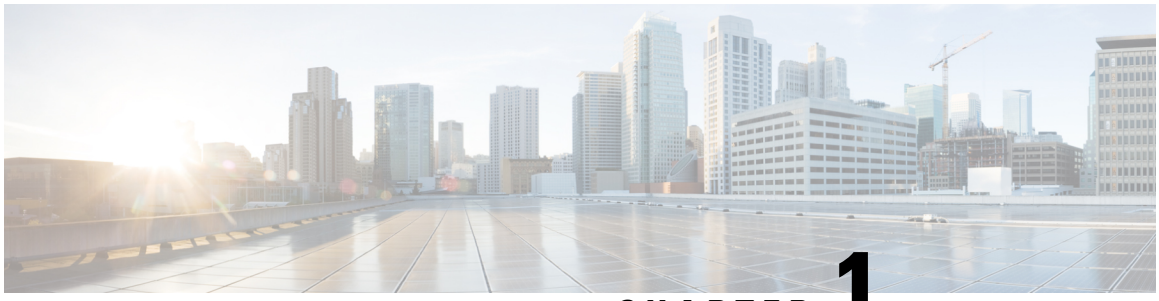
Cisco Intersight Assist Getting Started Guide

First Published: 2020-03-20

Last Modified: 2021-05-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview of Cisco Intersight Assist

Intersight Assist

Cisco Intersight Assist helps you add endpoint devices to Cisco Intersight. A datacenter could have multiple devices that do not connect directly with Cisco Intersight. Any device that is supported by Cisco Intersight but does not connect directly with it, will need a connection mechanism. Cisco Intersight Assist provides that connection mechanism, and helps you add devices into Cisco Intersight.

Cisco Intersight Assist is available within the Cisco Intersight Virtual Appliance, which is distributed as a deployable virtual machine contained within an Open Virtual Appliance (OVA) file format. You can install the appliance on an ESXi server. For more information, see the Cisco Intersight Virtual Appliance Getting Started Guide.

After claiming Intersight Assist into Intersight, you can claim endpoint devices using the **Claim Through Intersight Assist** option. For more information, see Getting Started.

Note Cisco Intersight Assist currently does not support IPv6 configurations.

Currently, you can add Pure Storage devices, Hitachi Virtual Storage Platform devices, and VMware vCenter devices into Intersight after claiming them using Cisco Intersight Assist.

System Requirements

VM Configuration Requirements

You can deploy Cisco Intersight Assist on VMware ESXi 6.5 and higher. This section describes the system requirements to install and deploy Cisco Intersight Assist. You can deploy Intersight Assist in the Tiny, Small, and Medium options.

Note

- Tiny deployment type applicable only for Intersight Orchestrator.
- The Tiny (8 vCPU, 16 GiB RAM) deployment option is applicable only for Intersight Assist deployment without Workload Optimizer or IST capabilities. Small deployment is the minimum requirement for Workload Optimizer and IST.

Table 1: Intersight Assist Resource Requirements

Resource Requirement	System Requirements		
	Tiny	**Small**	**Medium**
vCPU	8	16	24
RAM (GiB)	16	32	64
Number of servers		2000	5000
Supported Hypervisors	VMware ESXi 6.5 and higher VMware vSphere Web Client 6.5 and higher		

This following table lists the system requirements to deploy Cisco Intersight Assist for Intersight Workload Optimizer

Table 2: Intersight Assist Resource Requirements for Workload Optimizer

Resource Requirement	System Requirements	
	Small	**Medium**
vCPU	16	24
RAM (GiB)	32	64
Storage (Disk in GiB)	500	500
Deploy Configuration	Up to 1000 Virtual Machines	Up to 30,000 Virtual Machines
Supported Hypervisors	VMware ESXi 6.5 and higher	

**To deploy up to 100,000 Virtual Machines, increase the vCPU to 32 and RAM to 96 GB or more.

Table 3: Intersight Assist Resource Requirements for Intersight Service for HashiCorp Terraform Service (IST)

Resource Requirement	System Requirements	
	Small	**Medium**
vCPU	16	24
RAM (GiB)	32	64

Resource Requirement	System Requirements	
Number of Terraform Agents	5	5
Supported Hypervisors	VMware ESXi 6.5 and higher	

Port Requirements

The following table lists the port numbers that must be open for Cisco Intersight Assist communication.

Port	Protocol	Description
443	TCP/UDP	Required for communication between: • Intersight Assist and the user's Web browser. • Intersight Assist to and from the endpoint devices.
80	TCP	This port is optional for normal operation, but is required for initial monitoring of the Intersight Assist setup and when using the one-time device connector upgrade. This port is not used if the device connector is at the minimum supported version.

Supported Browsers

Cisco Intersight Assist and Cisco Intersight runs on the following minimum supported browser versions:

- Google Chrome 62.0.3202.94
- Firefox 57.0.1
- Safari 10.1.1
- Microsoft Edge (Chromium) Beta

Technical Assistance

Technical support offered by Cisco Technical Assistance Center (TAC) is included in your Essentials license. If you face any issue with the installation, set up, or operations of Cisco Intersight Assist, open a case with Cisco TAC for assistance.

The Cisco Technical Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies:

http://www.cisco.com/techsupport

Using the TAC Support Case Manager online tool is the fastest way to open S3 and S4 support cases. (S3 and S4 support cases consist of minimal network impairment issues and product information requests.) After you describe your situation, the TAC Support Case Manager automatically provides recommended solutions. If your issue is not resolved by using the recommended resources, TAC Support Case Manager assigns your support case to a Cisco TAC engineer. You can access the TAC Support Case Manager from this location:

https://mycase.cloudapps.cisco.com/case

For S1 or S2 support cases or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 support cases consist of production network issues, such as a severe degradation or outage.) S1 and S2 support cases have Cisco TAC engineers assigned immediately to ensure your business operations continue to run smoothly.

To open a support case by telephone, use one of the following numbers:

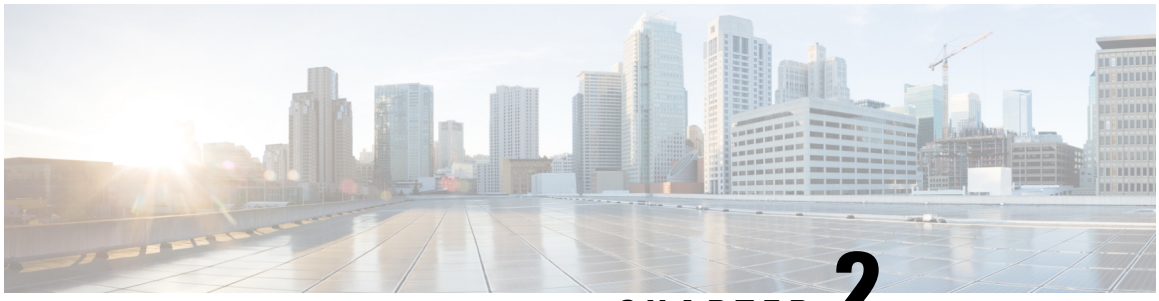
- Asia-Pacific: +61 2 8446 7411
- Australia: 1 800 805 227
- EMEA: +32 2 704 5555
- USA: 1 800 553 2447

For a complete list of Cisco TAC contacts for Enterprise and Service Provider products, see:

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

For a complete list of Cisco Small Business Support Center (SBSC) contacts, see:

http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html



CHAPTER 2

Installing Cisco Intersight Assist

Installing Cisco Intersight Assist Using VMware vSphere Web Client

Cisco Intersight Assist is available within the Cisco Intersight Virtual Appliance, which is distributed as a deployable virtual machine contained within an Open Virtual Appliance (OVA) file format. You can install the appliance on an ESXi server.

Before you begin

- Ensure that you have downloaded the Cisco Intersight Virtual Appliance package from the URL provided by your Cisco representative or a location accessible from your setup, such as a local hard drive, a network share, or a CD/DVD drive.
- Configure DNS with A/PTR and CNAME Alias records.

  Sample A/PTR record: intersightassist (ip.address)

  Sample CNAME Alias record: dc-FQDN hostname

Procedure

Step 1 Log in to VMware vSphere Web Client with administrator credentials.

Step 2 Right-click on the host, and select **Deploy OVF Template**.

Step 3 On the **Deploy OVF Template** wizard, in the **Source** page, specify the source location, and click **Next**.

You can specify a URL or browse to location accessible from your local hard drive, a network share, or a DVD/CD drive.

Step 4 On the **OVF Template Details** page, verify the OVF template details and click **Next**. No input is necessary.

Step 5 On the **Name and Location** page, add or edit the Name and Location for the Intersight Assist and click **Next**.

Step 6 On the **Deployment Configuration** page, select a configuration from the drop-down list and click **Next**.

You can choose either Tiny, Small or Medium.

Step 7 On the **Storage** page, select a destination storage (hard drives) for the VM files in the selected host (ESX station) and click **Next**. Select the Disk Format for the virtual machine virtual disks. Select **Thin Provision** to optimize disk usage.

Step 8 On the **Network Mapping** page, for each network that is specified in the OVF template, select a source network and map it to a destination network and click **Next**.

Step 9 On the **Properties** page, customize the deployment properties of the OVF template, and click **Next**.

OVF Property	Description
Enable DHCP	Enables the appliance to obtain IP addresses from the DHCP server running on the same network to avoid using static IP addresses. If you select this option, all static parameters will be ignored. For more information about DHCP, see the **Enabling DHCP** section.
IP Address*(Values you input will be ignored if you Enable DHCP)*	Enter the IPv4 address of the node. For example: 10.0.0.100
Net Mask*(Values you input will be ignored if you Enable DHCP)*	This field is pre-populated with the IPv4 Net Mask 255.255.255.0
Default Gateway*(Values you input will be ignored if you Enable DHCP)*	Enter the IPv4 Default Gateway. For example: 10.0.1.254
DNS Domain*(Values you input will be ignored if you Enable DHCP)*	Enter the DNS Search Domain
DNS Servers*(Values you input will be ignored if you Enable DHCP)*	Enter a comma-separated list of IPv4 addresses for your DNS servers
Administrator Password	Enter the admin password. This is the same password that you use to log in to the appliance. This password is also used to log in to the Appliance Maintenance Shell as the Diagnostic User with username **diag**. **Set Password**—Before you register the appliance with Intersight, you must create an admin password. The password can contain 0-9, A-Z, a-z, and all special characters except a colon (:) and space.
NTP Servers	Enter a comma-separated list of hostnames or IPv4 addresses for your NTP servers. You can add up to 3 NTP servers. This setting is still required even if you use DHCP to obtain IP addresses. **Note** vCenter and Cisco Intersight Assist appliance should be in sync with a NTP server.

Attention If the password you set at the time of registering your appliance is weak, Intersight prompts you to change your password to a stronger one. After a successful reset to a strong password, you are directly logged into the appliance.

Enabling DHCP

Dynamic Host Configuration Protocol (DHCP) allows the Cisco Intersight Virtual Appliance VM to obtain an IP address through a DHCP server running on the network that it is installed on. When this option is enabled, the Cisco Intersight Virtual Appliance VM is equipped to handle IP address updates through DHCP, subject to lease requirements.

Attention Ensure that the following requirements for using DHCP are met:

- If you use DHCP, ensure that the IP address returned to the appliance VM resolves to the **same FQDN** you use to set up the appliance. Cisco recommends that you configure your DHCP to return the same IP address for the appliance VM, and not change your IP address frequently.
- The appliance only reads the IP address, netmask, gateway, and DNS-Servers from the DHCP lease information. NTP information, if any, must be input into the OVF parameters at the time of the deployment.
- All IP addresses used in the appliance VM must be in the same subnet as that of the initial IP addresses assigned. For example, the VM cannot be assigned an IP from a different subnet, by connecting to a vSwitch which has a different DHCP server.

Limitations

- A forced lease renewal could impact the VM configuration settings and could render the appliance unusable.

Step 10 On the **Ready to Complete** page, select **Power On After Deployment** and click **Finish**.

What to do next

After the OVA deployment is complete, and the VM is powered on, wait for a few seconds and then access your VM using the <https://fqdn-of-your-appliance> URL to complete setting up Cisco Intersight Assist. For more information, see Initial Setup Wizard , on page 7.

Initial Setup Wizard

After the OVA deployment is complete, and the VM is powered on, complete the following steps to complete setting up Cisco Intersight Assist:

1. Access your VM using the <https://fqdn-of-your-appliance> URL and choose **Cisco Intersight Assist** and click **Proceed**.
2. In the Initial Setup Wizard, connect Intersight Assist with Cisco Intersight.
   - Enable Proxy from the **Settings** page. This is optional.

     Provide the proxy hostname/IP and the port number, and click **Save**. At this point, you can view the Device ID and Claim Code on the screen.
   - Copy the Device ID and the Claim Code that is displayed.

3. Login to Cisco Intersight, and choose **Devices** > **Claim a New Device** > **Direct Claim.**
4. Enter the Device ID and Claim code that you copied in this screen and click **Claim**. For information on claiming a device in Cisco Intersight, see Cisco Intersight Setup and Device Claim.
5. Return to the Initial Setup Wizard, and click **Continue**.

   The software download is initiated and the software packages are installed. The installation process could take upto an hour to complete, depending on the network connection to Cisco Intersight. After the installation is complete, the Cisco Intersight Assist user interface appears.

Logging in to Cisco Intersight Assist

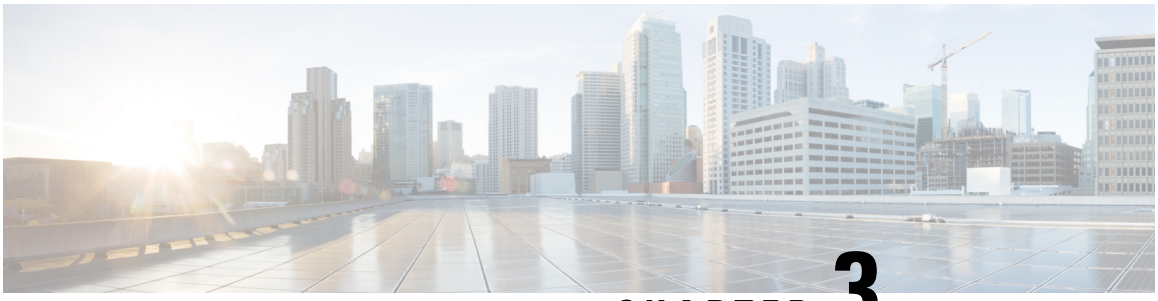
To log in to Cisco Intersight Assist user interface, enter the user name - admin@local and the password you set at installation. However, if the password you set at the time of registering is weak, you are prompted to modify the password to a stronger one. The new password must be between 8 to 127 characters and must contain atleast one uppercase letter, one lowercase letter, and one number. Click **Save and Continue**. After a successful reset to a strong password, you are logged into the Cisco Intersight Assist.

After logging in to Cisco Intersight Assist, you can view the following tabs on the left pane:

- **Cloud Connection**—Displays information on the Device connector such as the Device ID, and the connection status to Cisco Intersight. When the status shows as Claimed, you can claim Pure Storage devices and VMware vCenter devices in Cisco Intersight by using the **Claim Through Intersight Assist** option. For more information, see the Help Center.

  You can use the **Settings** option to perform additional tasks such as import certificates, enable or disable proxy configuration
- **Assist View**—Displays information on the system that is running Intersight Assist.
- **Software View**—Displays information on the software version. You can also create a software upgrade schedule from this page.
- **Audit Logs**—Displays a log of activities that have occurred on the system.
- **Sessions**—Displays a list of user sessions running in the system.

You can view detailed information about these options at the Help Center.



CHAPTER 3

Diagnostics and Troubleshooting

Intersight Appliance Maintenance Shell

Intersight Appliance Maintenance Shell

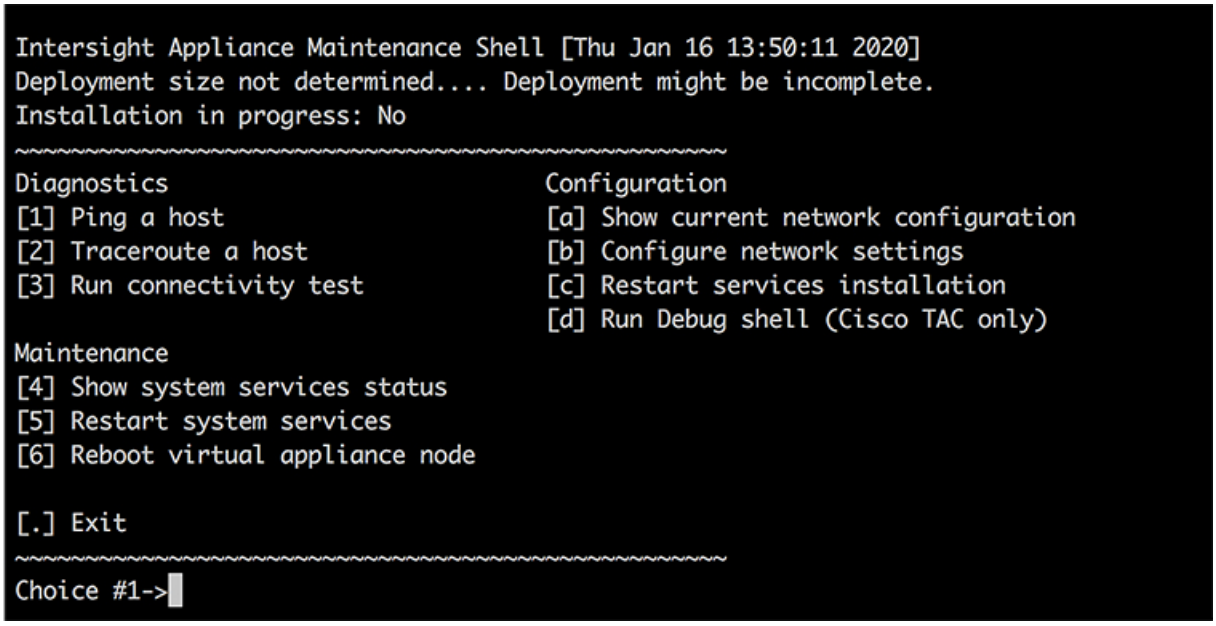
Cisco Intersight Virtual Appliance provides a diagnostic utility to monitor the installation and provide remediation steps to install the appliance successfully. This console-based utility helps in troubleshooting and addressing misconfiguration or networking issues during the appliance installation. The Maintenance Shell aims to:

- Detect and display issues with the installation prerequisites.
- Enable editing the inputs that are provided during the initial appliance deployment.
- Assist with continuing the installation after you fix the settings or change inputs during the appliance deployment.

Check the status of your installation by visiting <*http://fqdn-of-your-appliance*> after the VM is powered ON. If you notice that your VM does not respond after about 15 minutes since power-on, use the Intersight Appliance Maintenance Shell to troubleshoot networking or misconfiguration issues. When the login prompt appears, the diagnostic account is ready. Use the following instructions to troubleshoot:

1. From either vCenter or Hyper-V Manager, navigate to your virtual machine and open a console window.
2. To open the Appliance Maintenance Shell, log in as *admin User* with username **admin** and enter the administrator password that you used during the appliance deployment.

Figure 1: Intersight Appliance Maintenance Shell

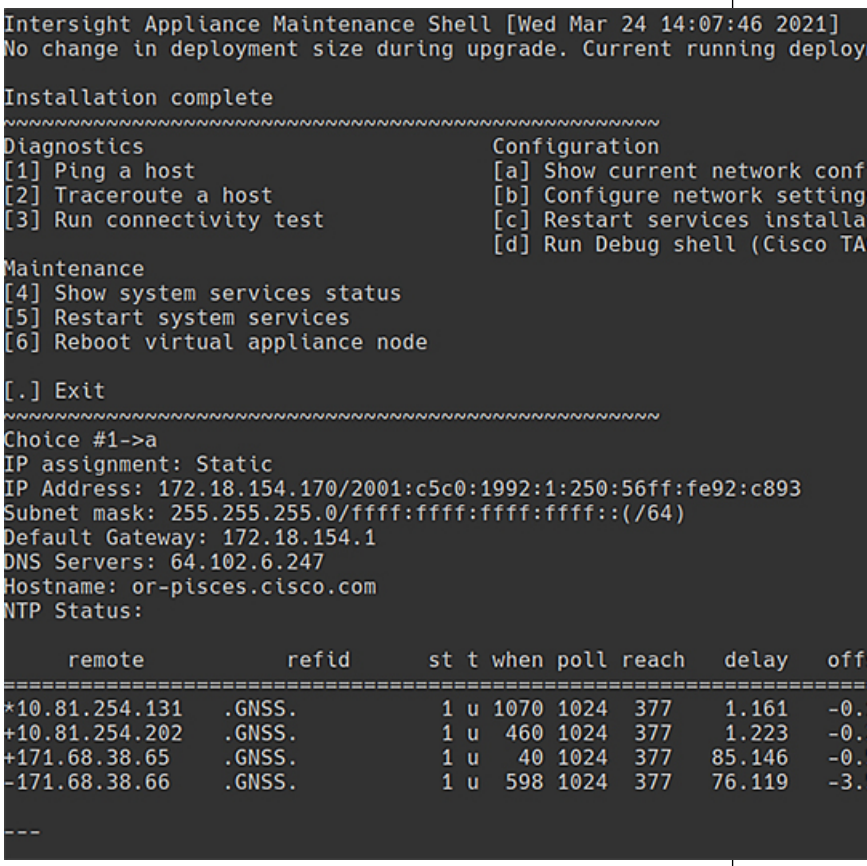


3. Select one of the options listed in the following table to learn more about the command and the outcome of the command:

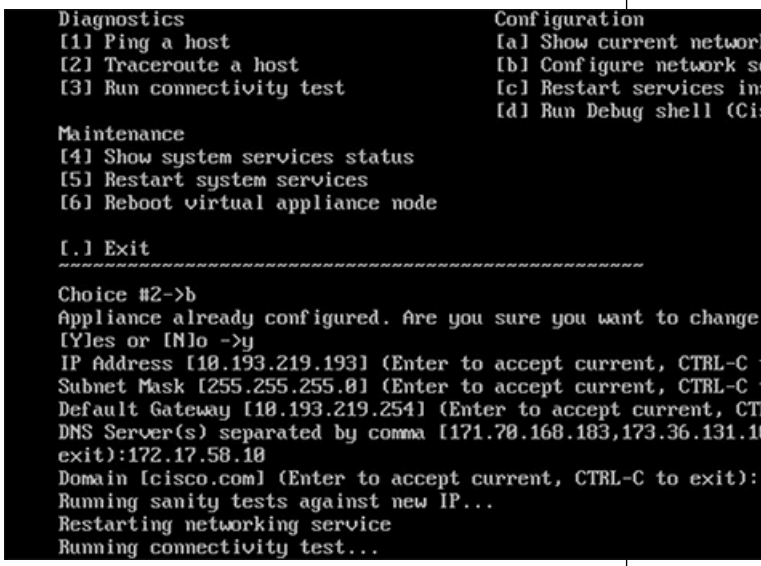
Intersight Appliance Maintenance Shell Options	Description
Diagnostic Options	• **[1] Ping a Host**—This option lets you ping a host to check why the installation is unsuccessful even after all properties and requirements are entered correctly. • **[2] Traceroute a host**—This option displays all IP addresses that the host has traversed through. • **[3] Run connectivity test**—This option runs a connectivity test and pings every host in the path from your host to the DNS server. The tool runs a few tests to verify if the IP address is valid, and checks for duplicate IPs to determine if it is used in multiple instances. The Run connectivity test option reaches the DNS server to resolve any connectivity issues.

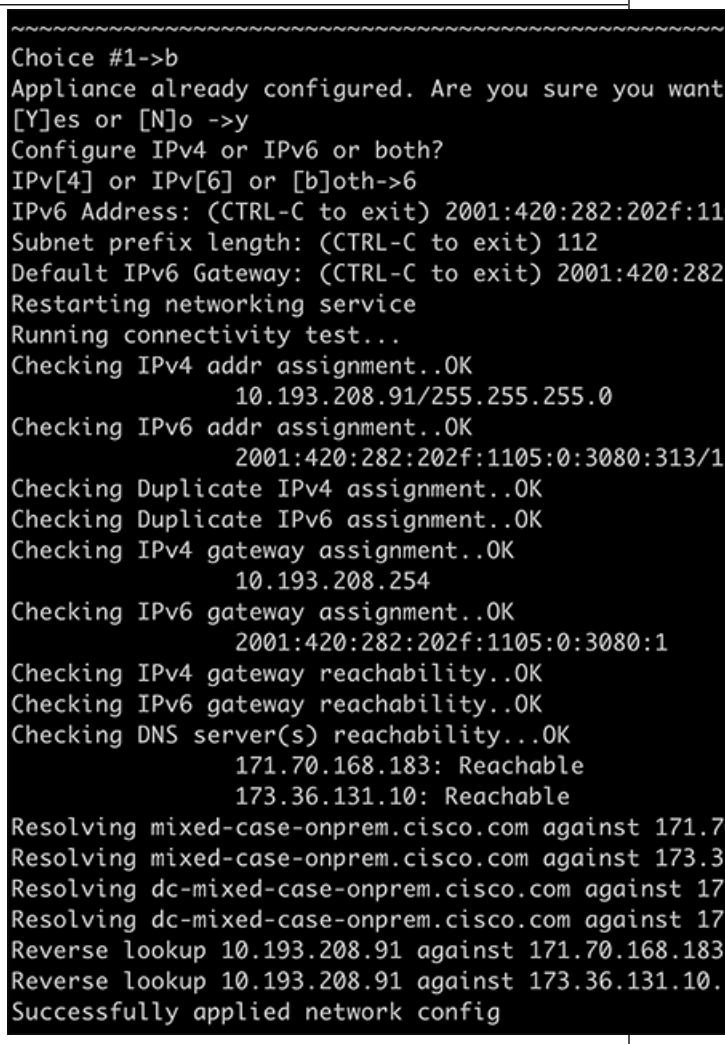
Intersight Appliance Maintenance Shell Options	Description
Configuration Options	

Intersight Appliance Maintenance Shell Options	Description

	• **[a] Show current network configuration**—This option displays the existing configuration settings such as IP address, subnet mask, Default Gateway, DNS servers, Hostname, and NTP connection status to help you verify that all configuration settings are entered correctly. You can run the connectivity test (**Option 3**) to determine the status of the connectivity.
	 
	• **[b] Set network interface properties**—This option displays the network interface properties that you have set. You can click **enter** to retain the existing properties or provide a different set of inputs. This option detects issues (if any) with the following properties:
	  • **An invalid or duplicate IP address**—The IP address could be incorrect even if you have configured your hostname with the correct credentials.
	  • **Invalid subnet mask**—An invalid subnet mask might allow you to navigate inside your own network, but could impact external traffic.
	  • **Incorrect or invalid Default Gateway**—If the DNS server is outside your network, an invalid default gateway impacts the connectivity to external hosts.

Intersight Appliance Maintenance Shell Options	Description
	Changing IP Address—Using this option, an **admin** user (with username **admin**) can make the following changes:

Intersight Appliance Maintenance Shell Options	Description
	• Assign a new IP address on the same network, connect the appliance VM to a different network and assign an IP on that network. • Change the IP address of an appliance VM after migrating it to a different vCenter or Hyper-V Manager deployment. **Attention** You must ensure that the DNS server records (A, CNAME, and PTR) are updated before the change is initiated and the new IP address resolves to the same FQDN as before. You can choose to change either just the IPv4 address or the IPv6 address, or change both at the same time. You can configure IPv6 addresses only after the appliance is completely installed. You will not experience any downtime with the services in your appliance after changing IPv6 addresses. Note that the appliance VM itself continues to be managed with the DNS name assigned to the IPv4 address of the appliance when it was first deployed. When you configure IPv6 addresses, it enables only the target claim of IPv6 endpoints. The IP change can take up to 15 minutes. Cisco recommends that you do not reboot the appliance VM during this time. After waiting for about 15 minutes, log back into the appliance from the UI. 

Intersight Appliance Maintenance Shell Options	Description
	 • **[c] Restart installation services** This option is useful when you fix the configuration on your network that was previously assumed to be working. A few examples are: • Missing PTR record for the IP you have chosen (static IP assignment). • VM connected to incorrect portgroup/vSwitch. • DHCP server not running when you chose an IP assignment via DHCP. • You can check the progress of the installation by visiting the url *<fqdn-of-your-appliance-vm>*.

Intersight Appliance Maintenance Shell Options	Description
	• **[d] Run Debug (requires authentication)—This utility is intended only for Cisco TAC to troubleshoot installation issues.**
Maintenance Options	This option enables you to gracefully reboot the appliance VM and restart the appliance services. **Options in this sub-menu are intended for debugging and recovery, and must be used as instructed by Cisco TAC**. You can access this option as a **admin** user. **[4] Show system service status**—This option provides a summary of the running/pending services and reports any errors. This option enables you to monitor the status of the appliance if the system is unresponsive or if there is a service disruption at any time. **[5] Restart system services**—This option enables you to troubleshoot the appliance and restarts the services running on it. **[6] Reboot virtual appliance node**—This option stops services, reboots the appliance, and restores the services when the appliance reboots.

For a demonstration of the Intersight Virtual Appliance Installation and troubleshooting, watch Cisco Intersight Appliance Installation and Debug.

Monitoring Virtual Appliance Sizing Options

The Intersight Appliance Maintenance Shell displays the status updates about the deployment size determination and the subsequent action. You can monitor the status of the deployment in the console and take remedial actions as required. The messages listed in the table below explain the scenario and the particular resource requirements for deployment.

Initial Message	Final Message
Installing <*size*>deployment size. This message is displayed when the required resources are adequate, and the desired size is being deployed. **Note** After evaluating the resources requirement, you can choose to deploy in the Small or Medium options.	**Installed <*size*>deployment size.**
Installing <*size* >deployment size, after being under resourced. This message is displayed when the existing deployment is under-resourced for the current deployment size, and upon restarting the VM after the necessary resources have been added. This deployment could be in either size.	**Installed <*size*> deployment size, after being under resourced.**

Initial Message	Final Message
Installed <*size*> deployment size. This message is displayed when the existing resources and the required resources are similar and no upgrade is required.	**No change in deployment size during reboot. Current running deployment size is Small.**
Downgrading deployment size from Medium to Small. This message is deployed when a Medium deployment size is downgraded to Small.	**Downgraded deployment size from Medium to Small.**
Upgrading deployment size from Small to Medium. This message is displayed when the deployment size is upgraded from Small to Medium.	**Upgraded deployment size from Small to Medium.**