Cisco Intersight Virtual Appliance and Intersight Assist Getting Started Guide, 1.0.9

First Published: 2019-01-25

Last Modified: 2024-05-17

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

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

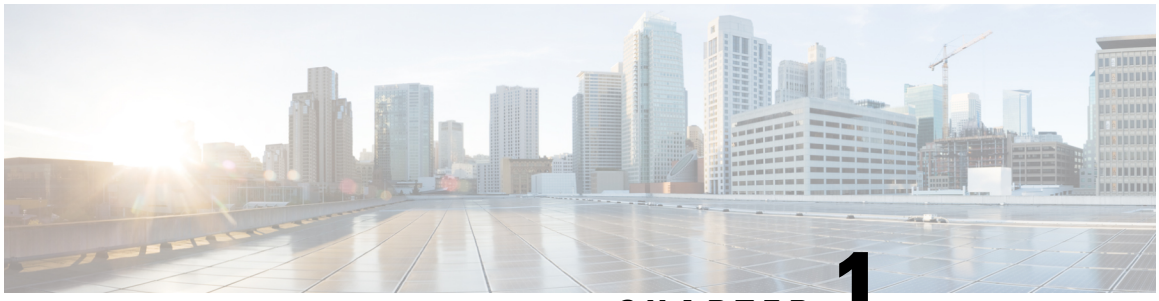
Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Communications, Services, Bias-free Language, and Additional Information



CHAPTER 1

About This Guide

Introduction

Cisco Intersight offers flexible deployment either as Software as a Service (SaaS) on Intersight.com or running on your premises as Cisco Intersight Virtual Appliance. The virtual appliance provides the benefits of Cisco Intersight while allowing more flexibility for those with additional data locality and security requirements. The Cisco Intersight connected Virtual Appliance software can be deployed on premises, allowing users to take advantage of the SaaS functionality. The Private Virtual Appliance can be deployed on premises with further security restrictions.

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.

The guide provides an overview of how to install and set up Cisco Intersight Virtual Appliance and Cisco Intersight Assist in your environment.

New and Changed Information

The following table provides an overview of the significant updates for the new features and functionality documented in this guide:

Table 1: New and Changed Features and Functionality

When Updated	Feature/Funtionality	Description	Where Documented
March 2024	Metrics Collection	Added information in the table about the supported configuration limits for the Metrics Collection feature.	Supported Configuration Limits for Intersight Virtual Appliance
	Local users	Updated task to include information on how to add local users.	Adding a User
	Reset password of local users	Added a new section that includes information about how to reset the password of local users.	Resetting the Password of Local Users
	Lockout local users account	Added a new task that describes the lockout of local users accounts feature. Updated the table in Step 4 to add the fields required for configuring the lockout of local users account feature.	Locking Out Local Users Accounts Configuring Password Policy for Local Users
December 2023	Backup Retention	Updated task to include information about the steps to follow for enabling backup retention.	Scheduling Backup
	Support for CIFS protocol	Updated task to include information pertaining to support for the CIFS protocol.	Create Backup
	Backup Retention Scenarios	Added a new table that describes the various backup retention scenarios and the expected outcomes.	Backup Retention Scenarios
	Port Requirements	Updated the topic to include port 9094 as a requirement for Intersight Virtual Appliance communication.	Port Requirements

When Updated	Feature/Funtionality	Description	Where Documented
October 2023	Resource requirements for existing appliance deployments.	New task includes information about resource requirements for existing appliance deployments as well as disk size requirements for VMware vSphere installations.	VM Resource Requirements for Existing Intersight Virtual Appliance Deployments
	Migration Path to expand existing single-node appliance deployment to multi-node cluster configuration.	New task that includes step on how to expand an existing single-node appliance deployment to a multi-node cluster configuration.	Migration Path for Existing Single-Node Deployment to Multi-Node Cluster Configuration
	Configuring External Syslog	Updated the task to include information that it is now possible to configure up to five external syslog servers.	Configuring External Syslog
	SSL Certificates	Updated task to include information about switching to a self-signed certificate.	Certificates
	Appliance Alarms	Updated information in the table for the appliance alarms.	Intersight Virtual Appliance Monitoring
	Single Sign-on	Updated the "IdP Requirements" section to include information for multi-node cluster configuration.	Single Sign-On with Intersight Virtual Appliance
July 2023	Collecting a Tech Support Bundle From Intersight Virtual Appliance	Added support for collecting tech support bundles for Intersight Connected Virtual Appliance.	Technical Assistance
	Configuring Cisco TAC Support Using a Serial Console	Added new task to configure Cisco TAC Support using a serial console.	Configuring Cisco TAC Support Using a Serial Console, on page 113
	Reserved IP Address Range Requirements	Updated information in this section	Reserved IP Address Range Requirements, on page 16

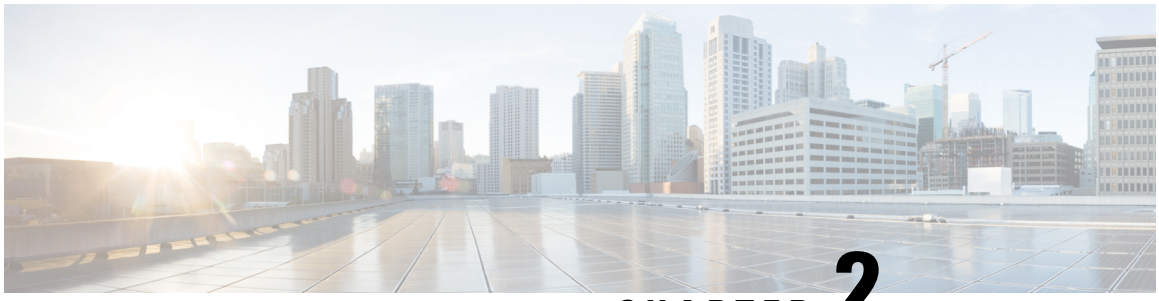
When Updated	Feature/Funtionality	Description	Where Documented
February 2023	Multi-Node Cluster Deployment **This feature is currently in Tech Preview. Tech Preview provides a preview of a functionality that is still under development. The Tech Preview features are not intended to be used in production environments. These features, including their GUI and API interfaces, may change between Tech Preview and General Availability.** **To provide your feedback for the tech preview, send an email to intersight-techpreview-feedback@cisco.com**	Added a new task that provides information on how to configure a multi-node cluster for Intersight Virtual Appliance.	Configuring a Multi-Node Cluster for Intersight Virtual Appliance
		Added a new task that provides information on how to replace a node in the multi-node cluster for Intersight Virtual Appliance.	Replacing a Node in the Multi-Node Cluster for Intersight Virtual Appliance, on page 47
January 2023	Reserved IP Address Range Requirements	Added new section to include information about the requirements for reserved IP address range.	Reserved IP Address Range Requirements, on page 16
November 2022	Configuring External Syslog	Updated the Configuring External Syslog task to include support for exporting all Intersight alarms to the configured external syslog server.	Configuring External Syslog, on page 78
	Supported Configuration Limits	Updated content to include information for large deployments.	Supported Configuration Limits for Intersight Virtual Appliance, on page 11

When Updated	Feature/Funtionality	Description	Where Documented
April 2022	Intersight Virtual Appliance Monitoring	Added a note in the Intersight Virtual Appliance Monitoring section to specify that UCS C-Series server-related faults are not forwarded by the Connected Virtual Appliance to an external syslog server.	Intersight Virtual Appliance Monitoring, on page 68
	Configuring External Syslog	Added a note in the Configuring External Syslog task to specify that UCS C-Series server-related faults are not forwarded by the Connected Virtual Appliance to an external syslog server.	Configuring External Syslog, on page 78
January 2022	High Availability and Disaster Recovery	This guide now includes information about how to leverage High Availability using a vendor-provided solution. It also includes information about disaster recovery using the existing Backup and Restore functionality in Intersight Virtual Appliance as well as other third-party solutions.	High Availability and Disaster Recovery for Cisco Intersight Virtual Appliance, on page 48
December 2021	Merge the Intersight Assist Getting Started Guide content with the Intersight Virtual Appliance Getting Started Guide	This guide now includes installation and set-up information for both Intersight Virtual Appliance and Intersight Assist.	About Cisco Intersight Virtual Appliance, on page 9 About Cisco Intersight Assist, on page 21
November 2021	Configuring Account Settings	Updated the Configuring Account Settings task to include information about the Audit Logs Retention Period field.	Configuring Account Settings
October 2021	Setting Up Intersight Virtual Appliance	Added new tasks for setting up Intersight Connected Virtual Appliance, Intersight Private Virtual Appliance, and Intersight Assist.	Setting Up Single-Node Intersight Connected Virtual Appliance
	Recovering Intersight Virtual Appliance	Added new tasks that provides information on how to recover Intersight Virtual Appliance.	Recovering Intersight Connected Virtual Appliance
	Updating the Intersight Virtual Appliance Software	Added tasks that provide information on how to update Intersight Connected Virtual Appliance and Intersight Private Virtual Appliance.	Updating the Intersight Connected Virtual Appliance Software

When Updated	Feature/Funtionality	Description	Where Documented
July 2021	Enhancement to Intersight Virtual Appliance Settings	Updated the configuring external syslog task to include support for UDP and TCP protocols, in addition to the existing TLS protocol.	Configuring External Syslog, on page 78
		Updated the role creation task to include information on configuring the maximum number of concurrent sessions per role.	Adding a Role, on page 92
May 2021	Enhancement to Intersight Virtual Appliance Settings	Updated the task that provides information on how to download software packages for Intersight Virtual Appliance.	Downloading Software Packages for Intersight Virtual Appliance, on page 51
	Configuring NTP Servers	Updated the task that provides information on how to configure a NTP server.	Configuring NTP , on page 77
February 2021	Enhancements to Intersight Virtual Appliance Settings	Added a new task that includes information about configuring password policy for local users. Added a new task that includes information about configuring a banner message for displaying before the login screen.	Configuring Password Policy for Local Users, on page 87 Configuring a Banner Message for Displaying Before the Login Screen, on page 76
	Installing Appliance on KVM Hypervisor	Added a new task that provides information on how to install Cisco Intersight Virtual Appliance on KVM Hypervisor.	Installing Cisco Intersight Virtual Appliance and Intersight Assist on KVM Hypervisor, on page 32
January 2021	Enhancement to Intersight Virtual Appliance Settings	Added a new task that includes information about updating Intersight Intelligence for Intersight Virtual Appliance.	Updating Intersight Intelligence for Intersight Connected Virtual Appliance , on page 74
October 2020	Enhancement to Intersight Virtual Appliance Settings	Added a new task that includes information about configuring external syslog.	Configuring External Syslog, on page 78
	Support for IPv6 for endpoints	Updated this section to include information about configuring IP addresses.	Maintenance Shell for Intersight Virtual Appliance and Intersight Assist, on page 101

When Updated	Feature/Funtionality	Description	Where Documented
July 2020	Licensing requirements	Updated this section to include licensing requirements for Intersight Private Virtual Appliance.	Licensing Requirements for Intersight Virtual Appliance, on page 10
	Technical assistance	Added a new section that includes information about collecting tech support bundles from Intersight Virtual Appliance.	Technical Assistance , on page 111
	Installing Appliance on Microsoft Hyper-V Server	Added a new task that provides information on how to install Cisco Intersight Virtual Appliance on Microsoft Hyper-V Server.	Installing Cisco Intersight Virtual Appliance and Intersight Assist on Microsoft Hyper-V Server, on page 29
	Creating Private Appliance Account	Added a new task that provides information about creating a Private Appliance Account for downloading software packages for Intersight Private Virtual Appliance deployments.	Creating an Appliance Account for Downloading Software Packages, on page 51
	Downloading Software Packages	Added a new task that provides information about downloading software packages for Intersight Private Virtual Appliance deployments.	Downloading Software Packages for Intersight Virtual Appliance, on page 51
	Uploading Software Packages	Added a new task that provides information about uploading software packages for Intersight Private Virtual Appliance deployments.	Uploading Software Packages for Intersight Private Virtual Appliance, on page 52
March 2020	Configuration selection	Added a step to the existing procedure.	Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere, on page 25
	Supported Configuration Limits for Intersight Virtual Appliance	The newly added **Tiny(8 vCPU, 16 Gi RAM)** option is applicable for Intersight Assist deployments only.	Supported Configuration Limits for Intersight Virtual Appliance, on page 11
February 2020	LDAP Configuration	Added support for multiple LDAP domains. Added support for LDAP/AD configurations without requiring email.	Configuring LDAP Settings , on page 82
	Change IP address	Added the ability to change IP address of the virtual appliance VM.	Maintenance Shell for Intersight Virtual Appliance and Intersight Assist, on page 101

When Updated	Feature/Funtionality	Description	Where Documented
January 2020	Organizations	Organizations to support multi-tenancy in an account and the ability to create user-defined roles with system-defined privileges.	Adding a Role, on page 92, and Adding an Organization, on page 95
	Certificates	Allow user-submitted certificates and ability to create a self-signed certificate.	Certificates, on page 84
December 2019	Supported Configuration Limits for Intersight Virtual Appliance	Intersight Virtual Appliance can be deployed in Small or Medium deployment sizes to support 2000 or 5000 servers.	Supported Configuration Limits for Intersight Virtual Appliance, on page 11
	Graceful reboot of the Appliance VM	Intersight Virtual Appliance can be gracefully rebooted from the Intersight Appliance Diagnostic Tool.	Maintenance Shell for Intersight Virtual Appliance and Intersight Assist
July 2019	Alerts based on Cloud Connection	Enhanced messages to alert users about cloud connectivity and impact of a disrupted connection.	Cloud Connection for Intersight Connected Virtual Appliance, on page 75
	Intersight Appliance Diagnostic tool	A console-based diagnostic tool that helps in troubleshooting and addressing misconfiguration or networking issues during the appliance installation.	Troubleshooting
June 2019	Support for DHCP	Enables the appliance to obtain IP addresses from the DHCP server running on the same network to avoid using static IP addresses.	Installing Cisco Intersight Virtual Appliance
	Scheduling Backup	Schedules a full state periodic backup of the data in the appliance based on a schedule and saves the backed-up data on a remote server.	Scheduling Backup, on page 72



CHAPTER 2

Overview

Overview of Cisco Intersight Virtual Appliance

About Cisco Intersight Virtual Appliance

Cisco Intersight Virtual Appliance delivers the management features of Intersight in an easy to deploy VMware OVA, Microsoft Hyper-V Server VM, and KVM hypervisor. Intersight Virtual Appliance provides the benefits of Cisco Intersight that offers an intelligent level of management to enable customers to analyze, simplify, and automate their environments in more advanced ways than the previous generations of tools, while allowing more flexibility with additional data locality, security, and compliance requirements.

You can deploy Intersight Virtual Appliance in one of the following modes:

- Intersight Connected Virtual Appliance
- Intersight Private Virtual Appliance

Intersight Connected Virtual Appliance delivers the management features of Intersight while allowing you to control what system details leave your premises. Intersight Connected Virtual Appliance deployments requires a connection back to Cisco and Intersight services for automatic updates and access to services for full functionality.

Intersight Private Virtual Appliance delivers the management features of Intersight and allows you to ensure that no system details leave your premises. Intersight Private Virtual Appliance deployments is intended for an environment where you operate data centers in a disconnected (air gapped) mode.

For an overview of Intersight Assist, see About Cisco Intersight Assist, on page 21.

You can deploy Intersight Virtual Appliance as a single-node virtual machine in your existing environment.

You can also deploy Intersight Virtual Appliance on VMware vSphere as a multi-node cluster which allows for high availability. Once you have completed the initial set up of the single-node appliance, you can add additional nodes. After you successfully add two additional nodes, you can create a multi-node cluster in Intersight Virtual Appliance.

This guide provides an overview of how to install and set up Intersight Virtual Appliance in your environment.

Attention Before installing and setting up Intersight Virtual Appliance, it is strongly recommended that you read the information provided in the VM Resource Requirements for New Intersight Virtual Appliance Deployments section.

For latest updates on Intersight features and functionality, see Intersight Appliance Help Center.

Licensing Requirements for Intersight Virtual Appliance

Cisco Intersight Virtual Appliance uses a subscription-based license that is required to use the features of the appliance. Intersight Essentials is a subscription license delivered via **Cisco Smart Licensing**. Please contact your Cisco sales representative, channel partner, or reseller to purchase Intersight Essentials. Enabled platforms are those Cisco UCS and Cisco HyperFlex systems with a Cisco Intersight device connector, including eligible Cisco UCS Manager, Cisco IMC, and Cisco HyperFlex software.

For a **Connected Virtual Appliance** deployment, you must register the license as part of the initial setup of Cisco Intersight Virtual Appliance. After you complete the installation of the appliance, launch the UI and log in with the password that you set during installation, connect the appliance to Intersight, and register the license.

Use the following instructions if you want to edit the settings after the initial setup:

1. In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **Licensing** > **Register License**.

   The **Smart Software Licensing Product Registration** window displays.

2. Generate a Product Instance Registration Token from your specific virtual account in **Cisco Smart Software Manager**, if you do not have one already.

3. Enter the Product Instance Registration Token that you obtained from **Cisco Smart Software Manager** and click **Register**. Click here to watch a video about Cisco Intersight licensing tiers and registration.

For a **Private Virtual Appliance** deployment, you must reserve the license as part of the initial setup of Cisco Intersight Virtual Appliance. For information on how to reserve a license as part of the initial setup, see Setting Up Single-Node Intersight Private Virtual Appliance, on page 39.

For instructions on how to **update** or **return** the license after the initial setup of your Private Virtual Appliance, see Updating Intersight Private Virtual Appliance License and Returning Intersight Private Virtual Appliance License.

You can obtain an Intersight evaluation license for Cisco Intersight Virtual Appliance from your Cisco sales representative, channel partner, or reseller. If you already have a Cisco Smart Account, the evaluation license will be added to your Cisco Smart Account. You can then generate a token for the virtual account in the Smart account and proceed with registering Cisco Intersight Virtual Appliance. For more information about how to activate and manage your license, and learn more about Smart Licenses, see Managing Smart Licenses.

For a complete understanding of **Reserve Licenses** feature in Cisco Smart Software Manager, see Introduction to Smart Software Manager.

System Requirements

Supported Configuration Limits for Intersight Virtual Appliance

Cisco Intersight Virtual Appliance is available in multiple deployment sizes to support the scaling requirements of your environment. You can deploy the Appliance as follows:

New Deployments—You can deploy Intersight Virtual Appliance in medium or large configuration. Before selecting the size, assess your resource requirements and choose an appropriate option in the Intersight Appliance Maintenance Shell, and select the required size to deploy. The selected size will be deployed when the appliance VM restarts. For information about resource requirements, see VM Resource Requirements for New Intersight Virtual Appliance Deployments.

The following table lists the supported configuration limits:

Items	Configuration Limits		
	Small (Supported on existing deployments only)	Medium	Large
Number of Servers	2000	5000	8000
Number of Intersight Managed Mode (IMM) Domains (FI)	4	Up to 32	64
Number of Intersight Managed Mode (IMM) Servers	170 (metrics collection is not supported on small deployments)	500 (with metrics collection enabled)	2000 (with metrics collection enabled)
		5000 (with metrics collection disabled)	8000 (with metrics collection disabled)
Number of UCSM Managed Mode (UMM) Domains	30	500	800
Number of UCSM Managed Mode (UMM) Servers	330	Up to 5000	8000
Number of UCS Standalone Rack Servers	1500	5000	8000
Number of parallel HyperFlex Installations	2	5	5
Number of Supported Concurrent Operations	50	100	100
Number of Concurrent User Sessions (GUI and API)	32	32	32

VM Resource Requirements for New Intersight Virtual Appliance Deployments

The Cisco Intersight Virtual Appliance can be deployed on VMware ESXi 7.0 or later, Microsoft Hyper-V Server 2016 and 2019, and KVM hypervisor on Linux. You can deploy Intersight Virtual Appliance in Medium or Large configuration.

For more information on the supported maximum configuration limits for Intersight Virtual Appliance Sizing Options, see Supported Configuration Limits for Intersight Virtual Appliance.

Table 2: Resource Requirements for New Intersight Virtual Appliance Deployments

Resource	Requirements	
	Medium	**Large**
vCPU	24	48
RAM(GiB)	64	96
Storage (Disk)	2TiB*	2TiB*
Supported Hypervisors	VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later Microsoft Hyper-V Server 2016 and 2019 KVM hypervisor on Linux	

*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, and might require a restore from backup.

Small configuration is still supported on existing deployments. For more information, see VM Resource Requirements for Existing Intersight Virtual Appliance Deployments, on page 13.

Attention

- Do not change the default settings for disk sizes while installing Intersight Virtual Appliance on VMware vSphere. The disk sizes are computed based on the deployment configuration.
- Metric collection:
  - Metric collection is an opt-in feature and is currently supported on single-node deployments only. For information on how to configure metrics collection, see Configuring Metrics Collection.
  - When metrics collection is enabled, you can claim a maximum of 500 IMM servers for medium configuration and a maximum of 2000 IMM servers for large configuration. However, you can claim additional UMM servers up to the supported limits for medium and large configuration.
  - When the active server count for which metrics is collected, exceeds the threshold that your appliance size can support, be it medium or large, Intersight Virtual Appliance automatically disables metrics collection. This precaution is taken to prevent any negative impacts on performance, allowing for smooth system operation without the need for manual intervention. Once the metrics collection is disabled, you will have to enable it manually, after the resource requirements are met for this feature.
  - Any metrics that have been collected while the metrics collection was enabled will remain accessible, even if metrics collection is later paused. This ensures the continued availability of a historical data set for future analysis and reference. Enforcement of the storage and retention policies for metrics continues, even when the metrics collection is disabled.
  - For more information about metrics collection, see Monitoring Overview.
- For the Sort and Filter feature, the VM processor must support the x86-64 instruction set as well as the SSE 4.2 and AVX instruction set extensions. For multi-node deployments, each VM must also meet this requirement. Note that the Sort and Filter feature is supported on Medium and Large deployments only.
- If the allocated resources fall below the default values required for a Medium deployment (24 for vCPU and 64 GiB for RAM), then Assist will be the only option available for deployment. Other options will be grayed out.
- **Additional Networking Requirements for Multi-node Deployments:**
  - Disk write speed must be greater than 150 megabytes per second.
  - Latency between nodes must be less than 9 milliseconds.
  - All three hostnames for the nodes must be resolved by the same set of DNS servers.

VM Resource Requirements for Existing Intersight Virtual Appliance Deployments

Intersight evaluates the changes that are required in the CPU, RAM, and disk to determine the deployment size during the reboot after an update from the cloud service. As a result of the evaluation, one of the following outcomes occurs:

- If the minimum required resources for a particular deployment size are not available, the Intersight services are shut down and the appliance remains powered on. However, the appliance may not be functional and the services running could be unstable. Intersight Appliance Maintenance Shell displays an error message regarding the resource status during the reboot. Log in to the Maintenance Shell to learn more about the error and the required remedial actions.

- If the deployment size is same as the existing deployment, the VM restarts without any change. You can upgrade to a higher deployment size after determining resource requirements.

Table 3: Resource Requirements for Existing Intersight Virtual Appliance Deployments

Resource	Requirements		
	Small	**Medium**	**Large**
vCPU	16	24	48
RAM(GiB)	32	64	96
Storage (Disk)	Minimum of 620GiB* (applicable starting with Appliance Release Version 1.0.9-631)	2TiB*	2TiB*
Supported Hypervisors	VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later Microsoft Hyper-V Server 2016 and 2019 KVM hypervisor on Linux		

Note

- *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, and might require a restore from backup.
- The Sort and Filter feature is supported on Medium and Large deployments only.

Managing Resources for Intersight Virtual Appliance Deployments

Managing Resources for Intersight Virtual Appliance Deployments

You can view the deployment size of Intersight Virtual Appliance and make changes to CPU, RAM, and disk size as follows:

1. From the **Service Selector** drop-down list, choose **System**.
2. Navigate to **Settings** > **GENERAL** > **Appliance** .
3. Review the other supported scaling options and choose the appropriate deployment size to suit your requirement.
4. After you review the details of the resource requirement for a supported deployment option, shut down the VM, change the CPU, RAM, and disk size as required, and restart the VM.

Note

- You cannot change the disk sizes when you have a snapshot.
- To use the Virtual Appliance sizing options, you must have the latest upgrades from the Intersight cloud service.

The following table provides information about the disk size requirements for Intersight Virtual Appliance installations.

Table 4: Disk Size Requirements for Intersight Virtual Appliance Installations

Disk	Minimum Disk Size Requirements for all Deployments	Recommended Disk Size Requirements for Medium and Large Deployments
Disk1	Do not change the disk size.	Do not change the disk size.
Disk2	25GiB	25GiB
Disk3	150GiB	150GiB
Disk4	150GiB	150GiB
Disk5	100GiB	190GiB
Disk6	30GiB	60GiB
Disk7	60GiB	360GiB
Disk8	60GiB	1190GiB

Note Alternatively, you can meet the disk requirements by performing a restore using the latest backup of the appliance. For more information, see Recovering Intersight Connected Virtual Appliance and Recovering Intersight Private Virtual Appliance .

IP Address and Hostname Requirements

IP Address and Hostname Requirements for Intersight Virtual Appliance

Setting up a single-node Intersight Virtual Appliance requires an IP address and 2 DNS records for that IP address. The DNS records must be in the following formats:

- **myhost.mydomain.com**—A DNS record in this format is used to access the GUI. This must be defined as an **A record and associated PTR record** in DNS. The PTR record is required for reverse lookup of the IP address. If an IP address resolves to multiple hostnames, the first resolved hostname is used.
- **dc-myhost.mydomain.com**—The **dc-** must be prepended to your hostname. This DNS record must be defined as the **CNAME of myhost.mydomain.com**. DNS records in this format are used internally by the appliance to manage target connections.

Setting up a multi-node cluster for Intersight Virtual Appliance requires three hostnames, three IP addresses, and one DC-CNAME for each hostname. The following is an example of the formats:

- **myhost1.mydomain.com**
- **myhost2.mydomain.com**
- **myhost3.mydomain.com**
- **dc-myhost1.mydomain.com**
- **dc-myhost2.mydomain.com**
- **dc-myhost3.mydomain.com**

Attention Ensure that the appropriate entries of type **A, CNAME, and PTR records** exist in the DNS, as described above.

Reserved IP Address Range Requirements

Intersight Virtual Appliance reserves the following IP address ranges for internal communication:

- **/20 subnet within the 172.16.0.0/12 range**—This subnet is one-time configurable during the appliance installation.
- **192.168.20.21/32**—This IP address is reserved by the appliance and is non-configurable.

Port Requirements

Port Requirements for Intersight Virtual Appliance

The following table lists the ports that are required for Intersight Virtual Appliance communication.

Port	Protocol	Appliance Configuration Mode	Description
443	TCP	Single-node and multi-node	This port is required for communication between: • **Intersight Virtual Appliance and the users' web browser.** • **Intersight Virtual Appliance to and from the endpoint targets.** For more information about connectivity, see the Network Connectivity Requirements for Intersight Connected Virtual Appliance section.
53, 67, 68	UDP	Single-node and multi-node	These ports are used to send and receive DNS and NTP traffic.

Port	Protocol	Appliance Configuration Mode	Description
2379, 6443, 2380, 9092, 9094, 9100, 10250	TCP	Multi-node	These ports are used for communication between the VMs in a multi-node configuration for Intersight Virtual Appliance.
51820, 51821	UDP	Multi-node	These ports are used for securing VPN between the VMs in a multi-node configuration for Intersight Virtual Appliance.

Network Connectivity Requirements for Intersight Connected Virtual Appliance

Note The information in this section is applicable only for Intersight Connected Virtual Appliance deployments.

- Ensure that Cisco Intersight Virtual Appliance has access to the following sites directly or through a proxy. For more information about setting up a proxy, see Cloud Connection for Intersight Connected Virtual Appliance, on page 75. All the following URLs are accessed through HTTPS.
  - Access to Cisco services (*.cisco.com).

Cisco Service	Description	Target Device
smartreceiver.cisco.com:443	For access to Cisco Smart Licensing Manager	Required for all servers
swapi.cisco.com:443	For access to Cisco Smart Licensing Manager	Required for all servers
tools.cisco.com:443	For access to Cisco Smart Licensing Manager	Required for all servers
download-ssc.cisco.com*, dl.cisco.com, dl1.cisco.com, dl2.cisco.com	For access to Cisco Software download site	Required for the following: • C-Series Standalone Servers • UCSM Managed B-Series and C-Series servers • UCSM Managed Fabric Interconnects • UCSM Managed Fabric Interconnects-attached Cisco UCS S3260 Chassis
api.cisco.com:443		
cloudsso.cisco.com:443		

* Cisco Intersight allows you to manage firmware downloads through a new domain *download-ssc.cisco.com*. Make sure that you add this new domain to the firewall and network rules. For more information, see Cisco Software Download.

- Access to Intersight Cloud services.

  Intersight Virtual Appliance connects to Intersight by resolving one of the following URLs:

Note IP address for any given URL could change. In case you need to specify firewall configurations for URLs with fixed IPs. The following are the static IP addresses corresponding to each region.

North America (us-east-1) region

- svc-static1.intersight.com **(Preferred)**.
- svc-static1.ucs-connect.com **(Will be deprecated in the future)**.
- Both these URLs resolve to the following IP addresses:
  - 3.208.204.228
  - 54.165.240.89
  - 3.92.151.78

EMEA (eu-central–1) region

- svc.eu-central-1-static1.Intersight.com
- This URL resolves to the following IP addresses:
  - 99.84.238.166
  - 99.84.238.204
  - 99.84.238.94
  - 99.84.238.110

Requirements for Successful Target Connection to Intersight Virtual Appliance

For a successful target connection to Intersight Virtual Appliance, ensure that the following connectivity requirements are met:

- Ensure that a network connection can be established from the Device Connector to the appliance.
- The Device Connector establishes an HTTPS connection to <*https://dc-fqdn-of-your-appliance*> and then upgrades the HTTPS connection to a web socket. Ensure that your security rules allow the device connector to establish a web socket connection.
- Ensure that **Intersight Management** is enabled in the device connector (it is enabled by default). You can find **Intersight Management** in **Admin** > **Device Connector** > **Intersight Management** in Cisco

UCS Manager/Cisco UCS Director/Cisco IMC, and **Settings** > **Device Connector** in the Cisco HyperFlex UI.

- Check if a firewall is introduced between the managed target and the appliance, or if the rules for an existing firewall have changed, thus affecting connectivity. If the rules are changed, ensure that the changed rules permit traffic through the firewall.
- Ensure that all applicable physical and Virtual IPs are allowed through the firewall.
- If you use an HTTP proxy to route traffic out of your premises, and if you have made changes to the HTTP proxy server's configuration, ensure that you change the device connector's configuration accordingly. This is required because the appliance does not automatically detect HTTP proxy servers.
- Configure DNS and resolve the DNS name. The Device Connector must be able to send DNS requests to a DNS server and resolve DNS records. The Device Connector must be able to resolve *dc-<fqdn-of-your-appliance>* to an IP address.
- Configure NTP and validate that the target time is properly synchronized with a time server.

Note When the target time is not properly synchronized, the Device Connector may be unable to establish a secure connection to the appliance and the TLS certificate may be considered invalid.

Attention You must configure DNS and NTP on the management interface (Cisco UCS Manager/Cisco IMC/Cisco HyperFlex) and not on the Device Connector UI.

- You must configure security targets that are in the network path by enabling network connectivity to the appliance.
- The Intersight Device Connector uses Amazon Trust Services to validate certificates. If you wish to leverage certificate validation, you must open port 80 and allow communication to amazontrust.com in your firewall settings. Allowing for certificate validation is optional but recommended.

Important Intersight uses the Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRL) servers to validate HTTPs certificates. These protocols are designed to distribute the revocation status over HTTP. CRLs and OCSP messages are public documents that indicate the revocation status of X.509 certificates. They are generated by the Certificate Authority that issues the certificates. To prevent spoofing, CRLs and OCSP messages are digitally signed by the Certificate Authority. Since the revocation status data is public and signed, there is no need to protect the CRL/OCSP connection with HTTPs.

A PKI client can query a CRL or use OCSP to verify a certificate prior to use. In particular, when a client establishes a TLS session to a server, it can determine the certificate revocation status of the X.509 certificate presented by the server. If the certificate is valid the TLS connection can proceed. If the certificate has been revoked, the client must terminate the TLS connection. The original TLS connection triggers a CRL or OCSP lookup, which in turns triggers another connection to get the revocation status. If that secondary connection were to be done over HTTPs, that itself could trigger another connection to check the revocation status recursively.

Supported Browsers

Supported Browsers for Intersight Virtual Appliance

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

Software Compatibility

Software Compatibility for Intersight Virtual Appliance

This section contains details about the minimum versions of the following software supported by the appliance:

Component	Minimum Supported Version
Cisco UCS Manager	3.2(1)
Cisco HyperFlex Connect and Data Platform	2.6

Component	Minimum Supported Version
Cisco IMC	3.1(3) for M5 Servers 3.0(4) for M4 Servers For more information about the Cisco IMC Software requirements for the M4 and M5 Servers, see the Supported Systems section in the Help Center. See Device Connector Requirements. for a complete list of the supported software and the required device connector versions.
Cisco UCS Director	6.7.2.0
Cisco Intersight Managed Mode	4.1(2a)

Overview of Cisco Intersight Assist

About Cisco 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 enables Cisco Intersight to communicate with targets that do not have a direct path to Cisco Intersight and do not have an embedded Intersight Device Connector. These include targets such as Storage Devices, Hypervisor Managers, Application Performance Management products, and much more. Intersight Assist communicates with the target's native APIs and serves as the communication bridge to and from Cisco Intersight. Intersight Assist services run as a standalone appliance when used with Cisco Intersight SaaS. For Connected Virtual Appliance and Private Virtual Appliance, a separate Assist Appliance is not needed as the services are collocated.

You can view the Intersight Assist details by navigating to **Appliance UI** > **Target**.

You can choose to install Cisco Intersight Assist from the installer during the set-up wizard. It can be installed on an ESXi server, Kernel-based Virtual Machine (KVM), and HyperV Hypervisors.

Note You cannot de-register Intersight Assist, and you cannot claim another Intersight Assist with the appliance.

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

Note Cisco Intersight Assist does not support IPv6 configurations.

Now, you can add Pure Storage devices, Hitachi Virtual Storage Platform devices, NetApp storage controllers, VMware vCenter, and much more devices into Cisco Intersight after claiming them using Cisco Intersight Assist.

Licensing Requirements for Intersight Assist

For more information on licensing, see Intersight Licensing.

System Requirements For Intersight Assist

VM Resource Requirements for Intersight Assist

You can deploy Cisco Intersight Assist on Kernel-based Virtual Machine (KVM), HyperV Hypervisors, and VMware ESXi 7.0 or later with VMware vSphere Web Client 7.0 or later Microsoft Hyper-V Server 2016 and 2019. This section describes the system requirements to install and deploy Cisco Intersight Assist. You can deploy Intersight Assist in Small, Medium, and Large options.

New Deployments—You can deploy Intersight Virtual Appliance in Small, Medium, or Large configuration.

Existing Deployments—Existing deployments are supported for Tiny, Small, Medium, and Large configuration. However, it is **recommended** that you migrate existing Tiny deployments to Small, Medium, or Large configuration.

Note
- Tiny deployment is supported only for existing Assist deployments and is applicable only for Intersight Orchestrator.

Table 5: Intersight Assist Resource Requirements

Resource	Requirements			
	Tiny (Supported for existing deployments only)	**Small**	**Medium**	**Large**
vCPU	8	16	24	48
RAM (GiB)	16	32	64	96
Supported Features	ICO and IKS	ICO, IWO, IST, and IKS	ICO, IWO, IST, and IKS	ICO, IWO, IST, and IKS

Resource	Requirements
Supported Hypervisors	VMware ESXi 7.0 and higher VMware vSphere Web Client 7.0 and higher Kernel-based Virtual Machine (KVM) HyperV Hypervisors

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

Table 6: Intersight Assist Resource Requirements for Intersight Workload Optimizer

Resource Requirement	System Requirements		
	Small	**Medium**	**Large**
vCPU	16	24	48
RAM (GiB)	32	64	96
Storage	500GiB	500GiB/2TiB*	2TiB*
Deploy Configuration	Up to 1000 Virtual Machines	Up to 30,000 Virtual Machines	Up to 100,000 Virtual Machines

- *Existing deployments can upgrade from **Small** configuration to **Medium** configuration by either remaining at 500GiB or upgrading to 2TiB.
- *New deployments for **Medium** and **Large** configuration will be supported only with full 2TiB disk size configuration.

This following table lists the resource requirements to deploy Cisco Intersight Assist for Intersight Service for HashiCorp Terraform Service (IST).

Table 7: Intersight Assist Resource Requirements for Intersight Service for HashiCorp Terraform Service (IST)

Resource	Requirements		
	Small	**Medium**	**Large**
vCPU	16	24	48
RAM (GiB)	32	64	96
Number of Terraform Agents	5	5	5

Port Requirements for Intersight Assist

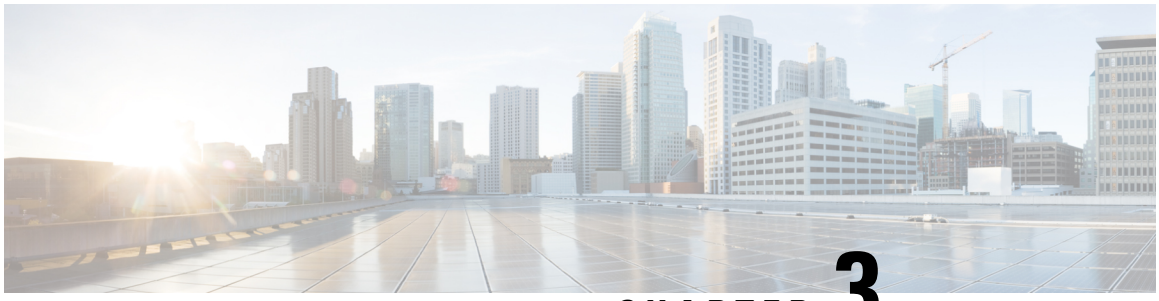
The following table lists the port numbers that must be open for Cisco Intersight Assist communication.

Port	Protocol	Description
443	TCP/UDP	Required for communication between: • Cisco Intersight Assist and the user's web browser. • Cisco Intersight Assist to and from the endpoint devices.

Supported Browsers for Intersight Assist

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



CHAPTER 3

Installation

Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format. Cisco Intersight Virtual Appliance supports VMware High Availability (VMHA) to ensure non-disruptive operation of the virtual appliance. For more information about VMHA, please refer to the documentation on vmware.com.

Attention Intersight Virtual Appliance and Intersight Assist OVA must be deployed using VMware vCenter. The OVA cannot be directly deployed on ESXi servers.

By default, VMware vCenter does not include a Certificate Authority (CA) that validates the Cisco digital signature on the Intersight Virtual Appliance OVA file. The VMware vCenter GUI will indicate that the OVA's certificate is invalid and is not trusted. Although possible, it is recommended that you **do not ignore this warning** and proceed with the installation. Instead, download and install the appropriate root CA from the table below that will validate the digital signature on the Intersight Virtual Appliance OVA file. Validating the signature ensures that the OVA was both issued by Cisco and has not been modified by a 3rd party.

The root CA certificates listed in the following table are available on Cisco's PKI page.

OVA version	CA Issuer	CA Serial Number	CA Expiration	OVA version
1.0.9-630	TrustID EV Code Signing CA 4	[illegible]	March 18, 2030	1.0.9-630
1.0.9-588	DigiCert Trusted G4 Code Signing 2021 CA1	[illegible]		1.0.9-588
1.0.9-499	None	None	None	1.0.9-499
1.0.9-342	DigiCert Trusted G4 Code Signing 2021 CA1	[illegible]	March 18, 2030	1.0.9-342
OVA version	CA Issuer	CA Serial Number	CA Expiration	OVA version

Use the steps in the following task to install and deploy the appliance on VMware vSphere. **To install and deploy a multi-node Intersight Virtual Appliance on VMware vSphere, repeat the steps in the following task three times.**

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.

Attention

- Before installing and setting up Intersight Virtual Appliance, it is strongly recommended that you read the information provided in the VM Resource Requirements for New Intersight Virtual Appliance Deployments section.
- Setting up a single-node Intersight Virtual Appliance requires an IP address and two DNS records for that IP address. For more information about IP addresses and Hostname requirements, see IP Address and Hostname Requirements.
- Setting up a multi-node cluster for Intersight Virtual Appliance requires three hostnames, three IP addresses, and one DC-CNAME for each hostname. For more information about IP addresses and Hostname requirements, see IP Address and Hostname Requirements.
- Use only HTTPS protocol and fully qualified domain name to access the appliance via the Web user interface.

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 **Select template** 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 **Select a name and location** page, add/edit the **Name** and **Location** for the Virtual appliance and click **Next**.

Step 6 On the **Select a resource** page, select the specific **Host** (ESX station), **Cluster**, **Resource Pool**, or **virtual appliance** you want to deploy and click **Next**.

Each VM must be assigned to a specific host on clusters that are configured with vSphere HA or Manual mode vSphere DRS.

Step 7 On the **Review details** page, verify the OVA template details and click **Next**.

Step 8 On the **Configuration** page, select a deployment configuration and click **Next**.

Step 9 On the **Select 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.

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, and might require a restore from backup.

Step 10 On the **Select networks** 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 11 On the **Customize Template** page, customize the deployment properties of the OVF template, and click **Next**.

OVF Property	Description
Enable DHCP (only for single-node appliance)	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 after this table.

OVF Property	Description
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. A maximum of 2 DNS servers are supported.
Admin Password	Enter the admin password. This is the same password that you use to log in to the appliance. **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.
Disk Size	**Attention:** Do not change the value of the disk size as it is computed based on the deployment configuration.

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. For more information about logging in, see** Logging In to Intersight Virtual Appliance, on page 50.

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 is equipped to handle IP address updates through DHCP, subject to lease requirements.

Attention **DHCP is not supported on multi-node Intersight Virtual Appliance.**

For a single-node appliance, ensure that the following requirements are met for using DHCP:

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

For information on how to complete the set-up of your appliance, see Setting Up Single-Node Intersight Connected Virtual Appliance.

Troubleshooting Tip: After providing the OVF parameters, if you notice that your VM does not respond when you visit <*https://fqdn-of-your-appliance*> after about 15 minutes since power-on, you may use the Intersight Appliance Maintenance Shell to troubleshoot networking or misconfiguration issues.

Troubleshooting Tip: If the diag shell displays a hostname such as **192:**, then it is possible that while deploying the appliance, the input for one or more network parameters (such as IP address, netmask, gateway, DNS servers, etc.) was entered incorrectly. It is also possible that the appliance VM is connected to a portgroup/vswitch that does not allow it to connect to the network and perform a successful DNS lookup. If you encounter this issue, check the inputs to the OVA as well as other network parameters. You can rectify the incorrect inputs using the diag shell.

The diagnostic tool aims to:

- Detect and display issues with the installation prerequisites.
- Enable editing the inputs that are provided during the OVA deployment.
- Assist with continuing the installation after you fix the settings, or set network interface properties such as IP addresses, subnet mask, and default gateway during the OVA deployment.

For more information, see Maintenance Shell for Intersight Virtual Appliance and Intersight Assist, on page 101.

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

Installing Cisco Intersight Virtual Appliance and Intersight Assist on Microsoft Hyper-V Server

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format. Install the appliance on Microsoft Hyper-V Server using the ZIP file format. For more information about Microsoft Hyper-V Server, refer to the Microsoft documentation.

Note Use the steps in the following task to install and deploy the appliance on Hyper-V Server Manager.

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.

Attention

- Before installing and setting up Intersight Virtual Appliance, it is strongly recommended that you read the information provided in the VM Resource Requirements for New Intersight Virtual Appliance Deployments section.
- Setting up a single-node Intersight Virtual Appliance requires an IP address and two DNS records for that IP address. For more information about IP addresses and Hostname requirements, see IP Address and Hostname Requirements.
- **Setting up a multi-node cluster for Intersight Virtual Appliance is NOT supported on Microsoft Hyper-V.**
- Use only HTTPS protocol and fully qualified domain name to access the appliance via the Web user interface.

Step 1 Log in to Hyper-V Server Manager with administrator credentials and select a server where you want to install the appliance.

Step 2 From the **Actions** pane, select **Import Virtual Machine**, and click **Next**.

a) Select the folder that contains the extracted virtual machine, for example, `onprem_vms`, and click **Next**.
b) Select the virtual machine to import and click **Next**.
c) In the **Choose Import Type** screen, select the **Copy the virtual machine (create a new unique ID)** option, and click **Next**.
d) Make your selection in the **Choose Destination** screen and click **Next**.
e) Make your selection in the **Choose Storage Folders** screen and click **Next**.
f) Verify your selections in the **Summary** screen, and click **Finish**.

After the import is completed, you will see the imported virtual machine in Hyper-V Manager.

Step 3 Right-click on the imported virtual machine and select **Settings**.

a) Navigate to **Network Adapter** and select a virtual switch from the drop-down list.
b) Click **Apply**.

Step 4 In the **Actions** pane, select **Start** to power-on the virtual machine.

Step 5 In the **Actions** pane, select **Connect** to connect to the virtual machine.

The **Virtual Machine Connection** console is displayed.

Step 6 On the **Virtual Machine Connection** console, customize the password configuration and IP properties.

Property	Description
Set password for user admin	Set a new password for admin user. **Note** Ensure that you remember this password as you will use the same one to log into the appliance.

Property	Description
Choose IP Assignment	Type in **S** for static IP assignment or **D** for DHCP Selecting DHCP for your IP assignment enables the appliance to obtain IP addresses from the DHCP server running on the same network to avoid using static IP addresses.
IP Address	Enter the IP address of the node. For example: 10.0.0.100
Subnet Mask	Enter the IP Net Mask. For example: 255.255.255.0
Default Gateway	Enter the IP Default Gateway. For example: 10.0.1.254
DNS Servers	Enter a comma-separated list of IP addresses for your DNS servers. A maximum of 2 DNS servers are supported.
DNS Domain	Enter the DNS Search Domain.
NTP Servers	Provide NTP information when configuring a static IP. Enter a comma-separated list of hostnames or IP addresses for your NTP servers. You can add up to 3 NTP servers. You cannot provide NTP information if you configured selected DHCP for your IP assignment.

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. For more information about logging in, see** Logging In to Intersight Virtual Appliance, on page 50.

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 is equipped to handle IP address updates through DHCP, subject to lease requirements.

Attention **For a single-node appliance, ensure that the following requirements are met for using DHCP:**

- 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 for the Hyper-V Server must be input into the Virtual Machine Connection console when configuring static IP.
- 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 7 Proceed to <*https://fqdn-of-your-appliance*> to complete the post-install set-up of your appliance.

For information on how to complete the set-up of your appliance, see Setting Up Single-Node Intersight Connected Virtual Appliance.

Troubleshooting Tip: After providing the password and IP property parameters, if you notice that your VM does not respond when you visit <*https://fqdn-of-your-appliance*> after about 15 minutes, you can use the Intersight Appliance Maintenance Shell to troubleshoot networking or misconfiguration issues.

The diagnostic tool aims to:

- Detect and display issues with the installation prerequisites.
- Enable editing the inputs that are provided during the OVA deployment.
- Assist with continuing the installation after you fix the settings, or set network interface properties such as IP addresses, subnet mask, and default gateway during the OVA deployment.

For more information, see Maintenance Shell for Intersight Virtual Appliance and Intersight Assist, on page 101.

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

Installing Cisco Intersight Virtual Appliance and Intersight Assist on KVM Hypervisor

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format. Install the appliance on KVM hypervisor using the TAR file format. The following procedure shows how to install and deploy the appliance on KVM hypervisor using Virtual Machine Manager (VMM).

Note Software Requirements:

- Linux operating system with support for KVM hypervisor or Linux operating system pre-configured with KVM hypervisor. On CentOS 7.9, the minimum supported KVM hypervisor version is 1.5.3.
- A virtual network bridge to provide network connectivity to VMs.

Note Use the steps in the following task to install and deploy the appliance on KVM hypervisor using Virtual Machine Manager (VMM).

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.

Attention

- Before installing and setting up Intersight Virtual Appliance, it is strongly recommended that you read the information provided in the VM Resource Requirements for New Intersight Virtual Appliance Deployments section.
- Setting up a single-node Intersight Virtual Appliance requires an IP address and two DNS records for that IP address. For more information about IP addresses and Hostname requirements, see IP Address and Hostname Requirements.
- **Setting up a multi-node cluster for Intersight Virtual Appliance is NOT supported on KVM hypervisor.** .
- Use only HTTPS protocol and fully qualified domain name to access the appliance via the Web user interface.

Step 1 Launch the Virtual Machine Manager (VMM) client.

Step 2 Select **File** > **New Virtual Machine** on the menu bar to install a new virtual machine on a KVM hypervisor.

The **New VM** dialog box appears and displays Step 1 of 4 of the New VM installation.

Step 3 Under **Choose how you would like to install the operating system**, select **Import existing disk image**, and click **Forward**.

Step 2 of 4 is displayed.

Step 4 Under **Provide the existing storage path**, click **Browse**.

Step 5 Under **Choose storage volume**, browse your directories to locate and select the first disk of the Intersight Virtual Appliance image file, (for example, *intersight-appliance-1.0.9-180-1.qcow2*) that you have extracted on your system.

a) Under **Advanced options**, select **VirtIO**.

Note VirtIO is the only supported disk bus for storage while installing Intersight Virtual Appliance and Intersight Assist on KVM Hypervisor.

Step 6 Under **Choose an operating system type and version**, select **Linux** for OS type and **CentOS 7.0** for Version, and click **Forward**.

Step 3 of 4 is displayed.

Step 7 Under **Choose Memory and CPU settings**, do the following, and click **Forward**.

- Select or enter 32768 for Memory (RAM)
- Set CPU at 16

Step 4 of 4 is displayed.

For more information about appliance deployment sizes, see Supported Configuration Limits for Intersight Virtual Appliance, on page 11 .

Step 8 In the dialog box, complete the following configuration:

- Under **Ready to begin the installation**, in the **Name** field, enter a name for the Intersight Virtual Appliance software. For example, *intersight-appliance-1.0.9-180*
- Ensure that you have selected the **Customize configuration before install** option.
- Under **Network selection**, ensure that you select the appropriate virtual network bridge.

Step 9 Click **Finish**.

You have now completed the process of adding the first disk of the Intersight Virtual Appliance image. You will need to add disks 2 through 8, one by one, before you can begin the installation process.

Step 10 On the VMM console, complete the following configuration:

a) Click **Add Hardware** that you can find at the bottom of the left navigation panel.
b) Under **Storage**, ensure that **Select or create custom storage** is selected.
c) Browse your directories to locate and select the second disk of the Intersight Virtual Appliance image file, (for example, *intersight-appliance-1.0.9-180-2.qcow2*) that you have extracted on your system, and click **Choose volume**.
d) Click **Finish**.

Repeat this step until you have added disk 3 through disk 8. Ensure that all eight disks appear on the left navigation panel.

Step 11 Click **Begin installation**.

Step 12 On the VMM console, customize the password configuration and IP properties.

Property	Description
Set password for user admin	Set a new password for admin user. **Note** Ensure that you remember this password as you will use the same one to log into the appliance.
Choose IP Assignment	Type in **S** for static IP assignment or **D** for DHCP Selecting DHCP for your IP assignment enables the appliance to obtain IP addresses from the DHCP server running on the same network to avoid using static IP addresses.
IP Address	Enter an IPv4 address of the node. For example: 10.0.0.100 **Note** You must have an IPv4 address configured in order for the appliance to be functional. It is recommended that you configure IPv6 addresses subsequent to completing the initial installation and deployment of the appliance using an IPv4 address.

Property	Description
Subnet Mask	Enter the IP Net Mask. For example: 255.255.255.0
Default Gateway	Enter the IP Default Gateway. For example: 10.0.1.254
DNS Servers	Enter a comma-separated list of IP addresses for your DNS servers. A maximum of 2 DNS servers are supported.
DNS Domain	Enter the DNS Search Domain.
NTP Servers	Provide NTP information when configuring a static IP. Enter a comma-separated list of hostnames or IP addresses for your NTP servers. You can add up to 3 NTP servers. You cannot provide NTP information if you configured selected DHCP for your IP assignment.

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. For more information about logging in, see** Logging In to Intersight Virtual Appliance, on page 50.

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 is equipped to handle IP address updates through DHCP, subject to lease requirements.

Attention **For a single-node appliance, ensure that the following requirements are met for using DHCP:**

- 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 for the KVM hypervisor must be input into the VMM console when configuring static IP.
- 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 13 Proceed to <*https://fqdn-of-your-appliance*> to complete the post-install set-up of your appliance.

For information on how to complete the set-up of your appliance, see Setting Up Single-Node Intersight Connected Virtual Appliance.

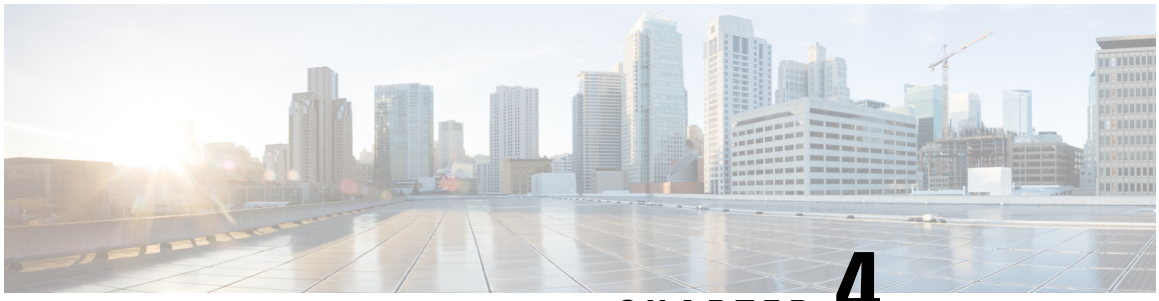
Troubleshooting Tip: After providing the password and IP property parameters, if you notice that your VM does not respond when you visit <*https://fqdn-of-your-appliance*> after about 15 minutes, you can use the Intersight Appliance Maintenance Shell to troubleshoot networking or misconfiguration issues.

The diagnostic tool aims to:

- Detect and display issues with the installation prerequisites.
- Enable editing the inputs that are provided during the appliance image deployment.
- Assist with continuing the installation after you fix the settings, or set network interface properties such as IP addresses, subnet mask, and default gateway during the appliance image deployment.

For more information, see Maintenance Shell for Intersight Virtual Appliance and Intersight Assist, on page 101.

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



CHAPTER 4

Set Up

Setting Up Single-Node Intersight Connected Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere, on page 25.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Intersight Appliance Installer** screen appears and allows you to complete the setup for either a new install, recover the appliance software from backup, or add a node to the appliance.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the installation.

Use the following instructions to complete the Intersight Connected Virtual Appliance setup:

Step 1 On the **Intersight Appliance Installer** screen, select **Intersight Connected Virtual Appliance** and click **Start**.

Step 2 Log in to the Intersight Virtual Appliance Connect page using your Cisco ID. If you do not have a Cisco ID, you can create one here.

a. **(Optional)** Click **Settings** to enable HTTPS Proxy Settings.

If an HTTP/S proxy is required to connect your Cisco Intersight Virtual Appliance to the internet, you must configure proxy settings before you can complete the connection step.

- Click **Settings** and enable the **HTTPS Proxy** option.
- Add the **Proxy Hostname** or **IP Address**, and the **Proxy Port**.

  The proxy port must be in the range between 1 and 65535. You can edit the Proxy settings from the appliance UI, **System** > **Settings** > **NETWORKING** > **Cloud Connection**.

b. Use the **Device ID** and **Claim Code** that is displayed on the Connect page to complete connecting to Intersight.

c. Ensure that the **Connection** status displays **Claimed**.

Note A new browser tab appears to display the status of the target claim in Intersight. If you do not have an Intersight account, you can create one in the **Account Creation** window and claim a target. If the target connection is successful, a success message is displayed. Click **Close** to exit the tab and return to the **Intersight Appliance Installer** setup wizard. If the target claim is unsuccessful, you will be taken to the Intersight login screen to restart target claim workflow.

Step 3 In the **Intersight Appliance Installer** setup wizard, do the following:

a) **Connect**—Click **Continue** to proceed to the **Check Network Requirements** step.

b) **Check Network Requirements**—View the results and click **Next** to proceed to the **Configure Internal Network** step.

Note that during the network requirements check if any of the DNS test fails, you cannot proceed with the configuration.

c) **Configure Internal Network**—If necessary, change the default Internal Network IP address and click **Next** to proceed to the **Select Software Version** step.

d) **Select Software Version**—You have the option to download the latest version of the appliance software, or you can upload any other supported version of the software that is the same as the installer version or greater than the installer version.

a) To download the latest version of the appliance software, select the **Download Latest Version** button and click **Finish** to proceed to the **Installation Result** screen.

b) To upload a version of the appliance software, select either **Local Machine** or **Network Share**, depending on where you saved the software packages.

Note In order to manually update, install, or restore Intersight Connected Virtual Appliance, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

- For Local Machine, browse to where you saved the software image, and then click **Finish** to proceed to the **Installation Result** screen.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish** to proceed to the **Installation Result** screen.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied

- **Port**—TCP port to use
- **Location**—Directory where the file to be copied is stored
- **Filename**—Name of the file to be copied from the network share
- **Username**—Username for authenticating with the network share
- **Password**—Password for authenticating with the network share

c) **Installation Results**—You can view the progress of the installation on this screen.

Step 4 Specify **Data Collection**.

Specify your preference to allow Intersight to send additional system information to Cisco. This option is enabled by default. For more information about what data is collected by Intersight, see Data Collected from Intersight Connected Virtual Appliance , on page 98.

Step 5 Click **Register License**.

Obtain a license registration token from Cisco Smart License Manager, and apply add the token to activate your license. The license registration process could take a few minutes to complete. For more information about registering your Intersight license, watch Cisco Intersight Licensing Tiers and Registration.

After you click **Finish**, the Intersight Connected Virtual Appliance dashboard displays.

What to do next

Once you have successfully completed the initial set up of the single-node Intersight Virtual Appliance, you can add additional nodes to create a multi-node cluster. For more information, see Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 42.

Setting Up Single-Node Intersight Private Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere, on page 25.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Intersight Appliance Installer** screen appears and allows you to complete the setup for either a new install, recover the appliance software from backup, or add a node to the appliance.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the installation.

Use the following instructions to complete the Intersight Private Virtual Appliance setup:

Step 1 On the **Intersight Appliance Installer** screen, select **Intersight Private Virtual Appliance** and click **Start** to proceed with setting up a single-node Private Virtual Appliance.

The **Upload Software** page displays. You can upload any supported version of the software that is the same as the installer version or greater than the installer version.

Step 2 In the **Intersight Appliance Installer** setup wizard, do the following:

a) **Check Network Requirements**—View the results and click **Next** to proceed to the **Configure Internal Network** step.

Note that during the network requirements check if any of the DNS test fails, you cannot proceed with the configuration.

b) **Configure Internal Network**—If necessary, change the default Internal Network IP address and click **Next** to proceed to the **Upload Software** step.

c) **Upload Software**—You can upload any supported version of the software that is the same as the installer version or greater than the installer version.

Select either **Local Machine** or **Network Share**, depending on where you saved the software packages.

Note In order to complete an Intersight Private Virtual Appliance deployment, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

- For Local Machine, browse to where you saved the software image, and then click **Finish** to proceed to the **Installation Result** screen.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish** to proceed to the **Installation Result** screen.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied
  - **Port**—TCP port to use
  - **Location**—Directory where the file to be copied is stored
  - **Filename**—Name of the file to be copied from the network share
  - **Username**—Username for authenticating with the network share
  - **Password**—Password for authenticating with the network share

d) **Installation Results**—You can view the progress of the installation on this screen.

Step 3 Log in to the Intersight Virtual Appliance Connect page. Use **admin** as the username, and enter the password that you set during the installation process.

Step 4 Complete the **Register License** process.

a. Use the Reservation Request Code that you obtain on this page to generate Reservation Authorization Code in Cisco Smart Software Manager.

b. Copy the Reservation Authorization Code that you generated in **Cisco Smart Software Manager** and paste it in the Reserve License page.

c. Click **Install**.

The license reservation process can take a few minutes to complete. For information about Intersight licensing tiers and registration, watch Cisco Intersight Licensing Tiers and Registration.

After you click **Close**, the Cisco Intersight Private Virtual Appliance dashboard displays.

What to do next

Once you have successfully completed the initial set up of the single-node Intersight Virtual Appliance, you can add additional nodes to create a multi-node cluster. For more information, see Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 42.

Setting Up Intersight Assist

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere, on page 25.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Intersight Appliance Installer** screen appears and allows you to complete the setup for either a new install, recover the appliance software from backup, or add a node to the appliance.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the installation.

Use the following instructions to complete the Intersight Assist setup:

Step 1 1. On the **Intersight Appliance Installer** screen, select **Intersight Assist** and click **Start**.

Step 2 Log in to the Intersight Virtual Appliance Connect page using your Cisco ID. If you do not have a Cisco ID, you can create one here.

a. (Optional) Click **Settings** to enable HTTPS Proxy Settings.

If an HTTP/S proxy is required to connect your Cisco Intersight Virtual Appliance to the internet, you must configure proxy settings before you can complete the connection step.

- Click **Settings** and enable the **HTTPS Proxy** option.
- Add the **Proxy Hostname** or **IP Address**, and the **Proxy Port**.

  The proxy port must be in the range between 1 and 65535. You can edit the Proxy settings from the appliance UI, **System** > **Settings** > **NETWORKING** > **Cloud Connection**.

b. Use the **Device ID** and **Claim Code** that is displayed on the Connect page to complete connecting to Intersight.

c. Ensure that the **Connection** status displays **Claimed**.

Note A new browser tab appears to display the status of the target claim in Intersight. If you do not have an Intersight account, you can create one in the **Account Creation** window and claim a target. If the target connection is successful, a success message is displayed. Click **Close** to exit the tab and return to the Intersight Virtual Appliance setup wizard. If the target claim is unsuccessful, you will be taken to the Intersight login screen to restart target claim workflow.

Step 3 In the **Intersight Appliance Installer** setup wizard, do the following:

a) **Connect**—Click **Continue** to proceed to the **Check Network Requirements** step.

b) **Check Network Requirements**—View the results and click **Next** to proceed to the **Configure Internal Network** step.

Note that during the network requirements check if the DNS test fails, you cannot proceed with the configuration.

c) **Configure Internal Network**—If necessary, change the default Internal Network IP address and click **Next** to proceed to the **Installations Results** screen.

d) **Installation Results**—You can view the progress of the installation on this screen.

Configuring a Multi-Node Cluster for Intersight Virtual Appliance

A multi-node cluster for Intersight Virtual Appliance allows for high availability, increased stability, and better resilience. Once you have completed the initial set up of the single-node appliance on VMware vSphere, you can add additional nodes. After you successfully add two additional nodes, you can create a multi-node cluster for Intersight Virtual Appliance.

Note Note that multi-node cluster configuration is supported only on VMware vSphere installations.

Important Once you have set up a multi-node cluster for Intersight Virtual Appliance, you cannot revert back to the single-node instance.

Requirements:

- You can set up a multi-node cluster for the appliance **only** after you have completed the initial set up of the single-node appliance. Ensure that you have set up single-node Intersight Virtual Appliance software as per the instructions in the following tasks:
  - Setting Up Single-Node Intersight Connected Virtual Appliance
  - Setting Up Single-Node Intersight Private Virtual Appliance
- You can set up a multi-node cluster at any time after you have completed the initial set up of your appliance.
- The first node must be in an **Operational** status to be able to add additional nodes for creating a multi-node cluster in Intersight Virtual Appliance.

To set up a multi-node cluster for Connected Virtual Appliance and Private Virtual Appliance, do the following:

Step 1 Access your VM using the <<https://myhost2.mydomain.com/ URL.

Step 2 On the **Intersight Appliance Installer** screen, click the **Add Node to Appliance** tab.

Step 3 On the **Add Node to Appliance** page, enter the details for the following fields, and click **Finish**.

- **Appliance Hostname/IP Address**—The hostname or the IP address of the existing stand-alone appliance to which the node will be added.
- **Appliance Username**—The admin username of the existing stand-alone appliance.
- **Admin User Password**—The admin password for the existing stand-alone appliance.

After the second node (node2) is successfully added, it is ready to join the cluster.

At this point, you can add a third node (node3) so that you can create a cluster.

Step 4 Repeat the instructions in Steps 1, 2, and 3 to add node3.

Step 5 Once the node3 has been successfully added, click **Go to Appliance Portal** to proceed to the appliance.

Step 6 Log into <<https:// myhost1.mydomain.com>>.

Step 7 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Appliance**.

Ensure that node2 and node3 are in the **Ready to Join** state.

Step 8 Click **Create Cluster**.

Important The action of creating a cluster is irreversible.

Note that the Appliance will switch to a maintenance mode while the cluster creation workflow is being executed. Allow 5-10 minutes for the progress page to load, after which you can view the progress of cluster creation on the **Multi-Node Cluster Creation Results** page. You can also view the progress of cluster creation on node2 and node3 which is available right away.

When the set up completes, the login screen appears.

Step 9 Log into the **Intersight Virtual Appliance Connect** page.

Use **admin** as the username and enter the password that you set during the initial single-node appliance setup. At this point, you can log into node2 and node3 as well.

Multi-node cluster will be fully operational when one node goes down. The appliance automatically stabilizes when one node is down. During the transition stage, your appliance might not be accessible.

When two nodes go down, the multi-node cluster will move to maintenance mode. During this state, the system will not be operational.

When the nodes come up, the multi-node cluster becomes **Operational** automatically.

Migration Path for Existing Single-Node Deployment to Multi-Node Cluster Configuration

To expand an existing single-node Intersight Virtual Appliance deployment to a multi-node cluster configuration, do the following:

1. Create a backup of your appliance.

   For more information, see Create Backup.

2. Restore Intersight Virtual Appliance.

For more information, see Recovering Intersight Connected Virtual Appliance and Recovering Intersight Private Virtual Appliance .

After you have successfully completed configuring the multi-node cluster for your existing single-node deployment, use the information in the following links to perform additional configuration for the multi-node cluster.

- Single Sign-On with Intersight Virtual Appliance
- Certificates

Recovering Intersight Connected Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

To restore a Connected Virtual Appliance configuration, you can recover the data from a backup file during the initial setup.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere, on page 25.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Installer Options** screen appears and allows you to complete the setup for either a new install or to recover the appliance software from backup.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the recovery.

Use these instructions to recover the configuration from a backup file:

Step 1 On the **Installer Options** screen, select the **Recover from Backup** tab and click **Start**.

Step 2 On the **Select Backup** page, select the protocol and enter details of the remote server from where you want to recover the backed up data.

- **Protocol**—Communication protocol option used in the backup process. Intersight Virtual Appliance currently supports SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) for backup.
- **Server IP/Hostname**—The host from which backed up data is recovered
- **Port**—TCP port on the backup server
- **Location**—Directory where the backup files are saved
- **Filename**—Name of the backup file to restore
- **Username**—Username for authenticating the backup client to the backup server
- **Password**—Password for authenticating the backup client to the backup server

Step 3 Click **Next**.

Important **The restore process cannot be modified once it has started.**

Step 4 Click **Continue** on the warning pop-up.

Step 5 On the **Select Software Version** page, you have the option to download the latest version of the appliance software, or you can upload any other supported version of the software that is the same as the installer version or greater than the installer version.

a) To download the latest version of the appliance software, select the **Download Latest Version** button and click **Finish**.

b) To upload a version of the appliance software, select either **Local Machine** or **Network Share**, depending on where you saved the software packages.

Note In order to manually restore Intersight Connected Virtual Appliance, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

- For Local Machine, browse to where you saved the software image, and then click **Finish**.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish**.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied
  - **Port**—TCP port to use
  - **Location**—Directory where the file to be copied is stored
  - **Filename**—Name of the file to be copied from the network share
  - **Username**—Username for authenticating with the network share
  - **Password**—Password for authenticating with the network share

You can view the progress of the recovery on the **Recovery Results** page. After the recovery process is complete, the Cisco Intersight Connected Virtual Appliance dashboard is displayed.

What to do next

For Recovering Multi-Node Cluster Deployments: If you are recovering from a back-up for a multi-node cluster deployment, first recover node1 and then add two additional nodes to create a multi-node cluster by following the steps in Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 42.

Recovering Intersight Private Virtual Appliance

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format.

To restore a Private Virtual Appliance configuration, you can recover the data from a backup file during the initial setup.

Before You Begin: Ensure that you have installed Intersight Virtual Appliance software as per the instructions in Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere, on page 25.

After the Cisco Intersight Virtual Appliance software deployment is complete, and the VM is powered on, access your VM using the <<https://your fqdn.com>> URL. The **Installer Options** screen appears and allows you to complete the setup for either a new install or to recover the appliance software from backup.

The wizard runs through a series of steps to download and install software packages. You can view the progress of the recovery.

Use these instructions to recover the configuration from a backup file:

Step 1 On the **Installer Options** screen, select the **Recover from Backup** tab and click **Start**.

Step 2 On the **Select Backup** page, select the protocol and enter details of the remote server from where you want to recover the backed up data.

- **Protocol**—Communication protocol option used in the backup process. Intersight Virtual Appliance currently supports SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) for backup.
- **Server IP/Hostname**—The host from which backed up data is recovered
- **Port**—TCP port on the backup server
- **Location**—Directory where the backup files are saved
- **Filename**—Name of the backup file to restore
- **Username**—Username for authenticating the backup client to the backup server
- **Password**—Password for authenticating the backup client to the backup server

Step 3 Click **Next**.

Important **The restore process cannot be modified once it has started.**

Step 4 Click **Continue** on the warning pop-up.

Step 5 On the **Select Software Version** page, you can upload any other supported version of the software that is the same as the installer version or greater than the installer version.

Note In order to manually restore Intersight Private Virtual Appliance, you will need to access the Appliance Account so that you can download the required software packages. For information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

- For Local Machine, browse to where you saved the software image, and then click **Finish**.
- For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Finish**.
  - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
  - **Server IP/Hostname**—The host server from where the file is copied
  - **Port**—TCP port to use
  - **Location**—Directory where the file to be copied is stored

- **Filename**—Name of the file to be copied from the network share
- **Username**—Username for authenticating with the network share
- **Password**—Password for authenticating with the network share

You can view the progress of the recovery on the **Recovery Results** page. After the recovery process is complete, the Cisco Intersight Private Virtual Appliance dashboard is displayed.

What to do next

For Recovering Multi-Node Cluster Deployments: If you are recovering from a back-up for a multi-node cluster deployment, first recover node1 and then add two additional nodes to create a multi-node cluster by following the steps in Configuring a Multi-Node Cluster for Intersight Virtual Appliance, on page 42.

Replacing a Node in the Multi-Node Cluster for Intersight Virtual Appliance

When a node in a multi-node cluster becomes **Impaired** or the status is **Unknown**, you can replace the defective node by adding another node to the existing cluster.

To replace a defective node in an existing cluster, do the following:

Step 1 Log into a node in your multi-node cluster that is operational.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Appliance**.

Step 3 In the table under **Node**, do the following:

a. In the row of the node that either displays the **Impaired** or **Unknown** status, click on the **ellipses**.

b. Click **Replace Node**.

The status for this node now displays as **Out of Service**.

Step 4 Power-off and delete the defective node from the VMware vSphere, Microsoft Hyper-V server, or KVM hypervisor installation.

Step 5 Deploy a fresh OVA using the same DNS Domain value as the defective node.

For more information about installing and deploying the appliance, see the Installing Cisco Intersight Virtual Appliance and Intersight Assist on VMware vSphere chapter.

Step 6 Access your VM using the <https://*fqdn-of-your-appliance*.com> URL.

Step 7 On the **Installer Options** screen, click the **Add Node to Appliance** tab.

Step 8 On the **Add Node to Appliance** page, enter the details for the following fields, and click **Finish**.

- **Appliance Hostname/IP Address**—The hostname or the IP address of the existing appliance VM to which the node will be added.
- **Appliance Username**—The admin username of the existing appliance VM.

- **Admin User Password**—The admin password for the existing appliance VM.

After the node is successfully added, it is ready to join the cluster.

Step 9 Log into one of the operational nodes.

Step 10 Click **Go to Appliance Portal** of the operational node and proceed to the appliance.

Step 11 Navigate to **Settings** icon > **Settings** > **General** > **Appliance**.

Step 12 In the row of the node that is ready to join the cluster, do the following:

a. Click on the ellipses.

b. Click **Join Cluster**.

c. On the pop-up screen, click **Join**.

You can monitor the progress of the workflow. Once the workflow runs successfully, the replaced node becomes completely operational.

High Availability and Disaster Recovery for Cisco Intersight Virtual Appliance

Cisco Intersight Virtual Appliance supports migration architectures for High Availability (HA) and Disaster Recovery (DR).

The following requirements must be met to successfully migrate Intersight Virtual Appliance.

- Intersight Virtual Appliance has a Fully Qualified Domain Name (FQDN). To migrate Intersight Virtual Appliance, the FQDN (hostname) of the appliance must remain the same. However, the IP address and DNS/NTP of the appliance can be changed during the recovery process.
- You can migrate the appliance from one site to another as long as the FQDN is reachable from the claimed end-point. This allows the back-up taken from one site to be restored on another site.
- Network connectivity between Intersight Virtual Appliance and its managed endpoints must be maintained.

High Availability for Intersight Virtual Appliance

You can leverage any vendor-provided solution to provide High Availability (HA) capabilities in Intersight Virtual Appliance.

Intersight Virtual Appliance deployed on VMware vSphere — Intersight Virtual Appliance supports VMware High Availability to ensure non-disruptive operation of the appliance. For more information about VMware HA, refer to the relevant documentation on VMware's website.

Intersight Virtual Appliance deployed on Microsoft Hyper-V Server — Intersight Virtual Appliance supports Microsoft Hyper-V High Availability to ensure non-disruptive operation of the appliance. Microsoft Hyper-V offers the Failed-Over Clustering High Availability solution to protect the workloads running on the host servers, thereby protecting the appliance. Failover Clustering feature allows users to experience minimum disruptions in service. For more information about Microsoft Hyper-V HA, refer to the relevant documentation on Microsoft's website.

Intersight Virtual Appliance deployed on KVM Hypervisor — KVM is supported by multiple Operating Systems (OS) vendors. The most common OS vendors are Red-Hat Virtualization and Ubuntu. For specific solutions for High Availability, refer to the documentation provided by the OS vendor.

Disaster Recovery for Intersight Virtual Appliance

For disaster recovery, you can use the existing Backup and Restore functionality in Intersight Virtual Appliance or other third-party solutions.

Backup and Restore in Intersight Virtual Appliance

Cisco strongly recommends taking periodic backup of Intersight Virtual Appliance.

For information on backing up Intersight Virtual Appliance, see Backing Up Data.

For information on restoring Intersight Connected Virtual Appliance, see Recovering Intersight Connected Virtual Appliance.

For information on restoring Intersight Private Virtual Appliance, see Recovering Intersight Private Virtual Appliance.

Third-Party Disaster Recovery Solutions

For disaster recovery configuration of the virtual machine, you can use any vendor-provided solutions to augment the DR capabilities. Refer to the vendor-specific documentation for configuration details.

VMware DR Solutions

- **VMware Snapshots** — In addition to the Intersight Virtual Appliance Backup and Restore functionality, VMware also provides VM snapshot for preserving the state and data of the virtual machine. Preserving the state includes the VM's power state, and preserving data includes all the files including the disk, memory, and other devices' virtual network interface cards. It is highly recommended that you power-off the appliance (VM) before you take the VM snapshot. For more information about VM snapshot, refer to the relevant documentation on the VMware website.
- **Intersight Virtual Appliance deployed on VMware vSphere** — VMware provides multiple solutions for DR:
  - VMware-SRM (VMware Site Recovery Manager)
  - VMware-VRS (VMware vSphere Replication)

Microsoft Hyper-V DR Solutions

Microsoft Hyper-V includes a set of built-in features that provides an efficient VM disaster recovery. Hyper-V virtual machine DR can be performed either by backing up or replicating VMs. Both options have certain aspects that should be considered when creating a DR plan. For more information, refer to the relevant documentation on the Microsoft website.

KVM Hypervisor DR Solutions

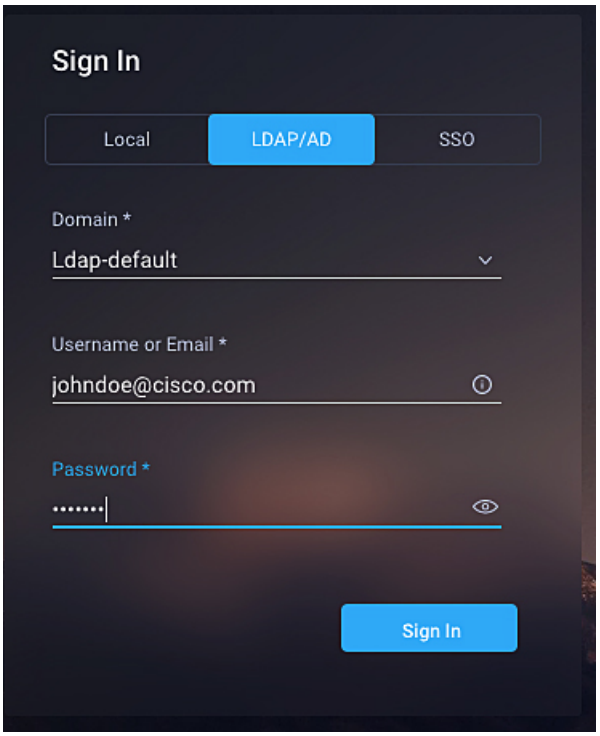
KVM is supported by multiple Operating Systems (OS) vendors. The most common OS vendors are Red Hat Virtualization and Ubuntu. For DR-specific solutions for Intersight Virtual Appliance deployed on KVM, refer to the documentation provided by the OS vendor.

For other approved Third-Party DR solutions, refer to the installation document of the Third-Party.

Logging In to Intersight Virtual Appliance

Logging In to Intersight Virtual Appliance

After installing Intersight Virtual Appliance, you can log in to the appliance as a user in one of the methods detailed below. The LDAP/AD and SSO tabs appear after you configure LDAP settings or SSO for the account.



- **Local User**—Use **admin** as the username, and use the same password that you set at the time of registering the appliance. If the password you set at the time of registering 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. Intersight supports only one local user (admin).
- **LDAP/AD**—Select the LDAP domain that you have configured, enter a **Username** or **Email** and the password that you have set up on the LDAP server. The username you use to log in must be the same as the **sAMAccountName** that you configure for the user in the LDAP server. For more information see LDAP Configuration, Add Users, and Adding a Group.
- **SSO**—Enter the email ID that you have used to set up SSO in the Identity Provider. Single Sign-On (SSO) authentication enables you to use a single set of credentials to log in to multiple applications. For more information about SSO, see Setting up SSO.

For Local User Only —If the local user login fails as a result of an incorrect username or password, details of the failed login information will be logged in Audit Logs. You will be able to view the details of the failed login, in Audit Logs, after you successfully log in to the appliance.

Creating an Appliance Account for Downloading Software Packages

In order to complete an Intersight Private Virtual Appliance deployment, or manually update Intersight Connected Virtual Appliance, you will need to access the Appliance Account so that you can download the Intersight Virtual Appliance, Hyperflex, or Cisco UCS Director software packages.

Note It is highly recommended that you check the Appliance Account regularly for updates and remain on the latest version of the Intersight Virtual Appliance software as it is continuously improved to include new features and enhancements. It is also important to note that only "N-3" software versions of the product are supported, with "N" being the latest version of appliance software.

Ensure that the version of the software that you are manually uploading for installation is always higher than the running version.

Use the steps in this task to create an Appliance Account:

Step 1 Log in to https://www.intersight.com/pvapp using your Cisco ID. If you do not have a Cisco ID, you can create one here.

Note: You will need to log in to https://www.intersight.com/pvapp only for creating an Appliance Account. After you have created the Appliance Account, you can access it by logging into Intersight.

Step 2 Accept the offer description and click **Next**.

Step 3 Enter a name for the Appliance Account in the **Appliance Account Creation** screen.

Step 4 Click **Create**.

After the Appliance Account is successfully created, you can log into Intersight to access the account and download the required Intersight Private Virtual Appliance, HyperFlex, or Cisco UCS Director software packages.

To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.

Note Account Administrators can enable users and groups to be able to access any of the Appliance Accounts that have been created. For more information on how to add users and groups, see Adding a User, on page 90 and Adding a Group, on page 91.

Downloading Software Packages for Intersight Virtual Appliance

Use the steps in this task to download Intersight Virtual Appliance, Cisco Hyperflex, and Cisco UCS Director software packages.

Note To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.

Before you begin

Ensure that you have created an Appliance Account. If you have not created an Appliance Account, see Creating an Appliance Account for Downloading Software Packages, on page 51.

Step 1 Log into Intersight using your Cisco ID. If you do not have a Cisco ID, you can create one here.

Step 2 Select the account that you created for accessing the Appliance Account.

The Software Download page is displayed. You can download the required software packages from the list displayed on this page.

You can proceed to upload the software on to the appliance. For more information, see Uploading Software Packages for Intersight Private Virtual Appliance, on page 52.

After uploading the software packages, you can install them on the claimed targets. To upgrade connector packs on Cisco UCS Director targets, see Upgrading Connector Packs on UCS Director Instances.

Note The ESXi software package is also downloaded as part of the Hyperflex software package. Hence, you do not have to download a separate ESXi software package.

Uploading Software Packages for Intersight Private Virtual Appliance

Intersight Private Virtual Appliance is intended for environments where you operate data centers in a disconnected (air gap) mode. Hence, you must download software packages from either the Cisco Software Central site or by accessing the Appliance Account on Intersight, and then uploading them on to the appliance.

Use this procedure to upload software packages for your Private Virtual Appliance.

Before you begin

Ensure that you have downloaded the required software packages as follows:

- To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.
- To download Cisco HyperFlex, Cisco UCS Director or Intersight Private Virtual Appliance software packages, you will need to access your Appliance Account. For more information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

Step 1 From the left navigation panel, click **Software Repository** > **Software**.

Step 2 Click **Upload Software**.

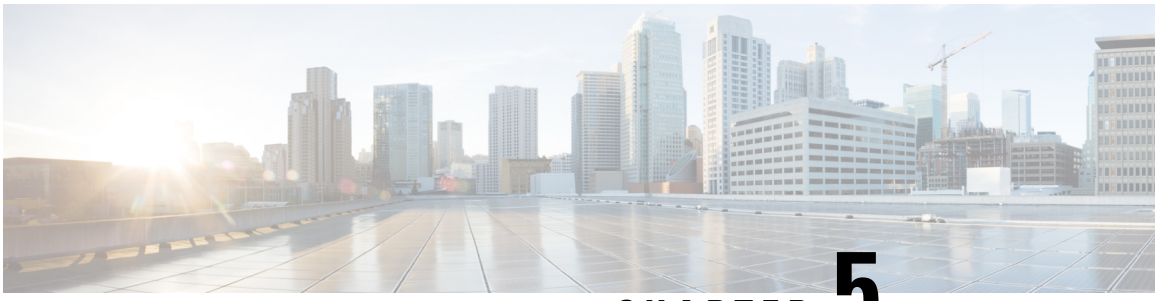
The Upload Software page is displayed.

a) Select either **Local Machine** or **Network Share**, depending on where you saved the software packages, and then click **Next**.

b) For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file.

- **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
- **Server IP/Hostname**—The network share server from where the file is copied
- **Port**—TCP port to use
- **Location**—Directory where the file to be copied is stored
- **Filename**—Name of the file to be copied from the network share
- **Username**—User name for authenticating with the network share
- **Password**—Password for authenticating with the network share

You can track the upload progress by clicking on the **Requests** icon. When the upload process completes successfully, the software that you uploaded will appear on the Software Repository page.



CHAPTER 5

Software Update

Updating the Intersight Connected Virtual Appliance Software

Intersight Connected Virtual Appliance provides a way to either update the software automatically when new versions are made available by the update service, or to manually update to any available version that is higher than the running version.

When Connected Virtual Appliance is configured to update in the **Automatic** mode, which is the default mode, it obtains the software directly from the cloud to update the service packages, OS packages including the kernel, and other security fixes. Based on the selection made during the configuration, installation will occur as per the grace period or will occur as per the custom installation schedule. In the automatic mode, if there are no new updates available for more than 90 days, ensure that the appliance is connected to Intersight.

Note

- It is recommended that you use the **Automatic** mode for updating the appliance software.
- There is no difference between a software upgrade on a multi-node appliance versus a software upgrade on a single-node appliance as the software upgrade is done at the cluster-level and not at the node-level.

When the appliance is configured to update in the **Manual** mode, you have a choice of either uploading the software image from the local machine or from a network share server, depending on where you saved the software image. Once the software image is uploaded, you can choose to install the update immediately, or you can schedule a date and time for the installation. Note that you need to download the required software packages from the Appliance Portal for manually updating your Connected Virtual Appliance. For more information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

Note It is highly recommended that you check the Appliance Account regularly for updates and remain on the latest version of the Intersight Virtual Appliance software as it is continuously improved to include new features and enhancements. It is also important to note that only "N-3" software versions of the product are supported, with "N" being the latest version of appliance software.

Ensure that the version of the software that you are manually uploading for installation is always higher than the running version.

Use the following instructions to configure a software update for **Connected Virtual Appliance**:

Before you begin: Ensure that Intersight Connected Virtual Appliance is connected to Intersight.

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Software**. The following details about the installed software are displayed:

In the Automatic mode of configuration, the following details are displayed:

- **Running Version**—The current software version number
- **Update Mode**—Automatic
- **Installation Schedule**—Displays the date and time when the update is scheduled

In the Manual mode of configuration, the following details are displayed:

- **Running Version**—The current software version number
- **Update Mode**—Manual

In both the modes, you may see the following details about the **Pending Update**:

- **Version**—Indicates the software version that is scheduled to be updated
- **Update Impact Type**—This could be **Disruptive**, **Disruptive-reboot**, or **None**. The impact could be disruptive because of an infrastructure upgrade or upgrade of other Intersight services. A disruptive update may cause Intersight to be unavailable for the duration specified in **Update Impact Duration**. The disruptive reboot of the appliance could be caused by kernel updates and restarting of services. A grace period is provided to help you plan and manage the update better. The UI displays appropriate messages to guide you if there is a disruptive reboot.

  Attention An appliance update could take about 90 minutes to complete.

  During this time, some features will be temporarily unavailable.

  It is recommended that you take a backup prior to triggering the update and do not reboot your appliance. If there is a requirement to reboot, Intersight Appliance does it automatically.

- **Installation Date/Time** —Displays the date and time when the update is scheduled. You can click on the pencil icon to edit the installation date and time.
- **Release Notes**—Link to the release notes for the pending software update

The **Software** page also displays a table view of the appliance software updates under **Update History**. This table lists the installation date, appliance software Version, a description of the software version, and the status of the installation

of the update. From this table view, you can search for a specific version of the software and the date it was installed on and the status of the installation.

Step 3 Click **Update Settings** to configure a software update.

Step 4 On the **Update Settings** page, make your selections for the update mode of configuration by choosing either the automatic or the manual mode.

For the Automatic mode:

a. Select **Automatic** mode of update.

b. Select between **System Default** and **Custom** for the installation schedule. When you select **System Default**, Intersight will install the update as per the grace period. When you select **Custom**, you can define the recurrence and Installation time for the update. The appliance will be updated automatically when an update is available, based on the selected installation schedule.

c. Enable **Blackout Dates** and specify a **Blackout Start Date** and **Blackout End Date** for an update blackout window and click **Save**. **The blackout window prevents the system from auto-updating the appliance.**

Attention The blackout window cannot be defined if the appliance has not been updated in the past 90 days. The blackout window duration cannot exceed 90 days.

d. Choose a strategy to update Intersight intelligence. For more information, see Updating Intersight Intelligence for Intersight Connected Virtual Appliance , on page 74.

e. Click **Save.**

For the Manual mode:

a. Select **Manual** mode of update.

Choose a strategy to update Intersight intelligence. For more information, see Updating Intersight Intelligence for Intersight Connected Virtual Appliance , on page 74.

b. Click **Save**.

c. From the appliance UI, navigate to **Settings** icon > **Settings** > **GENERAL** > **Software**, and click **Install Updates**.

The **Upload Appliance Software** page is displayed.

d. Select either Local Machine or Network Share, depending on where you saved the software image.

1. For the **Local Machine** option, browse to the location from where you want to upload the software and click **Next**.
2. For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file, and click **Next**.
   - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
   - **Server IP/Hostname**—The network share server from where the file is copied
   - **Port**—TCP port to use
   - **Location**—Directory where the file to be copied is stored
   - **Filename**—Name of the file to be copied from the network share
   - **Username**—Username for authenticating with the network share

- **Password**—Password for authenticating with the network share

3. Select to install immediately or to schedule the installation to a later date and time.
4. Click **Apply**.

a. You can track the upload progress by clicking on the **Requests** icon.

When the upload completes, you will see details about the **Pending Update** on the **Software** page. From the **Pending Update Details** section, you will be able to cancel an update, update immediately, or edit the installation date and time.

Note In the Manual mode, if you cancel a pending update, you will need to upload the appliance software again to be able to initiate an update.

Note If the update fails and if the update is recoverable, the **Update History** shows the installation as **Failed**, and the existing **Pending Update Details** remains as-is. You can try the upgrading process again. Contact Cisco TAC if you are unable to update successfully.

If the update fails and if the update is non-recoverable, the **Update History** shows the installation as **Failed**, and you will no longer see any existing **Pending Update Details**. However, all existing features and functionality continues to work as before. Contact Cisco TAC if you encounter an update failure.

After the update, if you use the same browser to log in to the appliance, you might encounter an Error code: *SEC_ERROR_REUSED_ISSUER_AND_SERIAL*. To fix this issue, you will need to remove the system-generated certificate of the server from the same browser that you are using to log in to the appliance. For example, to remove the system-generated certificate of the server from Google Chrome, navigate to **Settings** > **Privacy and security** > **Manage certificate**. Select the system-generated certificate that you want to remove, click **Remove**, and click **Close**. Close the browser, and then log in to the application from a new browser. For more information about certificate, see Certificates, on page 84.

Updating the Intersight Private Virtual Appliance Software

Intersight Private Virtual Appliance provides a way to manually update the software to any available version that is higher than the running version. You have a choice of either uploading the software image from the local machine or from a network share server, depending on where you saved the software image. Once the software image is uploaded, you can choose to install the update immediately, or you can schedule a date and time for the installation.

You can download the required software packages from the Appliance Portal for manually updating your Private Virtual Appliance. For more information, see Creating an Appliance Account for Downloading Software Packages, on page 51 and Downloading Software Packages for Intersight Virtual Appliance, on page 51.

Note

- It is recommended that you use the **Automatic** mode for updating the appliance software.
- There is no difference between a software upgrade on a multi-node appliance versus a software upgrade on a single-node appliance as the software upgrade is done at the cluster-level and not at the node-level.
- There is no difference between a software upgrade on a multi-node appliance versus a software upgrade on a single-node appliance as the software upgrade is done at the cluster-level and not at the node-level.

Before you begin: Ensure that you have downloaded the required software packages from the Appliance Account for upgrading your Intersight Private Virtual Appliance. For more information on how to create the Private Appliance Account, see Creating an Appliance Account for Downloading Software Packages, on page 51.

To configure a software update for **Private Virtual Appliance**, do the following:

Step 1 Log in to Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Software**. The following details about the installed software are displayed:

In the Automatic mode of configuration, the following details are displayed:

- **Running Version**—The current software version number
- **Update Mode**—Automatic

You may see the following details about the **Pending Update**:

- **Version**—Indicates the software version that is scheduled to be updated
- **Update Impact Type**—This could be **Disruptive**, **Disruptive-reboot**, or **None**. The impact could be disruptive because of an infrastructure upgrade or upgrade of other Intersight services. A disruptive update may cause Intersight to be unavailable for the duration specified in **Update Impact Duration**. The disruptive reboot of the appliance could be caused by kernel updates and restarting of services. A grace period is provided to help you plan and manage the update better. The UI displays appropriate messages to guide you if there is a disruptive reboot.

  Attention An appliance update could take about 90 minutes to complete.

  During this time, some features will be temporarily unavailable.

  It is recommended that you take a backup prior to triggering the update and do not reboot your appliance. If there is a requirement to reboot, Intersight Appliance does it automatically.

- **Installation Date/Time** —Displays the date and time when the update is scheduled. You can click on the pencil icon to edit the installation date and time.
- **Release Notes**—Link to the release notes for the pending software update

The **Software** page also displays a table view of the appliance software updates under **Update History**. This table lists the installation date, appliance software Version, a description of the software version, and the status of the installation of the update. From this table view, you can search for a specific version of the software and the date it was installed on and the status of the installation.

Step 3 Click **Install Updates**.

The Upload Software page is displayed.

Step 4 On the **Update Settings** page, make your selections for the update mode of configuration by choosing either the automatic or the manual mode.

For the Automatic mode:

a. Select either **Local Machine** or **Network Share**, depending on where you saved the software image.

1. For **Local Machine**, browse to where you saved the software image, and then click **Next**.
2. For the **Network Share** option, enter the protocol and enter details of the remote server from where you want to copy the file.
   - **Protocol**—Communication protocol used for the file transfer. SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) are supported.
   - **Server IP/Hostname**—The network share server from where the file is copied
   - **Port**—TCP port to use
   - **Location**—Directory where the file to be copied is stored
   - **Filename**—Name of the file to be copied from the network share
   - **Username**—Username for authenticating with the network share
   - **Password**—Password for authenticating with the network share
3. Select to install immediately or to schedule the installation to a later date and time.
4. Click **Apply**.

You can track the upload progress by clicking on the **Requests** icon.

When the upload completes, you will see details about the **Pending Update** on the **Software** page. From the **Pending Update Details** section, you will be able to cancel an update, update immediately, or edit the installation date and time.

Note If you cancel a pending update, you will need to upload the appliance software again to be able to initiate an update.

Note If the update fails and if the update is recoverable, the **Update History** shows the installation as **Failed**, and the existing **Pending Update Details** remains as-is. You can try the upgrading process again. Contact Cisco TAC if you are unable to update successfully.

If the update fails and if the update is non-recoverable, the **Update History** shows the installation as **Failed**, and you will no longer see any existing **Pending Update Details**. However, all existing features and functionality continues to work as before. Contact Cisco TAC if you encounter an update failure.

After the update, if you use the same browser to log in to the appliance, you might encounter an Error code: *SEC_ERROR_REUSED_ISSUER_AND_SERIAL*. To fix this issue, you will need to remove the system-generated certificate of the server from the same browser that you are using to log in to the appliance. For example, to remove the system-generated certificate of the server from Google Chrome, navigate to **Settings** > **Privacy and security** > **Manage certificate**. Select the system-generated certificate that you want to remove, click **Remove**, and click **Close**. Close the browser, and then log in to the application from a new browser. For more information about certificate, see Certificates, on page 84.

Updating the Intersight Assist Software

Cisco Intersight Assist software is auto-upgraded from Intersight Cloud, when new versions are made available by the upgrade service. If there are no new upgrades available for more than 90 days, ensure that Intersight Assist is connected to Intersight. Intersight Assist can be upgraded automatically from the cloud directly to update the service packages, OS packages including the kernel, and other security fixes. The appliance UI provides guidance about the upgrade including the impact of the upgrade, and any service interruptions. You can schedule an upgrade to occur automatically when an update is available during a weekly maintenance window.

Use the following instructions to configure a software upgrade schedule:

Before you begin

Ensure that Cisco Intersight Assist is connected to Intersight.

Step 1 Log into Intersight Assist as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Software**. The following details about the installed software are displayed:

New Version section:

- **Version**—The available software version number.
- **Upgrade Impact Type**—This could be **Disruptive**, **Disruptive-reboot**, or **None**. The impact could be disruptive because of an infrastructure upgrade or upgrade of other Intersight services. A disruptive update may cause Intersight to be unavailable for the duration specified in **Upgrade Impact Duration**. The disruptive reboot of the appliance could be caused by an update to the operating system or other component changes. A grace period is provided to help you plan and manage the upgrade better. The UI displays appropriate messages to guide you if there is a disruptive reboot.

Attention An Assist upgrade could take up to 90 minutes to complete.

During this time, some features will be temporarily unavailable.

It is recommended that you take a backup prior to triggering the upgrade and do not reboot your appliance. Do not reboot the appliance manually while the appliance is upgrading. If there is a requirement to reboot, Intersight Assist does it automatically.

- **Scheduled to Install On**—Date and time at which the new version is scheduled to be installed. When the upgrade is triggered, a progress bar displays the status of the update.
- **Features** section—Lists the features, enhancements, and defect fixes that are part of the new software version.

Depending on your upgrade schedule preferences, you can wait for the automatic upgrade on the scheduled install time or install the new version immediately by clicking **Install Now**.

Note Any new software version must be upgraded within seven days. If not, the Intersight Assist automatically completes the upgrade service.

The following details about the currently installed software are also displayed:

- **Version**—Currently installed appliance software version.
- **Schedule**—Displays one of the following upgrade status:
  - Automatic—If you have chosen automatic updates and scheduler is not configured
  - Day and Time, if a specific update time is scheduled
  - Click the pencil icon in the **Schedule** field to specify the following details:
    a. Select an update strategy to update the appliance. Choose **Automatic** or a **Weekly Maintenance Window**. When you choose the **Automatic** option, the appliance will be updated automatically when an update is available. Upgrade is auto triggered if the upgrade service detects any pending update during the interval, once the grace period expires. You can view details of the upgrade from **Settings** > **Software**.

    b. When you choose the **Weekly Maintenance Window** option, select the **Day of Week** and the **Time of Day** within the following week to initiate the upgrade process. The schedule is an interval from the time of the day it was set until the end of the day. Upgrade is triggered based on the specific time and day of the week selected in the schedule. The Weekly Maintenance Window option upgrades only if an update is available.

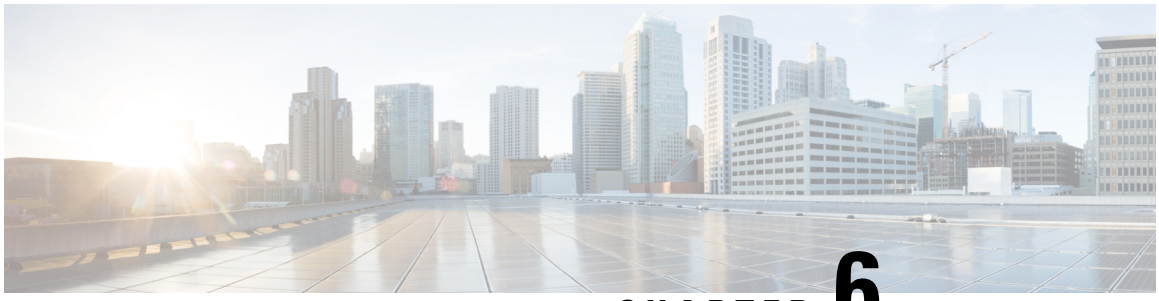
    c. Choose a strategy to update Intersight intelligence. The **Update Intersight Intelligence Immediately** option is enabled by default. It allows you to update Intersight intelligence such as Hardware Compatibility List (HCL) as soon as it becomes available, independent of the appliance software upgrade schedule. For more information, see Updating Intersight Intelligence for Intersight Connected Virtual Appliance , on page 74.

- **Update History**—A table view of the appliance software updates. This table lists the **Installation Date**, appliance software **Version**, a **Description** of the software version, and the **Status** of the installation of the update. From this table view, you can search for a specific version of the software and the date it was installed on and the status of the installation.

Note If the upgrade fails and if the upgrade is recoverable, the **Install Now** button remains enabled. You can try the upgrading process again. Contact Cisco TAC if you are unable to upgrade successfully.

If the upgrade fails and if the upgrade is non-recoverable, the **Install Now** button is disabled. However, all existing features and functionality continues to work as before. Contact Cisco TAC if you encounter an upgrade failure.

After the upgrade, if you use the same browser to log in to the appliance, you might encounter an Error code: *SEC_ERROR_REUSED_ISSUER_AND_SERIAL*. To fix this issue, you will need to remove the system-generated certificate of the server from the same browser that you are using to log in to the appliance. For example, to remove the system-generated certificate of the server from Google Chrome, navigate to **Settings** > **Privacy and security** > **Manage certificate**. Select the system-generated certificate that you want to remove, click **Remove**, and click **Close**. Close the browser, and then log in to the application from a new browser. For more information about certificate, see Certificates, on page 84.



CHAPTER 6

Dashboard Settings

Intersight Virtual Appliance Settings

You can monitor the appliance status, back up and restore data, upgrade the appliance software, configure network settings, add users and groups, and more on the Intersight Virtual Appliance **Settings** page.

Settings Option	Description
GENERAL > **Account Details**	View account details such as account name, account ID, access link, license type, default idle timeout, maximum number of concurrent sessions per user, and default session timeout. You can also configure account settings such as default idle timeout, default session timeout, and maximum number of concurrent sessions per user For more information, see Configuring Account Settings, on page 76.
GENERAL > **Access Details**	Displays the details of the user including the name, account name, email ID, role, idle timeout, session timeout, maximum concurrent sessions per user, login time, a brief description of the role, and a table view of the users and their privileges that is displayed in the bottom pane of this page.
GENERAL > **Appliance**	View the status of the appliance connection, view details including the appliance Health, Hostname, Version number, Deployment Size, and Data Collection policy. A list of the connected Nodes displays the IP address, Status, Gateway, and Netmask for the connected nodes. You can also view the Alarms on the connected nodes.
GENERAL > **Backup**	Create a full state backup of the appliance and save the image on a remote server. You can also schedule a backup from this page. For detailed instructions, see Create Backup and Scheduling Backup. You can recover the appliance configuration from a backup file using the instructions in Recovering Intersight Connected Virtual Appliance , on page 44 and Recovering Intersight Private Virtual Appliance , on page 45.
GENERAL > **Banner Message**	View the configuration details of the banner message. When enabled, the configured banner message will be displayed before the user login screen. For more information, see Configuring a Banner Message for Displaying Before the Login Screen, on page 76.
GENERAL > **Software**	View details of the current software version of the appliance, including the version number, the installed components, messages about the installation, and the Fingerprint of the installed software. For more information about updating the Intersight Virtual Appliance software, see Updating the Intersight Connected Virtual Appliance Software.

Settings Option	Description
General > **Device Connector**	**Note** This setting is applicable only for Connected Virtual Appliance deployments. View the status of the appliance connection to Intersight, the Access Mode, Device ID, and the Claim Code. From the **Settings** Menu in the Device Connector window, you can add an **HTTPS Proxy**. For more information, see Cloud Connection for Intersight Connected Virtual Appliance, on page 75.
NETWORKING > **DNS**	Configure DNS settings and add IPv4 DNS Server Addresses and Alternate IPv4 addresses of the DNS Servers. For more information, see Configuring DNS , on page 77.
NETWORKING > **NTP**	Configure NTP servers as well as edit existing NTP server settings. For more information, see Configuring NTP , on page 77.
NETWORKING > **External Syslog**	Configure the External Syslog settings including enabling and disabling sending audit logs and information of alarms to the external syslog servers. For more information, see Configuring External Syslog, on page 78.
AUTHENTICATION > **LDAP/AD**	Create and configure the settings for LDAP servers, DNS parameters, Binding methods, Search parameters, and Group Authorization preferences. For more information, see Configuring LDAP Settings , on page 82.
AUTHENTICATION > **Single Sign-On**	Set up Single Sign-on (SSO) authentication. SSO enables you to use a single set of credentials to log in to multiple applications. With SSO authentication, you can log in to Intersight with your corporate credentials instead of your Cisco ID. For more information about Single Sign-On in Intersight, see Single Sign-On with Intersight Virtual Appliance, on page 83.
AUTHENTICATION > **Certificates**	Add a trusted certificate to verify TLS communication with the LDAP or HTTPS server. You can generate a Certificate Signing request or Generate a Self-Signed Certificate. For more information, see Certificates, on page 84.
AUTHENTICATION > **Local Users**	View details of the current password policy configuration or configure a new password policy. For more information, see Configuring Password Policy for Local Users, on page 87.

Settings Option	Description
ACCESS & PERMISSIONS > **Users**	View the users or add new users to allow access to Intersight using their email, specify identity provider and permission settings. For more information, see Adding a User, on page 90.
ACCESS & PERMISSIONS > **Groups**	View the user **Groups** or add a new group for Single Sign-On or LDAP-based authentication. For more information, see Adding a Group, on page 91.
ACCESS & PERMISSIONS > **Roles**	View the existing roles or create a custom role and assign privileges. For more information, see Adding a Role.
ACCESS & PERMISSIONS > **Organizations**	View the list of organizations or create a new organization to manage access to your logical and physical resources. For more information, see Adding an Organization
API > **API Keys**	View a list of the existing API Keys in the account or generate a new API Key. For more information, see API Keys.
OAuth2 Tokens	View a list of OAuth2 tokens and the details of the Apps and the associated targets.

Intersight Virtual Appliance Monitoring

Intersight Virtual Appliance provides an overview of the appliance and health status and displays alarms when predefined limits are exceeded or when a threshold is raised.

In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Appliance** to view the following details under **Appliance**:

- **Health**—Overall status of the appliance
- **Hostname**—Your FQDN or hostname
- **Version**—Installed version of the appliance software
- **Deployment Size**—Appliance deployment size. For detailed information about Deployment size, see Supported Configuration Limits for Intersight Virtual Appliance, on page 11
- **Node**—A table view of the list of appliance nodes in Cisco Intersight Virtual Appliance. You can search for a specific node by the IP Address, Operational Status, Gateway, or Netmask. You can view the alarms on the right pane and filter them by their severity.

Intersight Virtual Appliance monitors certain critical parameters and raises alarms when predefined limits are exceeded or when a threshold is raised. The appliance currently reports system-level and node-level alarms. The following table shows the alarm levels and their descriptions:

Table 8: Alarms in Intersight Virtual Appliance

Level	Component	Description	Comments
System	Node	A node is down	One alarm per node
System	Node	A node is not ready for service deployment.	One alarm per node
Node	CPU Usage	CPU usage above threshold	One alarm per node. Threshold: 75%
Node	Memory Usage	Memory usage above threshold	One alarm per node. Threshold: 75%
Node	File System Disk Usage	File System disk usage above threshold	One alarm per file system. Threshold: 75%
System	Number of service instances running	Number of service instances running less than expected	One alarm for any service down
System	Number of service instances ready	Number of service instances ready less than expected	One alarm for any service down
System	Web certificate	Warning: Web certificate expires within 120 days Critical: Web certificate expires within 90 days	One alarm per appliance
System	Device certificate	Warning: Device certificate expires within120 days Critical: Device certificate expires within 90 days	One alarm per appliance
System	Appliance Backup	Warning: An Intersight Appliance backup has not been created within the past week. Please schedule or create a new backup.	One alarm per appliance
System	Appliance Backup	Critical: The most recent Intersight Appliance backup failed. Please schedule or create another backup.	One alarm per appliance

Level	Component	Description	Comments
System	Cloud Connectivity	Warning: Connection to Intersight cloud has been down for more than 30 days Critical: Connection to Intersight cloud has been down for more than 60 days Highly Critical: Connection to Intersight cloud has been down for more than 90 days;claiming new devices is not permitted until connection is restored.	One alarm per appliance
Node	Network Link Connectivity	Warning: The latency between cluster nodes is greater than 10ms	One alarm per link per node

Note Cisco UCS C-Series server-related faults such as power supply and fan failures are not forwarded by Intersight Virtual Appliance to an external syslog server. Please configure the external syslog server on the UCS C-Series CIMC side to handle the forwarding of the UCS C-Series events and faults.

Backing Up Data

Backing up of Cisco Intersight Virtual Appliance regularly is essential. Without regular backups, there is no automatic way to reconstruct the configuration settings and recreating the profiles and policies. You can perform a regular backup once a day using a scheduled backup or create backup on demand if there is a data loss or corruption event. Cisco Intersight Virtual Appliance enables you to take a full state backup of the data in the appliance and store it in a remote server. If there is a total site failure or other disaster recovery scenarios, the restore capability enables you to do a full state system restore from the backed-up system data.

The following options are available to backup data:

- **Create Backup**—Creates a full state backup of the data in Cisco Intersight Virtual Appliance on demand and saves the backed-up data on a remote server.
- **Schedule Backup**—Schedules a full state periodic backup of the data in the appliance based on the schedule and saves the backed-up data on a remote server.

Note There is no difference between a backup that is running on a multi-node appliance versus one that is running on a single-node appliance. The backup is done at the cluster level and not at the node level. The backup originates from one node, but there is no restriction on which node the backup originates from.

Note

- When you take a backup of the Intersight Virtual Appliance, the metrics collection data is not backed up.
- When you capture a snapshot of the Intersight Virtual Appliance VM, note the following storage size specifications:
  - **Without Metrics Collection**: The snapshot size on disk is 180 GB.
  - **With Metrics Collection Enabled**: The snapshot size on disk exceeds 1 TB.

For more information, see the Resource Requirements section in Cisco Intersight Virtual Appliance and Intersight Assist Getting Started Guide.

Create Backup

You can create a full state periodic backup of the Intersight Virtual Appliance and save the backed-up file on a remote server. To create a backup, do the following:

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Backup**.

Step 3 Click **Create Backup**.

The **Backup** window displays.

Step 4 Enter the following details:

- **Protocol**—Communication protocol option used in the backup process. Intersight Virtual Appliance currently supports CIFS (Common Internet File System), SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) for backup. Enter details of the remote server where you want to save the backed up data.
- **Remote Host**—The remote host for saving the backup files.
- **Remote Port**—Remote TCP port on the backup server (applicable only for SCP and SFTP).
- **Remote Path**—Directory where the backup files are saved.

  Note CIFS share names must contain alpha-numeric characters only and must conform to the regular expression such as *^(\w+)(/\w+)*/?$*. It cannot contain spaces. In addition, when specifying folders under the CIFS share, forward slash (/) must be used as a separator. For example, *backupshare/Intersight/Daily* and *backupshare/Monthly*.

- **Filename**—Name of the backup file to restore.
- **Username**—Username for authenticating the backup client to the backup server.

- **Password**—Password for authenticating the backup client to the backup server.
- **Password Confirmation**—Reenter the password to complete validation.

Step 5 Click **Start Backup**.

Scheduling Backup

Schedule Backup enables you to schedule a periodic backup of the data in the Intersight Appliance. The Appliance can store three copies of the backup locally on the appliance.

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Backup**.

Step 3 On the **Schedule Backup** window, enable **Use Backup Schedule**.

If you disable this option, you must enable the **Use Backup Schedule** option to schedule a backup.

Step 4 Provide the following details to complete creating the **Backup Schedule**.

- **Backup Schedule**
  - **Day of Week**—Specify the day in the week when you want to schedule a data backup.
  - **Time of Day**—Specify the time in the selected day when you want to schedule a data backup. The Time of Day follows the browser time of your session and displays your local time of the day.
- **Backup Destination**
  - **Protocol**—Communication protocol (CIFS/SCP/ STFP) used in the backup process.
  - **Remote Port**—Remote TCP port on the backup server (applicable only for SCP and SFTP).
- **Remote Host**—The remote host for saving the backup files.
- **Remote Path**—Directory location where the backup files are saved.

  Note CIFS share names must contain alpha-numeric characters only and must conform to the regular expression such as *^(\w+)(/\w+)*/?$*. It cannot contain spaces. In addition, when specifying folders under the CIFS share, forward slash (*/*) must be used as a separator. For example, *backupshare/Intersight/Daily* and *backupshare/Monthly*.

- **Filename**—Name of the backup file to restore
- **Username**—Username for authenticating the backup client to the backup server.
- **Password**—Password for authenticating the backup client to the backup server.
- **Password Confirmation**—Reenter the password
- **Backup Retention**—Number of backups to retain

  Click **Enable Backups Retention** to enter the number of backups to retain on the remote server. The default number is 15. You can enter a number from 1 to 100.

Note In order for the backup retention limits to function properly while using the SCP protocol, ensure that the SFTP protocol is also enabled on your remote host.

For more information regarding the various backup retention scenarios, see Backup Retention Scenarios.

Step 5 Click **Schedule Backup** to complete the process.

Backup Retention Scenarios

The following table describes the various backup retention scenarios and the expected outcomes.

Table 9: Backup Retention Scenarios

Backup Retention Scenarios	Expected Outcomes
You enable backup retention, allow backups to accrue, and then disable backup retention.	The backups taken under the retention policy will not be deleted.
You enable backup retention, allow backups to accrue, and then disable backup retention. Now, you re-enable backup retention again.	The backups taken when retention was originally enabled will not be affected. Only backups taken after retention has been re-enabled will be part of the retention policy.
You change the file path or hostname in the retention policy.	The backups taken before the change will not be affected. Only backups taken after the policy change will be part of the latest retention policy.
You increase the number of backups	Backups will continue to accumulate as part of the retention policy until the maximum number of backups is reached and then the oldest backup will be deleted.
You decrease the maximum number of backups from X to Y.	The older backups in the original retention policy will no longer be part of the policy. This means that the retention policy will be implemented only on the most recent backups for the number, Y. The backups before that will remain as-is. For example: Suppose you had a retention count of 5 and then you decrease the retention count to 3. In this case, the oldest 2 backups in the original retention policy will not be affected. Retention policy will be enabled only on the 3 backups.

-

Configuring Metrics Collection

Metrics collection within the Intersight Virtual Appliance is disabled by default. After you install or upgrade Intersight Virtual Appliance, to start metrics collection, you must enable metrics collection in the Intersight Virtual Appliance on the **Metrics** page.

In addition, the **Metrics** page displays the active server count along with the threshold limits for the Intersight Virtual Appliance.

Note Metrics collection can be enabled or disabled for the entire Intersight Virtual Appliance, not for individual devices.

To enable or disable metrics collection, do the following:

1. Log into **Intersight Virtual Appliance** as a user with the account administrator role.
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Metrics**.
3. Click **Configure**.
4. Use the **Enable Metrics** slider to enable or disable the metrics collection.

Note

- Enabling metrics collection results in the immediate triggering of metrics gathering from the endpoints.
- Disabling metrics collection may result in a delay of up to one hour before the configuration changes are complete and the collection of metrics stops.

5. Click **Configure**.

Updating Intersight Intelligence for Intersight Connected Virtual Appliance

Intersight Connected Virtual Appliance allows you to update Intersight intelligence such as Hardware Compatibility List (HCL) as soon as it becomes available, independent of the appliance software upgrade schedule. Updates for HCL include the compatibility validation results and compliance status for server model, processor, firmware, adapters, operating system and drivers. For more information about HCL, see Compliance with Hardware Combability List (HCL).

Use the following instructions to update Intersight intelligence:

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Software**.

Step 3 Click the pencil icon in the **Schedule** field.

The **Set Update Schedule** window displays.

Step 4 Select **Update Intersight Intelligence Immediately** and click **Save**.

Cloud Connection for Intersight Connected Virtual Appliance

Cisco Intersight Connected Virtual Appliance is connected to Cisco Intersight through an embedded device connector. The device connector provides a secure way for the connected targets to send information and receive control instructions from Cisco Intersight, using a secure Internet connection. You can view the following details of the connection to the Cloud and also configure the settings from the **Device Connector** page.

1. In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Device Connector**. The **Device Connector** window displays.

   You can view details such as Device ID, Claim Code, Access Mode, and device connector status. For more information about configuring the device connector, status, and error conditions, see **Configuring Device Connector** in **Resources**.

2. Click **Settings** and configure the following settings.

   - **General**—Enable **Device Connector** so that you can claim the appliance and leverage the capabilities of Cisco Intersight, and select an Access Mode. If the Device Connector option is disabled, no communication is allowed to Cisco Intersight. Click **Save**.
   - **Proxy Configuration**
     - Enable **Enable Proxy**. Add the **Proxy Hostname** or **IP Address**, and the **Proxy Port**. The proxy port must be in the range from 1 and 65535.
     - Enable **Authentication** and add a Username and Password for Authenticated Proxy. The proxy setting is automatically reset after restore, and you must manually reset the appliance proxy.

       Click **Save**.
   - **Certificate Manager**—Import proxy certificates.

Alerts Based on Connection to Intersight

When connection to Intersight cloud is interrupted and the connectivity is not restored with in 90 days, target claim capability will be lost. Intersight Appliance features including Connected TAC, Firmware Upgrade, HyperFlex Cluster Deployment, and User Feedback that require connectivity to Intersight cloud may also be impacted until connectivity is restored. Upon re-establishing connectivity, you can resume target claim operations and use all other functionality as before.

Intersight raises these alarms and warnings to alert you about the impact of the disrupted connectivity:

- **Warning**—A warning is displayed the Intersight appliance UI to alert you about the operational status. This is displayed between 30-60 days of lost connectivity. During this period, there will be no disruption to the normal operations of the appliance and you can continue to claim and manage targets.
- **Fault**—A fault is displayed between 60-90 days and after 90 days of interrupted connectivity. Until 90 days of loss of connectivity, you can continue to claim and manage targets in the appliance. If connectivity

is not restored after 90 days, target claim will be blocked. You must restore connectivity to claim targets and resume regular operations.

Configuring Account Settings

This task provides details on how to configure account settings in Intersight Virtual Appliance.

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Account Details**.

You can view the details of the existing account settings.

Step 3 Click **Configure**.

The **Configure Account Settings** window displays.

Step 4 Update the following fields as needed.

- **Account Name**—Name of the account.
- **Default Idle Timeout (Seconds)**—Provide the idle timeout interval for the web session in seconds. The system default value is 18,000 seconds (5 hours).
- **Default Session Timeout (Seconds)**—Provide the session expiry duration in seconds. The system default is 57,600 (16 hours).
- **Maximum Concurrent Sessions per User (Sessions)**—Provide the maximum number of concurrent sessions allowed per user. The system default as well as the maximum number of concurrent sessions is 32.
- **Audit Logs Retention Period (Months)**—Provide the time-period for audit logs retention. The system default is 48 months. The allowed range is between 6 months and 48 months. The Audit logs deletion task is set to run on a daily basis at 6.00 AM UTC, and all the audit logs that meet the retention period set in this field will automatically start getting deleted at this time. Once deleted, audit logs cannot be retrieved.

Step 5 Click **Save**.

Configuring a Banner Message for Displaying Before the Login Screen

This task provides details on how to configure a banner message in Intersight Virtual Appliance. When enabled, the configured banner message will be displayed before the user login screen.

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERALBanner Message**.

Step 3 Click **Configure**.

The **Configure Banner Message** window displays.

Step 4 Update the following fields.

- **Show banner message before login**—Enable this option.
- **Banner Title**—Enter a title for the banner message. The length of the title cannot exceed 128 characters.
- **Banner Content**—Enter the contents for the banner message. The content in this field has to be less than 2000 characters.

Step 5 Click **Save**.

The configured banner message content along with the title is displayed in the **Banner Message** preview window.

Configuring DNS

This procedure explains how to configure/**Edit** DNS settings in Cisco Intersight Virtual Appliance.

Step 1 Log into Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **NETWORKING** > **DNS**.

The details of the existing DNS settings displays.

Step 3 Click **Edit DNS**. The **Configure DNS** window displays.

Step 4 Update the following properties.

- **Preferred IPv4 DNS Server**—Provide the IP address of the primary DNS server.
- **Alternate IPv4 DNS Server**—Provide the IP address of the secondary DNS server.

Step 5 Click **Save**.

Configuring NTP

It is mandatory to have at least one Network Time Protocol (NTP) configured in Cisco Intersight Virtual Appliance to enable synchronizing the time on the appliance with the NTP servers. The authentication schema for the NTP servers can be either unauthenticated or authenticated. You can add up to 4 unauthenticated NTP servers and 4 authenticated NTP servers during the initial setup of the appliance and edit them later, if necessary.

Use the information in the following task to configure a NTP server.

Step 1 Log into Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **NETWORKING** > **NTP**.

The details of the existing NTP settings displays.

Step 3 Click **Configure**.

The **Configure NTP** window displays.

Step 4 Click **Add NTP Server**, to add a new NTP server.

a) Click +.

b) Enter a server hostname or an IP address for the **Server Name** and click **Save** to save the NTP server as an unauthenticated one.

c) Enable the **Enable NTP Authentication** button to add the NTP server as an authenticated one.

Enter the following information.

- **Server Name**—Server hostname or IP address
- **Symmetric Key Type**—Type of symmetric key to use for this server
- **Symmetric Key ID**—Positive integer that identifies a cryptographic key used to authenticate NTP messages
- **Symmetric Key Value**—Value of the symmetric key

d) Click **Save**.

To edit existing NTP server configurations, click + on any of the configured NTP servers, make your edits as needed, and save the edited configurations.

Configuring External Syslog

Intersight Virtual Appliance provides you the ability to configure up to five external syslog servers. When you enable external syslog in Intersight Virtual Appliance, you can export the following types of logs and alarms based on the details provided when configuring the external syslog.

- **Web Server Logs**—Web server access logs for all transactions involving user session activities.
- **Audit Logs**—Audit logs for events such as login, logout, created, modified, and deleted, that are displayed in the Audit Logs screen in Intersight Virtual Appliance.
- **Alarms** —All Intersight alarms including appliance alarms that provide alerts about a failure (fault) in the managed target or when a threshold has been crossed. For information about alarms in Intersight, see Alarms. For more information about alarms in Intersight Virtual Appliance, see the *Alarms in Intersight Virtual Appliance* table in Intersight Virtual Appliance Monitoring.

Attention

- In Intersight Virtual Appliance, you can use the TLS, UDP, and TCP protocols to provide secure communication to the external syslog server. However, it is strongly recommended that you use **only** TLS in your production environment.
- UCS C-Series server-related faults such as power supply and fan failures are not forwarded by Intersight Virtual Appliance to an external syslog server. Please configure the external syslog server on the UCS C-Series CIMC side to handle forwarding of the UCS C-Series events and faults.

To configure external syslog in Intersight Virtual Appliance, do the following:

Before you begin

Ensure that you have added the certificate for the external syslog server where you want to send the web server log, audit logs, and alarms in Intersight Virtual Appliance. This certificate is used to verify TLS communication with the external syslog server. For more information about how to add certificates, see Certificates, on page 84.

- If you plan on using FQDN in the **Hostname/IP Address** field while configuring the external syslog server, set up the certificate for the external syslog server with a proper FQDN entry in the Common Name or the DNS entry in the Subject Alternative Names. Enter this information in the **Hostname/IP Address** field while configuring the external syslog.
- If you plan on using either IPv4 or IPv6 address in the **Hostname/IP Address** field while configuring the external syslog server, set up the certificate for the external syslog server with the IP address in the Common Name. Enter this information in the **Hostname/IP Address** field while configuring the external syslog.

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **NETWORKING** > **External Syslog**.

You can view the details of the existing external syslog settings.

Step 3 Click **Add External Syslog Server**.

The **Add External Syslog Server** window displays.

Step 4 Update the following fields as needed.

- **Enable External Syslog**—When enabled, the Web Server Access Logs, Audit Logs, and Alarms are sent to the configured external syslog server as per the configuration details provided in the **Hostname/IP Address**, **Port**, **Protocol**, and **Minimum Severity of Alarms to Report** fields. Note that the **Minimum Severity of Alarms to Report** field is applicable only for **Alarms**.
- **Web Server Access Logs**—When enabled, you will be able to export the web server access logs for all transactions involving user session activities.

  Note It is highly recommended that you do not enable this option as it will quickly overpopulate your log files. This option is mainly made available for customers that require the ability to export web server access logs.

- **Audit Logs**—When enabled, the audit logs for events such as login, logout, created, modified, and deleted, that are displayed on the Audit Logs screen are sent to the configured external syslog server.
- **Alarms**—When enabled, the Intersight alarms including appliance alarms that provide alerts about a failure (fault) in the managed target or when a threshold has been crossed are sent to the configured external syslog server.
- **Hostname/IP Address**—Enter either FQDN, an IPv4 address, or an IPv6 address. This information must match the details that you provided in the certificate for the external syslog server.
- **Port**—Port to use for the external syslog server

- **Protocol**—Select a protocol from the drop-down list. It is strongly recommended that you use **only** TLS in your production environment.
- **Minimum Severity of Alarms to Report (Applicable for Alarms Only)** —Select either Warning, Info, or Critical as the minimum severity level for alarms to get reported. When the alarms of selected severity and above are cleared at the endpoints, the notification for the same also gets exported to the external syslog server.

Step 5 Click **Add**.

Configuring SMTP Settings for Email Notifications

Networking systems and software frequently create alarms that indicate a concerning event or a trend has been detected. Email notifications automatically poll for recent alarms, determine their severity, and direct concerning ones to a user's email address based on a rule you create.

To configure email notifications in Intersight Virtual Appliance, perform the following two tasks:

- Configure Simple Mail Transfer Protocol (SMTP) settings
- Create notification rules

Configuring SMTP settings

To configure SMTP settings, perform the following steps:

1. Log into Intersight Virtual Appliance as a user with account administrator role.
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **NETWORKING** > **SMTP**.

   You can view the details of the existing SMTP settings. If this session is your first instance of configuring SMTP for email notifications, the appliance displays default or no values in the fields.
3. Click **Configure**.
4. Enable the SMTP toggle button to configure email notifications.
5. In the SMTP Server Address field, type the IP address or domain name of the server in your domain that sends email notifications.
6. In the SMTP Port list, type or select the port number of the server that performs the email notification forwarding.

   Port 25 is the standard SMTP Relay port. Ports 465 or 587 are secure mail routing ports. The value range for port selection is 1 through 65535, and the default is 25.
7. In the SMTP Sender Name field, type the email address of the user that sends email notifications.
8. (Optional) Enable the TLS toggle button.

   TLS is a form of authorization that provides security by verifying the certificate authority (CA) of the SMTP email server. To apply TLS security, select the CA you want to apply from the list in the TLS region.

9. (Optional) Enable the Authentication toggle button, if your SMTP server requires authentication, and provide the username and password used to authenticate to the SMTP server.
10. Click **Configure**.

Next, complete the steps for creating notification rules.

Creating Notification Rules

Notifications are based on a rule you set for incoming alarms.

To configure an email notification rule, perform the following steps:

1. In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **GENERAL** > **Notifications**.

   You can view the notification rule list populated with the existing rules.

   Each rule is used as both a condition for notification generation (Alarms column) and a notification destination (Email column). If this session is your first time creating a notification rule for the email address set in the SMTP Sender Name in the Configure SMTP screen, no existing rules display in the list. The list displays the following columns:

   - **Name**—The name of the rule.
   - **Enabled**—The administrative state of the rule. A **Yes** setting indicates the rule is active, and will generate email notifications when the rule conditions are met. A **No** setting indicates the rule is inactive, and will not generate email notifications.
   - **Email**—The email address to which notifications will be sent.
   - **Alarms**—The required severity of an event for it to generate a notification.
   - **Last Updated**—The last time the notification was configured, either during a creation or an editing session. The timestamp is in the following format: <*day*>:<*hour*>:<*minute*>.

2. Click the **Add Rule** button in the upper right portion of the screen.

   The **Add Rule** screen displays.

3. To configure a rule, the **Enable Rule** toggle button MUST be enabled.
4. In the Name field, type a string of up to 32 characters that you want to be the name of the rule.
5. In the Email field, type an email address to which you want generated email notifications sent. Click the (+) icon to enter additional email addresses for other destinations.

Note You can create up to three email destinations for email notifications.

6. In the Severity region, select an urgency level of an alarm you want to be reached for a notification email to be sent.

   The urgency levels for alarms are Critical (the most urgent), Warning (second-least urgent), and Info (no urgency). You can select one or multiple urgency levels. In the case of multiple Severity settings, the least urgent level will be the one, when reached, that triggers an email notification to be sent.

7. Click **Add**.

The following warning message displays.

```
WARNING! Email notifications may contain sensitive data. Ensure the emails
contain no typos and are approved to receive data.
```

8. Click **Continue**.

   Intersight returns to the Notifications screen displaying the new rule in the list.

Limitations

Note the following restrictions for configuring email notifications.

- You can configure up to three emails per rule.
- You can configure up to five rules per account.
- Events are collected in a sliding time window of 10 seconds. Intersight initially waits a 10-second period where it polls for alarms. If an alarm or multiple alarms are detected in this initial period, Intersight waits an additional 10-second period to detect alarms. If it detects alarms in this period, additional periods occur until no alarms are detected. Once an additional 10-second period elapses with no alarms detected, Intersight bundles the discovered alarms into an alarm group and sends an email containing the alarms to the specified address.
- An email address can be associated with up to 100 alarms and the number of emails sent depends on how large the alarm group is. If an alarm group contains more than 100 alarms, then an additional email is sent. Some events may generate 1,000 alarms. In that case, 10 emails are sent.

Configuring LDAP Settings

Intersight Virtual Appliance supports LDAP/AD based remote authentication. You can configure the appliance to authenticate a user login using LDAP. You can configure multiple LDAP domains and choose a domain for the login.

An LDAP user can log in to Intersight Virtual Appliance with email ID or username, and select the corresponding domain in which the LDAP user is configured. You can add up to 6 LDAP domains per Intersight Account. You can view the list of configured LDAP domains in **Settings icon** > **Settings** > **NETWORKING** > **LDAP/AD** table view. Watch this video to learn how to integrate your virtual appliance with the LDAP/AD services.

To set up LDAP authentication in Intersight Virtual Appliance, do the following:

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **NETWORKING** > **LDAP/AD**.

The **Configure LDAP** window displays.

Step 3 On the **Configure LDAP** page, add the corresponding details in the fields that are listed below, and click **Save**.

- **Name**—Enter a name to easily identify the LDAP domain that you are configuring.
- **Base DN**—Enter a Base Distinguished Name (DN) for the server. For example, DC=Intersight, DC=com.
- **Bind DN**—Enter a DN used to authenticate against LDAP server and the password for the user.

- **Group Attribute**—Enter the Group member attribute to which an LDAP entry belongs. Cisco Intersight Virtual Appliance uses this Group attribute to map/assign Intersight roles to the user. The default value is **member** and you can change it from **Edit LDAP** settings.
- **Password**—Enter a DN password for the user.
- **Nested Group Search**—When enabled, an extended search runs through the chain of ancestry all the way to the root and returns all the groups and subgroups that each of the groups and subgroups belong to, recursively.
- **Enable Encryption**—You must enable Encryption to secure the communication over the LDAP server. If encryption is enabled, a trusted root certificate has to be added. For more information, see *Adding Certificates*.
  - In a future release, Intersight Virtual Appliance will be phasing out support for certificates signed with the SHA-1 hash functions. It is strongly recommended that you upgrade your certificates to use signature algorithms with hash functions that are stronger than SHA-1, such as SHA-256, SHA-384, or SHA-512.
  - Certificates created for the LDAP server must include Subject Alternative Names (SANs) since the use of Common Name has been deprecated. Certificates without SANs will fail verification, resulting in connectivity issues.
- In **Server**—Add an LDAP Server IP address or hostname. Cisco Intersight Virtual Appliance supports only one LDAP provider and port.

  Attention
  - LDAPS is supported on Port 636 and Port 3269. All other ports support LDAP on TLS.
  - **Intersight Virtual Appliance uses the email ID or username to log in an LDAP user**. If you want to use email ID to log in to the appliance, configure the mail attribute in the LDAP server. If you want to use the username, use the **sAMAccountName** configured for that user in the LDAP server.
  - **After you add the required details to configure LDAP settings, wait for the DeployApplianceLDAP workflow to complete before you add a User or Group to assign appropriate roles to LDAP users. You can check the status of the workflow in Requests. For more information, see Adding a User or** Adding a Group**.**
  - **If you are using the Intersight API to configure the Appliance LDAP login, ensure that the LDAP policies are tagged appliance.management:true. This is automatically done for the users configuring the LDAP under Settings.**

  After you add the required details to configure LDAP settings, wait for the **DeployApplianceLDAP** workflow to complete before you log in as an LDAP user. You can check the status of the workflow in **Requests**.
- In **Port**—Add the LDAP Server port.

Single Sign-On with Intersight Virtual Appliance

Single Sign-On (SSO) authentication enables you to use a single set of credentials to log in to multiple applications. With SSO authentication, you can log in to Intersight with your corporate credentials. Intersight supports SSO through SAML 2.0, and acts as a service provider (SP), and enables integration with Identity Providers (IdPs) for SSO authentication.

To set up SSO through the appliance, you must log in to Cisco Intersight Virtual Appliance as a user with administrator role, download the SP metadata, and register your Identity Provider (IdP) in the Intersight Virtual Appliance.

IdP Requirements

The IdP you add to Intersight must support SAML 2.0 and a service provider initiated SSO. The most commonly used IdPs have different instructions to complete the setup.

Note If you have a multi-node cluster setup for Intersight Virtual Appliance or if you are expanding from a single-node configuration to a multi-node cluster configuration, for some IdPs such as Okta you must manually configure the three SSOs, while for other IdPs such as ADFS you can directly import the xml file. For IdPs where the SSO configuration is a manual one, you must configure the three different SSO URLs specified in the metadata file downloaded from the appliance SSO screen. Once the three URLs are configured, you can proceed with the SSO login from any one of the three nodes.

Additional requirements for a multi-node cluster setup in appliance:

- SLO (Single Logout) is supported for a multi-node setup in appliance, but there is only one SLO endpoint. If the node specified in the SLO URL is down, then SLO will not work. In this case, you will only be logged out of Intersight.
- The IDP initiated SSO works only for the entity node.

For more information about setting up SSO with Intersight and examples of adding an Identity Provider, see, Single Sign On with Intersight. Click here to watch a video that shows how to enable Intersight Single Sign-On and set up a custom SAML 2.0 application in an external Identity Provider (IdP) with Intersight.

Certificates

To provide secure authentication to external targets (such as LDAP servers), you can add a third-party certificate from a trusted source that affirms the identity of your targets or add a self-signed certificate for secure **HTTPS** access of the appliance through the browser.

- In a future release, Intersight Virtual Appliance will be phasing out support for certificates signed with the SHA-1 hash functions. It is strongly recommended that you upgrade your certificates to use signature algorithms with hash functions that are stronger than SHA-1, such as SHA-256, SHA-384, or SHA-512.
- Certificates created for the LDAP server must include Subject Alternative Names (SANs) since the use of Common Name has been deprecated. Certificates without SANs will fail verification, resulting in connectivity issues.

Trusted Certificates

To provide secure authentication while connecting to external targets, you can add a third-party certificate from a trusted source or a self-signed certificate that affirms the identity of your targets. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA), an intermediate CA, or a trust anchor that is part of a trust chain that leads to a root CA.

The **Trusted Certificates** table view that is accessible from **Systems** > **Settings** > **AUTHENTICATION** > **Certificates** >**Trusted** displays the list of certificates that you added in Intersight.

Add Certificate

The following task provides details on how to add trusted certificates in Intersight Virtual Appliance.

1. Log into Intersight Virtual Appliance as a user with account administrator role.
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **AUTHENTICATION** > **Certificates** > **Trusted**.

   The following details about the Trusted Certificates are displayed in the table view:

   - **Name**—Common name of the CA certificate
   - **Issued By**—Certificate issuing authority
   - **Usage**—Displays the number of targets using the certificate
   - **Expires**—The expiry date of the certificate

3. Click **Add Certificate** to add a trusted certificate.
4. Click **Browse** to select the certificate that is stored in your system and click **Save**. After the certificate is successfully imported, it is displayed in the **Trusted Certificates** table view.

Important The trusted certificate that you want to import must be in base64 encoded X.509(PEM) format.

Adding SSL Certificates

To enable secure **HTTPS** access of the appliance through the browser, you can generate a Certificate Signing Request and import a certificate, or you can switch to a self-signed certificate. You can access these tasks by navigating to **System** > **Settings** > **AUTHENTICATION** > **Certificates** > **SSL** in the Intersight Virtual Appliance UI.

Note While migrating from a single-node deployment to a multi-node cluster configuration, if the SSL certificate is already generated on the single-node deployment, once the migration to the multi-node cluster configuration is complete and the cluster is in a **Healthy** state, then delete and regenerate the SSL certificate.

To create a Certificate Signing Request (CSR):

1. In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **AUTHENTICATION** > **Certificates** > **SSL**.

   The following details about the **Current Certificate** are displayed:

   - **Name**—Common name of the CA certificate
   - **Added By**—User that added the certificate to the account
   - **Issued By**—Certificate issuing authority

- **Expires**—Expiration date of the certificate

Click **View All** to display the **View Certificate** window. In addition to the details listed above, you can also view these details about the certificate: Fingerprints, Country, Locality, Organization, Organizational Unit, and the details of the Issuer Name, Organization, Common Name, and the Signature Algorithm.

2. From the **Action** drop-down menu, select **Create CSR**.

   The **Create Certificate Signing Request** wizard displays. Enter the following details as required.

   - Organization—The legal name of your organization
   - Organizational Unit—The subdivision of your organization that handles the certificate. For example HR, IT etc
   - Locality—The city/town where your organization is located
   - State—The state where your organization is located
   - Country—The two-letter country code where your organization is located. For a complete list of the country codes, see ISO 3166
   - Email Address—An email address used to contact your organization
   - Modulus—Modulus of the RSA private key used to sign the CSR

3. Click **Create CSR**.

When you click **Create CSR**, a new Certificate Signing Request (CSR) is generated. You can select one of the following options:

- **Download CSR**—Allows you to download and store the CSR locally to use it to obtain a trusted certificate from a **Certificate Authority** (CA).

Note Use only the appliance FQDN in the Subject Alternative Names (SAN) field during the certificate-issue request process. Do not enter hostnames or IP addresses in the SAN field while obtaining a trusted certificate for Intersight Appliance and Intersight Assist from a Certificate Authority.

- **Delete CSR**—Delete the CSR if you do not want to use it to generate a trusted certificate.
- **Apply Certificate**—After the CA issues a certificate, click **Apply** to paste the contents of the certificate in the **Certificate** field in the **Apply Certificate** window. You can also click the **Upload** button and upload a certificate. Click **Apply** to complete the process. The CA-issued certificate can be in *.csr*, *.pem* or *.crt* format.

To switch to a self-signed certificate:

1. In the appliance UI, from the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **AUTHENTICATION** > **Certificates** > **SSL**.
2. From the **Action** drop-down menu, select **Switch to Self-Signed**.

   A popup window appears warning you that switching to self-signed certificates will take a few minutes.

3. Click **Apply** to proceed.

   - Cisco recommends that you use CA signed certificates to access the appliance. The latest browsers may disable access to the appliance if self-signed certificates are used. Intersight Virtual Appliance provides the option to switch to self-signed certificate to extend the validity of the certificate, if the self-signed certificate provided by Cisco expires.
   - When you choose to switch to a self-signed certificate, the current SSL certificate will be replaced by the newly generated self-signed certificate. You can verify if the new certificate is applied by clicking the lock or the warning icon preceding the URL in the address (location) bar of your browser. After the refresh, you will be taken directly to the **Settings** > **Certificates** page without having to log into the appliance once again.

Configuring Password Policy for Local Users

This task provides details on how to configure password policy for local users in Intersight Virtual Appliance.

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **AUTHENTICATION** > **Local Users**.

You can view the details of the existing password policy.

Step 3 Click **Configure**.

The **Configure Local Users** window displays.

Step 4 Configure the password policy by updating the following password policy options as needed.

Password Policy Options	Allowed Range/Default Value
Minimum Length of Password	8-127 characters Default is 8
Minimum Number of Required Upper Case Characters	1-64 characters Default is 1
Minimum Number of Required Lower Case Characters	1-64 characters Default is 1
Minimum Number of Required Numeric Characters	1-64 characters Default is 1
Minimum Number of Special Characters	0-64 characters Default is 0 **Note** Special characters include punctuation and symbol characters.

Password Policy Options	Allowed Range/Default Value
Number of Previous Passwords Disallowed	0-10 Default is 0
Minimum Number of Characters Different From Previous Password	0-15 Default is 0 **Note** Differences from the previous password are verified based on the same character location within the specified password.
Minimum Days Allowed Between Password Changes	0-7 days Default is 0 **Note** If you specify a value of 0 for this password policy option, then the user is not limited on time between password changes.
Time Duration for Incorrect Login Attempts (Seconds)	300 - 3600 seconds (5 – 60 minutes) Default is 1800 seconds (30 minutes) Time duration is tracked for consecutive incorrect login attempts. Users will be locked out if they exceed the configured number of max incorrect login attempts during this duration. For more information about the lockout capability, see Locking Out Local Users Accounts.
Max Consecutive Incorrect Login Attempts Allowed	3 -10 Default is 5 Users will be locked out after exceeding the max consecutive incorrect login attempts allowed within the configured time duration.
Enable Lockout for Admin User	Default is false. Determines if the user lockout feature must be enabled for the local “admin” user. This option is always enabled for other local users. For more information about the lockout capability, see Locking Out Local Users Accounts.
Lockout Time Period (Seconds)	60 – 3600 seconds (1 – 60 minutes) Default is 900 (15 minutes) Duration, in seconds, during which a local user account will remain locked. The account is automatically unlocked after the configured lockout time period elapses.

Step 5 Click **Save**.

You can verify the password policy changes on the next password change.

Locking Out Local Users Accounts

Consecutive incorrect login attempts within a configured time duration are tracked for local users and the accounts will be locked out if they exceed the configured number of maximum incorrect login attempts during this duration. Once the local user account is locked, the Local User table displays a warning icon next to the user. The account is automatically unlocked after the configured lockout period elapses. The Account Administrator or the User Access Administrator can unlock the account by resetting the password, during the configured lockout period.

Note The lockout capability:

- Applies to only local users and does not apply to remote users.
- Applies to local “admin” user only if the setting is enabled.

Resetting the Password of Local Users

Account Administrators can reset the password of local users. User Access Administrators can also reset the password of local users except for users with the role of Account Administrator.

To reset the password of a local user:

1. Log into Intersight Virtual Appliance as a user with account administrator role.
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **ACCESS & PERMISSIONS** > **Users**.
3. Select the local user that you want to reset the password.
4. Click the pencil icon and change the password.
5. Click **Save**.

Attention When an Account Administrator resets the password for the local “admin” user, only the GUI password is changed. The SSH password of the local “admin” user remains unchanged. The local “admin” user must log into the appliance using the newly reset password. Once the local “admin” user is logged in, a prompt appears that mandates the local “admin” user to change the password, which then resets both the GUI and the SSH passwords.

Adding a User

Intersight Virtual Appliance allows you to override Group role assignments to users. On the **User** page, you can view a list of the Users added to an account. The list displays the **Name**, **Identity Provider**, **Email**, **Role**, and the **Last Login Time** for a user. You can add Remote Users as well as Local Users. Note that you can add up to 100 Local Users.

- Remote Users—authenticated via IDP (LDAP and SSO)
- Local Users—authenticated via Intersight Virtual Appliance

Attention You must be an Account Administrator or User Access Administrator to create a user or assign user roles.

Use these instructions to add a user in Intersight Virtual Appliance:

Step 1 Log into Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **ACCESS & PERMISSIONS** > **Users**.

Step 3 In the **Add User** window, add the following details:

You have the option of adding a Remote User or a Local User. Note that you can add up to 100 Local Users.

To add a Remote User, enter the following details:

- **Identity Provider**—Select the Identity Provider that you want to add to this account. This can be any one of the Intersight validated Identity Providers. For more information, see **Validated Identity Providers** in the Supported Systems page in *<Your FQDN>/help*.

  If you add an LDAP user, you must add them under the appropriate Identity Provider (IDP). The name of the IDP will be the same as the LDAP Domain Name that you have configured in LDAP Settings.

- **User ID**—Enter a valid email ID or username used to register the account with the Identity Provider. **The username must be the same as the sAMAccountName that is configured on the LDAP server**. If you are using email to log in, ensure that the email ID is the same as configured in the mail attribute in the LDAP server.

- **Role**—You can assign one role for a remote user account. For more information, see Roles and Privileges.

To add a local user, enter the following details:

- **First Name**—First name of the local user
- **Last Name**—Last name of the local user
- **User ID**—Enter an email ID or username which is used by the local user to log into the appliance.
- **Password**—Enter a valid password as per the local user password policy.
- **Role**—You can assign multiple roles for a local user account. For more information, see Roles and Privileges.

Step 4 Click **Save** to add the new user to your account.

Attention The UserID and password that is entered while adding the new local user must be conveyed to the new local user directly as there is no mechanism currently in Intersight Virtual Appliance to automatically notify the login credentials to the new local user. Once the new local user logs in using these credentials, a prompt appears that mandates the new local user to change the password.

Local users can change their passwords any time by navigating to **Profile Menu** in the top right of the screen and then clicking **Change Password**.

Adding a Group

A Group represents a collection of users with a specific role, permission, and privileges. You can create multiple user groups to assign common roles and privileges to a set of users. On the **Group** page, you can view a list of the Groups added to an account. The list displays the **Name**, **Identity Provider**, **Role,** and the **Group Name in Identity Provider**. Use these instructions to add a group:

Step 1 Log into Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **ACCESS & PERMISSIONS** > **Groups**.

Step 3 Click the **Add Group** button at the top right. The **Add Group** window displays.

Step 4 In the **Add Group** window, add the following details:

- **Identity Provider**—Select the Identity Provider you want to add to this account. This can be any one of the Intersight validated Identity Providers. For more information, see **Validated Identity Providers** in the Supported Systems page in *<Your FQDN>/help*. You must select the appropriate LDAP domain for groups that would log in with their LDAP credentials.
- **Name**—Enter a name to identify the group in Intersight.
- **Group Name in Identity Provider**—Enter the user group name you have added in the Identity Provider. Group name must be in the LDAP distinguished name (DN) format. For example:

  ```
  cn=Finance,cn=Users,dc=example,dc=com
  ```

- **Role**—You can assign one of following System Defined roles to a user group as well as assign User Defined Roles.
  - **Account Administrator**—In this role, members of the group can claim targets, cross launch element managers, create profiles and policies, collect tech support bundles, and make configuration changes to the claimed targets or the account.
  - **Read-Only**—In this role, members of the group can view details, and status of the claimed targets within the account. However, you cannot make any configuration changes to the claimed targets or the account.
  - **Device Technician**—In this role, members of the group can claim a target in Intersight and view a list of the claimed targets in the Targets table view.
  - **Device Administrator**—In this role, members of the group can claim a target in Intersight, view a list of the claimed targets, and delete (unclaim) a target.
  - **Server Administrator**—In this role, members of the group can perform all server actions including firmware upgrade, collect tech support bundles, set server tags, create, edit, and deploy a server profile or policy, and view server details.

- **HyperFlex Cluster Administrator**—In this role, members of the group can create, edit, and deploy a HyperFlex cluster profile, upgrade a cluster, set cluster tags, view cluster dashboard and summary, collect tech support bundles, monitor alarms, and launch and manage **HX Connect**.
- **User Access Administrator**—In this role, members of the group can view account details, perform all User Access related actions, including adding a User, adding a Group, setting up Identity Providers and Single Sign-On, generate API keys related to the account.

Attention You must be an Account Administrator or User Access Administrator to create a group or assign user roles.

Step 5 Click **Save** to add the new group to the account.

Adding a Role

Creating a User Defined Role

In addition to the system-defined roles in Intersight, you can create a user-defined role. On the **Roles** page, you can view a list of the roles added to an account. This list displays the **Name**, **Type**, **Usage**, **Scope**, and a **Description** of the roles. Use these instructions to create a user-defined role:

Attention **Only users with Account Administrator or User Access Administrator privileges can create a user-defined role.**

1. Log into Cisco Intersight.
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **ACCESS & PERMISSIONS** > **Roles**.
3. From **Roles**, click **Create Role**.
4. Enter a **Name** to identify the role in Intersight and a **Description** about the usage of the role.

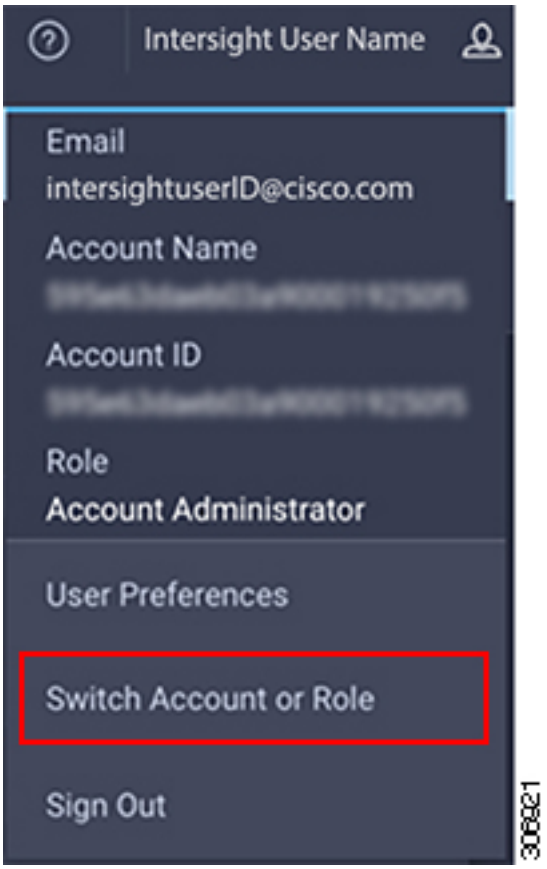
   You can choose to retain the default account level settings for Session Timeout, Idle Timeout, and Concurrent Sessions, or you can choose to customize these settings.
5. Under **Session & Idle Timeout** settings, you can choose to do one of the following:
   - Enable **Use Account Default Settings**—This option is enabled by default. You can inherit the session timeout values from the Account level settings. The values will be used as the default settings during role creation. To check the account level Session Timeout and Idle Timeout details, navigate to the **Settings** icon > **Settings** > **General** > **Account Details**.
   - Disable **Use Account Default Settings**—You can disable this option to set values for the following fields at the Role level.
     - **Session Timeout (Seconds)** is the session expiry duration in seconds. The minimum value is 300 seconds and the maximum value is 31536000 seconds (1 year). The system default value is 57600 seconds.

- **Idle Timeout (Seconds)** is the interval for the web session in seconds. When a session is not refreshed for this duration, the session is marked as idle and removed. The minimum value is 300 seconds and the maximum value is 18000 seconds (5 hours). The system default value is 1800 seconds.
- **Maximum Number of Concurrent Sessions (Sessions)** is the number of concurrent sessions allowed in an account or permission. The minimum number of sessions is 1 and maximum number of sessions is 128. The default value is 128.

6. Click **Next**.
7. Select a **Scope** to delegate the user access to resources in the account. You can choose to give a user access to the entire account or restrict access to a selected organization.
   - **All**—User has access to all account resources. Add Privileges to assign roles to the user. The selected privileges will be applied to the entire account.
   - **Organization**—User has access to the specified organizations only. Select one or more **Organizations** from the drop-down list and **Add Privileges** to assign roles to the user. For more information on Privileges, see the **Roles** section.
8. Click **Create** to add the new User Defined Role to the account.

Switching an Account or Role

You can switch between accounts or roles in Cisco Intersight without logging out of the application. If you are logged into multiple accounts or roles, the **Profile** menu in the Intersight dashboard provides the option to **Switch Account or Role**.



Note

- The Switch Account or Role option is not available if you are authorized to access a single account, and have only one role mapped to that account.
- If you use the account URL to log in to Intersight, the **Switch Account and Role** option enables you to switch only between roles within the same account.
- At the time of switching, accounts are re-evaluated based on the attributes returned by the Identity Provider (IdP) after authentication. The users added to the account are also re-authenticated for their roles by the Identity Provider. Therefore, before you switch between accounts, if Intersight detects that there is a change in your account or role, it appears in the **Select Account and Role** list.
- For Intersight Virtual Appliance, you must configure LDAP or log in with SSO to view the Switch Account or Role option.

Use the following steps to switch accounts:

1. Navigate to **Profile** > **Switch Account or Role**. The **Select Account and Role** window displays.
2. In the **Select Account and Role** window, select the account (or role) that you want to switch to. You will be logged in to the new account.
3. To change the role, navigate to **Settings** > **ACCESS & PERMISSIONS** > **Users**, and select the user that you want to change the role for, and click the **Edit** icon.

4. In the **Edit User** window, select the role and click **Save**.

Adding an Organization

Creating an Organization

On the **Organizations** page, you can view a list of organizations added to an account. This list displays the **Name**, **Memberships**, **Usage**, and **Description**. Use these instructions to add an organization:

Attention **Only users with Account Administrator privileges can create organizations. Users with User Access Administrator privileges cannot create organizations but can view them in the User Account and assign the organizations to roles.**

1. Log into Cisco Intersight.
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **ACCESS & PERMISSIONS** > **Organizations**.
3. From **Organizations**, click **Create Organization**.
4. Enter a **Name** to identify the organization in Intersight and a **Description** about the usage of the organization.
5. Under **Memberships**, you can choose to assign access to all resources or restrict access to a selective group of resources. Select one of the following options for memberships:
   - **Custom**—From the list of targets available in the account, select the required targets, to allocate a set of physical resources to the organization.

Important Profiles and Policies that are created within a custom organization are applicable only to the targets in the same organization.

   - **All**—All the targets available in the account will be included in this organization.
6. Click **Create** to add the new organization to the account.

To learn more about Organizations and how to leverage them to support multi-tenancy in an account, see the Role Based Access Control under Resources in the Help Center or <*https://your fqdn.com*>/help.

Generating and Managing API Keys

An API key is used to register your application with Cisco Intersight.

Step 1 Log into Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **API** > **API Keys**.

Step 3 In the **Generate New API Key** screen, enter the purpose for the API Key, and click **Generate**. The API Key ID and RSA Private Key are displayed.

Step 4 Save the private key information in a *.pem* file.

Note Make sure to save it in a location accessible from your scripts.

OAuth2 Tokens

You can view a list of OAuth2 tokens used by an application to access Intersight and the corresponding target details in the OAuth2 section under API.

Step 1 Log into Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the **Service Selector** drop-down list, choose **System**, and navigate to **Settings** > **API** > **OAuth2 Tokens**.

A table view of the OAuth2 tokens with the Application Name that uses the tokens, the Device Model, Login and Expiration time, the Client IP address, the User Role, and the Email ID is displayed.

Device Connector Requirements

You can claim a target in Cisco Intersight Virtual Appliance through the embedded device connector. Before you claim a target, ensure that the device connector requirements are met. The following table lists the software compatibility and the supported device connector versions for Intersight Virtual Appliance:

Table 10: Device Connector Requirements

Component	Minimum software version for Connected Virtual Appliance	Minimum software version for Private Virtual Appliance	Supported Device Connector version	Minimum supported versions that include supported Device Connectors
Cisco UCS Manager	3.2(1)	4.0(2a)	1.0.9-2290	4.0(2a)
Cisco IMC Software	For M5 Servers: 3.1(3a) For M4 Servers: 3.0(4)	4.0(2d)	1.0.9-335	4.0(2d)
HyperFlex Connect and Data Platform	2.6	3.5(2a)	1.0.9-1335	3.5(2a)
CIsco UCS Director	6.7.2.0	6.7.2.0	1.0.9-911	6.7.2.0

Device Connector Upgrade

When the Device Connector on an endpoint is not at the compatible version, you can upgrade it in the following ways:

- Perform a complete firmware upgrade to the version that has the supported Device Connector. This process could involve updating your configuration settings.
- Manually upgrade the Device Connector. This option is supported only on Cisco UCS Manager. For more information, See Manual Upgrade of Device Connector (applicable only to Cisco UCS Fabric Interconnect).
- Cisco Intersight Virtual Appliance supports upgrading the device connector from the cloud. When the target claim process detects that the device connector at the endpoint is not at the compatible version, it triggers an upgrade of the device connector from Intersight cloud. To facilitate this upgrade, port 80 must be open between the appliance and the endpoint target. The HTTPS proxy running on port 80 requires that your firewall settings allow communication through port 80.

  Device Connector upgrade from Intersight cloud is optional. During the upgrade from the cloud, some target data (server inventory) from the appliance leaves your premise. When you choose this option the following data leaves your premises:

  - The endpoint target type - Cisco UCS Fabric Interconnect, Integrated Management Controller, Cisco HyperFlex System, Cisco UCS Director
  - The firmware version(s) of the endpoint
  - The serial number(s) of the endpoint target
  - The IP address of the endpoint target
  - The hostname of the endpoint target
  - The endpoint device connector version and the public key

Attention Target claim could fail if the device connector is at an older version that does not support the appliance, and you have disabled the data collection option during the initial setup. This failure is caused due to details about the endpoint being required to leave the premises for the one time upgrade to work. To avoid a target claim failure, select the Enable Data Collection option temporarily or upgrade the device connector in the other methods mentioned above.

Manual Upgrade of Device Connector (applicable only to Cisco UCS Fabric Interconnect)

If you do not want to share the target data as part of the automatic device connector upgrade, you can choose to manually upgrade the device connector on a Cisco UCS Fabric Interconnect. Use these instructions to upgrade the device connector:

```
Log in to your UCS Fabric Interconnect as an admin user and run the following command:
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on local Fabric interconnect
```

```
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

Data Collected from Intersight Connected Virtual Appliance

Cisco Intersight Connected Virtual Appliance works in a connected mode and requires connectivity to hosted Intersight services. You must register the appliance with Intersight to manage your UCS or HyperFlex infrastructure.

If you enable the option to allow collecting additional information, Intersight may collect other details about the managed systems, beyond what is listed in the table **Minimum Data Collected**. When any of the options under **Data Collection** in the **Security & Privacy** screen of the appliance UI is enabled, Cisco reserves the right to collect more data for diagnosis and proactive troubleshooting purposes.

The tables below list the details of the minimum data collected by Intersight:

Table 11: Minimum Data Collected

Component	Details of Data Collected
From Intersight Virtual Appliance	• The appliance ID (Serial Number) • The IP address of the appliance • The hostname of the appliance • The device connector version and public key on the appliance
Appliance Software Auto-Upgrade	Version of software components or the services running on the appliance
Appliance Health	• CPU usage • Memory usage • Disk usage • Service statistics
Licensing	Server count
Information about the endpoint target	• Serial number and PID (to support Connected TAC) • UCS Domain ID • Platform Type

Table 12: Data Collected During One time Device Connector Upgrade

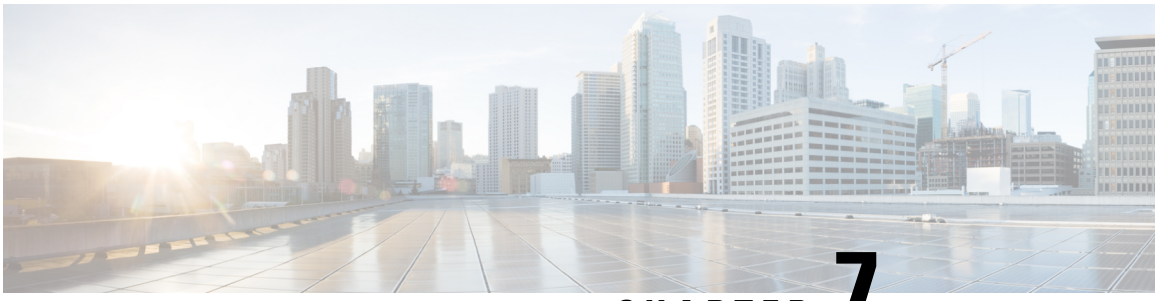
Component	Details of Data Collected
From the endpoint target, only if the one time device connector upgrade is used	• The endpoint target type - Cisco UCS Fabric Interconnect, Integrated Management Controller, Cisco HyperFlex System • One or more firmware versions of the endpoint • The serial number of the endpoint target • The IP address of the endpoint target • The hostname of the endpoint target • The endpoint device connector version and the public key

For information about Proactive Support, see Proactive Support enabled through Intersight.

For detailed information about the Proactive Support workflow, supported faults, configuring the advanced options, setting tags, and caveats, see Proactive RMA for Intersight Connected Devices.

Tech Support Diagnostic File Collection

When you open a case with Cisco TAC, Intersight collects Tech Support diagnostic files to assist with an open support case. The data collected could include (but is not limited to) hardware telemetry, system configuration, and any other details which aid in active troubleshooting of the TAC case. Tech Support collection is allowed to occur regardless of data collection options you specify. However, this information is not collected arbitrarily, but only when you open a case against a system, requiring assistance with the system support.



CHAPTER 7

Diagnostics

Maintenance Shell for Intersight Virtual Appliance and Intersight Assist

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 <*https://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 Virtual 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. Launch the Intersight Virtual Appliance Maintenance Shell using one of the following three options:
   - Open a console window in your hypervisor.
     a. From either VMWare vCenter or Microsoft Hyper-V Manager, navigate to your virtual machine and open a console window.
     b. Log in as the admin user with username **admin** and enter the administrator password that you used during the appliance deployment.
   - Open an SSH session.
     a. SSH to the IP address of your Intersight Virtual Appliance.
     b. Log in as the admin user with username **admin** and enter the administrator password that you used during the appliance deployment.

- Open a telnet session to a serial console.
  a. In cases where opening an SSH session to the Intersight Virtual Appliance is not possible, use the information described in Configuring Cisco TAC Support Using a Serial Console to add a serial console to your Intersight Virtual Appliance VM.
  b. Telnet to the vCenter host IP at the PORT_NUMBER specified in the serial console setup.
  c. Log in as the admin user with username **admin** and enter the administrator password that you used during the appliance deployment.

2. 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.

```
Intersight Appliance Maintenance Shell [Wed Jul  5 05:24:45 2023]
System Mode : Single-node ['or-pisces.cisco.com']
No change in deployment size during install. Current running deployment size is

Installation complete
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Diagnostics                          Configuration
[1] Ping a host                      [a] Show current network configuration
[2] Traceroute a host                [b] Configure network settings
[3] Run connectivity test            [c] Restart services installation
                                     [d] Run Debug shell (Cisco TAC only)
                                     [e] Configure Logon Banner
                                     [f] Generate and Upload Tech Support
                                     [g] Prepare Node for IP change (Multi-node

Maintenance
[4] Show system services status
[5] Restart system services
[6] Reboot virtual appliance node
[7] Show node status

[.] Exit
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Choice #1->
```

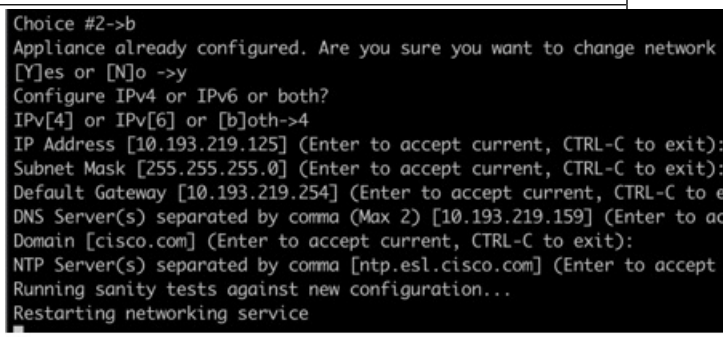
```
Choice #1->a
IP assignment: Static
IP Address: 10.193.219.125
Subnet mask: 255.255.255.0
Default Gateway: 10.193.219.254
DNS Servers: 171.70.168.183,173.36.131.10
Hostname: or-pisces.cisco.com
NTP Servers: ntp.esl.cisco.com,time-a-g.nist.gov,time-b-g.nist.gov
NTP Status:

     remote           refid      st t when poll reach   delay   offset  j
==============================================================================
*171.68.38.66    .GNSS.           1 u  457 1024  377    0.946    0.103
+129.6.15.28     .NIST.           1 u  286 1024  377   72.141   -2.006
+129.6.15.29     .NIST.           1 u  561 1024  377   72.125   -1.585

---
```

	• **[b] Set network interface properties**—This option displays the network interface properties that you have set. You can click **enter**

Intersight Appliance Maintenance Shell Options	Description
	to retain the existing properties or provide a different set of inputs. This option detects issues (if any) with the following properties:

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

	
	 
	• **For Multi-Node Only** - Do the following on the Maintenance Console:
	  • Enter configuration option **g** to prepare the appliance for IP change and input the IP address of your choice to configure on the appliance. This option allows you to add a new IP to the firewall policy to ensure that the other two nodes can communicate with the appliance when it is assigned the new IP address.
	  • Update the DNS server records (A, CNAME, and PTR) to ensure that the appliance's hostname now points to the new IP address
	  • Enter option **b** to configure the new IP. The appliance will reboot after the configuration is applied. 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>*. • **[d] Run Debug (requires authentication)—This utility is intended only for Cisco TAC to troubleshoot installation issues.** • **[e] Configure Logon Banner**—This option enables you to configure a new banner message or edit an existing one to be displayed before the login screen.
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, Medium, or large 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.**
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.**

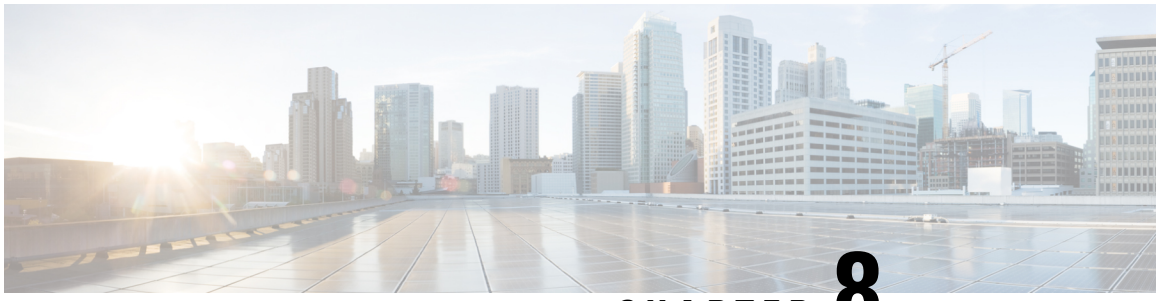
Console Messages

You may encounter messages such as the following on the console during installation or during normal operation of Intersight Virtual Appliance and Intersight Assist. The exact content of the messages can vary depending on different circumstances.

```
kernel:NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [watchdog/0:11]
```

These messages can appear when Intersight Virtual Appliance or Intersight Assist is partially or fully paused by the hypervisor, such as when the hypervisor is creating a "snapshot" of the VM or when the hypervisor host is resource constrained. The Intersight Virtual Appliance and Intersight Assist will continue to operate normally, even in the presence of these messages.

If you encounter many such messages, particularly in a short period of time, we highly recommend that you investigate your hypervisor environment to find the root cause.



CHAPTER 8

Technical Assistance and Feedback

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 Virtual Appliance, 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.

Opening a TAC Case directly from Intersight Virtual Appliance

After completing your setup and claiming a target, you can create a Cisco TAC Service Request (SR) directly from Cisco Intersight Virtual Appliance by launching Cisco Support Case Manager from the **Server Details** page. Before you open a case, please ensure that the following requirements are met:

- A valid service contract (entitlement) exists for the hardware.
- Your Cisco ID is associated with the service contract.

Note Your browser must be connected to the internet so that you can access Cisco Technical Assistance Center (TAC) and create a service request.

To open a Cisco TAC case directly from Cisco Intersight Virtual Appliance:

1. From the appliance UI, select a server from the **Servers** table view.
2. Click the ellipsis (**...**) button for your selected server and select **Open TAC Case**.

   The **Open a TAC Case** window displays with the name and serial number of the selected server.
3. Click **Continue** to launch Cisco Support Case Manager.
4. In the Cisco Support Case Manager UI, verify the auto-populated details of your case, add a description and a title for your TAC Case, and click **Submit**.

Collecting a Tech Support Bundle From Intersight Virtual Appliance

After completing your appliance setup and claiming a target, you can collect a tech support bundle for Intersight Virtual Appliance as well as for target claimed into the appliance, and attach it to your Cisco TAC Service Request (SR). You can collect tech support bundles from Cisco UCS Fabric Interconnects and connected UCS B, C, S Series Servers, Cisco UCS C-Series Standalone Servers, Cisco Hyperflex Clusters, and Cisco UCS Director.

To collect tech support bundles for targets claimed into your Appliance, do the following:

1. Log into the Appliance as a user with one of the following roles:
   - Account administrator
   - Server administrator
   - Hyperflex administrator
2. From the Appliance dashboard, navigate to the target for which you want to collect a tech support bundle.
   - In the case of **Servers**, **Fabric Interconnects**, and **UCS Director**, click the ellipsis (**...**) button for your selection and then select **Collect Tech Support Bundle**.
   - In the case of **Hyperflex Clusters**, after selecting a cluster and a corresponding node for the cluster, click the ellipsis (**...**) button for your selection and then select **Collect Tech Support Bundle**.

Note You may have to provide tech support bundles for all the nodes in the cluster while creating a service request in Cisco Technical Assistance Center (TAC).

3. From the **Service Selector** drop-down list, choose **System**, and navigate to **Admin** > **Tech Support Bundles** and download your tech support bundle for the target after the generation is complete.

To collect a tech suport bundle for your Appliance, do the following:

1. Log into the Appliance as a user with one of the following roles:
   - Account administrator
   - Server administrator
   - Hyperflex administrator
2. From the **Service Selector** drop-down list, choose **System**, and navigate to **Admin** > **Tech Support Bundles** .
3. Click **Collect Appliance Tech Support Bundle** on the Tech Support Bundle page.

   You can download the tech support bundle for your appliance after the generation is complete.

You can now proceed to Cisco Support Case Manager and create a service request.

Configuring Cisco TAC Support Using a Serial Console

In extreme cases where your Intersight Virtual Appliance becomes unreachable via SSH on the network and you need Cisco TAC support, it is not possible to enable the Cisco TAC support mode on the Appliance via the VMWare Remote Console (VMRC). Hence, you will need to add a Serial Port device to the Appliance virtual machine. This Serial Port will enable Cisco TAC, with your assistance, to connect to your Intersight Virtual Appliance and enter a Cisco TAC support mode.

Note Serial console support is only available on Intersight Virtual Appliance version 1.0.9-589 and later.

To add a Serial Port device to the Appliance virtual machine, do the following:

1. On the VMWare vSphere host where the Intersight Virtual Appliance virtual machine is running:
   a. Select the **Configure** tab.
   b. Under the **System** group, select **Firewall**.
   c. Click the **Edit** button to edit the firewall rules.
   d. Ensure that the rule named *VM serial port connected over network* is enabled.
      - Note the range of TCP ports that are allowed for this rule (an example being 23 and 1024-65535) as you need to enter this port range in Step 3.c (Port URI).

- Optionally, allow only designated source IP addresses in the firewall rule.

e. Save this rule.

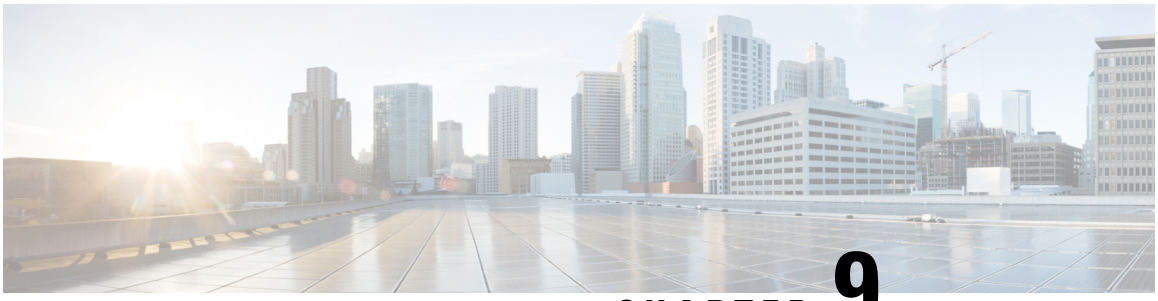
2. Power down the Intersight Virtual Appliance virtual machine.
3. Edit the vSphere settings of the Intersight Virtual Appliance virtual machine.
   a. Select **Add a New Device**.
   b. Under **Other Devices**, select **Serial Port**.
   c. Select the following settings on the new Serial Port:
      1. New Serial port: *Use Network*
      2. Status: *Connect At Power On* is checked
      3. Direction: *Server*
      4. Port URI: *telnet://:PORT_NUMBER*, where PORT_NUMBER is an integer representing an available port on the vCenter host that is within the range allowed by the firewall rule enabled in Step 1 (example is 12345).
      5. Save this new device.
4. Power on the Intersight Virtual Appliance virtual machine.

You will now be able to telnet to the vCenter host IP address at the port you specified (example is 12345) and connect to the login prompt on your Intersight Virtual Appliance. Cisco TAC, via a screen-sharing session, will be able to use this connection to enable Cisco TAC support mode on the Appliance to recover its functionality.

Send Feedback

Note This feature is available only for Intersight Connected Virtual Appliance deployments.

You can share feedback about your experience with Cisco Intersight Virtual Appliance from the appliance UI. Click the **Help** drop-down list (the question mark representation) on the appliance dashboard, and select **Send Us Feedback**. You can rate your experience, report a defect, or leave a comment for enhancement of any feature or functionality.



CHAPTER 9

Related Documentation

Links to Related Documentation

- Cisco Intersight provides a cloud-based RESTful API to manage Cisco UCS and Cisco HyperFlex systems across multiple Data Centers. To learn more about the Intersight API, see API Docs.
- Learn more about the Faults and Alarms in Intersight:
  - UCS Faults and Error Messages
  - HyperFlex HX Data Platform Events

For more information about Enabling Intersight Management on the Management Interfaces, see the appropriate guide listed below:

- Cisco UCS Manager Administration Guide
- Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide
- Cisco HyperFlex Systems Installation Guide for Cisco Intersight