



Performing a System Upgrade, Downgrade or Recovery

- [Upgrading the Software, on page 1](#)
- [Downgrading the Software, on page 19](#)
- [Performing a System Recovery, on page 21](#)

Upgrading the Software

The method that you use to upgrade your Cisco Cloud APIC software varies, depending on the situation:

- If you are upgrading from a pre-5.0(1) release to Release 5.0(2), you will use a migration-based process to upgrade your software. Go to [Migration-Based Upgrade, on page 2](#) for those instructions.



Note The same migration-based procedures used for an upgrade can also be used for a system recovery, as described in [Performing a System Recovery, on page 21](#).

- If you are upgrading from Release 5.0(1) to Release 5.0(2), you will use a policy-based process to upgrade your software. Go to [Policy-Based Upgrade, on page 15](#) for those instructions.



Note If the policy-based upgrade from Release 5.0(1) to Release 5.0(2) does not work for some reason, you can upgrade from Release 5.0(1) to Release 5.0(2) using the migration-based process as described in [Migration-Based Upgrade, on page 2](#).

Guidelines and Limitations For Upgrading the Software

Following are the guidelines and limitations that you must be aware of before upgrading the Cisco Cloud APIC software:

Beginning with release 5.0(2), the configuration drift feature became available as described in the "Configuration Drifts" chapter in the [Cisco Cloud APIC for Azure User Guide](#), Release 5.0(x) or later. After you upgrade your Cisco Cloud APIC, if you had configuration drifts enabled prior to the upgrade, you will see that the configuration drift feature is restarted after the upgrade is completed. When the feature is restarted, the previous configuration drift analysis is cleared (no configuration drifts are shown after the upgrade) and a fresh analysis is started for the configuration drift when the feature is restarted after the upgrade. This is expected behavior.

Migration-Based Upgrade

Follow these procedures if you are upgrading from Release 4.2(4) or earlier to Release 5.0(2), where you will use a migration-based process to upgrade your software.



Note These migration-based procedures used for an upgrade can also be used for a system recovery, as described in [Performing a System Recovery, on page 21](#).

Gathering Existing Cloud APIC Configuration Information

Before upgrading your Cisco Cloud APIC software, follow the instructions in this topic to locate the existing configuration information for certain fields and make a note of the entries for each of these fields. You will use the same entries for these fields below, in a step later in the following procedures, when you use the Release 5.0(2) recovery template to upgrade your Cisco Cloud APIC.

For each of the following fields, make a note of the entries that you entered as part of the original deployment that you performed in [Deploying the Cloud APIC in Azure](#):

- [Subscription, on page 2](#)
- [Resource Group, on page 3](#)
- [Location, on page 3](#)
- [Fabric Name, on page 3](#)
- [External Subnets, on page 4](#)
- [Virtual Machine Name, on page 4](#)
- [Infra VNET Pool, on page 4](#)
- [Storage Account Name, on page 5](#)

Subscription

1. Navigate to **Application Management > Tenants**.
2. Locate the row for the tenant that has **infra** underneath the name in the **Name** column.
3. Note the value in the **Azure Subscription** column.

This is the **Subscription** entry for your Cisco Cloud APIC.

Resource Group

1. Navigate to **Cloud Resources > Virtual Machines**.

The **Virtual Machines** window appears.

2. Locate and note the Cisco Cloud APIC VM in the VM list.

The value for the VM is typically shown with the format `<vm_name><resource_group>`, where:

- `<vm_name>` is the virtual machine name, as described in [Virtual Machine Name, on page 4](#).
- `<resource_group>` is the **Resource Group** entry for your Cisco Cloud APIC.

Location

1. Navigate to **Cloud Resources > Virtual Machines**.

The **Virtual Machines** window appears.

2. Locate the Cisco Cloud APIC VM in the VM list.
3. Click the value for the Cisco Cloud APIC VM in the VM list.

A nav panel with details about the Cisco Cloud APIC VM slides in from the right side of the screen.

4. In the **General** area, locate and note the value in the **Region** field.

This is the **Location** entry for your Cisco Cloud APIC.

Fabric Name

1. SSH to your Cisco Cloud APIC through the CLI:

```
# ssh admin@<cloud_apic_ip_address>
```

Enter the password if prompted.

2. Enter the following in the CLI:

```
ACI-Cloud-Fabric-1# acidiag avread
```

3. Locate the **FABRIC_DOMAIN** area in the output:

```
Local appliance ID=1 ADDRESS=10.100.0.13 TEP ADDRESS=10.100.0.12/30 ROUTABLE IP
ADDRESS=0.0.0.0
CHASSIS_ID=afe36d66-042a-11eb-ab21-7b2dc494b182

Cluster of 1 lm(t):1(zeroTime) appliances (out of targeted 1
lm(t):1(2020-10-01T21:15:48.743+00:00))
with FABRIC_DOMAIN name=ACI-Cloud-Fabric set to version=5.0(2i)
lm(t):1(2020-10-01T21:15:48.746+00:00);
discoveryMode=PERMISSIVE lm(t):0(zeroTime); drrMode=OFF lm(t):0(zeroTime); kafkaMode=OFF
lm(t):0(zeroTime)

appliance id=1 address=10.100.0.13 lm(t):1(2020-10-01T21:14:23.001+00:00) tep
address=10.100.0.12/30
lm(t):1(2020-10-01T21:14:23.001+00:00) routable address=0.0.0.0 lm(t):1(zeroTime)
oob address=10.100.0.29/28 lm(t):1(2020-10-01T21:14:26.723+00:00) version=5.0(2i)
lm(t):1(2020-10-01T21:14:26.841+00:00) chassisId=afe36d66-042a-11eb-ab21-7b2dc494b182
lm(t):1(2020-10-01T21:14:26.841+00:00) capabilities=0X7EEFFFFFFF--0X2020--0X1
lm(t):1(2020-10-01T21:20:27.483+00:00) rK=(stable,present,0X206173722D687373)
```

```

lm(t):1(2020-10-01T21:14:26.728+00:00) aK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobrK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobaK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) cntrlSbst=(APPROVED, E8E6DDB1D800)
lm(t):1(2020-10-01T21:14:26.841+00:00) (targetMbSn= lm(t):0(zeroTime),
failoverStatus=0 lm(t):0(zeroTime)) podId=1 lm(t):1(2020-10-01T21:14:23.001+00:00)
commissioned=YES lm(t):1(zeroTime) registered=YES lm(t):1(2020-10-01T21:14:23.001+00:00)


standby=NO lm(t):1(2020-10-01T21:14:23.001+00:00) DRR=NO lm(t):0(zeroTime) apicX=NO
lm(t):1(2020-10-01T21:14:23.001+00:00) virtual=YES lm(t):1(2020-10-01T21:14:23.001+00:00)

active=YES(2020-10-01T21:14:23.001+00:00) health=(applnc:255
lm(t):1(2020-10-01T21:16:16.514+00:00) svc's)
-----
clusterTime=<diff=-1 common=2020-10-02T07:46:19.717+00:00
local=2020-10-02T07:46:19.718+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):1(2020-10-01T21:15:50.026+00:00)>>
-----

```

This is the **Fabric Name** entry for your Cisco Cloud APIC.

External Subnets


1. Navigate to **Application Management > EPGs**.
2. Locate the EPG with the name **ext-networks** and click that EPG.
A nav panel slides in from the right side of the screen.
3. In the nav panel, click the **Details** icon ()
The **Overview** page for this EPG appears.
4. In the **Endpoints** area, locate the row for **ext-Network1** and note the value in the **Subnet** column.
This is the **External Subnets** entry for your Cisco Cloud APIC. Note that a value of 0.0.0.0/0 meant that anyone is allowed to connect to your Cisco Cloud APIC.

Virtual Machine Name

1. Navigate to **Cloud Resources > Virtual Machines**.
The **Virtual Machines** window appears.
2. Locate and note the value for the Cisco Cloud APIC VM in the list.
The value for the VM is typically shown with the format `<vm_name>(<resource_group>)`, where:
 - `<vm_name>` is the **Virtual Machine Name** entry for your Cisco Cloud APIC.
 - `<resource_group>` is the resource group, as described in [Resource Group, on page 3](#).

Infra VNET Pool

For the infra VNET pool, you might have multiple infra subnet pools, so be sure to locate the information for the infra subnet that was used when you launched the original Cisco Cloud APIC through the ARM template as part of the procedures in [Deploying the Cloud APIC in Azure](#).

1. In your Cisco Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
2. In the Region Management area, click **Edit Configuration**.
The **Regions to Manage** window appears.
3. Click **Next**.
The **General Connectivity** window appears.
4. In the **Subnet Pools for Cloud Routers** area underneath **General**, locate the row that has a **System Internal** value in the **Created By** column and note the value in the **Subnet** column.
This is the **Infra VNET Pool** entry for your Cisco Cloud APIC.

Storage Account Name

Navigate to the **Storage accounts** page in Azure under the resource group where the Cisco Cloud APIC was deployed previously:

1. Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:
<https://portal.azure.com/#home>
2. Under **Services**, select **Storage accounts**.
The **Storage accounts** page appears.
3. Locate and note the storage account name for your Cisco Cloud APIC resource group.
This is the **Storage Account Name** entry for your Cisco Cloud APIC.

What to do next

Follow the procedures in [Performing Pre-Upgrade Procedures, on page 5](#).

Performing Pre-Upgrade Procedures

Before you begin

Complete the procedures in [Gathering Existing Cloud APIC Configuration Information, on page 2](#) before proceeding with these procedures.

Step 1

Enable the encrypted passphrase control, if it is not enabled already.

- a) In your Cisco Cloud APIC GUI, navigate to **Infrastructure > System Configuration**.

It should be underneath the **General** tab by default; if not, click the **General** tab.

- b) Determine if the encrypted passphrase control is enabled already.

- In the **Global AES Encryption** area, if you see **Yes** underneath the **Encryption** and **Key Configured** fields, then you have the encrypted passphrase control enabled already. Go to [Step 2, on page 6](#).

- If you do not see **Yes** underneath the **Encryption** and **Key Configured** fields:

1. Click the pencil icon at the upper right part of the **Global AES Encryption** area.

The **Global AES Encryption Settings** window appears.

2. Click the box next to the **Encryption: Enabled** area, enter a passphrase in the **Passphrase/Confirm Passphrase** fields, then click **Save** at the bottom of the window.


Make a note of the passphrase that you entered in this step, as you will need it in a step later in the following procedures.

Step 2 Back up your existing Cisco Cloud APIC configuration.

There are a number of different ways that you can back up your Cisco Cloud APIC configuration. See the [Cloud APIC for Azure Users Guide](#) for more information. Note that if you want to use a remote backup, you will also need to add a remote location first.

Step 3 If you have non-home region CSRs in your deployment, remove the CSRs from all regions *except the home region*.

Note You do not have to perform the procedures in this step if you do not have non-home region CSRs in your deployment. Skip to [Step 4, on page 6](#) in that case.

- a) In your Cisco Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

- c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.

You will be unselecting the boxes in the **Cloud Routers** column in the next step. When you restore the backed-up configuration later in these procedures, these same cloud router selections should be selected automatically. However, you can use the list that you note in this step if you want to verify that the same cloud routers were correctly selected.

- d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).
- e) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

After you click **Save and Continue**, wait until the following changes to take place:

- All of the non-home region CSR virtual machines are deleted from the Azure portal
- All of the public IP addresses for the CSR interfaces are deleted from the Azure portal
- All of the **Network interfaces** assigned to these virtual machines are deleted from the Azure portal

The process of removing the CSRs might take roughly a half hour. You can monitor the process of the CSR removal by looking at the virtual machines for the infra resource group in the Azure portal.

Step 4 Delete the Cisco Cloud APIC VM.

- a) In the Microsoft Azure portal, navigate to **Services > Virtual Machines**.
- b) Locate the Cisco Cloud APIC VM in the **Virtual Machines** window and click on the Cloud APIC VM.

The **Overview** page for the Cisco Cloud APIC VM appears.

- c) Click **Delete**, then click **Yes** when asked for confirmation of this action.

You can view the deletion process in the Notifications area.

What to do next

Follow the procedures in [Downloading and Deploying the Recovery Template, on page 7](#).

Downloading and Deploying the Recovery Template

Before you begin

Complete the procedures in [Performing Pre-Upgrade Procedures, on page 5](#) before proceeding with these procedures.

Step 1

Download the Release 5.0(2) recovery template for Cisco Cloud APIC.

- a) Go to the Cisco Software Download site for Cisco Cloud APIC and select the latest release, if it is not selected already:
<https://software.cisco.com/download/home/286323635/type/286325191/release/>
- b) Locate the **Cloud ACI image for recovery template** entry and click the download icon to download the json file.
Accept the license agreement when prompted to initiate the download.

Step 2

Deploy the Release 5.0(2) recovery template in the Azure portal.

- a) In the Azure portal, go to the **All Services** page:
<https://portal.azure.com/#allservices>
- b) In the **General** area, click **Templates**.
- c) In the **Templates** page, click **Add**.
The **Add Template** page appears.
- d) Enter the necessary information in the **Add Template** page.
 - **Name**: Enter a unique name that will identify this template as the Release 5.0(2) recovery template (for example, `template-502-recovery`).
 - **Description**: Enter descriptive text for this template, if necessary.
- e) Click **OK**.
The **ARM Template** page appears.
- f) In the **ARM Template** page, delete the default text that is automatically added in the template.
- g) Navigate to the area where you downloaded the Release 5.0(2) recovery template in [Step 1, on page 7](#).
- h) Using a text editor, open the Release 5.0(2) recovery template and copy the contents in the template.
- i) In the Azure portal window, paste the contents into the **ARM Template** page.
- j) Click **OK**.
The **Add Template** page appears again.
- k) Click **Add**.
The new Release 5.0(2) recovery template is added to the **Templates** page. If you do not see the new Release 5.0(2) recovery template in the **Templates** page, click **Refresh** to refresh the page.

Step 3

Use the recovery template to deploy the Cisco Cloud APIC VM in the same resource group.

- a) In the Templates page, click the new Release 5.0(2) recovery template that you just added.
- b) Click **Deploy**.

The **Custom Deployment** page appears.

- c) Enter the necessary information in the recovery template.

- **Basics:**

- **Subscription:** Choose the same subscription that you used when you first deployed your Cisco Cloud APIC, as described in [Subscription, on page 2](#).
- **Resource Group:** You must choose the same resource group that you used when you first deployed your Cisco Cloud APIC, as described in [Resource Group, on page 3](#).
- **Location:** Select the same region that you used when you first deployed your Cisco Cloud APIC, as described in [Location, on page 3](#).

Note The **Location** option might not be available when you are using the same resource group.

- **Settings:**

- **Vm Name:** Enter the same VM name that was used previously, as described in [Virtual Machine Name, on page 4](#).
- **Vm Size:** Select the size for the VM.
- **Image Sku:** Select the 5_0_2_byo1 image SKU.
- **Admin Username:** Leave the default entry for this field as-is. The admin username login will work once the Cisco Cloud APIC is up.
- **Admin Password or Key:** Enter an admin password.
- **Admin Public Key:** Enter the admin public key (the ssh key).
- **Fabric Name:** Enter the same fabric name that was used previously, as described in [Fabric Name, on page 3](#).
- **Infra VNET Pool:** Enter the same infra subnet pool that was used previously, as described in [Infra VNET Pool, on page 4](#).
- **External Subnets:** Enter the IP addresses and subnets of the external networks that were used previously to allow access to the Cisco Cloud APIC, as described in [External Subnets, on page 4](#). This would be the same external subnet pool for Cisco Cloud APIC access that you entered as part of the original deployment that you performed in [Deploying the Cloud APIC in Azure](#).
- **Storage Account Name:** Enter the same storage account name that was used previously, as described in [Storage Account Name, on page 5](#).
- **Virtual Network Name:** The name for the virtual network.
 - If you are performing an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default value for the virtual network name as-is for this field.
 - If you are performing a recovery from 5.0(2), verify that the virtual network name in this field matches the virtual network name that was originally used to deploy the Cisco Cloud APIC.
- **Mgmt Nsg Name:** The name for the management network security group.

- If you are performing a recovery or an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default value for the management network security group name as-is for this field.
 - If you are performing a recovery from 5.0(2), verify that the management network security group name in this field matches the management network security group name that was originally used to deploy the Cisco Cloud APIC.
 - **Mgmt Asg Name:** The name for the management application security group.
 - If you are performing a recovery or an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default value for the management application security group name as-is for this field.
 - If you are performing a recovery from 5.0(2), verify that the management application security group name in this field matches the management application security group name that was originally used to deploy the Cisco Cloud APIC.
 - **Subnet Prefix:** The entry for this field will be the subnet prefix that needs to be used for the automatically-configured infra subnet.
 - If you are performing an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default values as-is for this field.
 - If you are performing a recovery from 5.0(2), verify that the subnet prefix in this field matches the subnet prefix that was originally used to deploy the Cisco Cloud APIC. You can check that prefix by looking at the format of the subnet names on the Cisco Cloud APIC Virtual Network. For example, if subnet names shown there are **subnet-10.10.0.0_28**, then the subnet prefix for this field should be **subnet-**.
- d) Click the box next to the agreement statement, then click **Purchase**.
- The **Azure services** window appears, with a small popup window saying **Deployment in progress**. Click the Notifications icon to continue to monitor the progress of the deployment. The deployment usually takes roughly five or so minutes to complete.
- After a period of time, you will see the **Deployment succeeded** window.

What to do next

Follow the procedures in [Performing Post-Upgrade Procedures, on page 9](#).

Performing Post-Upgrade Procedures

Before you begin

Complete the procedures in [Downloading and Deploying the Recovery Template, on page 7](#) before proceeding with these procedures.

Step 1 Give the contributor role to the Cisco Cloud APIC VM on the infra subscription.

- a) In the Microsoft Azure portal, under **Services**, select **Subscription**.
- b) Select the subscription where Cisco Cloud APIC was deployed.
- c) Select **Access Control (IAM)**.
- d) On the top menu, click **Add > Add role assignment**.
- e) In the **Role** field, select **Contributor**.
- f) In the **Assign access to** field, select **Virtual Machine**.
- g) In the **Subscription** field, select the subscription where the Cisco Cloud APIC was deployed.
- h) In **Select**, click on the Cisco Cloud APIC Virtual Machine.
- i) Click **Save**.

Note Also give the contributor role to the Cisco Cloud APIC VM if you have managed user tenants. You must do this on user subscriptions that are used to deploy the user tenants. See [About Tenants](#) and [Adding a Role Assignment for a Virtual Machine](#) for more information.

Step 2 Enable the same encryption passphrase.

- a) In the Microsoft Azure portal, under **Services**, select **Virtual machines**.
- b) In the **Virtual machines** window, click the Cisco Cloud APIC.

The **Overview** page for the Cisco Cloud APIC appears.

- c) Locate the **Public IP address** field and copy the IP address.
- d) In another browser window, enter the IP address and hit Return:

```
https://<IP_address>
```

The **Welcome to Cloud APIC** screen appears after logging in for the first time.

- e) Click **Begin First Time Setup**.

The **Let's Configure the Basics** window appears. Click the **X** in the upper right corner to exit out of this window to proceed with procedures to enable the same encryption passphrase.

- f) In your Cisco Cloud APIC GUI, navigate to **Infrastructure > System Configuration**.

It should be underneath the **General** tab by default; if not, click the **General** tab.

After first login, welcome screen appears. Click begin first time setup. first time setup page opens, close the first time setup pagethen user can proceed to setting the pass phrase.

- g) In the **Global AES Encryption** area, click the pencil icon at the upper right part of the **Global AES Encryption** area.

The **Global AES Encryption Settings** window appears.

- h) Click the box next to the **Encryption: Enabled** area, enter the same passphrase in the **Passphrase/Confirm Passphrase** fields that you used in [Step 1, on page 5 in Performing Pre-Upgrade Procedures, on page 5](#), then click **Save** at the bottom of the window.

Step 3 Import the configuration that you backed up in [Step 2, on page 6 in Performing Pre-Upgrade Procedures, on page 5](#).

If you configured a remote location when you backed up your configuration, you might have to create the remote location again to access the backup.

- a) In your Cisco Cloud APIC GUI, navigate to **Operations > Backup & Restore**.
- b) In the **Backup & Restore** window, click the **Backups** tab.
- c) Click the **Actions** scrolldown menu, then choose **Restore Configuration**.

The **Restore Configuration** window appears.

- d) Enter the necessary information to restore the configuration that you backed up in [Step 2, on page 6](#) in [Performing Pre-Upgrade Procedures, on page 5](#).

If you are upgrading from a 4.2(x) release to Release 5.0(x) or later, for this particular backup restore, use the following settings:


- In the **Restore Type** field, choose **Merge**.
- In the **Restore Mode** field, choose **Best Effort**.

Click **Restore Configuration** when you have entered the necessary information in this window.

- e) Wait until the restore process is complete before proceeding to the next step.

Click the **Job Status** tab in the **Backup & Restore** window to get the status of the restore process and verify that the restore process was successful.

Step 4 Review the naming policy.

- a) In your Cisco Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

- c) Verify that the selections that you had prior to the migration were transferred over successfully with the backup import, then click **Next**.

Note Do not modify the managed region or CSR configuration at this point.

- d) Navigate to the last page in the setup and review the information in the **Cloud Resource Naming Rules** area.
- If you are performing a recovery or an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the default cloud resource naming rules. Leave the default cloud resource naming rules as-is in this case.
 - If you are performing a recovery from 5.0(2), verify that the cloud resource naming rules match the cloud resource naming rules that were originally used to deploy the Cisco Cloud APIC.

Click the box next to **Deploy cloud resources based on these naming rules**, then click **Save and Continue** after reviewing the information in this screen. Resources will not be deployed to the cloud until the naming rules have been reviewed and accepted.

At this point in the process, the non-home region CSRs will be deployed automatically with the new CSR image.

Note Allow for some time to pass for the Cisco Cloud APIC to clear all of the faults before proceeding to the next step. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 5 Wait for the non-home region CSRs to come up on the cloud, and ensure that all of the VGW tunnels are up with the newly-created CSRs and the configuration reconciliation is complete.

In addition, you may see that the home region CSR is deleted and recreated at this point in the process if a CSR upgrade is required. Ignore these actions and any faults that might appear as a result, as they will clear up when you complete the following steps in this procedure.

Wait until the home region CSRs are upgraded to the latest CSR version in this case. For example, for Release 5.0(2i), the latest CSR version would be 17_1.

Step 6 (Optional) If you have intersite connectivity and you want to avoid a complete intersite traffic drop, reconfigure the non-home region intersite tunnels and bring up the tunnels through the ACI Multi-Site Orchestrator before bringing down the home region CSRs in the next step.

This step is not necessary if you do not have intersite connectivity or if you have intersite connectivity but you're not concerned with traffic loss.

a) In the ACI Multi-Site Orchestrator, in the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

b) In the left pane, under **SITES**, click on the cloud site.

c) Click **Reload Site Data**.

d) Verify that the new CSRs are added in the UI.

e) Click the **Deploy** button at the top right of the screen, then choose the **Deploy & Download IPN Device config files** option.

This action pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect connectivity between the on-premises and the cloud site. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

Note If you delete and recreate intersite tunnels on the cloud CSRs from the Cisco Cloud APIC in this step, and you need to program the new keys on the on-premises IPsec termination device, where you are going to change the key for the same public IP address of the cloud CSRs, you must first manually delete the existing keys on the on-premises IPsec termination device and add a new key. There should be only one matching IPsec pre-shared key for a given cloud CSR destination IP address on the on-premises IPsec termination device.

Step 7 Undeploy the home region CSRs.

Note If you are upgrading from 4.2(3) to 5.0(2), undeploying and redeploying the home region CSRs also migrates the CSR public IP SKU from the basic SKU to the standard SKU.

a) In your Cisco Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.

b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate the home region (the region that has the text **Cloud APIC Deployed**) and unselect the boxes in the **Cloud Routers** column for the home region.

d) Click **Save**.

This removes the old CSRs for the home region.

e) Wait for home region CSR VMs, CSR NICs, and CSR public IP addresses to get deleted on the cloud.

Once the home region CSR VMs, CSR NICs, and CSR public IP addresses are deleted on the cloud, you can redeploy the CSRs back in the home region.

Step 8 Redeploy the home region CSRs.

The previously-configured home region CSRs are deleted and the new home region CSRs are re-created in this step.

a) Click **Previous** to return to the **Regions to Manage** screen, then click the boxes in the **Cloud Routers** column for the home region to re-enable the CSRs for the home region.

- b) Click **Save**.

If you are upgrading from 4.2(3) to 5.0(2), this action migrates the CSR Public IP SKU to the standard SKU for the home region.

Step 9 (Optional) Complete the procedures in this step if intersite connectivity is required.

- If intersite connectivity is not required, then you do not have to complete the procedures in this step. Skip to [Migrating to VNet Peering \(Optional\), on page 13](#) in that case.
- If intersite connectivity is required, then complete the following procedures:
 - a) Once the new home region CSRs come up, in the ACI Multi-Site Orchestrator, in the **Sites** screen, click **CONFIGURE INFRA**.
The **Fabric Connectivity Infra** page appears.
 - b) In the left pane, under **SITES**, click on the cloud site.
 - c) Click **Reload Site Data**.
 - d) Verify that the new CSRs are added in the UI.
 - e) Click the **Deploy** button at the top right of the screen, then choose the **Deploy & Download IPN Device config files** option.
 - f) Reconfigure the IPN IPsec tunnels on the on-premises CSR with the downloaded IPN configuration.

See [Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices](#).

Note If you delete and recreate intersite tunnels on the cloud CSRs from the Cisco Cloud APIC for any reason, and you need to program the new keys on the on-premises IPsec termination device, where you are going to change the key for the same public IP address of the cloud CSRs, you must first manually delete the existing keys on the on-premises IPsec termination device and add a new key. There should be only one matching IPsec pre-shared key for a given cloud CSR destination IP address on the on-premises IPsec termination device.

What to do next

If you want to migrate to Azure VNet peering for inter-VNet connectivity, follow the procedures in [Migrating to VNet Peering \(Optional\), on page 13](#).

Migrating to VNet Peering (Optional)


Follow the procedures in this task if you want to migrate to Azure VNet peering for inter-VNet connectivity rather than using the traditional tunnel-based VPN connectivity through the CSRs. For more information on the VNet peering feature, see the [Configuring VNet Peering for Cloud APIC for Azure](#) document.



Note Migrating to VNet peering mode is a disruptive operation. Be aware that there will be traffic loss during the process.

Before you begin

Complete the procedures in [Performing Post-Upgrade Procedures, on page 9](#) before proceeding with these procedures.

Step 1 In your Cisco Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.

Step 2 In the **Region Management** area, click **Edit Configuration**.

The **Regions to Manage** window appears.

Step 3 Locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.

Step 4 Click **Virtual Network Peering** to enable the Azure VNet peering feature.

This enables VNet peering at the Cisco Cloud APIC level, deploying NLBs in all the regions with CSRs in the infra VNet.

After you have enabled VNet peering at the Cisco Cloud APIC level, on each user cloud context profile, you will have to enable the **VNet Peering** option and disable the **VNet Gateway Router** option.

Note The following steps describe how to enable VNet peering on each cloud context profile through the Cisco Cloud APIC GUI. You can also perform the following steps through the ACI Multi-Site Orchestrator, if you want.

Step 5 In the left navigation bar, navigate to **Application Management > Cloud Context Profiles**.

The existing cloud context profiles are displayed.

Step 6 Click Actions and choose **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

Step 7 Locate the **VNet Gateway Router** field and click to uncheck (disable) the **VNet Gateway Router** check box.

Step 8 Locate the **VNet Peering** field and click to check (enable) the **VNet Peering** check box.

Step 9 Click **Save** when finished.

Step 10 Configure the Network Contributor role for both the infra and user tenant subscriptions.

For example, assume the following:

- The infra tenant is using subscription **S1** with access credentials/service principal **C1**
- The user tenant is using subscription **S2** with access credentials/service principal **C2**

In this situation, you will have to configure the following for peering to work between the user tenant and the infra VNets:

- You will have to give C1 Network Contributor role permissions to S2 for the hub to spoke peering link
- You will have to give C2 Network Contributor role permissions to S1 for the spoke to hub peering link

a) In the yellow window that appears, copy the **az** command provided.

- If you have configured the Network Contributor role for the user tenant, copy the text in the area **Command to run for User Subscription**.
- If you have configured the Network Contributor role for the infra tenant, copy the text in the area **Command to run for Infra Subscription**.

- b) Return to the Azure management portal and click **Registrations** in the left navigation bar.
- c) Open the Cloud Shell.
- d) Select **Bash**.
- e) Paste the **az** command that you copied in [10.a, on page 14](#).

Policy-Based Upgrade

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software, if you are upgrading from Release 5.0(1) to Release 5.0(2).

Downloading an Image

- Step 1** Log in to your Cisco Cloud APIC, if you aren't logged in already.
- Step 2** From the **Navigation** menu, choose **Operations > Firmware Management**.
The **Firmware Management** window appears.
- Step 3** Click the **Images** tab in the **Firmware Management** window.
- Step 4** Click **Actions**, then choose **Add Firmware Image** from the scroll-down menu.
The **Add Firmware Image** pop-up appears.
- Step 5** Determine if you want to add the firmware image from a local or a remote location.
- If you want to add the firmware image from a *local* location, click the **Local** radio button in the **Image Location** field. Click the **Choose File** button, then navigate to the folder on your local system with the firmware image that you want to import and select the file. Go to [Step 6, on page 16](#).
 - If you want to import the firmware image from a *remote* location, click the **Remote** radio button in the **Image Location** field, then perform the following actions:
 - a) In the **Protocol** field, click either the **HTTP** or the **SCP** radio button.
 - b) In the **URL** field, enter the URL from where the image will be downloaded.
 - If you selected the **HTTP** radio button in the previous step, enter the http source that you want to use to download the software image. An example URL is `10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`. Go to [Step 6, on page 16](#).
 - If you selected the **SCP** radio button in the previous step, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image, using the format `<SCP server>:/<path>`. An example URL is `10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`.
 - c) In the **Username** field, enter your username for secure copy.
 - d) In the **Authentication Type** field, select the type of authentication for the download. The type can be:
 - **Password**
 - **SSH Key**

The default is **Password**.

- e) If you selected **Password**, in the **Password** field, enter your password for secure copy. Go to [Step 6, on page 16](#).
- f) If you selected **SSH Key**, enter the following information:
 - **SSH Key Content** — The SSH Key Content is used to create the SSH Key File which is required when creating a Remote location for the download.
 - Note** The public key is generated at the time of the transfer. After the transfer the key files that were generated in the background are deleted. The temporary key files are stored in dataexport directory of the Cisco Cloud APIC.
 - **SSH Key Passphrase** — The SSH Key Passphrase is used to create the SSH Key File which is required when creating a Remote location for the download.
 - Note** The Passphrase field can remain empty.

Step 6 Click **Select**.
Wait for the Cisco Cloud APIC firmware images to download.

Upgrading the Software Using the Policy-Based Upgrade Process

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software, if you are upgrading from Release 5.0(1) to Release 5.0(2).


Before you begin

- You have downloaded an image using the procedures provided in [Downloading an Image, on page 15](#).

- Step 1** Subscribe to the 17.1 image for the Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL) for Release 5.0(2).
- a) In the [Azure Marketplace](#) search text field, type *Cisco Cloud Services Router (CSR) 1000V* and select the option that appears.
The **Cisco Cloud Services Router (CSR) 1000V** option appears as a search suggestion.
 - b) Click the **Cisco Cloud Services Router (CSR) 1000V** option.
You should be redirected to the **Cisco Cloud Services Router (CSR) 1000V** page in the Microsoft Azure Marketplace.
 - c) Locate the **Select a software plan** drop-down menu.
If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.
 - d) In the **Select a software plan** drop-down menu, select the **Cisco CSR 1000V Bring Your Own License - XE 17.1** option.
 - e) Locate the **Want to deploy programmability?** field and click **Get Started**.
 - f) In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.
 - g) Click **Save**.

Step 2 Remove the CSRs from all regions *except the home region*.

Note Do not remove the CSR from the home region at this point. Removing the CSR for the home region at this point will cause an outage.

- a) In your Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.
The **Regions to Manage** window appears.
- c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.
You will be unselecting the boxes in the **Cloud Routers** column in the next step, so make sure you know which regions will need to be selected again at the end of this procedure.
- d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).
- e) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

The process of removing the CSRs might take roughly a half hour. You can monitor the process of the CSR removal by looking at the virtual machines for the resource group in the Azure portal.

Step 3 When the necessary CSRs have been completely removed, from the **Navigation** menu, choose the **Operations > Firmware Management**.

The **Firmware Management** window appears.

Step 4 Click **Schedule Upgrade**.

The **Schedule Upgrade** pop-up appears.

If you see a message that says that faults are present in your fabric, we recommend that you resolve these faults before performing an upgrade. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 5 In the **Target Firmware** field, choose a firmware image from the scroll-down menu.

Step 6 In the **Upgrade Start Time** field, determine if you want to begin the upgrade now or later.

- Click **Now** if you want to schedule the upgrade for now. Go to [Step 7, on page 17](#).
- Click **Later** if you want to schedule the upgrade for a later date or time, then select the date and time from the pop-up calendar for the scheduled upgrade.

Step 7 In the **Ignore Compatibility Check** field, leave the setting in the default off (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

In Cloud APIC, there is a compatibility check feature that verifies if an upgrade path from the currently-running version of the system to a specific newer version is supported or not. The **Ignore Compatibility Check** setting is set to off by default, so the system automatically checks the compatibility for possible upgrades by default.


Note If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Ignore Compatibility Check** field, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

Step 8 Click **Schedule Upgrade**.

You can monitor the progress of the upgrade in the main **Firmware Management** window, under the **Upgrade Status** area.

Step 9 When the upgrade is completed, add the necessary CSRs back again.

Verify that the home region CSR is stabilized before adding the CSRs in the other regions back again.


- a) In your Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.
The **Regions to Manage** window appears.
- c) Locate all of the regions that had CSRs and check the boxes in the **Cloud Routers** column for each of those regions to add the CSRs back again.
- d) Click Next, then enter the necessary information in the following page and click **Save and Continue**.

Step 10 Determine if you want to migrate to Azure VNet peering for inter-VNet connectivity rather than using the traditional tunnel-based VPN connectivity through the CSRs.

For more information on the VNet peering feature, see the [Configuring VNet Peering for Cloud APIC for Azure](#) document.

Note Migrating to VNet peering mode is a disruptive operation. Be aware that there will be traffic loss during the process.

Follow these instructions to enable the VNet peering feature:

- a) In your Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
- b) In the **Region Management** area, click **Edit Configuration**.
The **Regions to Manage** window appears.
- c) Locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.
 - If the **Virtual Network Peering** is available, then the home region CSR has already been successfully migrated from the basic SKU to the standard SKU. Go to [10.i, on page 18](#) in this case.
 - If the **Virtual Network Peering** is not available, that means that the home region CSR is still set to the basic SKU rather than the updated standard SKU. Continue to [10.d, on page 18](#) to migrate the home region CSR to the standard SKU.
- d) Locate the home region (the region that has the text **Cloud APIC Deployed**) and unselect the box in the **Cloud Routers** column for the home region.
- e) Click **Save**.
This action removes the CSR with the basic SKU for the home region.
- f) Click **Previous** to return to the **Regions to Manage** screen, then click the box in the **Cloud Routers** column for the home region to re-enable the CSR for the home region.
- g) Click **Save**.
This action adds the CSR with the standard SKU for the home region.
- h) Click **Previous** to return to the **Regions to Manage** screen, then locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.
- i) Click **Virtual Network Peering** to enable the Azure VNet peering feature.

This enables VNet peering at the Cloud APIC level, deploying NLBs in all the regions with CSRs in the infra VNet.

Note The **VPN Connectivity via CSR** option is used to enable the traditional VPN connectivity through the overlay IPsec tunnels between CSRs and Azure VPN Gateway routers, instead of using VNet peering.

After you have enabled VNet peering at the Cloud APIC level, on each user cloud context profile, you will have to enable the **VNet Peering** option and disable the **VNet Gateway Router** option.

- j) In the left navigation bar, navigate to **Application Management > Cloud Context Profiles**.

The existing cloud context profiles are displayed.

- k) Click Actions and choose **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

- l) Locate the **VNet Gateway Router** field and click to uncheck (disable) the **VNet Gateway Router** check box.

- m) Locate the **VNet Peering** field and click to check (enable) the **VNet Peering** check box.

- n) Click **Save** when finished.

Downgrading the Software

The following sections provide the necessary information that you will need to successfully downgrade your Cisco Cloud APIC software.

Downgrading the Software

Before you begin

The following prerequisites apply if you are downgrading from 5.0(2) to a release prior to 5.0(2):

- If your Cisco Cloud APIC has always been running on Release 5.0(2) [if you never upgraded from a release prior to 5.0(2) to Release 5.0(2)], then you cannot downgrade to a release prior to Release 5.0(2) on your Cisco Cloud APIC. Downgrading to a release prior to 5.0(2) when your Cisco Cloud APIC never ran on that prior release is not supported.
- If you upgraded your Cisco Cloud APIC to Release 5.0(2) and you completed certain Release 5.0(2)-specific configurations afterwards, such as VNet peering, and you want to downgrade to a release prior to Release 5.0(2), you will have to remove the CSRs from all the regions except the home region. Go to [Step 1, on page 19](#) for those instructions.
- If you upgraded your Cisco Cloud APIC to Release 5.0(2) but you never completed any Release 5.0(2)-specific configurations afterwards, such as VNet peering, and you want to downgrade to a release prior to Release 5.0(2), you do not have to remove CSRs from any regions. Go to [Step 4, on page 20](#) in that case.

Step 1

Remove the 5.0(2)-specific configurations before downgrading.


For example, to remove the VNet peering configurations, first disable Azure VNet peering at the local level, through the Cloud Context Profile:

- a) Navigate to the **Create Cloud Context Profile** page:

Application Management > Cloud Context Profiles, then click **Actions** and choose **Create Cloud Context Profile**

- b) Double-click the cloud context profile where you want to disable VNet peering.
- c) Uncheck (disable) the **Hub Network Peering** field.

Then disable Azure VNet peering at the global level:

- a) In the Cloud APIC GUI, click the Intent icon () and select **cAPIC Setup**. In the **Region Management** area, click **Edit Configuration**.
- b) In the **Regions to Manage** screen, change the **Connectivity for Internal Network** setting from **Virtual Network Peering** to **VPN Connectivity via CSR**.

Step 2 Remove the CSRs from all regions except the home region.

- a) In your Cloud APIC GUI, click the Intent icon (the icon with an arrow pointing into several circles) and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

- c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.
You will be unselecting the boxes in the **Cloud Routers** column in the next step, so make sure you know which regions will need to be selected again at the end of this procedure.
- d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).
- e) Click Next, then enter the necessary information in the following page and click **Save and Continue**.

The process of removing the CSRs might take roughly a half hour.

Step 3 Verify that the necessary CSRs have been completely removed before proceeding.

- a) Click the Intent icon again and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

- c) Locate the **Connectivity for Internal Network** area and wait for the **Virtual Network Peering** option to become available.

If the **Virtual Network Peering** is not available, that means that the CSRs are still in the process of being deleted.

Wait for the **Virtual Network Peering** option to become available before proceeding with the next step.

Step 4 Download an image for the downgrade using the procedures provided in [Downloading an Image, on page 15](#).

Step 5 When the image is fully downloaded, from the **Navigation** menu, choose the **Operations > Firmware Management**.

The **Firmware Management** window appears.

Step 6 Click **Schedule Upgrade**.

The **Schedule Upgrade** pop-up appears.

If you see a message that says that faults are present in your fabric, we recommend that you resolve these faults before performing a downgrade. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 7 In the **Target Firmware** field, choose a firmware image from the scroll-down menu.

Step 8 In the **Upgrade Start Time** field, determine if you want to begin the downgrade now or later.

- Click **Now** if you want to schedule the downgrade for now. Go to [Step 9, on page 21](#).
- Click **Later** if you want to schedule the downgrade for a later date or time, then select the date and time from the pop-up calendar for the scheduled downgrade.

Step 9 In the **Ignore Compatibility Check** field, leave the setting in the default off (unchecked) setting, unless you are specifically told to disable the compatibility check feature.


In Cloud APIC, there is a compatibility check feature that verifies if an downgrade path from the currently-running version of the system to a specific newer version is supported or not. The **Ignore Compatibility Check** setting is set to off by default, so the system automatically checks the compatibility for possible downgrades by default.

Note If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Ignore Compatibility Check** field, you run the risk of making an unsupported downgrade to your system, which could result in your system going to an unavailable state.

Step 10 Click **Schedule Upgrade**.

You can monitor the progress of the downgrade in the main **Firmware Management** window, under the **Upgrade Status** area.

Step 11 When the downgrade is completed, add the necessary CSRs back again.

- a) In your Cloud APIC GUI, click the Intent icon () and choose **cAPIC Setup**.
- b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

- c) Locate all of the regions that had CSRs and check the boxes in the **Cloud Routers** column for each of those regions to add the CSRs back again.
- d) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

Performing a System Recovery

The procedures for performing a system recovery is identical to the procedures for performing a migration-based upgrade. Refer to the section [Migration-Based Upgrade, on page 2](#) for those procedures.

