Cisco Intersight Virtual Appliance Settings

- Intersight Virtual Appliance Settings, on page 1
- Intersight Virtual Appliance Monitoring, on page 4
- Backing Up Data, on page 5
- Upgrading the Intersight Connected Virtual Appliance Software, on page 7
- Updating Intersight Intelligence for Intersight Connected Virtual Appliance , on page 9
- Upgrading the Intersight Private Virtual Appliance Software, on page 10
- Intersight Virtual Appliance Sizing Options , on page 12
- Cloud Connection for Intersight Connected Virtual Appliance, on page 14
- Configuring Account Settings, on page 15
- Configuring a Banner Message for Displaying Before the Login Screen, on page 16
- Configuring DNS , on page 16
- Configuring NTP , on page 17
- Configuring External Syslog, on page 18
- Configuring LDAP Settings , on page 19
- Single Sign-On with Intersight Virtual Appliance, on page 20
- Certificates, on page 20
- Configuring Password Policy for Local Users, on page 23
- Adding a User, on page 24
- Adding a Group, on page 25
- Adding a Role, on page 26
- Adding an Organization, on page 28
- Generating and Managing API Keys , on page 29
- OAuth2 Tokens, on page 29

Intersight Virtual Appliance Settings

On the Intersight dashboard, you can access **Settings** from the **Settings** icon. On the **Settings** page, you can view the following information and perform the following actions:

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 15.
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 Appliance Configuration.
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 16.

Settings Option	Description
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. The details of a Pending update including the firmware version, upgrade impact type and messages, the number of days and hours by which the update will be installed, and the fingerprint are also displayed. Click **Upgrade Now** to upgrade to the available version if you do not want to wait until the maintenance window for the upgrade. You can also schedule an upgrade from this page. For a Private Virtual Appliance deployment, you can upload the required software from this page to complete the upgrade process.
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 14.
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 16.
NETWORKING > **NTP**	Configure NTP servers as well as edit existing NTP server settings. For more information, see Configuring NTP , on page 17.
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 18.
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 19.

Settings Option	Description
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 20.
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 20.
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 23.
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 24.
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 25.
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.

From the appliance UI, navigate to **Settings** icon > **Settings** > **General** > **Appliance** to view the following details:

- **Health**—Overall status of the appliance
- **Hostname**—Your FQDN or hostname
- **Version**—Installed version of the appliance software
- **Deployment Size**—Appliance deployment size. This can be **Small** or **Medium**, depending on your requirement to support 2000 or 5000 servers. For detailed information about Deployment size, see Intersight Virtual Appliance Sizing Options , on page 12
- **Data Collection**—**(For Connected Virtual Appliance only)** Data Collection option. Click the Edit icon to enable/disable the option to allow Intersight to send additional system information to Cisco.
- 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, 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 1: Alarms in Intersight Virtual Appliance

Alarm	Description
System Readiness	A system is not ready for service deployment
CPU Usage	CPU usage above threshold. Threshold: 75%
Memory Usage	Memory usage above threshold. Threshold: 75%
File System Disk Usage	File System disk usage above threshold. Threshold: 75%
Number of service instances running	Number of service instances running less than expected
Number of service instances ready	Number of service instances ready less than expected
Web certificate and target certificate	Warning alarm is generated when either of the certificates expires within 120 days Critical alarm is generated when either of the certificates expires within 90 days

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.

Create Backup

Create a full state periodic backup of the Cisco Intersight Virtual Appliance and save the backed-up file on a remote server.

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

Step 2 From the Appliance UI, navigate to **Settings** icon > **Settings** > **Backup**, click **Create Backup**.

Step 3 On the **Appliance Backup** window, select the protocol and enter other details of the remote server where you want to save 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.
- **Remote Host**—The remote host for saving the backup files. For example, if you select SCP, the remote host should be *myscpserver*.
- **Remote Port**—Remote TCP port on the backup server. For example, port 22 for SCP.
- **Remote Path**—Directory location where the backup files are saved. For example, the remote path will be *localsystem/backups/<myfolder>*.
- **Filename**—Name of the backup file to restore. For example, *localsystem/backups/<myfolder>/<mybackup.tgz>*
- **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 4 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 in to Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the Appliance UI, navigate to **Settings** icon > **Settings** > **General** > **Backup**, click **Schedule Backup**.

Step 3 On the **Schedule Backup** window, toggle ON **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 (SCP/ STFP) used in the backup process.
  - **Remote Port**—Remote TCP port on the backup server.
- **Remote Host**—The remote host for saving the backup files.
- **Remote Path**—Directory location 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.
- **Password Confirmation**—Reenter the password and click **Schedule Backup** to complete the process.

Upgrading the Intersight Connected Virtual Appliance Software

Cisco Intersight Connected Virtual Appliance 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 Virtual Appliance is connected to Intersight. Intersight Virtual Appliance 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 Connected Virtual Appliance is connected to Intersight.

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

Step 2 From the appliance UI, navigate to **Settings** icon > **Settings** > **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 appliance 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 Virtual Appliance 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**.

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
  - Blackout Period, if you have set a blackout period for updates
  - Date and Time and Blackout Period, if you have chosen a specific update time and also set up a blackout period. For more information about a blackout period, see Blackout in step c, below:

    The upgrade happens automatically when the time specified in **Scheduled to Install on** is reached. If you want to override the automatic upgrade, click the **Install Now** to trigger an immediate upgrade.
  - 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. Enable **Blackout Dates** and specify a **Blackout Start Date** and **Blackout End Date** for an upgrade blackout window and click **Save**. **The blackout window prevents the system from auto upgrading the appliance.**

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

d. 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 9.

- **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 20.

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

Step 2 From the appliance UI, navigate to **Settings** icon > **Settings** > **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**.

Upgrading the Intersight Private Virtual Appliance Software

You can upgrade the Intersight Private Virtual Appliance software to update the service packages, OS packages including the kernel, and other security fixes. The appliance UI provides details about the upgrade including the impact of the upgrade, and any service interruptions. You can schedule an upgrade to occur automatically during a weekly maintenance window.

Use the following instructions to upload the software and configure a software upgrade schedule:

Before you begin

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

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

Step 2 From the appliance UI, navigate to **Settings** icon > **Settings** > **Software**, and 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**—Username 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, navigate to **Settings** icon > **Settings** > **Software**. The **Upgrade** button will appear on this page.

Step 3 Click **Upgrade**. 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 appliance 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 Virtual Appliance does it automatically.

- **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**.

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 **Schedule Updates** 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.
- **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 20.

Intersight Virtual Appliance Sizing Options

Cisco Intersight Virtual Appliance is available in multiple deployment sizes to support the scaling requirements of your environment. You can deploy the Appliance in the **Small** or **Medium** options to support 2000 or 5000 servers respectively. 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. This feature is made available through an update from the Intersight cloud service.

The following table lists the currently supported Intersight Virtual Appliance sizing options, the required resources, and the supported maximum configuration limits:

Resource Requirements	**Deployment Size**	
	Small	**Medium**
Number of Servers	2000	5000
vCPU	16	24
RAM(GiB)	32	64
Disk (GiB)	500	500
Supported Maximum Configuration Limits		
Number of parallel HyperFlex Installations	2	5
Number of Supported Concurrent Operations	50	100
Concurrent User Sessions (GUI and API)	32	32
Number of parallel workflows	25	50

Attention

- To use the Virtual Appliance sizing options, you must have the latest upgrades from the Intersight cloud service.
- Any existing deployment size will be considered **Small** and you can choose to upgrade to **Medium**.
- The **Tiny(8 vCPU, 16 Gi RAM)** option is applicable only for Intersight Assist deployment.
- To upgrade to the next higher size, shut down the VM, change the CPU and RAM as required, and then restart the VM.

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.

```
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

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

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

- If the deployment size is same as the existing deployment, the VM restarts without any change. You can upgrade to a higher size after determining resource requirements.
- After an upgrade from the cloud service, all deployment is considered Small. The Maintenance Shell and the Intersight Appliance User Interface display Small as the deployment size. You can choose to remain in the same size or upgrade to Medium.

```
Intersight Appliance Maintenance Shell [Thu Jan 16 18:23:02 2020]
Deploying Small deployment size.

Installation in progress: No, Installer log: 261972 bytes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
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)
Maintenance
[4] Show system services status
[5] Restart system services
[6] Reboot virtual appliance node

[.] Exit
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Choice #2->
```

Changes in the Appliance User Interface for Intersight Appliance Sizing Options

The deployment size of Intersight Virtual Appliance is displayed in **Settings** > **Settings** > **General** > **Appliance** . Review the other supported scaling options and choose the appropriate deployment size to suit your requirement. After you review the details of the resource requirement for a supported deployment option, shut down the VM, change the CPU and RAM as required, and restart the VM.

Backup and Restore

The deployment size of the appliance is backed up as part of the regular backup data. However, this data will be refreshed when the appliance is restored and the size is determined based on the resource availability on the VM at the time of restoring the data.

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. From the appliance UI, navigate to **Settings** icon > **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 procedure provides details on how to configure account settings in Intersight Virtual Appliance.

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

Step 2 From the appliance UI, navigate to the **Settings** icon > **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.

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

Step 2 From the appliance UI, navigate to the **Settings** icon > **Settings** > **General** > **Banner 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 in to Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the appliance UI, navigate to the **Settings** icon > **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 in to Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the appliance UI, navigate to the **Settings** icon > **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

This procedure provides details on how to configure external syslog in Intersight Virtual Appliance. When **External Syslog** is enabled, the audit logs that are displayed in the **Audit logs** page as well as the alarms that are provided in Intersight Virtual Appliance are sent to an external syslog server as per the details provided when configuring external syslog.

Note In Intersight Virtual Appliance, you can use the TLS, UDP, and TCP connection types protocols to provide communication to the external syslog server. However, it is strongly recommended that you use **only** TLS connection type in your production environment.

Before you begin

Ensure that you have added the certificate for the external syslog server where you want to send the audit logs and the alarms provided in Intersight Virtual Appliance. This certificate is used to verify TLS communication with the external syslog server. For more information about certificates and how to add one, see Certificates, on page 20.

- 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 in to Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the appliance UI, navigate to the **Settings** icon > **Settings** > **NETWORKING** > **External Syslog**.

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

Step 3 Click **Configure**.

The **Configure External Syslog** window displays.

Step 4 Update the following fields as needed.

- **Enabled**—When enabled, the audit logs that are displayed on the **Audit Logs** page as well as the alarms provided in Intersight Virtual Appliance are sent to an external syslog server as per the configuration details provided in the **Hostname/IP Address** and the **Port** fields.
- **Export 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 such as the Department of Defense that require the ability to export web server access logs.

- **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.

Step 5 Click **Save**.

Configuring LDAP Settings

Cisco 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.

Use these instructions to set up LDAP authentication for Cisco Intersight Virtual Appliance.

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

Step 2 From the appliance UI, navigate to **Settings** icon > **Settings** > **NETWORKING** > **LDAP/AD**, click **Create LDAP**.

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.
- **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 **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.
- **Cisco 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. For more information about setting up SSO with Intersight and examples of adding an Identity Provider, see, Single Sign On with Intersight. Click here 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 obtain and install a third-party certificate from a trusted source that affirms the identity of your appliance, or generate a CA-signed certificate or self-signed certificate for secure **HTTPS** access of the appliance through the browser. You can import the certificates from the **AUTHENTICATION** section in the Cisco Intersight Virtual Appliance **Settings** menu.

Note Wildcard certificates are not supported in Intersight Virtual Appliance.

LDAP/AD

Importing LDAP/AD Certificates

To secure communication over the LDAP/AD server, you must enable encryption while configuring the LDAP Settings and provide a certificate obtained from the LDAP Server. 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 accessible from **Settings** icon **Settings** > **AUTHENTICATION** > **Trusted Certificates** displays the list of certificates that you import into the Cisco Intersight Virtual Appliance.

Add Certificate

Use these instructions to add trusted certificates in Cisco Intersight Virtual Appliance:

1. Log in to Cisco Intersight Virtual Appliance as a user with account administrator role.
2. From the appliance UI, navigate to **Settings** icon > **AUTHENTICATION** > **Certificates** > **LDAP/AD**. 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
   - **Expires**—The expiry date of the certificate
3. Click **Add Certificate** at the top-right corner to import a trusted certificate. The **Add SSL/TLS Certificate** window displays.
4. Click **Browse** to select the certificate that is stored in your system and click **Save**. The certificate must be in the *.pem* (base64 encoded) format. 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. This certificate is used to verify TLS communication with the LDAP server.

HTTPS

Create Certificate Signing Request (CSR)

To enable secure **HTTPS** access of the appliance through the browser, you can generate a Certificate Signing Request and generate a Self-Signed certificate and import the certificate to Intersight. You can trigger these from the **Actions** menu in **Settings** icon **Settings** icon **Settings** > **AUTHENTICATION** > **Trusted Certificates** > **HTTPS**.

1. From the appliance UI, navigate to **Settings** icon **Settings** icon **Settings** > **AUTHENTICATION** > **Certificates** > **HTTPS**. 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

Note 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. Fill in the following details as required and click **Create CSR**.
   - 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

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 self-signed certificate from a **Certificate Authority** (CA).
- **Delete CSR**—Delete the CSR if you do not want to use it to generate a self-signed 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 radio button and upload a certificate. Click **Apply** to complete the process. The CA issued certificate can be in *.csr*, *.pem* or *.crt* format.

Generate Self-Signed Certificate

From the **Action** drop-down menu, select **Generate Self-Signed Certificate**. The **Generate Self-Signed Request** window displays. Review the warning message and click **Generate & 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 generate a self-signed certificate to extend the validity of the certificate if the Cisco provided self-signed certificate expires.
- When you choose to generate a self-signed certificate, the current SSL certificate will be replaced by the newly generated self-signed certificate, and you could be logged out of the current browser session. If not logged out, refresh the browser to load the new 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 in to 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 in to Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the appliance UI, navigate to the **Settings** icon > **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.
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

Password Policy Options	Allowed Range/Default Value
	Note If you specify a value of 0 for this password policy option, then the user is not limited on time between password changes.

Step 5 Click **Save**.

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

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.

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

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

Step 2 From the Appliance UI, navigate to **Settings** icon > **Settings** > **Users**, and click the **Add User** button at the top right. The **Add User** window displays.

Step 3 In the **Add User** window, add 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*.You must select the appropriate LDAP domain for users that would log in with LDAP credentials.

  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 of following system-defined roles to a user as well as assign user-defined roles:

  - **Account Administrator**—In this role, you can claim targets, cross launch element managers, collect tech support bundles, create profiles and policies, and make configuration changes to the claimed targets or the account.

  - **Read-Only**—In this role, you 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, you can claim a target in Intersight and view a list of the claimed targets in the Targets table view.

  - **Device Administrator**—In this role, you can claim a target in Intersight, view a list of the claimed targets, and delete (unclaim) a target.

- **Server Administrator**—In this role, you 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, you can create, edit, and deploy a HyperFlex cluster profile, upgrade a cluster, set cluster tags, view cluster dashboard and summary, monitor alarms, collect tech support bundles, and launch and manage **HX Connect**.
- **User Access Administrator**—In this role, you can create, edit, and manage user accounts, groups, set up Identity Providers, and Single Sign-On and generate API keys related to this role.

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

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

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 in to Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the Appliance UI, navigate to **Settings** icon > **Settings** > **Groups**, and click the **Add Group** button at the top right. The **Add Group** window displays.

Step 3 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 4 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 in to Cisco Intersight and navigate to the **Settings** icon > **Settings** > **ACCESS & PERMISSIONS** > **Roles**.
2. From **Roles**, click **Create Role**.
3. Enter a **Name** to identify the role in Intersight and a **Description** about the usage of the role.

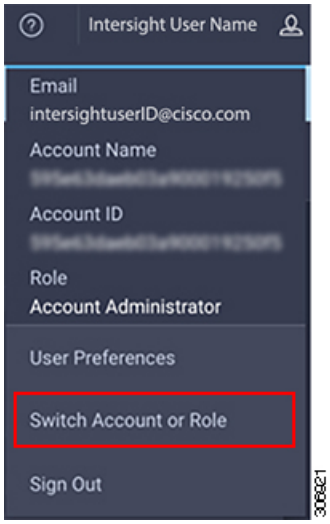
   You can choose to retain the default account level settings for Session Timeout, Idle Timeout, and Concurrent Sessions, or you can choose to customize these settings.
4. Under **Session & Idle Timeout** settings, you can choose to do one of the following:
   - Enable **Use Account Default Settings**—This 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.

5. Click **Next**.
6. 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.
7. 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** icon > **Settings** > **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 in to Cisco Intersight and navigate to the **Settings** icon > **Settings** > **ACCESS & PERMISSIONS** > **Organizations**.
2. From **Organizations**, click **Create Organization**.
3. Enter a **Name** to identify the organization in Intersight and a **Description** about the usage of the organization.
4. 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.

5. 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 <*http://your fqdn.com*>/help.

Generating and Managing API Keys

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

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

Step 2 From the Appliance UI, navigate to **Settings** icon > **Settings** > **API Keys**, and click **Generate 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 in to Cisco Intersight Virtual Appliance as a user with account administrator role.

Step 2 From the Appliance UI, navigate to **Settings** icon > **Settings** > **API** , and click **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.