYPER_REL_CERT.pem
```

**Command 3 (local Cisco rootCA & subCA example)**

```
./cisco_x509_verify_release.py3 -e CX_COLLECTOR_HYPER_REL_CERT.pem -i
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip -s
CXCloudAgent_3.1_Build-348_SHA1.vhdx_RELEASE_signed.zip.signature -c
/cert/store -v dgst --algo sha512 –failExpiredCerts
```

*Command Output*

```
Using locally-provided rootCA certificate /cert/store/vuefirca.cer

Using locally-provided subCA certificate /cert/store/vuefiscav2.cer

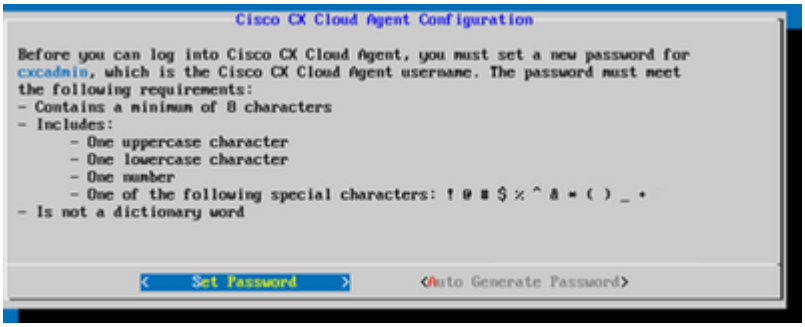
Successfully verified root, subca and end-entity certificate chain.

Successfully fetched a public key from CX_COLLECTOR_HYPER_REL_CERT.pem.

Successfully verified the signature of CXCloudAgent_3.1_Build-
348_SHA1.vhdx_RELEASE_signed.zip using CX_COLLECTOR_HYPER_REL_CERT.pem
```

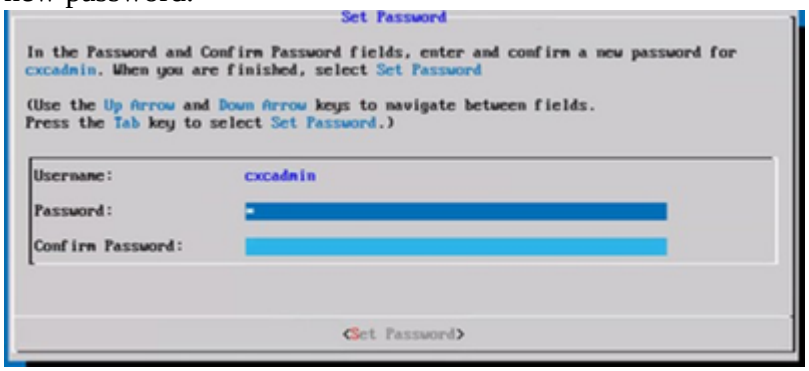
## Network Configuration

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




*Set Password*

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

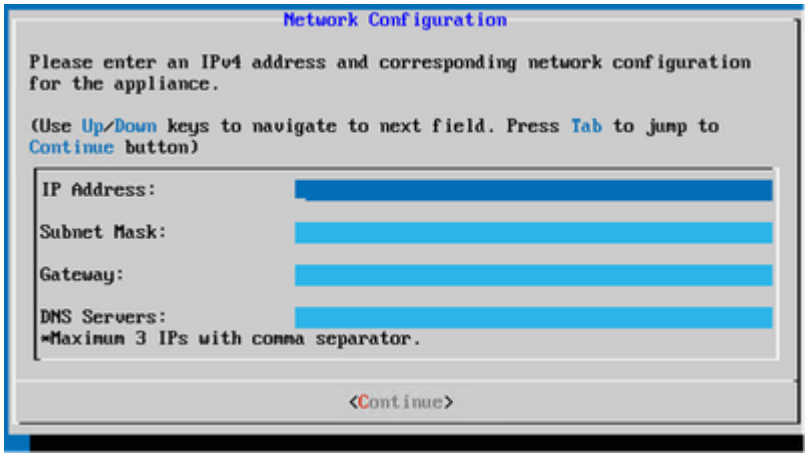



*Auto Generated Password*



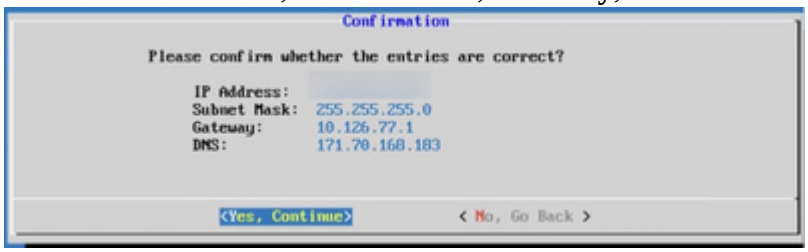

*Save Password*

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



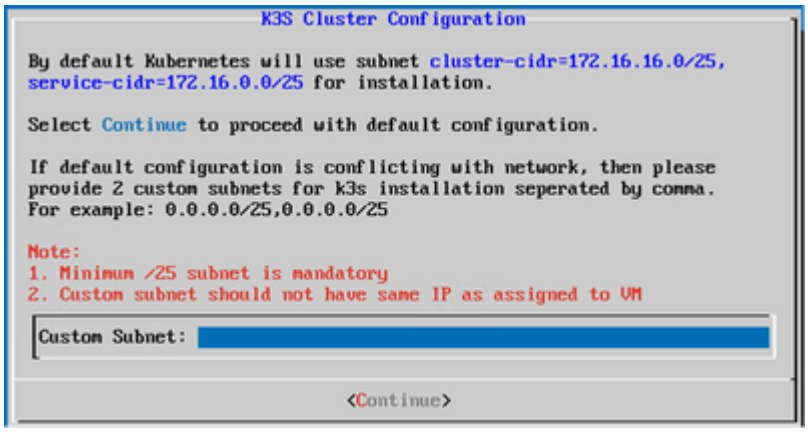

*Network Configuration*

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



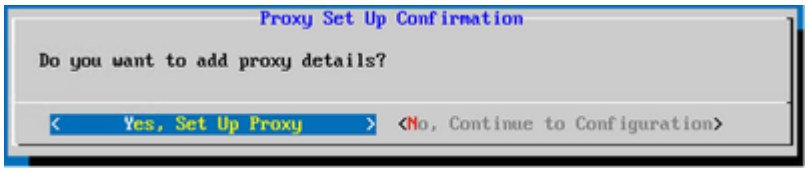

*Confirmation*

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



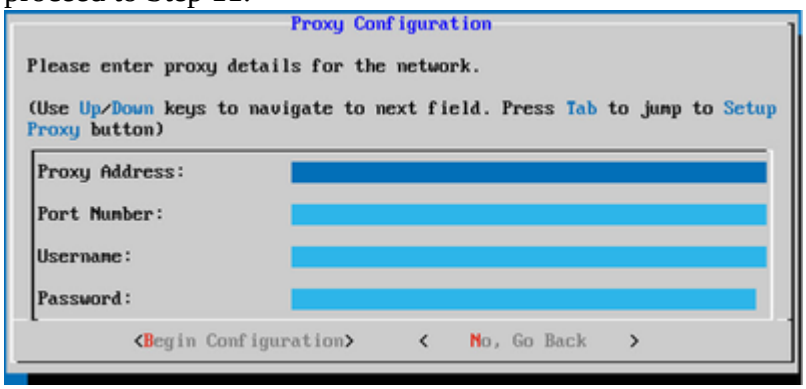

*Custom Subnet*

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**.



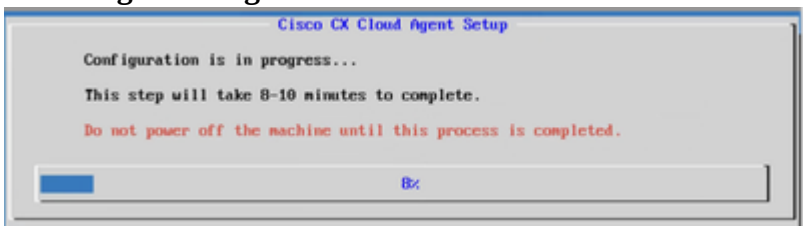

*Proxy Set Up*

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

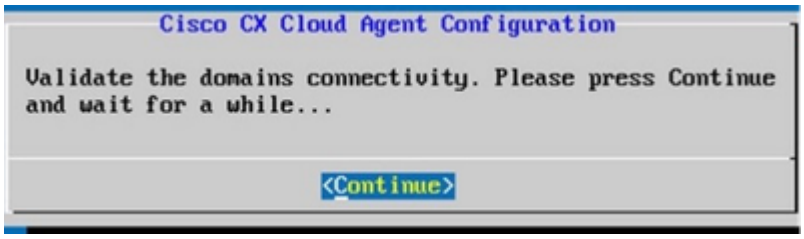



*Proxy Configuration*

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

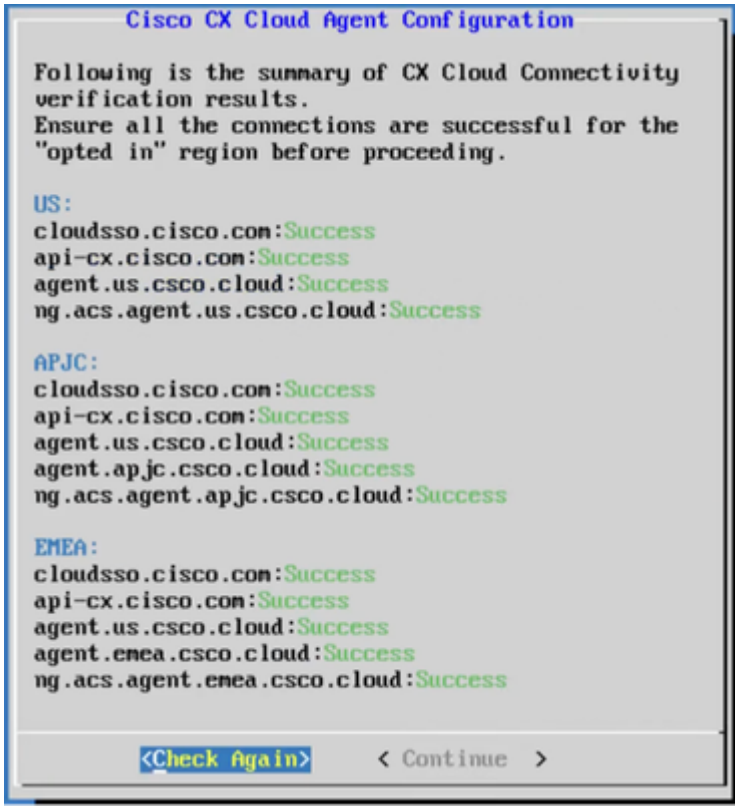



*CX Cloud Agent Set Up*




*CX Cloud Agent Configuration*

11. Click **Continue.**



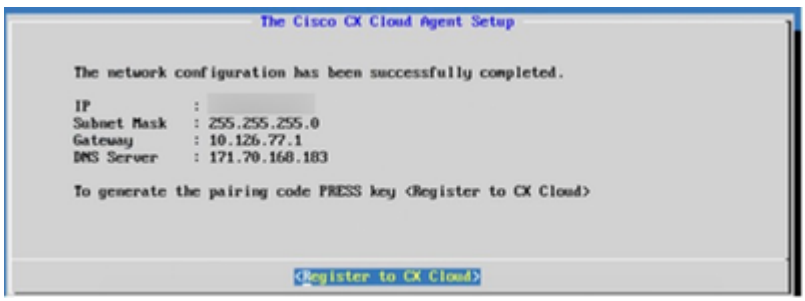

*Configuration Continues*

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

---

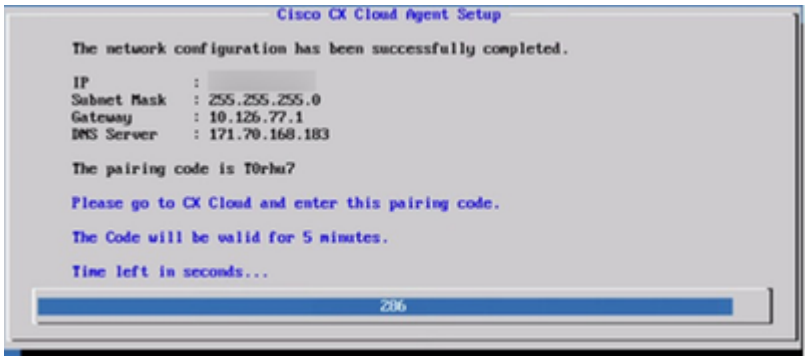
**Note**: If the domains cannot be reached successfully, the customer must fix domain reachability by making changes in their firewall to ensure that domains are reachable. Click **Check Again** once the domains reachability issue is resolved.

---




*Register to CX Cloud*

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




*Pairing Code*

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




*Registration Successful*

---

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

---

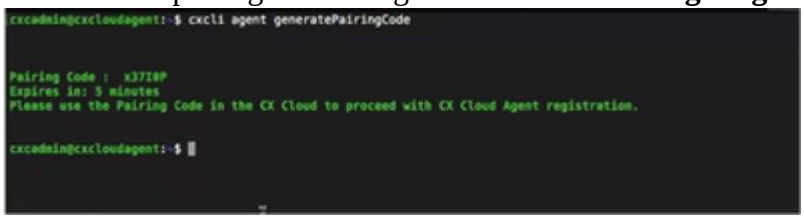
15. Click **OK**.

## 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**.




*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

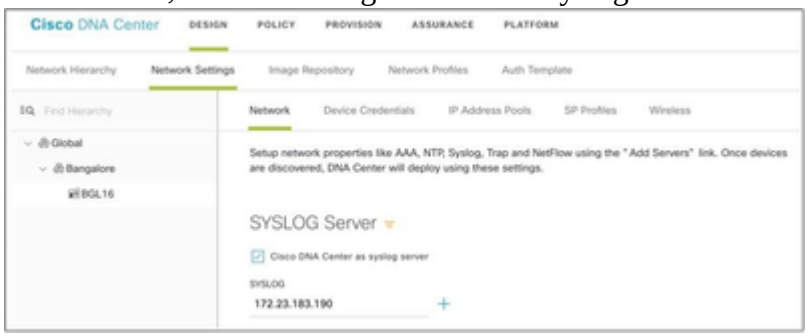
### Prerequisites

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.




*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 Menu*

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




*Site View*

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

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




*Actions*

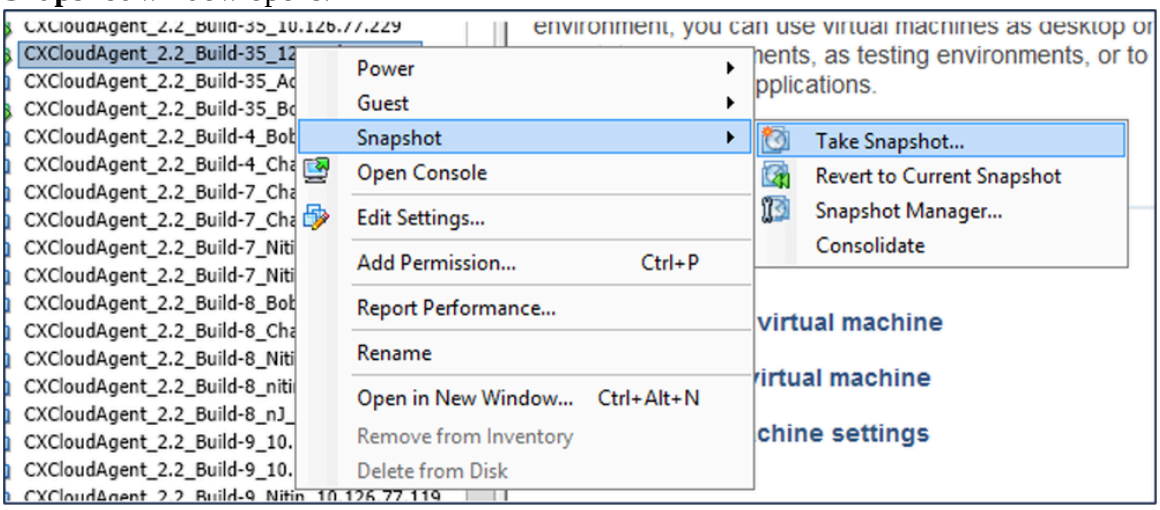
# Backing Up and Restoring the CX Cloud VM

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.

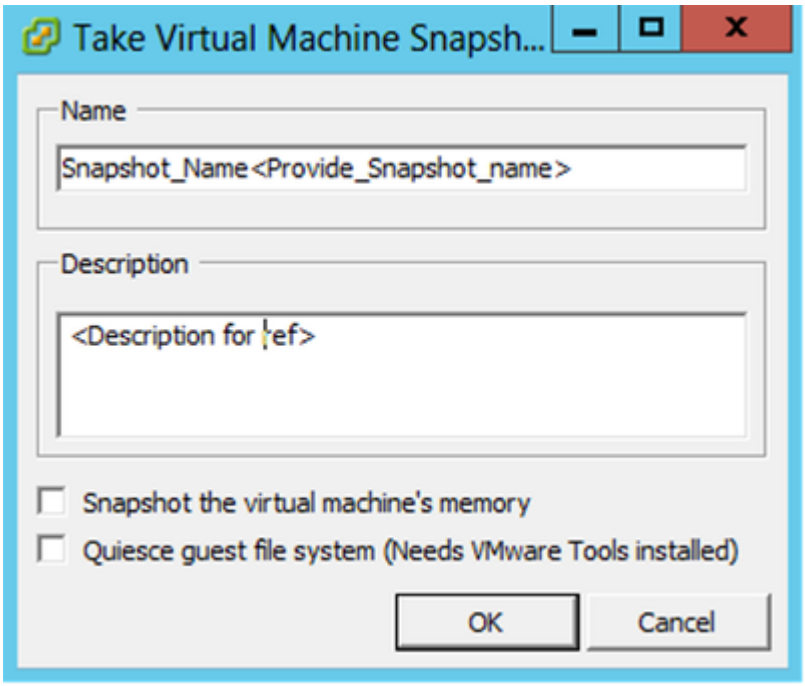
## Backing Up the CX Cloud VM

To back up the CX Cloud VM:

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




*Select VM*

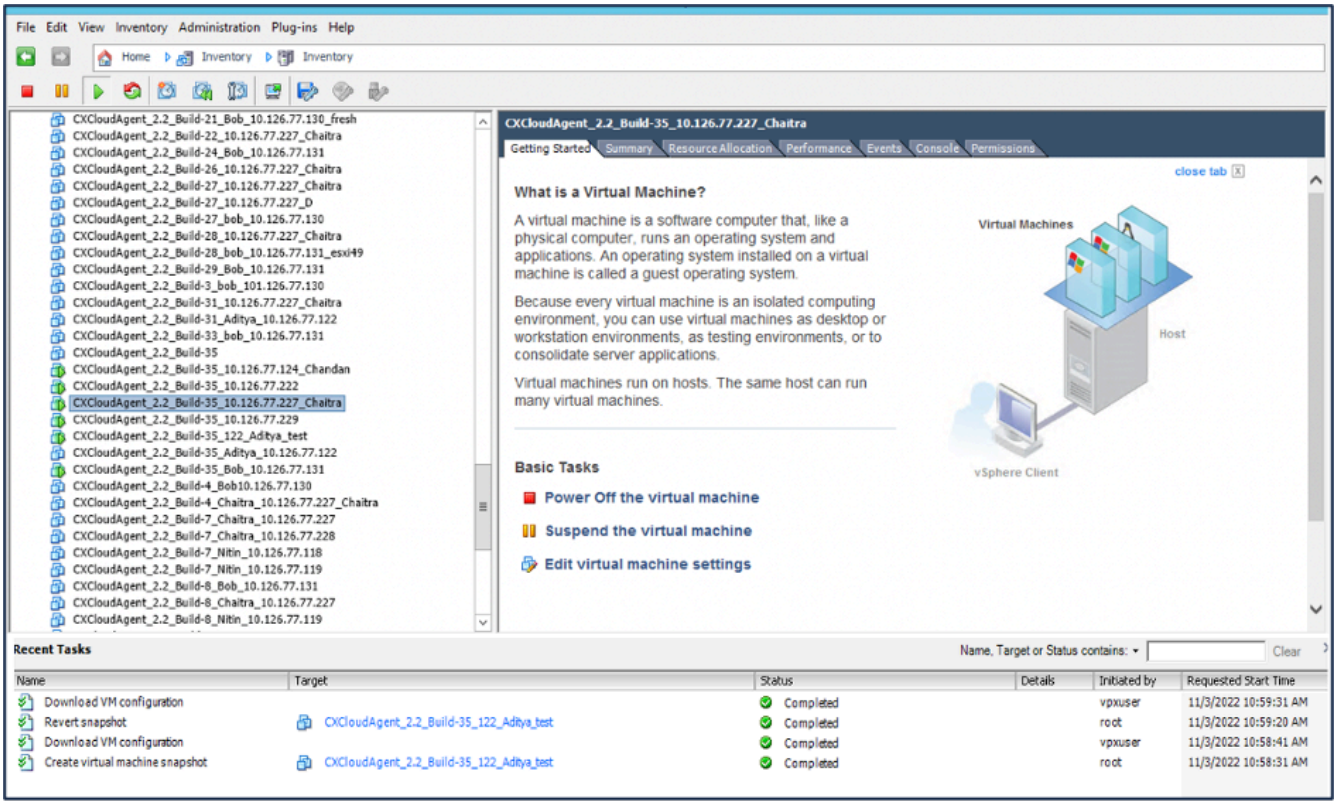



*Take Virtual Machine Snapshot*

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

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

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

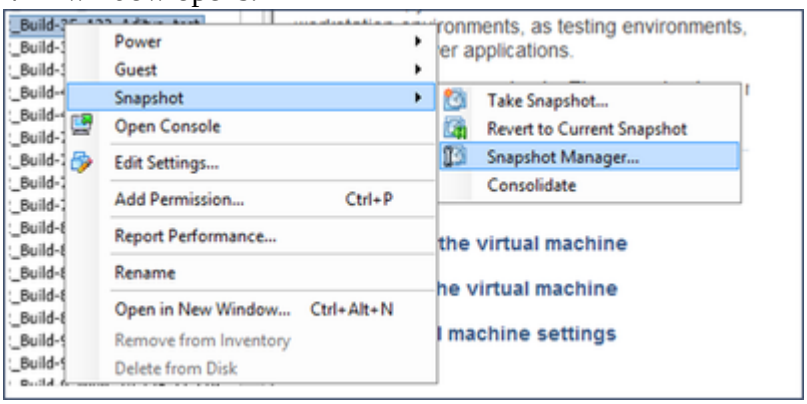


*Recent Tasks*

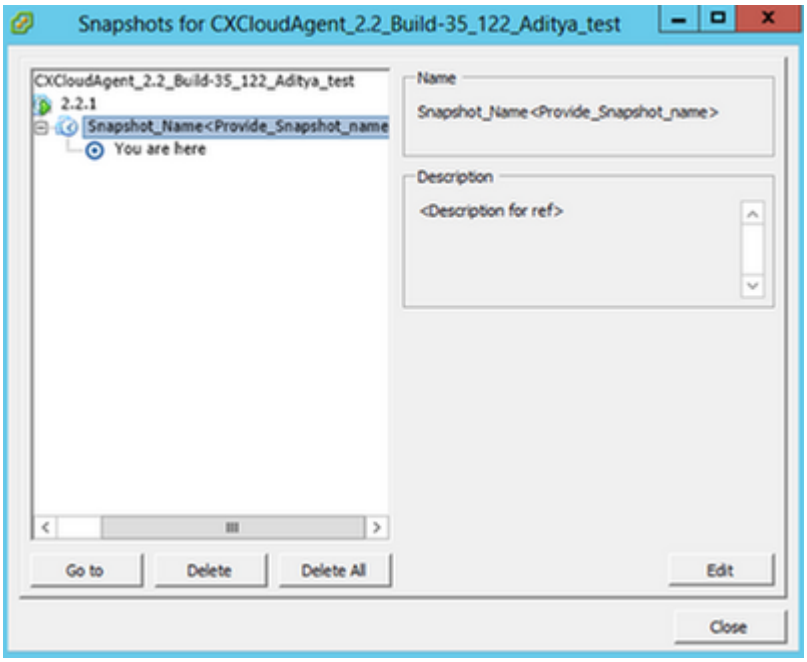
## Restoring the CX Cloud VM

To restore the CX Cloud VM:

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

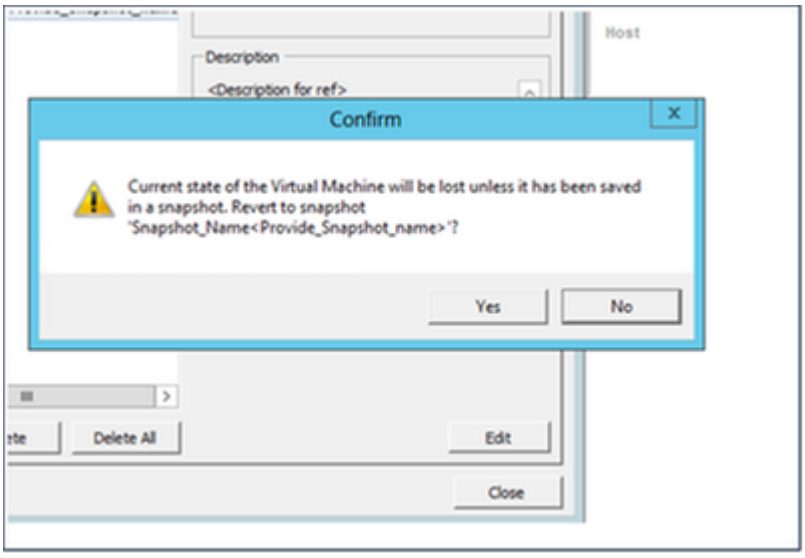



*Select VM window*



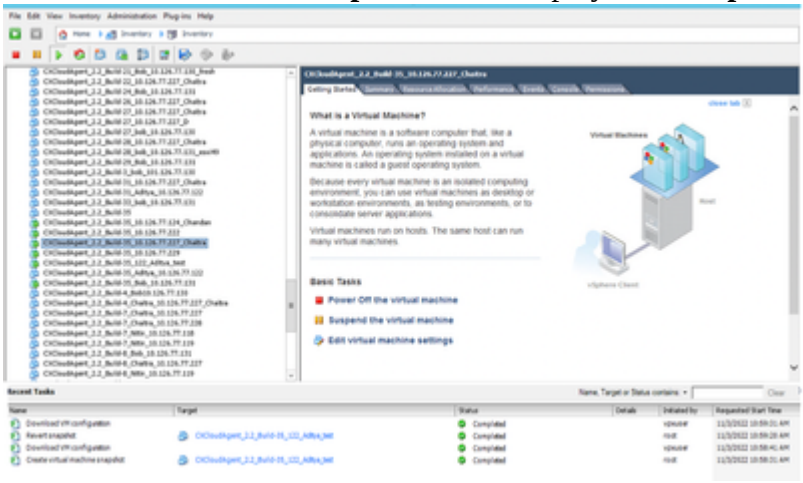

*Snapshots Window*

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



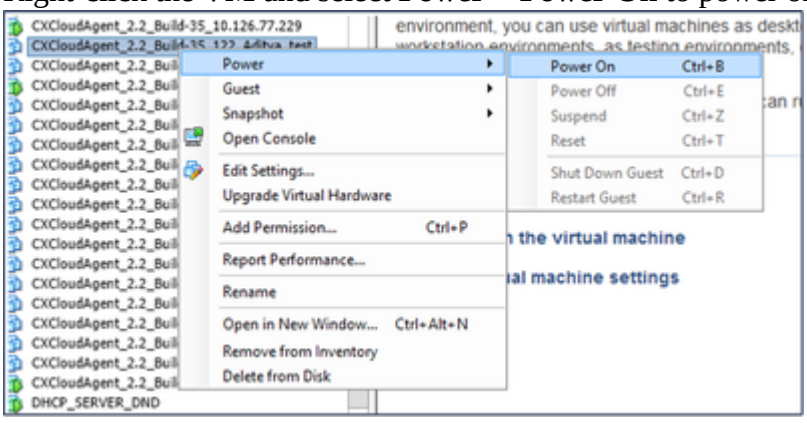

*Confirm Window*

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



*Recent Tasks*

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




# Security

CX 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:<br>· Access to appliance using cxcadmin user requires credentials created during installation.<br>· 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.<br>· 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<br>· The passphrase generated needs to be decrypted in SWIM portal.<br>· 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.<br>· 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.<br>· No Device data stored.<br>· Cisco Catalyst Center server credentials encrypted and stored in the database. |