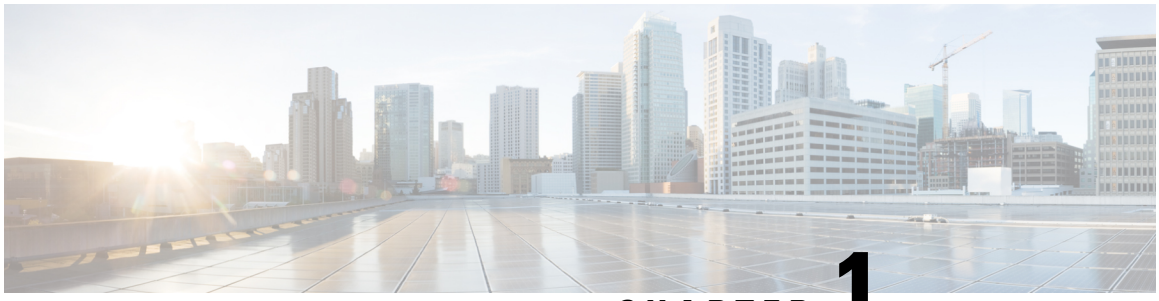
Cisco Application Services Engine User Guide, Release 1.1.3

First Published: 2020-05-06

Last Modified: 2021-01-14

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

CONTENTS



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

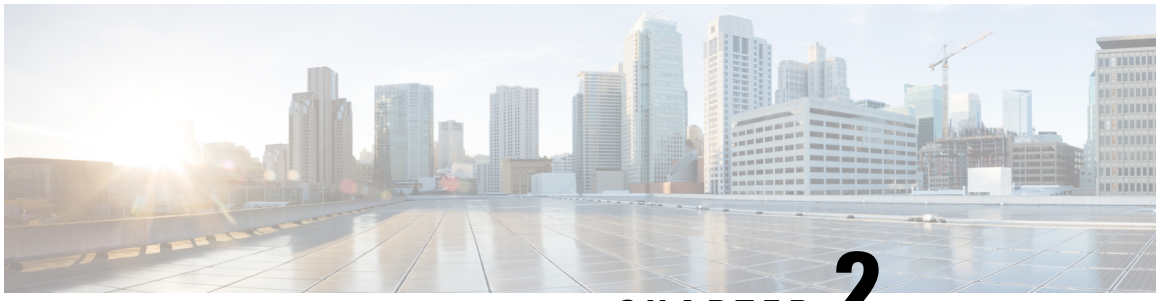
New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide from the release the guide was first published to the current release. The table does not provide an exhaustive list of all changes made to the guide

Table 1: Latest Updates

Release	Description	Where Documented
1.1.3	Moved the deployment procedures into a separate guide.	Cisco Application Services Engine Deployment Guide
1.1.3	This guide was first published.	

New and Changed Information



CHAPTER 2

Overview

This chapter contains the following sections:

Cisco Application Services Engine Overview

Cisco Application Services Engine provides a common platform for deploying Cisco Data Center applications. These applications provide real time analytics, visibility, and assurance for policy and infrastructure.

Cisco Data Center apps are resource intensive applications that rely on modern technology stacks. Cisco Application Services Engine can host containerized applications on a common platform.

Cisco Application Services Engine is deployed as a cluster of three service nodes. This clustering provides reliability and high-availability software framework.

Cisco Application Services Engine is deployed in the Fabric external mode. In this mode, the Cisco ACI fabric does not provide the configuration and montoring of the Cisco Application Services Engine cluster from the Cisco APIC GUI. Cisco Application Services Engine can be deployed in the fabric external mode using a number of different form factors, such as:

- **Physical appliance form factor:**
  - ISO form factor.

Virtual form factors:

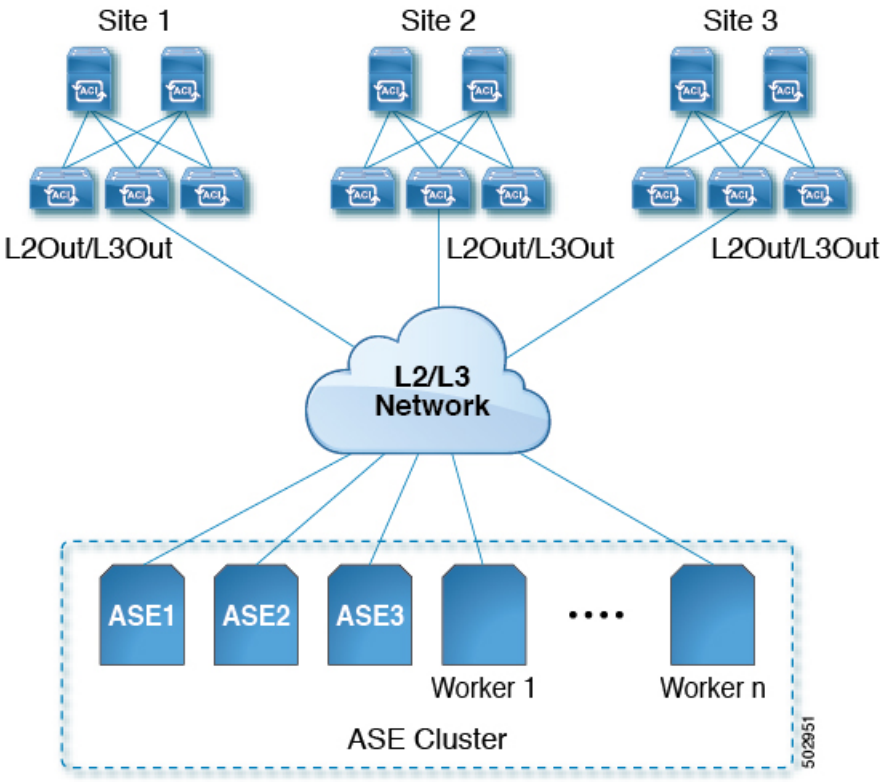
- AWS - AMI form factor.
- OVA form factor.
- KVM form factor.

Note Beginning from Cisco Application Services Engine Release 1.1.3, fabric internal mode is not supported. To migrate from the fabric internal mode to fabric external mode please refer, Migrating from Fabric Internal Mode (Release 1.1.2) to Fabric External Mode (Release 1.1.3).

Note Cisco Multisite Orchestrator, Cisco Network Insights Resources application, and Cisco Network Insights Advisor application are supported.

Architecture

Figure 1: Cisco Application Services Engine Architecture



Service node: The service node is an appliance or a system that is attached to a network and is capable of creating, receiving, or transmitting information over Cisco ACI fabric. These are also known as master nodes and they manage the state of the cluster.

Cluster: Cluster is a set of three connected service nodes. It supports the life cycle management of the apps.

- New service nodes can be dynamically added without disrupting services from existing apps.
- Service nodes can be taken out of service for graceful maintenance. Apps can be re-provisioned on the other nodes without disrupting service.

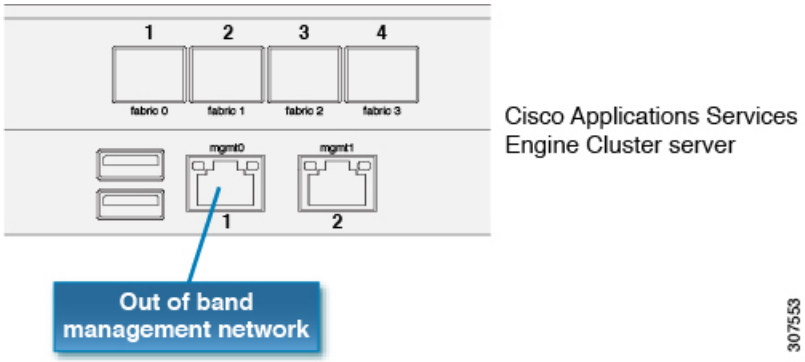
Worker Nodes: Worker nodes are additional service nodes executing the application workloads as decided by the master nodes. Upto four worker nodes can be added to an existing cluster.

Management and Network Connectivity

Cisco Application Services Engine is deployed as a cluster, connecting each service node to two networks.

1. Management network using management interfaces. (mgmt0, mgmt1)
2. Data Network using the fabric interfaces. (fabric0, fabric1)

Figure 2: Network Connectivity for Cisco Application Services Engine



Management network is used for:

- Accessing the Cisco Application Services Engine GUI.
- Accessing the CLI over SSH.
- DNS and NTP.
- Firmware uploads.
- Intersight device connector.

Data Network is used for:

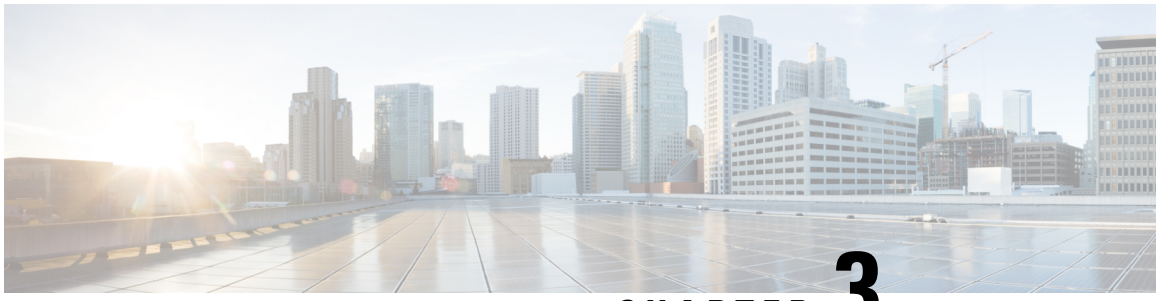
- Cisco Application Services Engine Clustering.
- App to app communication.
- Access the management network of the Cisco ACI fabric.
- All app to ACI fabric comunications.

Management and Data networks can be on the same or different subnets. Each service node should have IP reachability to all the Cisco ACI fabrics over the Cisco Application Services Engine data network.

Cisco Application Services Engine clustering uses the following TCP ports, these TCP ports should be allowed on the data network:

- DNS 53
- HTTPS 443
- SSH 22, 1022

- NIA 2022, 8884
- NIR 5640-5656
- KMS. 3379, 3380, 9969, 9979, 9989, 15223
- Confd 19999
- SE infra services: 30000 - 30100
- Kuberentes node ports: 30500 - 30600



CHAPTER 3

Multi Fabric Deployment

Multifabric Support

Cisco Application Services Engine supports multifabric. In multifabric deployment, service nodes can be spanned across the fabrics.

With multifabric support, multiple Cisco ACI fabrics can be on-boarded on to a single Cisco Application Services Engine cluster. Once the Cisco ACI fabric is on-boarded as a site onto the Cisco Application Services Engine cluster, apps running on the Cisco Application Services Engine cluster can access this site.

Cisco APIC data network IP and admin credentials are needed to on-board a site. Cisco Application Services Engine should have IP reachability to the Cisco APIC Inband Management IP. Admin credentials of Cisco APIC are not stored in the Cisco Application Services Engine cluster, they are used only one time to copy the SSL keys to Cisco APIC. Sites added to the Cisco Application Services Engine cluster are not enabled in the apps by default, they need to be explicitly enabled for each app in their respective GUI.

In Cisco Application Services Engine release 1.1.3, only Cisco NIR and Cisco NIA will use the sites on-boarded on to Cisco APIC. Cisco ACI Multi-Site Orchestrator does not use these sites.

Adding a Site

In the Sites Details page, perform the following actions:

Before you begin

1. Cisco ACI fabric Inband management must be pre-configured.
2. EPG/L3Out for Cisco Application Services Engine data network IP connectivity must be pre-configured.

   Additional information is available in the "Fabric Connectivity" section of the *Cisco Application Services Engine Deployment Guide*. Specific EPG or L3Out configuration procedures are described in Cisco APIC Layer 2 Networking Configuration Guide and Cisco APIC Layer 3 Networking Configuration Guide respectively.

3. IP connectivity from Cisco Application Services Engine to Cisco APIC over data network must be configured.
4. IP connectivity from Cisco Application Services Engine to the leaf nodes or spine nodes must be configured.

Note Points 3 and 4 are applicable only for the Cisco NIR app.

Step 1 Choose **Infrastructure** > **Sites**.

Step 2 Click **Actions**. Click **Add site**.

Step 3 Enter the Site name. This can be any string of characters.

Step 4 Enter the **Host name/ Data Network IP address of APIC**.

Step 5 Enter the **User name**.

Step 6 Create and enter the **Password**. Confirm the password.

Step 7 Enter the **Domain Name**.

Step 8 In the **Login Domain** field, enter the domain name for the site.

Step 9 Click **Create**.

The site is added to the Cisco Application Services Engine.

Step 10 Repeat these steps to add additional sites.

Note If a site is deleted, importing the configuration of the site, does not help in the recovery of the site. The site needs to be manually created.

Removing a Site from Cisco Application Services Engine

Use this procedure to delete or remove a site from Cisco Application Services Engine.

Step 1 Log in to the Cisco Application Services Engine GUI.

Step 2 Ensure you unbind the site from any Schema's before trying to delete the site.

Note When Cisco ACI fabric is added as a site on to Cisco Application Services Engine, some policies are created on Cisco APIC. If the Cisco Application Services Engine is clean rebooted without deleting the on-boarded site, the policies created on Cisco APIC will not be deleted. To clean up these policies on Cisco APIC, the site should be re-added and deleted.

Note Deleting a site will cause an interruption in all the apps running on this site. This operation cannot be undone.

Step 3 Choose **Infrastructure** > **Sites**.

Step 4 In the **Sites** List page, place a check in the box next to the site you want to delete and choose **Action**> **Delete**.

Step 5 Click **Submit**.

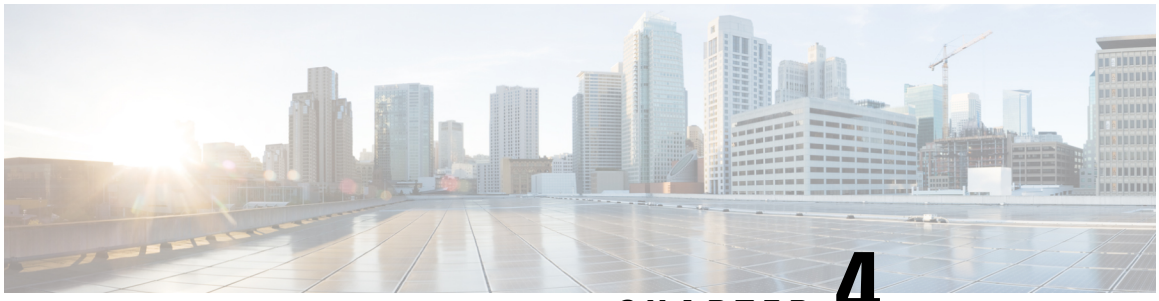
Step 6 **Confirm Delete** dialog box appears.

a) Enter the **User name**.
b) Create and enter the **Password**. Confirm the password.
c) In the **Login Domain** field, enter the domain name for the site.
d)

Step 7 Place a check box next to the box in **Force Delete**.

Note Use **Force Delete** options if apps are using the site and you can not follow recommended actions of removing the sites from app or if the site is not reachable.

Step 8 Click **OK**.



CHAPTER 4

Cisco Application Services Engine GUI Overview

This chapter describes the graphical user interface for Cisco Application Services Engine.

This chapter contains the following sections:

Cisco Application Services Engine GUI

Once the Cisco Application Services Engine is bootstrapped, the remaining actions can be performed using the Cisco Application Services Engine GUI.

To access Cisco Application Services Engine GUI, use management network IP of any master node : https://<node-mgmt-ip>

Dashboard

The **Dashboard** provides a wholistic view of the Cisco Application Services Engine. An administrator can use this view to monitor system health, sites and apps connectivity status and resource utilization.

The **Dashboard** has the following information:

- **Overview** tile displays system status, cluster status and Cisco Intersight status.
- The **Sites, Apps, and Infra Services** tile displays the sites by connectivity, apps by status and infra services by status.
- The **Inventory** tile provides details of the node type, nodes, containers, pods, deployments, stateful sets, daemon sets, and services.
- The **Service Node Storage** tile provides details about the registered service nodes.
- The **Utilization** tile provides details about the CPU usage.

- The **Memory** tile provides details about the memory usage.

Apps

The **Apps** component in the left navigation pane displays the apps that are hosted on the Cisco Application Services Engine.

When clicked upon, the app work pane shows the app details including **Description**, **Version**, **Pods**, and the **Containers** running on the selected app.

- The **Containers** tab displays all the configured containers, container status, IP address, and the configured service nodes .
- The **Pods** tab displays the configured pods running on the selected app.
- The **Version** tab displays the the app version number.

The **Enable** enables the selected app.

The **Launch App** allows the enabled app to be launched. This opens a new window where the app is launched. Login to the Cisco Application Services Engine user interface to perform any further operations.

Resource Overview

The **System Resources** component in the left navigation pane displays the application resources that are configured on the service node.

The **System Resources** tab opens a navigation work pane, which displays the **Nodes**, **Pods**, **Containers**, **Deployments**, **Statefulsets**, **Deamonsets**, and the **Namespaces** running on the node.

The **Nodes** tab on the navigation work pane displays the details of the service nodes configured and running on the selected app. Upto seven nodes are admitted in a cluster; three master nodes and four worker nodes.

Note Only worker nodes can be registered using the GUI. Master nodes are brought up using the command line as specified in Deploying the Cisco Application Services Engine section.

The **Pods** tab on the navigation work pane displays the configured pods running on the selected app.

The **Containers** tab on the navigation work pane displays all the configured containers, container status, IP address, and the configured service node.

The **Deployments** tab on the navigation work pane displays all the deployments, status, IP address, and the configured service node.

The **Statefulsets** tab on the navigation work pane displays all the configured statefulsets, status, IP address, and the configured service node.

The **Deamonsets** tab on the navigation work pane displays all the configured deamonsets, status, namespaces, IP addresses.

The **Services** tab from the navigation work pane displays the service name, cluster IP, configured ports and the selectors for the app.

The **Namespaces** tab from the navigation work pane displays the services, pods, containers, deployments and replicasets of the apps.

Operations

The **Operations** component in the left navigation pane displays the actions that can be performed on Cisco Application Services Engine. Four actions that can be performed under **Operations** such as :

Firmware Management:

Firmware Management is used to perform cluster (firmware) upgrade or downgrade.

Note Refer to Upgrading Existing Release 1.1.3 to Later Releases, on page 26 for more information.

Tech Support:

An administrator can perform technical support collections.

Audit Logs:

Audit Logs are user triggered configuration changes.

Backup and Restore:

Backup and Restore displays the backed up and restored configuration.

Tech Support

Tech support enables user to collect logs and activities in the system for further troubleshooting by Cisco TAC. Cisco Application Services Engine provides best efforts tech support collection and gives ability to download tech support for individual nodes or consolidated one. Tech support files are hosted on the Cisco Application Services Engine and can be downloaded any time.

Use this procedure to collect Tech Support.

Step 1 For collecting tech support, click **Tech Support** > **Actions** and **Collect Tech Support**.

Step 2 Enter the description of the issue and click **Collect**.

Step 3 For deleting tech support, click **Tech Support**. Place a check in the tech support log to be deleted. Click **Actions** > **Delete Tech Support**.

Step 4 After tech support is complete, user can download the file for troubleshooting further.

Audit logs

Use this procedure to view the audit logs.

Step 1 Choose **Operations** > **Audit Logs**.

Step 2 Click **Audit Logs**.

An administrator can monitor configuration modification in the **Audit Logs** view. Audit logs are unsorted by default. Click on any column to sort them.

To check more details about an action, click on the row and you can find out what configuration was changed in the given action.

Back up and Restore

Use this procedure to back up and restore cluster configuration details.

Step 1 Click **Backup and Restore** > **Actions**.

Step 2 To back up the configuration, click **Back up configuration**.

Step 3 Enter the Encryption key (this is the key to encrypt the data) and the file name. Click **download**.The configuration is backed up and the details are displayed on the **Backup and Restore** page.

Step 4 To restore the configuration, click **Actions** and **Restore configuration**.

Step 5 In the Restore configuration window, enter the import type. Choose **replace** or **merge** based on the action needed to be performed.

Note Cisco Application Services Engine does not store configuration backup, user needs to download the backup and maintain it in their local environment.

replace will replace existing configuration with backedup configuration. **merge** will try to merge existing configuration with backed up configuration.

Step 6 Enter the Encryption key (used to back up the configuration), choose the file for import and click **import**.

Cluster Management

The **Infrastructure** component is an embedded management controller that enables addition or deletion of sites, cluster configuration and Cisco Intersight to the Cisco Application Services Engine.

Sites:

APIC cluster domain or single fabric, treated as an ACI region and availability zone. It can be located in the same metro-area as other sites, or spaced world-wide.

Cluster Configuration:

Cluster Configuration provides cluster details such as name, app subnet, and service subnet. It also provdes details of the NTP and DNS servers.

Intersight:

The Intersight component is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

Note The Cisco NIA app depends on the Intersight Device Connector for the app to be configured and available on the service node.

User Management

The **Administrative** component in the left navigation pane displays the users for Cisco Application Services Engine. The Users tab allows the admin to give access to other users.

Creating a User

Use this procedure to give access to other users.

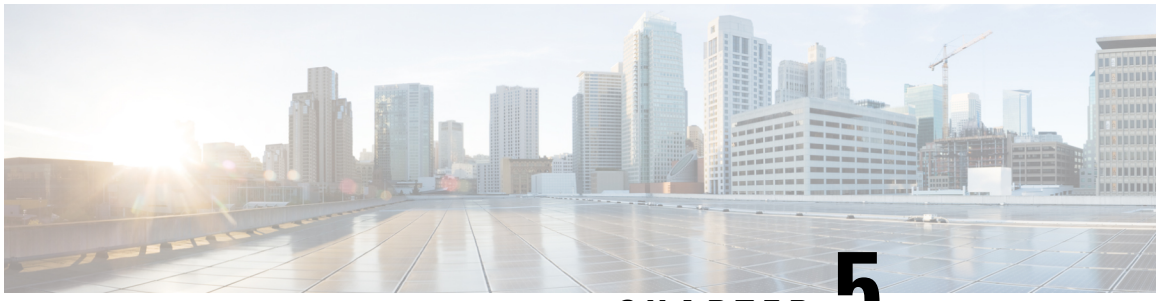
Step 1 Choose **Administrative** > **Users**.

Note The users can be either administrative users or read only users.

Step 2 Click **Actions** and then **Create local user** to create a user.

Step 3 Click **Actions** and then **Delete local user** to delete a user.

Step 4 The tile displays the user ID, status, first name, last name, email ID, and privileges of the users.



CHAPTER 5

Application Management

Hosting Apps on Cisco Application Services Engine

Use this procedure to upload the apps on the Cisco Application Services Engine.

Before you begin

- You have downloaded the app from the Cisco Data Center and moved the downloaded app file to a http server.
- You must have administrator credentials to install the app.

Step 1 Log into Cisco Application Services Engine.

Step 2 Click **Apps** from the side navigation bar.

Step 3 Click **Actions**.

Step 4 Click **Upload App** from the far-right side of the work pane.

Select **local** tab to upload the apps to Cisco Application Services Engine. Download the app to your computer and save it. Browse to the location to upload it to Cisco Application Services Engine.

Step 5 For uploading larger apps use the **remote** upload option. Copy the URL of the app that you have downloaded from Cisco App Center and hosted the app file to a http server.

Step 6 In the **URL** field enter the copied http address and click **Submit**.

Click Refresh to check the upload status.Once the app is hosted, the **Apps** tab is displayed.

Step 7 Click the **Apps** tab. The work pane displays **App Installing in progress**.

Step 8 Once the installation is complete, then click **Enable** to enable the app on the Cisco Application Services Engine.

Onboard a Site on Cisco Application Services Engine Using GUI

Use this procedure to onboard a site on to the Cisco Application Services Engine using GUI. Any apps installed on Cisco Application Services Engine can access the onboarded sites.

Before you begin

You have installed and configured the Cisco Application Services Engine.

You must have administrator credentials to install an application.

Step 1 Log in to the Cisco Application Services Engine GUI with admin privileges.

Step 2 Create and add a site using the procedure in Adding a Site, on page 7.

Step 3 Creating a site onboards a site to the node. Any apps installed on Cisco Application Services Engine can access the onboarded sites.

Step 4 Continue with the installation of applications on Cisco Application Services Engine using GUI. Refer to Hosting Apps on Cisco Application Services Engine, on page 17 for uploading apps.

Step 5 After the app is launched, follow the User Guides for the app to configure the sites.

Uninstalling App

Use this procedure to delete an application on the Cisco Application Services Engine .

Log in to the Cisco APIC GUI with admin privileges

Before you begin

You must disable the app before you delete the app on the Cisco ApplicationServices Engine.

Step 1 Log in to the Cisco ApplicationServices Engine GUI.

Step 2 Click **Apps**.

Step 3 Click **Delete** on the top right corner of the application dialog.

Step 4 Click **Yes** on the delete application dialog.

Disabling an App

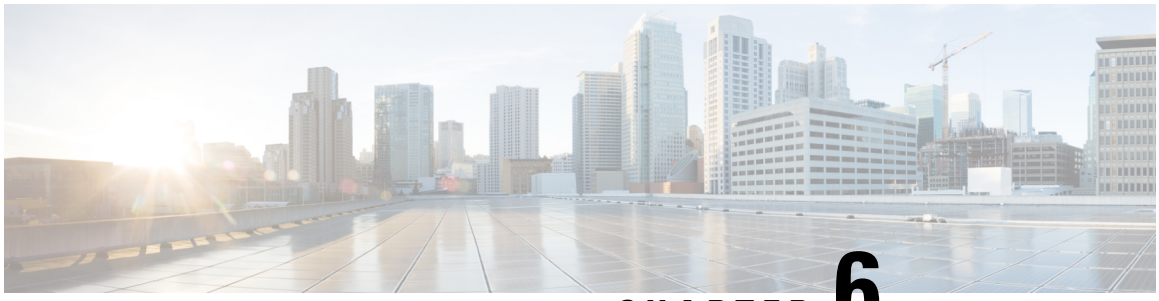
Use this procedure to disable an application on the Cisco Application Services Engine.

Step 1 Log in to the Cisco Application Services Engine GUI.

Step 2 Click **Apps**. The apps page appears.

Step 3 Choose the app to be deleted and the app tile. Click **Disable** on the top right corner of the application dialog.

Step 4 Click **Yes** on the disable application dialog.



CHAPTER 6

Horizontal Scaling of Cisco Application Services Engine

Adding a Worker Node

Use this procedure to add a worker node to an existing cluster.

Note Only worker nodes can be registered using the GUI.

Before you begin

Make sure all three service nodes are bootstrapped.

Step 1 Power on the new worker node and complete the bootstrap. Note down serial number of this node.

Refer to *Cisco Application Services Engine Deployment Guide* for deploying nodes. Upto 4 worker nodes can be admitted in a cluster.

Note Once a worker node is bootstrapped using command line, Cisco Application Services Engine discovers the worker node. User can then click on register action to admit this node into existing case cluster without needed to provide any additional information.

Step 2 Log in to the Cisco Application Services Engine GUI.

Step 3 Choose **System Resources** > **Nodes**.

In the GUI, a worker node entry should show up as **Register**. Verify that the serial number matches that of the new node.

Pre-registering a Worker node

Use this procedure to register a worker node.

Before you begin

Make sure all three service nodes are bootstrapped.

Step 1 Enter the **Name** and the **Serial Number** of the node.

Step 2 Enter the **Data Network IP Address** and the **Data Network Gateway** of the node.

Step 3 Enter the **Management IP Address** and the **Management Gateway** of the node.

Step 4 Click **Save** and **Finish**.

The worker node will be registered upon bootstrapping.

Registering a Worker node

Use this procedure to register a worker node.

Before you begin

Make sure all three service nodes are bootstrapped.

Step 1 In the GUI, select the checkbox next to the bootstrapped worker node. Click **Actions** > **Register** to admit a worker node.

Step 2 The **Data Network IP Address** and the **Data Network Gateway** of the node are auto-populated.

Step 3 The **Management IP Address** and the **Management Gateway** of the node are auto-populated.

Step 4 Click **Save** and **Finish**.

The worker node will be registered upon bootstrapping.

Deleting a Worker node

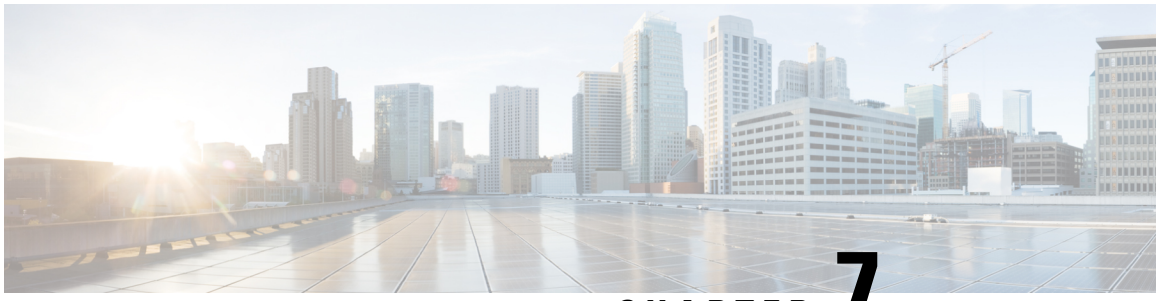
Use this procedure to delete a worker node.

Before you begin

1. Make sure all three service nodes are bootstrapped.
2. The new worker node is pre-registered or registered.

Step 1 In the GUI, select the checkbox next to the bootstrapped worker node. Click **Actions** > **Delete** to delete a worker node.

Step 2 Click **Delete** and **Finish**.



CHAPTER 7

Upgrading the Cisco Application Services Engine

Migrating from Fabric Internal Mode (Release 1.1.2) to Fabric External Mode (Release 1.1.3)

You can use this procedure to upgrade the Cisco Application Services Engine from version 1.1.2 to 1.1.3.

Note Stateful migration is not supported. Upgrading from 1.1.2 to 1.1.3 will not preserve any app data. All apps should be re-installed after the migration.

Note Same procedure has to be performed on each service node separately

Before you begin

- You must have Cisco Application Services Engine installed and the cluster configured.
- Ensure that you have a working software image for the upgrade.

Step 1 Log in to the Cisco Application Services Engine GUI.

Step 2 Disable Cisco NIR and Cisco NIA apps on the Cisco APIC.

Step 3 Note down the Cisco Application Services Engine data network subnet and Cisco Application Services Engine connected ports.

Step 4 Clean the Service Node related configuration from Cisco APIC.

To clean the Service Engine configuration from the APIC simply POST to the `https://<apic-ip>/appcenter/Cisco/ServiceEngine/api/wipeClean.json` API endpoint with `DEVCOOKIE=<apic-auth-token>` in the header.

You can obtain the `<apic-auth-token>` by first posting to `https://<apic-ip>/api/aaaLogin.xml` with your login credentials and using the value of the returned `aaaLogin` field. For more information on using the APIC API, see *Cisco APIC REST API Configuration Guide*.

Step 5 Disable and delete the Cisco Application Services Engine app.

Step 6 Configure the Bridge Domain (BD), subnet, and Endpoint Groups (EPG) for Cisco Application Services Engine connectivity in management tenant using the information from Step 3.

Note Refer to Cisco APIC Layer 3 Networking Configuration Guide for configuring EPG/L3Out.

Step 7 Create a contract between the fabric data network EPG and Cisco Application Services Engine EPG.

Step 8 Upgrade all the service nodes to Release 1.1.3.

Step 9 Start the upgrade using the **acidiag installer update** -f *iso_filepath* command.

```
node # acidiag installer update -f /tmp/apic-sn-dk9.1.1.3.iso
```

Run the command on all nodes individually. Once the command is executed successfully, reboot the service nodes.

Step 10 Clean the previous version of the deployment using the **acidiag touch setup** command.

```
node # acidiag touch setup
```

Step 11 Reboot individual nodes using the **acidiag reboot** command.

```
node # acidiag reboot
```

Step 12 Complete the first time setup on all three nodes as described in *Cisco Application Services Engine Deployment Guide*.

Step 13 Verify the version after the upgrade using the **acidiag version** command.

```
node # acidiag version
```

Step 14 Add the new site using the procedure described in Adding a Site, on page 7.

Step 15 Reinstall the Cisco NIR and Cisco NIA apps and enable the sites in Cisco Application Services Engine GUI.

Upgrading Existing Release 1.1.3 to Later Releases

GUI firmware upgrades are supported starting with Release 1.1.3c. You can use the following procedure to upgrade your Application Services Engine, Release 1.1.3 to a later release or patch.

Before you begin

- We recommend using this procedure to upgrade from Release 1.1.3 to later 1.1.3 patches.
- If you are upgrading from a release prior to Release 1.1.3, follow the steps described in Migrating from Fabric Internal Mode (Release 1.1.2) to Fabric External Mode (Release 1.1.3), on page 25 instead.
- If you want to upgrade to Nexus Dashboard, Release 2.0.1:
  - Ensure you have upgraded to at least Release 1.1.3d

- Follow the procedures described in *Cisco Nexus Dashboard Deployment Guide*

Step 1 Navigate to the **Operations** component in the left navigation pane.

Step 2 Click the **Operations** > **Firmware Management**

Firmware Management tab displays the node details including the current firmware version, number of nodes, and last update made on the firmware.

Step 3 Click **images** tab and download the new image.

Step 4 Click on **Firmware Management**, then **Set an update**.

Step 5 Click on **Available Target Firmware Versions**, then select the applicable version and click **confirm**.

Step 6 Click **Install**, then click **next**.

Step 7 After the installation is complete, click **Activate** and after the activation is done, click **Complete**.

Manual Upgrade Procedure

Use this prcedure for manual uprade of the service nodes.

Step 1 Log in to the Cisco Application Services Engine server as a rescue-user.

Step 2 Copy the ISO image file into the /tmp directory on all the nodes.

Step 3 Start the upgrade using the **acidiag installer update** command.

Run the command on all nodes individually. Once the command is executed successfully, reboot the service nodes. Wait till you see the success message on all nodes, before moving to Step 4.

```
[rescue-user@node1 ~]$ acidiag installer update -f /tmp/case-dk9.1.1.3a.iso
Warning: This command will initiate node update to new version. Proceed? (y/n): y
Update in Progress ... Do not press Ctrl^C
Update succeeded, reboot your host
```

Step 4 Reboot node using **acidiag reboot** command.

Wait for each node to come up with the new version and a healthy status, before proceeding to next node.

```
[rescue-user@node1 ~]$ acidiag reboot
This command will restart this device, Proceed? (y/n): y
Connection to 172.20.6.119 closed.

[rescue-user@node1 ~]$ acidiag version
APIC-SN 1.1.3a

[rescue-user@node1 ~]$ acidiag health
All components are healthy
```

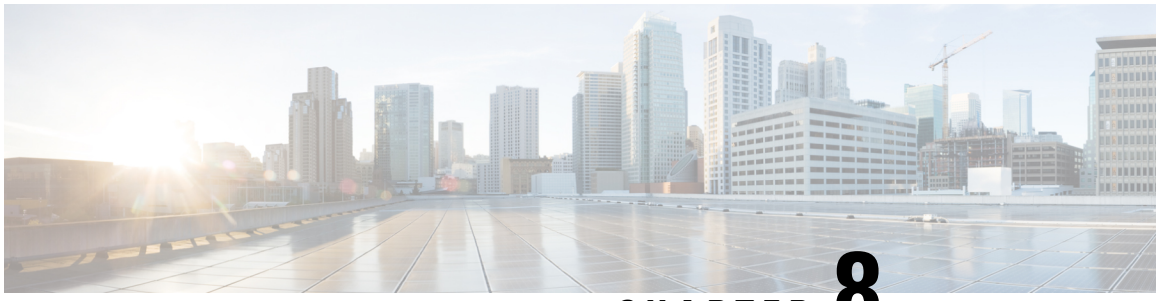
Note Do this on nodes one after the other. More than one node should not be unavailable at any time.

Step 5 Once all nodes are up with new version and healthy, run **acidiag installer post-update** on all nodes in parallel.

```
[rescue-user@node1 ~]$ acidiag installer post-update
Warning: This command will run the post-update scripts. Proceed? (y/n): y
```

```
Update in Progress ... Do not press Ctrl^C
Post-update succeeded
```

Step 6 Upgrade is complete at this point. Use **acidiag health** to monitor the health of the cluster as services get updated to the new version.



CHAPTER 8

Maintenance of Cisco Application Services Engine

RMA of Single Master Node

Use this procedure for RMA of the master nodes.

Step 1 Log in to the UI on one of the healthy master nodes. Select the **System Resources** tab, select **Nodes**.

Step 2 Power off the old master node that is being removed. In the UI, make sure the status for this node changes to **Inactive**. Verify that the serial number matches that of node that needs to be removed.

Step 3 Power on the new node and complete bootstrap. Use the same parameters that were used to set up the old node (including name and network information). Note down the serial number of this node.

Step 4 In the UI, select the checkbox next to the inactive master node. Click on **Actions** and select **Replace**. When prompted, enter the new node's serial number under **New Serial Number** and proceed.

Step 5 In the UI, you should see the serial number get updated. The status will change to **Active** once the master has successfully joined the cluster.

RMA of Two Master Nodes

Use this procedure for RMA of the master nodes.

Step 1 Power down the two master nodes that have failed.

Step 2 Power on and bootstrap the two new nodes with the same parameters that were used to bootstrap the old nodes.

Refer to *Cisco Application Services Engine Deployment Guide* for deploying the nodes. Up to 4 worker nodes can be admitted in a cluster.

Step 3 Log in to the healthy master (cli) and run the **acidiag recover save** command.

```
[rescue-user@node1 ~]$ acidiag recover save
Warning: Cluster recovery can be a disruptive operation and should only
be performed as last resort option to recover cluster from disasters
where two master nodes have lost their state due to hardware faults. Proceed? (y/n): y

cluster snapshot '/tmp/cluster_snapshot.tar.gz' generated successfully.
Copy to other devices as '/tmp/cluster_snapshot.tar.gz' before performing restore.
```

Step 4 Copy the `.tar` file that was generated in previous step to the two new nodes as `/tmp/cluster_snapshot.tar.gz` and perform the **acidiag recover restore** command on all the nodes. The nodes will reboot.

```
[rescue-user@node1 ~]$ acidiag recover restore
Warning: This command will restart this device to perform recovery.
Make sure, you have copied cluster snapshot to other devices
if you are recovering the cluster from this device. Proceed? (y/n): y
Connection to 172.20.6.119 closed.
```

Step 5 Wait for all nodes to form the cluster and show their status as healthy. Use the **acidiag health** command to verify the total cluster health.

Single Worker RMA

Use this procedure to replace a failed worker node.

Note For cleaning up or recovering a node in bad software state, please use **acidiag touch clean** or **acidiag touch setup** followed by **acidiag reboot**.

Note Please not that **Delete** option has been provided so that you can RMA the node for hardware issues that require it to be physically replaced. If you **Delete** a worker node, expectation is that you will **Register** a new node with the same bootstrap information.

Step 1 Log in to the GUI of one of the healthy master nodes. Select the **System Resources** < **Nodes**.

Step 2 Power off the old worker node that is being removed. In the GUI, make sure the status for this node changes to **Inactive**. Verify that the serial number matches that of node needs to be replaced.

Step 3 In the GUI, select the checkbox next to the worker node that needs to be removed. Click **Actions** < **Delete**. The entry for this node is removed from the **Nodes** page.

After you delete the node from the cluster, use the following command to clean reload it to remove any old configurations:

```
# acidiag touch clean
```

Then reboot it:

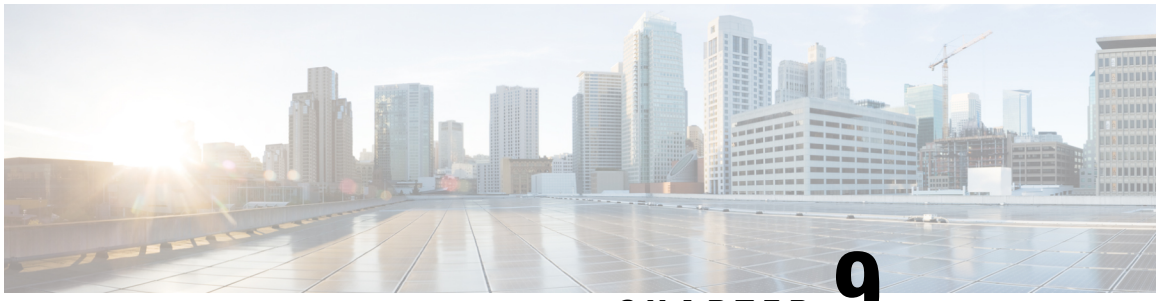
```
# acidiag reboot
```

Step 4 Power on the new worker node and complete bootstrap. Use the same parameters that were used to set up the old worker node. Note down the serial number of this node.

Step 5 In the GUI, a worker node entry should show up as **Unregistered**. Verify that the serial number matches that of the new node.

Step 6 In the GUI, select the checkbox next to this worker node. Click on **Actions** and select **Register**. Verify the details in the next screen and select **Save**.

Step 7 In the GUI, you should see the node's status change to **Discovering**, and then it changes to **Active**.



CHAPTER 9

Troubleshooting Cisco Application Services Engine

This chapter contains the following sections:

Working with Cisco Application Services Engine

You can use the following commands to perform various operations in Cisco Application Services Engine.

Command(s) for app operations:

- **acidiag cluster get config**: Checks the cluster configuration.

  ```
  acidiag cluster get config
  ```

- **acidiag cluster get masters**: Checks the status of the cluster masters.

  ```
  acidiag cluster get masters
  ```

- **acidiag cluster get workers**: Checks the status of the cluster worker.

  ```
  acidiag cluster get workers
  ```

- **acidiag health**: Checks the status of the cluster health.

  ```
  acidiag health
  ```

- **acidiag app show**: Displays the installed application(s).

  ```
  acidiag app show
  ```

- **acidiag app install**: Installs application(s).

  ```
  acidiag app install <filepath or url>
  ```

- **acidiag app enable**: Enables an installed (or disabled) application (s).

  ```
  acidiag app enable <application id>
  bash-4.2$ acidiag app
  [ { 'adminState': 'Enabled',
  'apiEntrypoint': '/query',
  'appID': 'MSO',
  'creationTimestamp': '2019-12-08T22:02:08.513217541Z',
  'description': 'Multi-Site Orchestrator application',
  'displayName': 'cisco-mso',
  ```

```
'id': 'cisco-mso:2.2.3',
'name': 'cisco-mso',
'operStage': 'Enable',
'operState': 'Running',
'schemaversion': '',
'uiEntrypoint': '/ui/app-start.html',
'vendorID': 'Cisco',
'version': '2.2.3'}]
bash-4.2$
```

- **acidiag app disable**: Disables an enabled application (s).

```
acidiag app disable <application id>
```

- **acidiag app delete**: Deletes an application (s).

```
acidiag app delete <application id>
```

Command(s) for app image operations:

- **acidiag image show**: Displays all the application images present.

```
acidiag image show
```

- **acidiag image show <image file name>**: Displays information about the specified application image.

```
acidiag image show <image file name>
```

Command(s) for app import operations:

- **acidiag import show**: Displays information on all the application imports made to the Cisco Application Services Engine.

```
acidiag import show
```

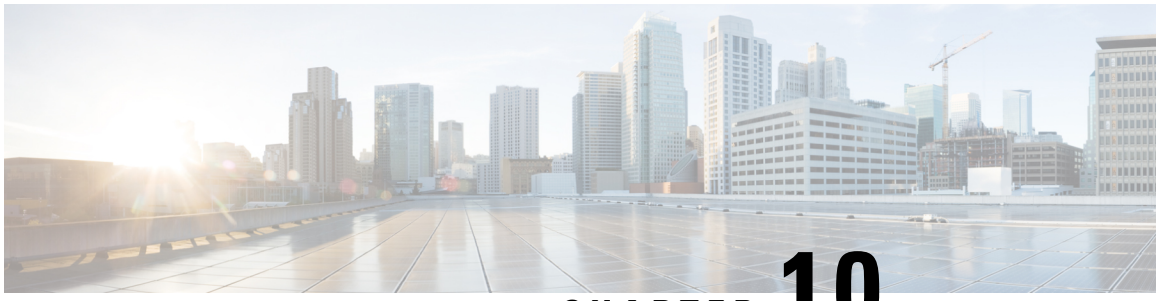
- **acidiag import show <import id>**: Displays info about the specified import. Import id is an optional parameter.

```
acidiag import show <import id>
```

Command(s) for Tech Support:

- **acidiag techsupport collect**

```
acidiag techsupport collect
Started: TS collection may take 15-20 minutes to complete. Monitor /techsupport/ for
the file
```



CHAPTER 10

Setting Up the Device Connector

This chapter describes the tasks for configuring and claiming a Ciso Intersight Device Connector on the Cisco Application Services Engine platform.

This chapter contains the following sections:

About the Intersight Device Connector

Devices are connected to the Cisco Intersight portal through a Device Connector that is embedded in the management controller of each system. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure internet connection.

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default, and attempts to connect to the cloud service. If the **Auto Update** option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Intersight service when you connect to Cisco Intersight. For more information on the **Auto Update** option, see Configuring the Device Connector, on page 35.

Configuring the Device Connector

Data center apps such as the Cisco NIA app is connected to the Cisco Intersight cloud portal through a Device Connector which is embedded in the management controller of the Cisco Application Services Engine platform.

Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure management platform that is augmented by other intelligent systems. It provides global management of the Cisco Unified Computing System (Cisco UCS) and Cisco HyperFlex hyperconverged infrastructure, Cisco APIC, and other platforms including Cisco Application Services Engine. The Device Connector provides a secure way for a connected Cisco Application Services Engine to send and receive information from the Cisco Intersight cloud, using a secure Internet connection.

Use this procedure to setup the Device Connector:

Step 1 Open Cisco Application Services Engine GUI.

Step 2 In the **Navigation** pane, click **Infrastructure** then **Intersight**.

- If you see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** page, and the text **Claimed**, then your Intersight Device Connector is already configured and connected to the Intersight cloud service, and the device is claimed.
- If you see yellow dotted lines and a caution icon connecting **Internet** to **Intersight** in the **Device Connector** page, and the text **Not Claimed**, then your Intersight Device Connector is not yet configured and connected to the Intersight service, and the device is not yet claimed. Follow these procedures to configure the Intersight Device Connector and connect to the Intersight cloud service, and claim the device.

Note Red dotted lines connecting **Internet** to **Intersight** in the **Device Connector** page, indicate that you have configured the proxy incorrectly in step 8.

Step 3 Determine if you would like to update the software at this time, if there is a new Device Connector software version available.

If there is a new Device Connector software version available and you do not have the **Auto Update** option enabled, you will see a message towards the top of the screen,informing that Device Connector has important updates available (refer to step 5c).

- If you do not want to update the software at this time, go to step 5 to begin configuring the Intersight Device Connector.
- If you would like to update the software at this time, click one of the two links in the yellow bar towards the top of the page, depending on how you would like to update the software:
  - **Update Now**: Click this link to update the Device Connector software immediately.
  - **Enable Auto Update**: Click this link to go to the **General** page, where you can toggle the **Auto Update** field to ON, which allows the system to automatically update the Device Connector software. See step 6c for more information.

Step 4 Locate the **Settings** link to the right of the **Device Connector** heading and click the **Settings** link.

The **Settings** page appears, with the **General** tab selected by default.

Step 5 In the **General** page, configure the following settings.

a) In the **Device Connector** field, determine if you want to allow communication between the device and Cisco Intersight.

The **Device Connector** option (enabled by default) enables you to claim the device and leverage the capabilities of Intersight. If it is turned OFF, no communication will be allowed to Cisco Intersight.

b) In the **Access Mode** field, determine if you want to allow Intersight the capability to make changes to this device.

Access Mode enables you to allow full read or write operations from the cloud or restrict changes made to this device from Cisco Intersight.

- The **Allow Control** option (selected by default) enables you to perform full read or write operations from the cloud, based on the features available in Cisco Intersight.

- The **Read-only** option ensures that no changes are made to this device from Cisco Intersight. For example, actions such as upgrading firmware or a profile deployment will not be allowed in the Read-Only mode. However, the actions depend on the features available for a particular system.

c) In the **Auto Update** field, determine if you want to allow the system to automatically update the software.

We recommend that you toggle the **Auto Update** option to ON so that the system automatically updates the software. Note that toggling the **Auto Update** option to ON means that the Device Connector will automatically upgrade its image whenever there is any upgrade push from Intersight.

- Toggle ON to allow the system to automatically update the software.
- Toggle OFF so that you can manually update the software when necessary. You will be asked to manually update the software when new releases become available in this case.

Note If the **Auto Update** option is turned OFF, that may periodically cause the Device Connector to be out-of-date, which could affect the ability of the Device Connector to connect to Cisco Intersight.

Step 6 When you have completed the configurations in the **General** page, click **Save**.

The **Intersight - Device Connector** overview pages appears again. At this point, you can make or verify several configure settings for the Intersight Device Connector:

- If you want to configure the proxy that the Device Connector will use to communicate with the Cisco Intersight cloud, go to step 8.
- If you want to manage certificates with the Device Connector, go to step 11.

Note The Cisco Application Services Engine requires you to configure the Proxy Settings for the Intersight Device Connector.

Step 7 If you want to configure the proxy that the Device Connector will use to communicate with the Cisco Intersight cloud, click **Settings**, then click **Proxy Configuration**.

The **Proxy Configuration** page appears.

Step 8 In the **Proxy Configuration** page, configure the following settings.

In this page, you can configure the proxy that the Device Connector will use to communicate with the Cisco Intersight cloud.

Note The Device Connector does not mandate the format of the login credentials; they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name depends on the configuration of the HTTP proxy server.

a) In the **Enable Proxy** field, toggle the option to ON to configure the proxy settings.
b) In the **Proxy Hostname/IP** field, enter a Proxy Hostname and the IP address.
c) In the **Proxy Port** field, enter a proxy port number.
d) In the **Authentication** field, toggle the **Authentication** option to ON to configure the proxy authentication settings, then enter a proxy username and password for authentication.

Step 9 When you have completed the configurations in the **Proxy Configuration** page, click **Save**.

The **Intersight - Device Connector** overview pages appears again.

If you want to make manage certificates with the Device Connector, go to the next step.

Step 10 If you want to manage certificates with the Device Connector, click **Settings**, then click **Certificate Manager**.

The **Certificate Manager** page appears.

Step 11 In the **Certificate Manager** page, configure the following settings.

By default, the device connector trusts only the built-in svc.ucs-connect.com certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in svc.ucs-connect.com certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device or not.

Click **Import** to import a CA signed certificate. The imported certificates must be in the *.pem (base64 encoded) format. After a certificate is successfully imported, it is listed in the list of **`Trusted Certificates`** and if the certificate is correct, it is shown in the **In-Use** column.

View these details for a list of certificates that are used to connect to svc.ucs-connect.com (intersight.com):

- **Name**—Common name of the CA certificate.
- **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server.
- **Issued By**—The issuing authority for the certificate.
- **Expires**—The expiry date of the certificate.

Delete a certificate from the list of **`Trusted certificates`**. However, you cannot delete bundled certificates (root+intermediate certificates) from the list. The lock icon represents the bundled certificates.

Step 12 When you have completed the configurations in the **Certificate Manager** page, click **Close**.

You can claim the device using the instructions provided in Claiming a Device, on page 38.

Claiming a Device

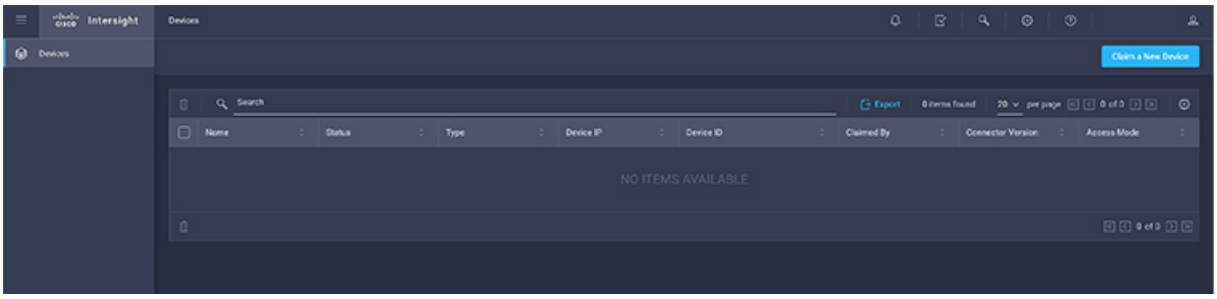
Before you begin

You have configured the Intersight Device Connector from the Cisco Application Services Engine.

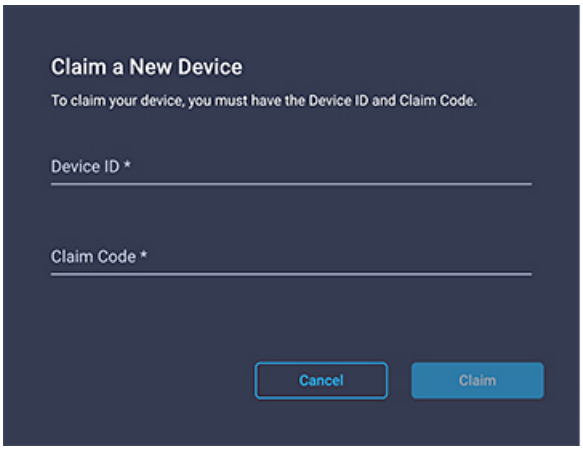
Step 1 Log into the Cisco Intersight cloud site:

https://www.intersight.com

Step 2 In the Cisco Intersight cloud site, click **Devices** tab, and then click **Claim a New Device**.



The **Claim a New Device** page appears.



Step 3 In the Cisco APIC UI navigate to the **Apps** page.

a) On the list of **Apps** page, select Cisco Application Services Engine.

b) In the **Navigation** pane, click **Intersight**.

Step 4 Copy the **Device ID** and **Claim Code** from the Cisco Application Services Engine App UI running on Cisco APIC and

Step 5 In the Cisco Intersight cloud site, paste them into the proper fields

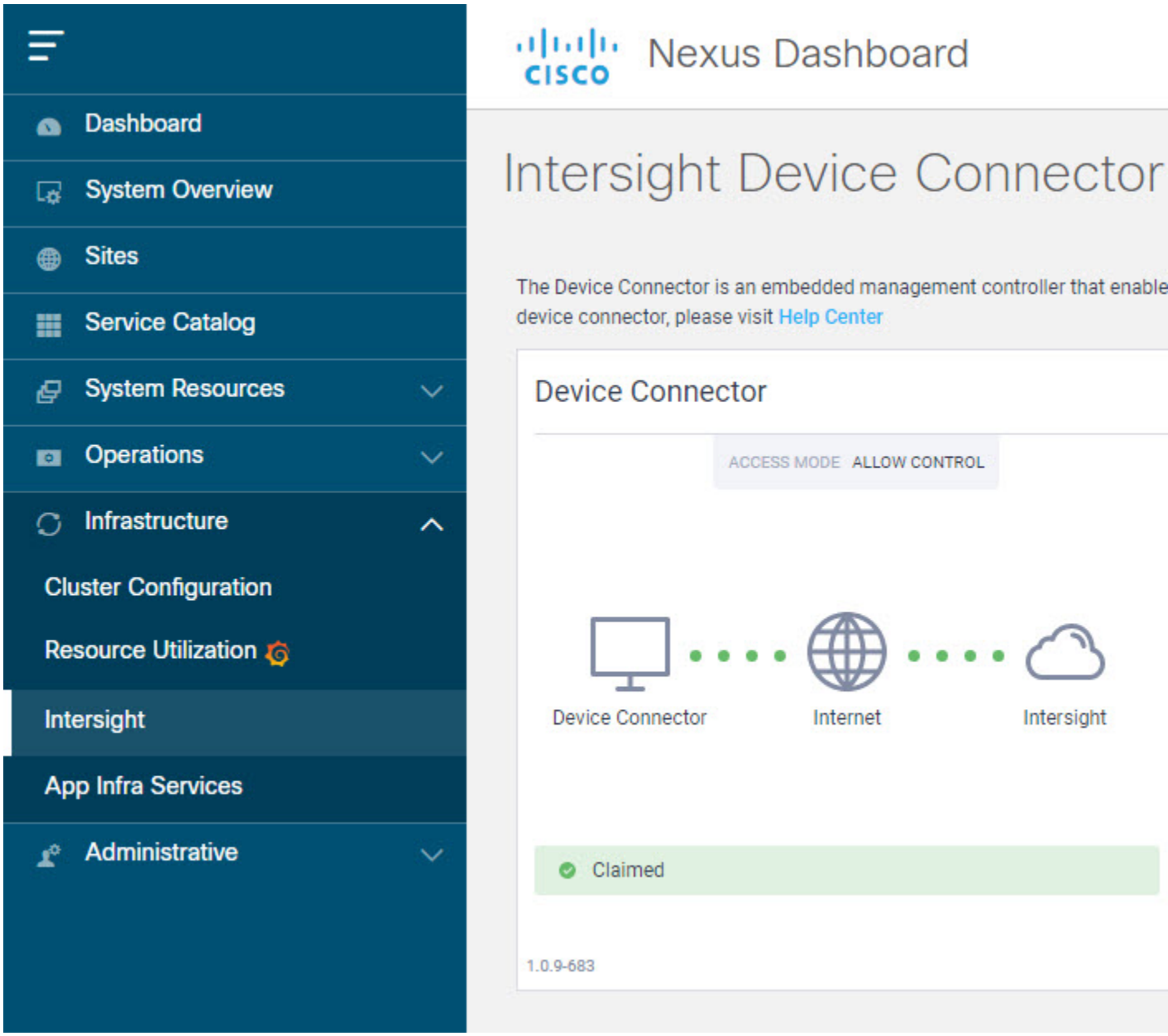
Step 6 **Claim a New Device** page in the Intersight cloud site.

Step 7 Click **Claim**.

The message "Your device has been successfully claimed" is displayed in the **Claim a New Device** page. Also, in the main page, you should see your Cisco Application Services Engine platform, with Connected shown in the Status column.

Step 8 Go back to the **Intersight - Device Connector** page in the Cisco Application Services Engine App UI in Cisco APIC GUI and verify that the system was claimed successfully.

You should see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** page, and the text **Claimed**.



Note You may have to click **Refresh** in the **Intersight - Device Connector** page to update the information in the page to the current state.

To unclaim this device, click the **Unclaim** link in the **Intersight - Device Connector**.