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 3.

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.