

Cisco IQ Virtual Appliance Getting Started Guide

Introduction

Cisco IQ™ provides customers with enhancements and features designed to improve asset visibility, deliver smarter insights across their environments, and streamline case management. In addition, AI features such as the AI Assistant optimize operational outcomes and the Cisco IQ user experience by providing contextual understanding that empowers users to make proactive, informed decisions and streamline processes for customer engagement and success.

Cisco IQ On-Prem Air-Gapped is one of the deployment modes of Cisco IQ, designed for customers in highly regulated industries with stringent compliance, data sovereignty, and security requirements. In this mode, Cisco IQ is delivered as a self-contained Virtual Machine (VM) referred to as the Cisco IQ Virtual Appliance (VA). The VA runs entirely on the customer's premises and operates in complete isolation from external networks. To maintain this isolation, software updates and maintenance packages are obtained from Cisco IQ SaaS and transferred to the VA through an approved, manual process.

Cisco IQ On-Prem Air-Gapped extends key capabilities of Cisco IQ SaaS to air-gapped environments, enabling mission-critical teams to operate with speed and diagnostic intelligence comparable to cloud-connected enterprises.

This guide provides instructions for configuring and deploying Cisco IQ VA for Air-Gapped, including the process of setting up the required network environment.



Note: The Cisco IQ VA is currently limited to customers enrolled in the Controlled Release program. Download access for the VA and its operational systems (modules, rules, and entitlements) is available exclusively to selected customers. Please contact your account representative for more information.

Deployment Options

Cisco IQ VA offers a flexible deployment model designed to deliver value with options to fit different operational needs. The core deployment provides essential capabilities like Asset and Inventory management, Assessments, and other operations.

For customers seeking advanced AI-driven insights and automation, VA also offers an AI-powered deployment option enabled through Graphics Processing Unit (GPU) hardware. You can unlock powerful AI features such as the AI Assistant, Key Insights, and Full Insights with AI add on.

This approach lets you choose the best fit for your operational and security requirements, making VA a scalable and future-ready solution.

Prerequisites

Ensure the following prerequisites are met before configuring and installing Cisco IQ VA.

Hardware and VM Resource Requirements

Cisco IQ VA is tested for multiple scale capacity and offers multiple deployment sizes to support your environment’s scaling needs. See the table below to select the appropriate resource configuration based on your planned device discovery count.

Table 1: Hardware and VM Resource Requirements

Resource	Up to 5K Devices (Non-GPU Based)	Up to 20K Devices (Non-GPU Based)	Up to 20K Devices (GPU Based)
vCPU	48	64	96
RAM	96GB	128GB	256GB
Storage (SSD) (Recommended for better performance)	1.3TB	1.3TB	1.3TB
Collection Schedule	24 hours or more	24 hours or more	24 hours or more
Supported Hypervisors	- VMware ESXi v8.0 or later with VMware vSphere Web Client v8.0 or later - Hyper-V on Microsoft Server 2022 and 2025 - Kernel-based Virtual Machine (KVM) Hypervisor on RHEL v9.7 or later		
Server	Unified Computing System M6 or newer models		
Additional Recommendation	- Cisco recommends that you use thick provisioning. While it is possible to use thin provisioning, over-provisioning can lead to a lack of storage capacity which can then result in degradation and loss of service. - It is highly recommended to place appliance disks on a volume backed by SSDs. - Disk write speed must be greater than 70 megabytes per second.		

AI Feature Resource Requirements

Cisco IQ VA is tested and supported on the NVIDIA RTX Pro 6000 Blackwell Server Edition GPU. This GPU configuration meets the performance and latency requirements at the planned deployment scale.

Table 2: AI Feature Resource Requirements

Resource	Recommended
Validated GPU	NVIDIA RTX Pro 6000 Blackwell Server Edition
Additional GPU Options (Not validated)	• NVIDIA H200 (141 GB)
Additional GPU Options (Not validated, suggested with one (1) concurrent user)	• NVIDIA H100 (80 GB) • NVIDIA H100 NVL (94 GB) • NVIDIA A100 (80 GB)

 **Note:** GPUs other than NVIDIA RTX Pro 6000 Blackwell Server Edition have not been validated in Cisco labs at the supported scale. Performance and latency are not guaranteed for non-validated GPUs. Please validate all non-supported hardware against your projected workload in a pre-production environment prior to production deployment.

Network Requirements

VA supports a single network interface.

IP Address and Hostname Requirements

The following IP address and hostname requirements must be met:

- **Domain Name System (DNS):** DNS simplifies system management by replacing numeric IP addresses with consistent, human-readable hostnames. This approach facilitates easier maintenance, seamless service integration, and reliable certificate validation in secure environments. Ensure that the IPv4 address is configured in your DNS with the following:
 - **A Record:** Maps the hostname to the IPv4 address
 - **Associated Pointer (PTR) record:** Required to support reverse DNS lookups; if an IP address resolves to multiple hostnames, the first resolved hostname is used to access the UI

 **Note:** DHCP is currently not supported.

Port Requirements

The following table outlines the network ports required for Cisco IQ VA communication.

Table 3: Port Requirements

Port(s)	Protocol	Description
22	TCP	Used for Administrator CLI and Cisco Support debugging sessions
443	TCP	Used for communication between Cisco IQ On-Prem and web browsers, as well as endpoint targets
53, 123, 161	UDP	Used to send and receive DNS, NTP, and SNMP traffic

Supported Browsers

You must use the latest stable release of the following browsers to install and launch VA:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox



Note: Support is limited to current browser versions, and older versions may not provide full functionality or may be unsupported as new updates are released.

Installing Virtual Appliance Setup

This section outlines the installation procedures for VA. The current scope includes instructions for the following hypervisors:

- VMware ESXi
- Microsoft Hyper-V Server
- Red Hat KVM

Download Virtual Appliance

VA installer files are available to be downloaded from Cisco IQ SaaS. To download VA:

1. Log in to [Cisco IQ](#) (SaaS).
2. Navigate to **System Settings > Package Catalog**.
3. From the Cisco IQ VA card, choose **Download options**. The **Install Package** window opens.
4. Select one of the following **Hypervisor** options from the drop-down list:
 - **ESXi**: for VMware ESXi
 - **Hyper-V**: for Microsoft Hyper-V
 - **KVM**: for Linux Kernel-based Virtual Machine (KVM)
5. Select a **Version** from the drop-down list.
6. Click **Download** to save the file locally.

 **Note:** Installation files are large (20-25 GB); ensure you have sufficient disk space before downloading.

Installing Virtual Appliance on VMware ESXi

The downloaded VA installer file is ready to be installed. To install VA on VMware ESXi:

 **Note:** The OVA must be deployed using VMware vCenter and cannot be directly deployed on ESXi servers.

1. Log in to VMware vSphere Web Client with administrator credentials.
2. Right-click on the appropriate vCenter object (data center, cluster, or ESXi host) and choose **Deploy OVF Template**.
3. On the **Deploy OVF Template** wizard, choose the template page, specify the source location, and click **Next**. You can specify a URL or browse to any accessible location.
4. On the **OVF Template Details** page, verify the OVF template details and click **Next**. No input is necessary.
5. On the **Select a name and location** page, add or edit the **Name** and **Location** for the VA and click **Next**.
6. On the **Select a resource** page, choose the specific **Host** (ESXi host), **Cluster**, or **Resource Pool** on which you want to deploy and click **Next**.

 **Note:** Each VM must be assigned to a specific host on clusters that are configured with vSphere High Availability (HA) or Manual mode vSphere Distributed Resource Scheduler (DRS).

7. On the **Review details** page, verify the OVA template details and click **Next**.
8. On the **Configuration** page, choose a deployment configuration and click **Next**.
9. On the **Select storage** page, choose the destination storage location for the VM files in the selected ESXi host and click **Next**.
10. Choose the **Disk Format** for the VM virtual disks.

 **Note:** It is recommended to use thick provisioning. While it is possible to use thin provisioning, over-commitment of storage can lead to a lack of storage capacity resulting in degradation and loss of service.

11. On the **Select networks** page, choose a source network and map it to a destination network and click **Next**.
12. On the **Ready to Complete** page, select **Power On After Deployment** and click **Finish**.
13. Ensure that VMs are configured with the following additional settings by right-clicking the desired

VM in VMware ESXi and clicking **Edit Settings**.

- **CPU**: Select **Low** from the first **Shares** drop-down list
- **Memory**: Check the **Reserve all guest memory (All locked)** check box
- Set CPU and RAM based on your scale size; see [Hardware and VM Resource Requirements](#) for more information

14. In VMware ESXi, select the desired VM.

15. Click the **Summary** tab.

16. Click the displayed image or the **Launch Console** icon to launch the console.

17. See [Network Configuration](#) for next steps.

Installing Virtual Appliance on Microsoft Hyper-V Server

To install VA on Hyper-V:

1. Log in to Hyper-V Server Manager with administrator credentials.
2. Extract the VA package to the location defined by the Hyper-V Administrator to store all the virtual hard disks.
3. Verify that all the disks from the original Cisco IQ .tar.gz are in the *Virtual Hard Disks* folder.
4. From the **Actions** pane of Hyper-V Manager, choose **New > Virtual Machine** and click **Next**.
5. Enter the **Name** you want to assign to the VA and click **Next**.
6. Choose **Generation 2** and click **Next**.
7. Enter the memory value based on the recommended memory size in [Hardware and VM Resource Requirements](#) and click **Next**.
8. Verify **Use Dynamic Memory** remains unchecked.
9. Choose the appropriate network adapter for your VA and click **Next**.
10. Add the provided VA virtual hard disk, ensuring disk one (1) is the first disk, and click **Next**.



Note: The other two (2) virtual hard disks are added at a later step.

11. Verify the selections in the **Summary** and click **Finish**. Hyper-V displays the newly created VA VM.
12. Right click the VM and choose **Settings**.
13. Under **Security**, uncheck the **Enable Secure Boot** check box.
14. Add the other two (2) virtual hard disks to the VM by repeating the same steps used for adding the first hard disk.
15. In the **Advanced Features** under the Network Adapter, verify that the **Enable device naming** is selected.
16. Set the number of processors to the recommended vCPUs as listed in [Hardware and VM Resource Requirements](#).
17. In the **Actions** pane, select **Start** to power on the VM.
18. In the **Actions** pane, select **Connect** to connect to the VM. The **VM Connection** console is displayed.
19. See [Network Configuration](#) for more details.

Installing Virtual Appliance on Red Hat KVM

Ensure that the following supported requirements are met before installing VA on KVM.

- RHEL host OS
- Administrative access on the Red Hat server

To install VA on a KVM Hypervisor, VM Manager is required.

1. Log in to Red Hat host OS server with administrator credentials.
2. Download and extract the VA package on the host.
3. Launch the Virtual Machine Manager (VMM) client.
4. Choose **File > New Virtual Machine** on the menu to install a new VA.
5. Choose Import existing disk image and click **Forward**.
6. Under **Provide the existing storage path**, click **Browse**.
7. Create a new storage pool using the path where you extracted the VA package.
8. Choose the first disk of the VA from the storage pool created on the previous step and click **Choose Volume**.
9. Under **Choose an operating system type and version**, choose **AlmaLinux 9**, and click **Forward**.
10. Under **Choose Memory and CPU settings**, enter details based on your scale size and click **Forward**.
See [Hardware and VM Resource Requirements](#) for more details.
11. In the dialog box, complete the following configuration:
 1. Under **Ready to begin the installation**, enter a **Name** for the VA instance.
 2. Click the **Customize configuration before install** option.
 3. Under **Network selection**, ensure that you select the appropriate virtual network.
12. Click **Finish** to complete the addition of the first disk.
13. Add the remaining two (2) disks:
 1. On the VMM console, click **Add Hardware**.
 2. Under **Storage**, ensure that the **Select or create custom storage** check box is checked and click **Manage**.
 3. Browse to select the second disk of the VA file that you extracted on your system.
 4. Click **Choose volume**.
14. Repeat the same (Add Hardware) steps to add the third VA disk.
15. Ensure all disk Bus Types are **SCSI**.
16. Click **Finish**.
17. Under the **Overview** section, choose **UEFI** for Firmware.
18. Click **Begin installation**.
19. See [Network Configuration](#) for next steps.

Network Configuration

1. Launch VA from VM console.

```
***** WARNING!!! *****  
***** READ THIS BEFORE ATTEMPTING TO LOGON *****  
#  
# This System is for the use of authorized users only. Individuals #  
# using this computer without authority, or in excess of their #  
# authority, are subject to having all of their activities on this #  
# system monitored and recorded by system personnel. In the course #  
# of monitoring individuals improperly using this system, or in the #  
# course of system maintenance, the activities of authorized users #  
# may also be monitored. Anyone using this system expressly #  
# consents to such monitoring and is advised that if such #  
# monitoring reveals possible criminal activity, system personnel #  
# may provide the evidence of such monitoring to law enforcement #  
# officials. You cannot copy, disclose, display or otherwise #  
# communicate the contents of this server except to other Cisco #  
# employees who have been authorized to access this server. #  
#  
***** Confidential Information *****  
cisc-infra login: admin  
Password:
```

Log In

2. Log in to the console using the default network credentials by entering “admin” for both the login name and password. The main menu displays.



Note: The default credentials are provided for initial setup only as there is no data to protect at this stage of installation.



Navigation **Main Menu** > Configure Network Settings

CONFIGURATION SETTINGS

Configured network settings:

Please provide the following network settings:

```
Enter IP Address/Mask
(e.g., 192.168.1.100/24): 
Valid IP/Mask format ✓
Enter Gateway IP
(e.g., 192.168.1.1): 
Valid Gateway IP ✓
Enter DNS IP List (comma-separated)
(e.g., 8.8.8.8,8.8.4.4): 
Valid DNS list (1 servers) ✓
Enter Search Domain
(default: local.domain) - press Enter to use default:
```

Main Menu

3. Enter “1” and press **Enter** to configure network settings.
4. Provide the following network settings:

 **Note:** Users can press Enter to use detected values where available.

- IP address
- Gateway IP
- DNS IP list
- Search domain
- NTP server list

 **Note:** Inputting multiple NTP servers using a comma-separated format is supported.

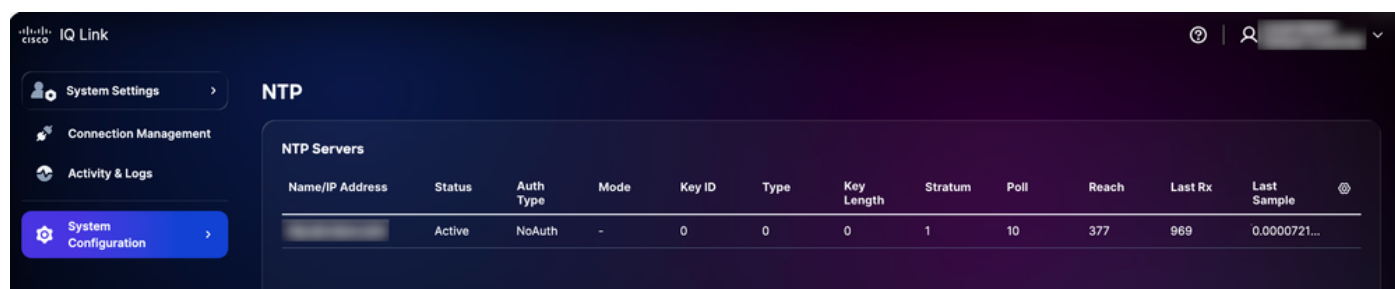
5. Configure the NTP authentication by pressing **N** to proceed without an authentication method

OR

Press **Y** and enter the corresponding number of an option listed below:

- **Traditional key-based authentication:** Uses provided credentials for secure time synchronization; after selecting this option, enter a valid algorithm and a hex key
- **Network Time Security (NTS):** Uses the NTS protocol to provide secure NTP communication

 **Note:** NTP information can be validated in the UI after installation by navigating to **System Settings**.



Name/IP Address	Status	Auth Type	Mode	Key ID	Type	Key Length	Stratum	Poll	Reach	Last Rx	Last Sample	
[REDACTED]	Active	NoAuth	-	0	0	0	1	10	377	969	0.0000721...	

NTP Validation in UI

6. Enter and confirm a password after reviewing the on-screen password requirements.
7. Review the summary and press **Y** to continue. Setup can take a few minutes.
8. Once a success message is received, press **Enter** to return to the main menu.



Cisco IQ Menu

Network settings are now configured, but VA has not yet been installed. It is recommended to return to

hypervisor and take a Snapshot of the new VM for future reference. At this point, you can also initiate a Secure Shell connection using the newly configured IP address and credentials.

This completes manual configuration of VA.

Installing VA for Air-Gapped Mode

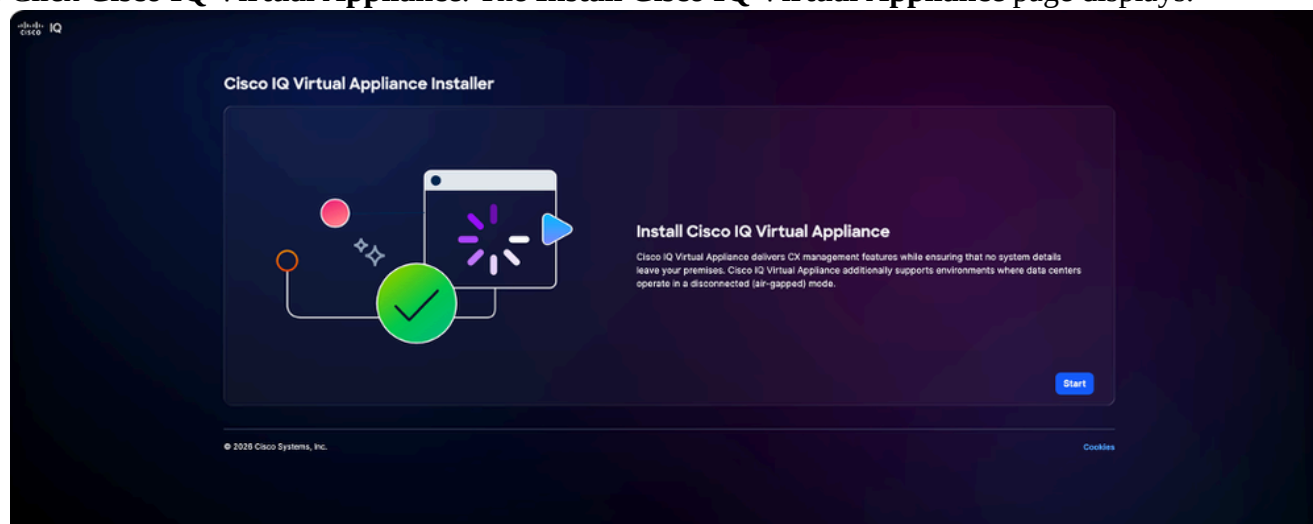
To install VA:

1. Navigate to the VA installer web interface (<https://<CIQ-HOST>/installer/welcome>) (received after configuring VA in VMs.). The **Cisco IQ Virtual Appliance Installer** page displays.



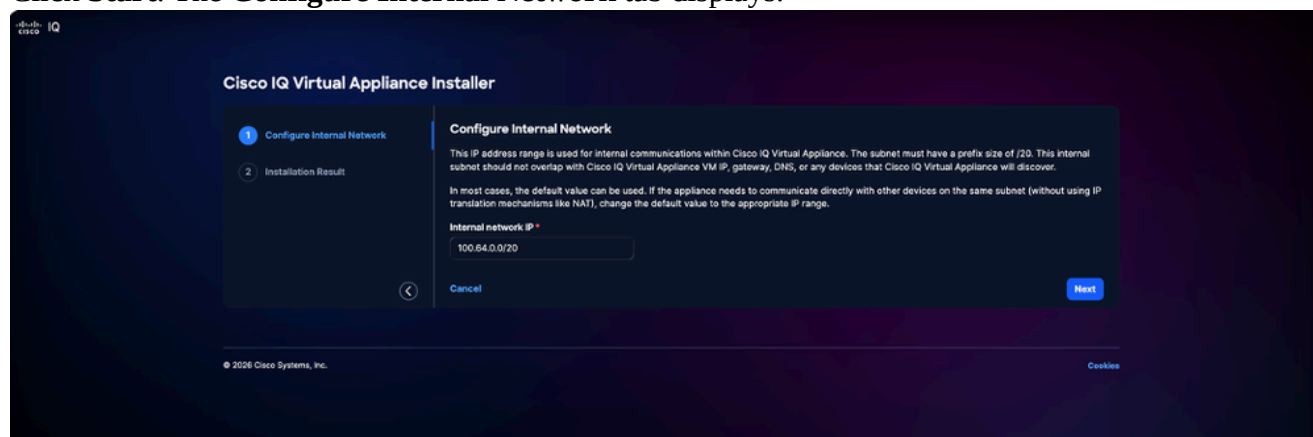
Virtual Appliance Installer Page

2. Click **Cisco IQ Virtual Appliance**. The **Install Cisco IQ Virtual Appliance** page displays.



Install Virtual Appliance

3. Click **Start**. The **Configure Internal Network** tab displays.



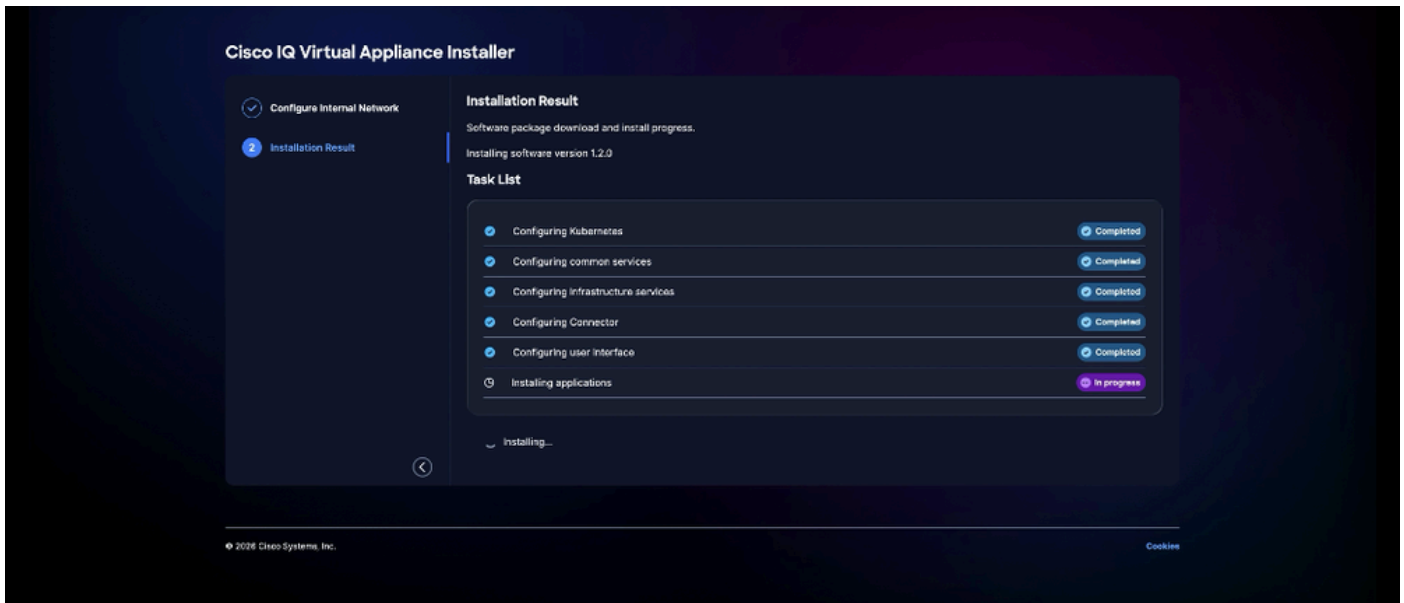
Configure Internal Network

4. Enter the **Internal IP Range**.



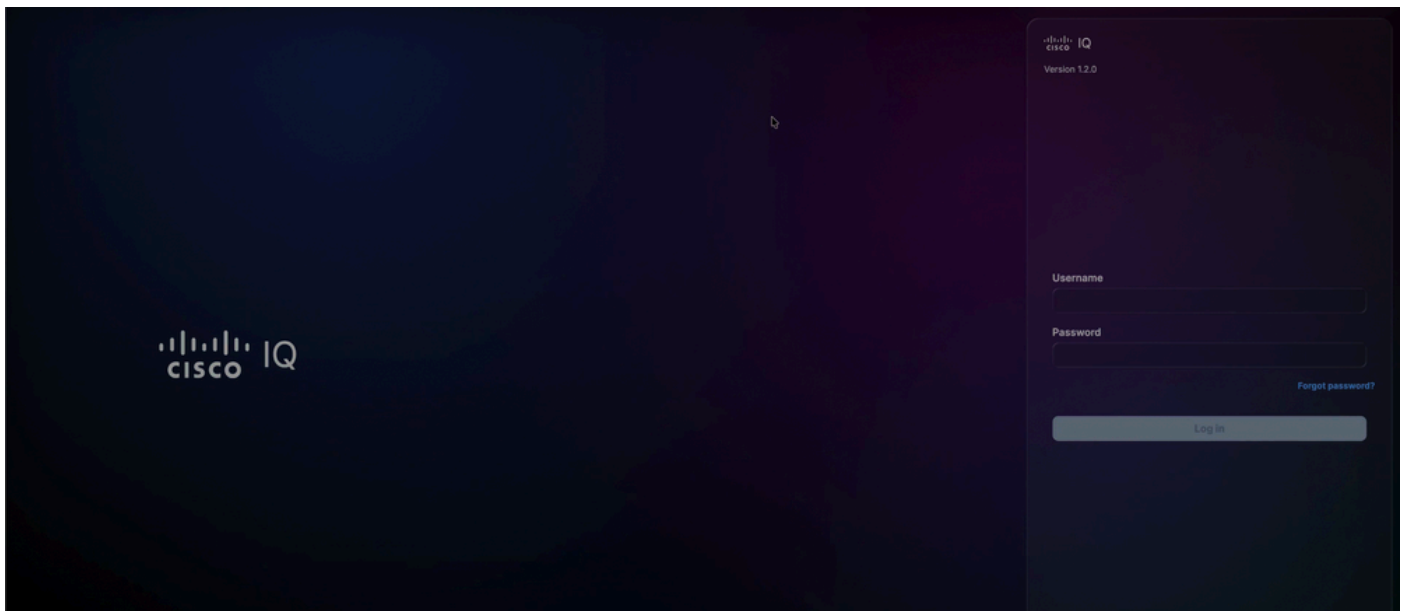
Note: Ensure the internal subnet does not overlap with your VM IP, gateway, DNS, or reachable network ranges.

5. Click **Next**. The **Installer Result** page displays.



Installation Result

6. Wait until all tasks displayed are complete. Upon successful completion, the browser automatically navigates to the Cisco IQ VA login page. The installation completion can take up to two (2) hours.



Login

Once successfully logged in, the system is ready to discover devices and supports the Assets application without AI support.

Modules and Rules Installation

To expand your system's capabilities, you can download additional modules and rules directly from the Cisco IQ SaaS portal and complete the installation in VA. See Installing Packages in [Operations Guide](#) for more details.



Note: The Assets module is pre-installed in VA installer, and available for immediate use. You can upgrade the asset module or asset rule version like any other module and rules as needed.

AI-Powered Features

Cisco IQ offers a flexible deployment model that includes an add-on AI-powered feature to enhance customer insights and automation capabilities. Cisco IQ VA can be installed with or without GPU support.

Virtual Appliance Deployment Without GPU Support (Non-AI Features)

1. Log into [Cisco IQ](#).
2. Navigate to **System Settings** > **Package Catalog** to download Cisco IQ VA Installer and desired Cisco IQ modules Installer. See Installing Packages in [Operations Guide](#) for more details.
3. Allocate IP and VM resources and deploy the VM. Minimum of one (1) VM is required for CPU workload.
4. Install the Cisco IQ VA Installer to prepare the system. See [Installing Virtual Appliance Setup](#) for more details.
5. Once installed, log in to the Cisco IQ VA UI.
6. Install the downloaded modules by navigating to **System Settings** > **Package Management** in VA. See Installing Packages in the [Operations Guide](#) for more details.

The system is now ready to use without AI support.

Virtual Appliance Deployment With GPU Support (AI-Enabled Features)

To enable AI-powered features, the system must be configured as "AI Ready."

Prerequisites

- Ensure the primary node is fully configured and operational.
- Review GPU hardware requirements and select a supplemental node with GPU capabilities. See [AI Feature Resource Requirements](#) for more information.
- Follow the multi-node deployment procedure, designating the supplemental node as the GPU node. See [Adding Supplementary Node](#) and [Multi-Node Support](#) for more information.

Deployment With GPU Support (AI-Enabled Features)

1. Log into [Cisco IQ](#).
2. Navigate to **System Settings > Package Catalog** to download Cisco IQ VA Installer, desired Cisco IQ modules and Cisco IQ AI Inference Infrastructure. See Installing Packages and AI-Powered features in [Operations Guide](#) for more details.
3. Allocate IPs and VM resources and deploy the VMs. A minimum two (2) VMs are required: one (1) for CPU workload and one (1) for GPU workload.
4. Install the Cisco IQ VA Installer to prepare the system. See [Installing Virtual Appliance Setup](#) for more details.
5. Once installed, log in to the Cisco IQ VA UI.
6. Install the AI Inference Infrastructure by navigating to **System Settings > Package Management**. See AI-Powered Features in [Operations Guide](#) for more details.
7. Install any additional downloaded modules by navigating to **System Settings > Package Management**. See Adding Modules in [Operations Guide](#) for more details.

The system is now ready to use with AI-powered features.

To learn more about enabling AI-powered features, see the [Operations Guide](#).

Multi-Node Support

The multi-node architecture allows you to expand a standalone VA into a cluster, providing increased resource capacity for processing and application deployment. This configuration enables the addition of supplementary nodes to a primary management node, allowing the system to scale based on your specific workload requirements.

Enabling the multi-node capability is essential to add a GPU node. This integration allows the On-Prem environment to leverage GPU resources for AI inferencing. This section provides detailed guidance on connecting the GPU as a supplemental node for the On-Prem, which is necessary for users to utilize GPU capabilities effectively.

Network Requirements

VA supports a single network interface. See [Network Requirements](#) for complete details.

Port Requirements

The following table outlines the network ports required for Cisco IQ VA communication in a multi-node environment.

Table 4: Multi-Node Port Requirements

Port(s)	Protocol	Description	Node Type
22	TCP	Used for Administrator CLI and Cisco Support debugging sessions	Management and supplementary nodes
443	TCP	Used for communication between Cisco IQ On-Prem and web browsers, as well as endpoint targets	Management and supplementary nodes
53, 123, 161	UDP	Used to send and receive DNS, NTP, and SNMP traffic	Management and supplementary nodes
10250, 10256	TCP	Used for Kubernetes communication between the node	Management and supplementary nodes
179	TCP	Used for VXLAN control plane (BGP) between nodes	Management and supplementary nodes
4789	UDP	Used for VXLAN traffic between nodes	Management and supplementary nodes
500, 4500	UDP	Used for IPSec IKE traffic between nodes	Management and supplementary nodes
All	ESP (50)	Used for IPSec ESP traffic between node	Management and supplementary nodes
6443	TCP	Used for Kubernetes API server	Management node only

 **Note:** Multi-node clustering is supported only for standard VA deployments.

 **Note:** A supplementary node must be the exact same version as the primary management node during the initial join process.

 **Note:** The current multi-node implementation does not provide High Availability (HA) for the management plane. If the primary management node becomes unavailable, cluster operations will be impacted.

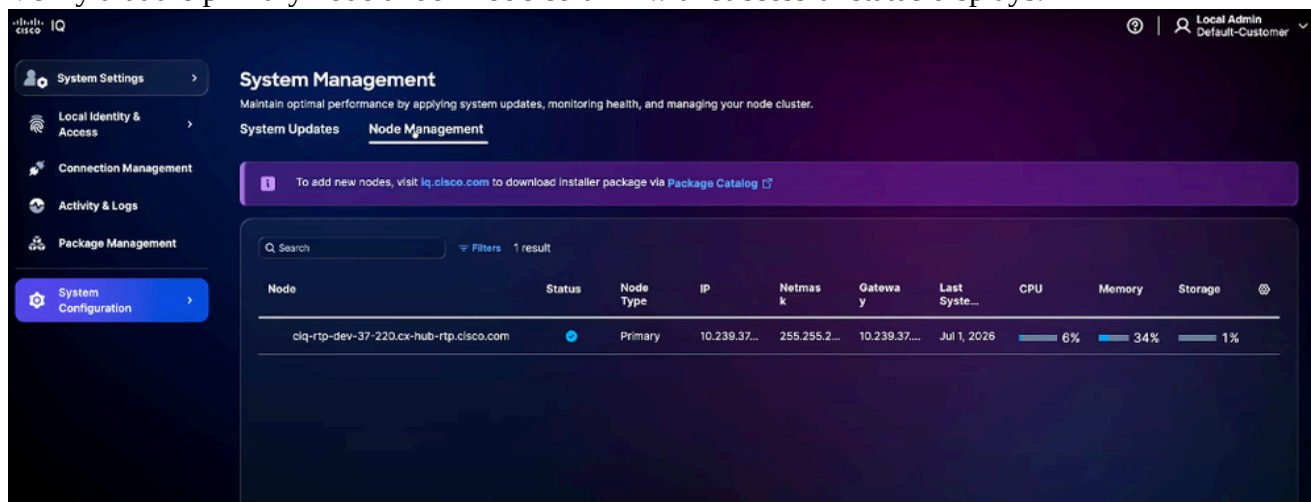
Adding a Supplemental Node

Adding a supplementary node requires the same process as installing the VA. Once you have downloaded the VA installer from the Package Catalog in Cisco IQ (SaaS), install it on the chosen hypervisor. See

[Installing Virtual Appliance Setup](#) for more details.

Before adding a supplementary node, ensure the first node is fully configured as a standard VA. To add a supplementary node:

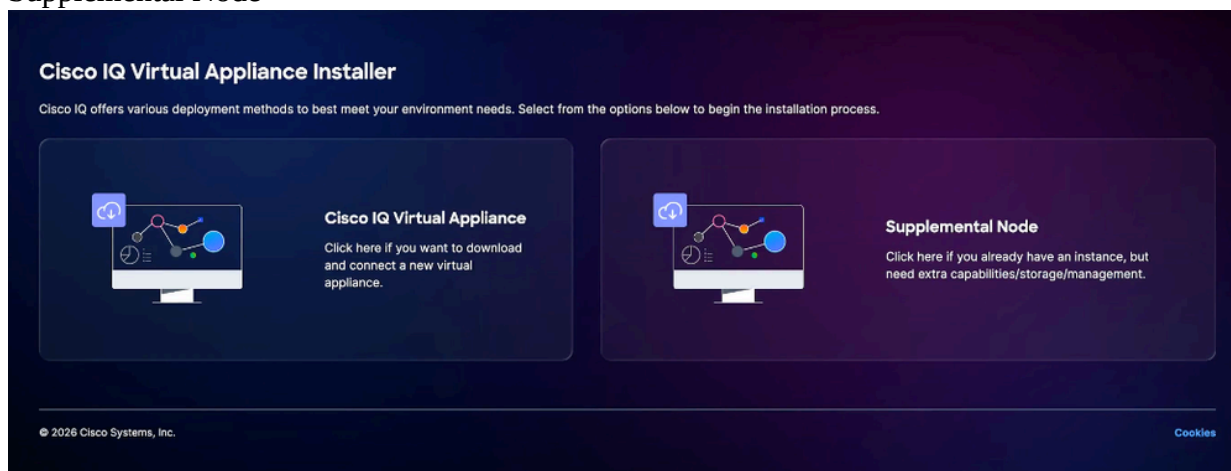
1. Navigate to **System Configuration > Node Management**.
2. Verify that the primary node under **Node** column with successful status displays.



Node Management

3. Navigate to Virtual Appliance Installer. The following options display:

- Cisco IQ Virtual Appliance
- Supplemental Node



Supplemental Node

4. Click **Supplemental Node** option. The **Supplemental Node Installer** page displays.

Supplemental Node Installer

Connect to node

Select an action and provide your credentials to establish connection to your cluster.

Primary node FQDN

Local admin username

Password

 [Show](#)

Node type

GPU ▼

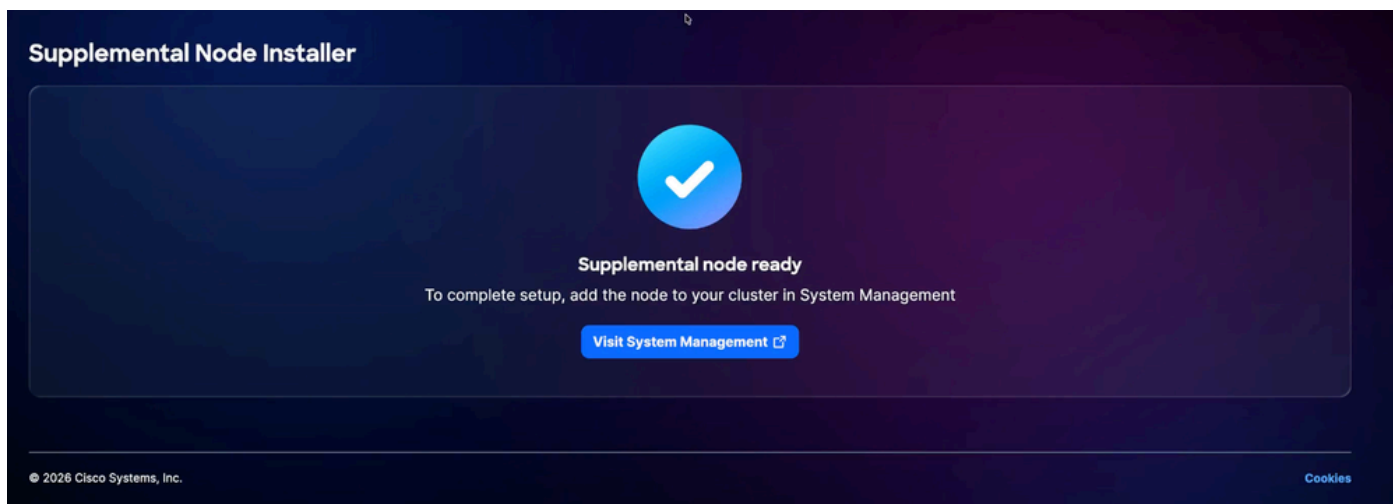
[Add node](#) [Cancel](#)

Supplemental Node Page

5. Enter **Primary node FQDN**.
6. Enter **Local admin username**.
7. Enter **Password**.
8. Choose **Node type** from the drop-down list.

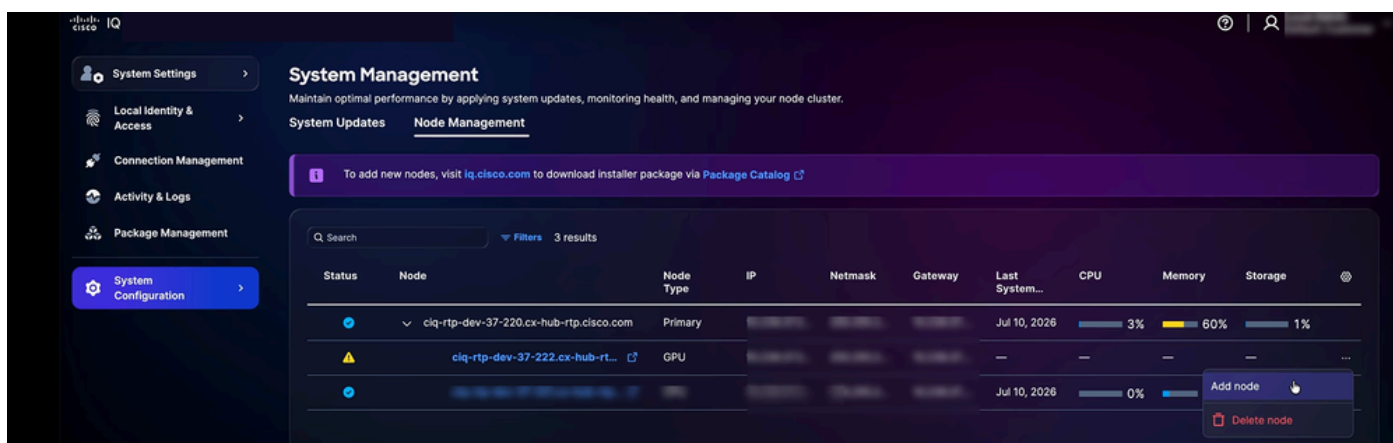
 **Note:** You can choose GPU worker node. When choosing GPU worker nodes, ensure your hypervisor environment (for example, VMware or Hyper-V) is configured with the necessary hardware to support GPU devices, as these are required for GPU node accessibility. See [Deployment Options](#) to learn more.

9. Click **Add node**. The "Supplemental node ready" message displays after successful node addition.



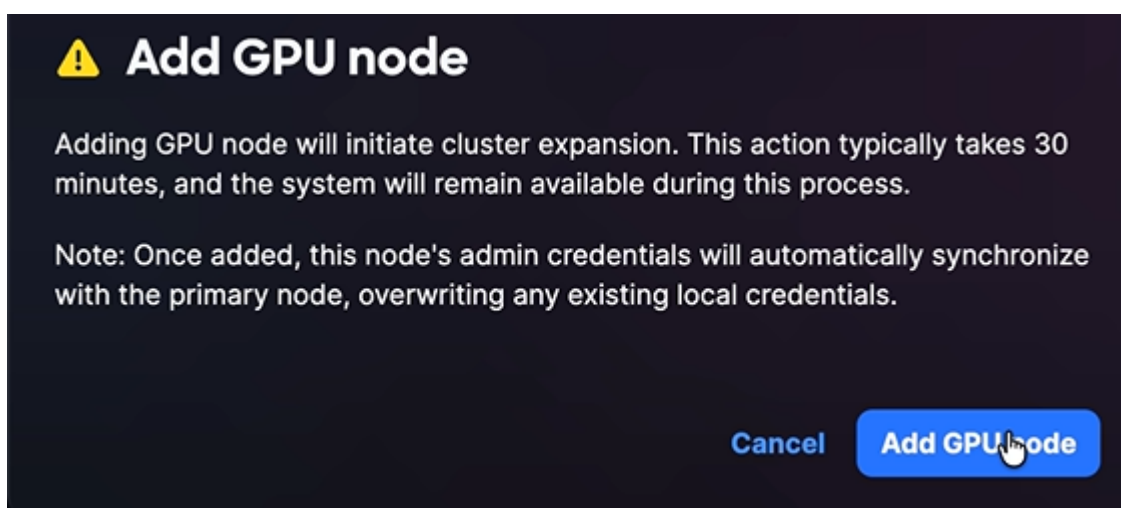
Supplemental Node Ready

10. Once “Supplemental node ready” displays, click the **Visit System Management** link or navigate to **System Management > Node Management** to trigger the add node action to complete the integration.



Add Node

11. Click **More menu icon > Add Node**. The **Add GPU Node** window displays.



12. Click **Add GPU Node**. Once the node is successfully added, it displays in cluster.

Cluster Synchronization and Management

Upon adding a worker node, the administrative credentials of the primary management node automatically synchronize with the worker node. The access to the worker node must be performed using these synchronized credentials.

 **Note:** The cluster dynamically manages application distribution. When an application requires advanced processing capabilities, the system checks for the availability of GPU-enabled nodes. If a GPU worker is present and the appropriate application package is installed, the system enables these advanced features. If the cluster lacks the necessary hardware resources, the system will operate in a non-accelerated mode to maintain stability.

Support

You can create VA and module-specific support cases from Cisco IQ SaaS. The Support module is available in Cisco IQ SaaS and offers a consolidated view of your support cases. It enables you to filter, sort, and customize the case list view, providing visibility into both open and closed cases you are entitled to access. For more detailed information about the Support module in Cisco IQ SaaS, see the [Cisco IQ SaaS Getting Started Guide](#).

 **Note:** Cisco IQ VA customers can access most Cisco IQ SaaS Support module features, including opening Technical Assistance Center (TAC) cases related to Cisco IQ VA and its modules, as well as creating and managing product cases.

Creating a Support Case

You can create VA and module-specific cases in Cisco IQ SaaS. To create a case:

1. Log in to [Cisco IQ \(SaaS\)](#).
2. Click the **Help** icon > **Report an Issue**. The **Report an Issue** window opens.

Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel

Submit

Report an Issue

3. Provide the required details.
4. Click **Submit**.

Appendix A

Reference BOM for On Prem Virtual Appliance with GPU

Following is the Reference Bill of Materials (BOM) for On-Prem VA supporting up to 10K devices:

Table 5: Reference BOM

Part Number	Description	Quantity
UCS-M8-MLB	UCS M8 RACK MLB	1

UCSC-C240-M8SX	UCS C240 M8 Rack w/o CPU, mem, drives, 2U w SFF backplane	1
CON-L1NCO-UCSCCX4S	CX LEVEL 1 8X7XNCDOS UCS C240 M8 Rack wo CPU, mem, drives, 2	1
RHEL-2S2V-D3A	Red Hat Enterprise Linux (1-2 CPU,1-2 VN); 3-Yr Support Req	1
CON-ISV1-RHEL62S2	ISV 24X7 Red Hat Enterprise Linux 1-2 CPU,1-2 VN	1
COMPUTE-AI	Compute Artificial Intelligence Use Case	1
ISM-MANAGED	Deployment mode for C Series Servers in Standalone mode	1
UCSC-GPUAD-240M8	GPU AIR DUCT FOR C240M8	1
UCSC-M-V5Q50GV2-D	Cisco VIC 15427 4x 10/25/50G mLOM C-Series w/Secure Boot	1
UCS-TPM-002D-D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant	1
UCSC-RAIL-D	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	1
CIMC-LATEST-D	IMC SW (Recommended) latest release for C-Series Servers	1
UCSC-HSLP-C220M8	Heatsink for C220M8, C240M8L and C240M8 w/GPU	2
UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	24
UCSC-BBLKD-M7	UCS C-Series M7 SFF drive blanking panel	20

CBL-RAID16-240M8	C240M8 Y cable MB to RAID16/HBA	1
CBL-NVME-240M8-P4	C240M8SFF NVMe cable for drive 1-4 (P4)	1
CBL-NVME-240M8-P2	C240M8SFF NVMe cable for drive 21-24 (P2)	1
UCSC-SDBKT-24XM7	UCS C-Series M7 2U SD RAID Controller Bracket	1
CBL-G5GPU-C240M7	C240M7 PCIe CEM compliant 12VHPWR power cable (up to 450W)	1
UCS-MRX64G2RE5	64GB DDR5-6400 RDIMM 2Rx4 (16Gb)	4
UCSC-RIS1A-240M8	UCS C240 M8 Riser 1A PCIe Gen5 (x8, x16, x8)	1
UCSC-RIS2A-240M8	UCS C240 M8 Riser 2A PCIe Gen5 (x8, x16, x8) (CPU2)	1
UCSC-RIS3C-240M8	UCS C240 M8 Riser 3C PCIe Gen5 (x16)(CPU2)	1
UCSC-RAID-MP1L32	24G Tri-Mode MP1 RAID Controller w/4GB FBWC 32Drv w/2U Brkt	1
UCSC-GPU-RTXP6000	NVIDIA RTX Pro 6000: 600W, 96GB, 2-Slot FHFL GPU	1
NV-GRID-OPT-OUT	NVIDIA GRID SW OPT-OUT	1
UCS-M2-HWRAID2	Cisco Boot optimized M.2 Raid controller for SATA drives	1
UCS-M2-480G-D	480GB M.2 SATA SSD	2

UCSC-M2I-240M8	UCS C240 M8 Internal M.2 module	1
UCS-SDB1T9SA1VD	1.9TB 2.5in 6G SATA 1X Samsung G1PM893A SSD	4
UCS-CPU-I6520P	Intel I6520P 2.4GHz/210W 24C/144MB DDR5 6400MT/s	2
UCSC-PSU1-2300W-D	Cisco UCS 2300W AC Power Supply for Rack Servers Titanium	2
CAB-C19-CBN	Cabinet Jumper Power Cord, 250 VAC 16A, C20-C19 Connectors	2
UCSC-RISAB-24XM7	UCS C-Series M7 2U Air Blocker GPU only	2
DC-MGT-SAAS	Cisco Intersight SaaS	1
DC-MGT-ISSAAS-ES	Infrastructure Services SaaS/CVA - Essentials	1
SVS-DCM-SUPT-BAS	Cisco Support Basic for DCM	1
DC-MGT-UCSC1S	UCS Central Per Server - 1 Server License	1
DC-MGT-ADOPT-BAS	Intersight - Virtual adopt session http://cs.co/requestCSS	1