



Performing a System Upgrade, Downgrade or Recovery

- [Important Notes, on page 1](#)
- [Upgrading the Software, on page 4](#)
- [Downgrading the Software, on page 22](#)
- [Performing a System Recovery, on page 27](#)
- [Triggering an Upgrade of the CCRs, on page 27](#)

Important Notes

- [Important Notes For Release 25.0\(3\), on page 1](#)
- [General Important Notes, on page 3](#)

Important Notes For Release 25.0(3)

Following are important notes for release 25.0(3) regarding the installation, upgrade or downgrade procedures for the Cisco Cloud APIC:

- The Cisco Catalyst 8000V supports subscription-based licensing. Before upgrading from a release prior to 25.0(3) to release 25.0(3), you must first subscribe to one of the tier-based Cisco Catalyst 8000V licenses.
 - For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see [Cisco Catalyst 8000V Edge Software](#).
 - For more information on different throughputs based on the tiers, see [Requirements for the Azure Public Cloud](#).

Cisco Cloud APIC makes use of the “Cisco DNA Advantage” subscription. For features supported by the “Cisco DNA Advantage” subscription, see [Cisco DNA SoftwareSD-WAN and Routing Matrices](#).

- When you upgrade your Cisco Cloud APIC to release 25.0(3), you should then upgrade the CCRs as soon after the Cisco Cloud APIC upgrade as possible. For those instructions, see:
 - [Upgrading the Software, on page 4](#)
 - [Triggering an Upgrade of the CCRs, on page 27](#)

Following are examples of how you would go through these upgrade processes:

- **Single-Site Upgrade:** You normally would have CCRs for a single-site Azure deployment. Once the Cisco Cloud APIC has completed the upgrade to release 25.0(3) and reached the ready state, you must then start the upgrade of the older CCRs (the Cisco Cloud Services Router 1000v) to the newer CCRs (the Cisco Catalyst 8000V) before making any configuration changes.
- **Multi-Cloud/Hybrid-Cloud Upgrade:** As an example of this upgrade process, assume that you have the following setup:
 - Site 1: AWS
 - Site 2: Azure
 - Site 3: On-premises site

You would then upgrade these sites the following way:

1. Upgrade Nexus Dashboard Orchestrator to the 3.7(1) release.
2. Upgrade site 1 (AWS site) to the Cisco Cloud APIC release 25.0(3) using the procedures in [Upgrading the Software, on page 4](#).

Wait until this upgrade has reached the steady state before proceeding to the next step.

3. Upgrade the CCRs on site 1 (AWS site) from the older CCRs (the Cisco Cloud Services Router 1000v) to the newer CCRs (the Cisco Catalyst 8000V) using the procedures in [Triggering an Upgrade of the CCRs, on page 27](#).

Wait until the CCRs are fully upgraded to the newer Cisco Catalyst 8000Vs before proceeding to the next step.

4. Once the CCRs on site 1 (AWS site) are fully upgraded, repeat these steps for site 2 (Azure site), where you will first upgrade the Cisco Cloud APIC software to release 25.0(3). After that upgrade has reached the steady state, then you will upgrade the CCRs on site 2 to the newer Cisco Catalyst 8000Vs.

- Prior to Cisco Cloud APIC release 25.0(3), the older Cisco Cloud Services Router 1000v routers were configured with number-based throughput, as described in [Requirements for the Azure Public Cloud](#). Since the Cisco Catalyst 8000V routers will only support tier-based throughput options, during upgrades to release 25.0(3), the Cisco Cloud APIC will map the throughput values from the number-based throughput used by the older Cisco Cloud Services Router 1000v routers to the tier-based throughput used by the newer Cisco Catalyst 8000V routers.

The following table shows the mapping of throughput from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade:

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
10M	T0 (up to 15M throughput)
50M	T1 (up to 100M throughput)
100M	T1 (up to 100M throughput)
250M	T2 (up to 1G throughput)

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
500M	T2 (up to 1G throughput)
1G	T2 (up to 1G throughput)
2.5G	T3 (up to 10G throughput)
5G	T3 (up to 10G throughput)
7.5G	T3 (up to 10G throughput)
10G	T3 (up to 10G throughput)

When migrating from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade, the Cisco Cloud APIC will migrate the comparable bandwidth as described above. When these Cisco Catalyst 8000V routers come up, they will try to register for that bandwidth to the smart licensing account. If the smart licensing server does not have these licenses, then the Cisco Catalyst 8000V will fall back to the default bandwidth and will fail to service the existing workload traffic. So you must procure and provision the required Cisco Catalyst 8000V licenses in your smart account before migrating from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade.

- Similarly, when downgrading from release 25.0(3) to an earlier release, the Cisco Cloud APIC will map the throughput values from the tier-based throughput used by the newer Cisco Catalyst 8000V routers to the number-based throughput used by the older Cisco Cloud Services Router 1000v routers.

The following table shows the mapping of throughput from the newer Cisco Catalyst 8000V routers to the number-based throughput used by the older Cisco Cloud Services Router 1000v routers during a downgrade:

Throughput on Cisco Catalyst 8000V	Throughput on Cisco Cloud Services Router 1000v
T0 (up to 15M throughput)	10M
T1 (up to 100M throughput)	100M
T2 (up to 1G throughput)	1G
T3 (up to 10G throughput)	10G



Note Do not make any configuration changes when the Cisco Cloud APIC and the CCRs are in incompatible mode. When upgrading to release 25.0(3), verify that both the Cisco Cloud APIC and the CCRs are upgraded to that latest release before making any configuration changes.

General Important Notes

Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths:

- Release 5.2(1) to 25.0(2), 25.0(3), or 25.0(4)

- Release 25.0(1) to 25.0(2), 25.0(3), or 25.0(4)
- Release 25.0(2) to 25.0(3) or 25.0(4)
- Release 25.0(3) to 25.0(4)

Upgrading the Software

The following sections provide information on upgrading the Cisco Cloud APIC software using either a migration-based upgrade or a policy-based upgrade. Before upgrading your Cisco Cloud APIC software, review the information provided in [Guidelines and Limitations For Upgrading the Software, on page 5](#).

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(x) release to release 5.1(2) or later, you will use a migration-based process to upgrade your software. Go to [Migration-Based Upgrade, on page 5](#) 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 27](#).

- If you are upgrading from release 5.0(x) or later to release 5.1(2) or later, you will use a policy-based process to upgrade your software.

For example, Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths:

- Release 5.2(1) to 25.0(2), 25.0(3), or 25.0(4)
- Release 25.0(1) to 25.0(2), 25.0(3), or 25.0(4)
- Release 25.0(2) to 25.0(3) or 25.0(4)
- Release 25.0(3) to 25.0(4)

Go to [Policy-Based Upgrade, on page 17](#) for those procedures.



Note If the policy-based upgrade does not work for some reason, you can upgrade using the migration-based process as described in [Migration-Based Upgrade, on page 5](#).

Upgrading the CCRs

Regardless of the method that you use to upgrade your Cisco Cloud APIC software, the Cloud Routers (CCRs) must also be upgraded whenever the Cloud APIC software is upgraded.

- Prior to release 5.2(1), the CCRs are upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC.

- Beginning with release 5.2(1), you can trigger upgrades to the CCRs and monitor those CCR upgrades, independent from the Cisco Cloud APIC upgrades. This is useful to reduce traffic loss by allowing you to split up the upgrades for the management plane (Cisco Cloud APIC) and the data plane (CCRs).

See [Triggering an Upgrade of the CCRs, on page 27](#) for more information.

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 to use a migration-based process to upgrade your software.

Review the information provided in [Guidelines and Limitations For Upgrading the Software, on page 5](#) before performing the procedures in this section.



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 27](#).

Gathering Existing Cloud APIC Configuration Information

Before upgrading or downgrading 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 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 6](#)
- [Resource Group, on page 6](#)
- [Location, on page 6](#)
- [Fabric Name, on page 6](#)
- [External Subnets, on page 7](#)
- [Virtual Machine Name, on page 7](#)
- [Infra VNET Pool, on page 8](#)

- [Storage Account Name, on page 8](#)

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 7](#).
- `(<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=0X7EEEEEEEEEE--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 6](#).

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.

Backing Up Your Existing Configuration

We recommend that you back up your existing configuration before performing a migration-based upgrade, in case you decide to roll back to the previous release for any reason afterwards.

Before you begin

Complete the procedures in [Gathering Existing Cloud APIC Configuration Information, on page 5](#) before proceeding with these procedures.

-
- Step 1** Enable Global AES encryption before performing the backup.

- a) In your Cisco Cloud APIC GUI, navigate to **Infrastructure > System Configuration**.
You should see the **General** tab selected by default; if not, click the **General** tab.
- b) Click the pencil icon at the upper right part of the **Global AES Encryption** area.
The **Global AES Encryption Settings** window appears.
- c) 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 if you need as part of the backup restoration process.

Step 2 Back up your existing configuration.

- a) Navigate to **Operations > Backup & Restore**.
- b) Click the **Backup Policies** tab.
- c) Click **Actions > Create Backup Configuration**.
- d) Back up your existing configuration.

For more information on the options available in the **Create Backup Configuration**, see the "Creating a Backup Configuration Using the Cisco Cloud APIC GUI" procedure in the *Cisco Cloud APIC for Azure User Guide*.

Step 3 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.

Downloading and Deploying the Recovery Template

Before you begin

Complete the procedures in [Backing Up Your Existing Configuration, on page 8](#) before proceeding with these procedures.

Step 1 Download the appropriate recovery template for your release for Cisco Cloud APIC.

Contact Cisco TAC to get the appropriate recovery template:

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Step 2 Deploy the 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 a release-specific recovery template (for example, for the release 25.0(1) recovery template, you might use `template-2501-recovery` as the release-specific unique name).
 - **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 recovery template in [Step 1, on page 9](#).
- h) Using a text editor, open the 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 recovery template is added to the **Templates** page. If you do not see the new 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 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 6](#).
 - **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 6](#).
 - **Location:** Select the same region that you used when you first deployed your Cisco Cloud APIC, as described in [Location, on page 6](#).
 - 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 7](#).
 - **Vm Size:** Select the size for the VM.
 - **Image Sku:** Select the appropriate image SKU. For example, for release 25.0(1), select `25_0_1_byo1`.

- **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 6](#).
- **Infra VNET Pool:** Enter the same infra subnet pool that was used previously, as described in [Infra VNET Pool, on page 8](#).
- **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 7](#). 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 8](#).
- **Virtual Network Name:** 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:** 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:** 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.

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-**. 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 12](#).

Performing Post-Upgrade Procedures

Before you begin

Complete the procedures in [Downloading and Deploying the Recovery Template, on page 9](#) 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 [Understanding Tenants, Identities, and Subscriptions](#) 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 page then 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 [Backing Up Your Existing Configuration, on page 8](#), then click **Save** at the bottom of the window.

Step 3

If you are performing a migration-based upgrade to release 25.0(1), run the Python script to clean up the necessary configuration before importing the configuration that you backed up earlier.

Contact Cisco TAC to get the Python script to address the issue raised in [CSCvy42684](#) to clean up the necessary configuration:

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Step 4

Import the configuration that you backed up in [Backing Up Your Existing Configuration, on page 8](#).

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** scroll-down menu, then choose **Restore Configuration**.

The **Restore Configuration** window appears.

- d) Enter the necessary information to restore the configuration that you backed up in [Backing Up Your Existing Configuration, on page 8](#).

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 5

Review the naming policy.

- a) In your Cisco Cloud APIC GUI, click the Intent icon () and choose **Cloud APIC 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 CCR configuration at this point.

- d) Navigate to the last page in the setup and review the information in the **Cloud Resource Naming Rules** area.

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 CCRs will be deployed automatically with the new CCR 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 6 Wait for the non-home region CCRs to come up on the cloud, and ensure that all of the VGW tunnels are up with the newly-created CCRs and the configuration reconciliation is complete.

In addition, you may see that the home region CCR is deleted and recreated at this point in the process if a CCR 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 CCRs are upgraded to the latest CCR version in this case.

Step 7 (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 Cisco Nexus Dashboard Orchestrator before bringing down the home region CCRs 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 Cisco Nexus Dashboard 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 CCRs 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 CCR 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 CCRs 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 CCRs, 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 CCR destination IP address on the on-premises IPsec termination device.

Step 8 Undeploy the home region CCRs.

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 CCRs for the home region.

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

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

Step 9

Redeploy the home region CCRs.

The previously-configured home region CCRs are deleted and the new home region CCRs 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 CCRs for the home region.
- b) Click **Save**.

Step 10

(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 15](#) in that case.

- If intersite connectivity is required, then complete the following procedures:

- a) Once the new home region CCRs come up, in the Cisco Nexus Dashboard 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 CCRs 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 CCR 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 CCRs 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 CCRs, 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 CCR 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 15](#).

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 CCRs. 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 12](#) 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 CCRs 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 Cisco Nexus Dashboard 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 17](#).
-

Policy-Based Upgrade

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software.

Review the information provided in [Guidelines and Limitations For Upgrading the Software, on page 5](#) before performing the procedures in this section.

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 18](#).
 - 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-capic-dk9.25.0.2f.iso`. Go to [Step 6, on page 18](#).

- 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-capic-dk9.25.0.2f.iso**.

- In the **Username** field, enter your username for secure copy.
- In the **Authentication Type** field, select the type of authentication for the download. The type can be:

- **Password**
- **SSH Key**

The default is **Password**.

- If you selected **Password**, in the **Password** field, enter your password for secure copy. Go to [Step 6, on page 18](#).
- 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.

Before you begin

- You have downloaded an image using the procedures provided in [Downloading an Image, on page 17](#).

- Step 1** Subscribe to the correct image for the CCR.

- For releases prior to release 25.0(3), to subscribe to the image for the **Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL)**:
 - 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.
 - 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 17.3.1a** 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**.
 - For release 25.0(3) or later, to subscribe to the image for the **Cisco Catalyst 8000V Edge Software - Bring Your Own License (BYOL)**:
 - a) In the [Azure Marketplace](#) search text field, type *Cisco Catalyst 8000V Edge Software* and select the option that appears.
The **Cisco Catalyst 8000V Edge Software** option appears as a search suggestion.
 - b) Click the **Cisco Catalyst 8000V Edge Software** option.
You should be redirected to the **Cisco Catalyst 8000V Edge Software** 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 Catalyst 8000V Edge Software-BYOL-17.7.1** 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

If you are upgrading from **release 5.0(1)**, remove the CCRs from all regions *except the home region*.

Note If you are upgrading from **release 5.0(2)** or later, do not remove any CCRs. Go to [Step 3, on page 20](#) in this case.

Do not remove the CCR from the home region at this point. Removing the CCR 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 CCRs might take roughly a half hour. You can monitor the process of the CCR removal by looking at the virtual machines for the resource group in the Azure portal.

Do not proceed to the next step until the necessary CCRs have been completely removed.

Step 3 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 20](#).
- 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 If you are upgrading from **release 5.0(1)**, when the upgrade is completed, add the necessary CCRs back again.

Note This step is necessary only if you are upgrading from **release 5.0(1)**. If you are upgrading from **release 5.0(2)**, you do not have to perform any more steps in this section.

Verify that the home region CCR is stabilized before adding the CCRs 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 CCRs and check the boxes in the **Cloud Routers** column for each of those regions to add the CCRs back again.
- d) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

Step 10

Verify that all of the CCRs (home region CCR and non-home region CCRs) have come up with release 17.7.1.

Do not power off your Cisco Cloud APIC VM until all of the CCRs have come up with release 17.7.1.


Step 11

If you are upgrading from release 5.0(1) to release 5.1(2) or later, 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 CCRs.

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 CCR has already been successfully migrated from the basic SKU to the standard SKU. Go to [11.i, on page 21](#) in this case.
 - If the **Virtual Network Peering** is not available, that means that the home region CCR is still set to the basic SKU rather than the updated standard SKU. Continue to [11.d, on page 21](#) to migrate the home region CCR 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 CCR 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 CCR for the home region.
 - g) Click **Save**.
This action adds the CCR 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 CCRs in the infra VNet.
- Note** The **VPN Connectivity via CCR** option is used to enable the traditional VPN connectivity through the overlay IPsec tunnels between CCRs 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.

Prerequisites for Downgrading the Software

Following are prerequisites that you must follow before downgrading the Cisco Cloud APIC software:

- If your Cisco Cloud APIC is part of a Cisco Multi-Site ACI fabric, where it is orchestrated with Cisco Multi-Site, you must first downgrade the Cisco Cloud APIC software to an equivalent or earlier release before you can downgrade the Cisco Nexus Dashboard Orchestrator software. In other words, the release of the Cisco Nexus Dashboard Orchestrator software should always be equal to or later than the release of the Cisco Cloud APIC software.
 - To determine the release date for the Cisco Nexus Dashboard Orchestrator software, go to [Multi-Site Software](#) in the Software Download site, then select the appropriate release in the left nav bar to see the release date for that release
 - To determine the release date for the Cisco Cloud APIC software, go to [Cloud Application Policy Infrastructure Controller](#) in the Software Download site, then select the appropriate release in the left nav bar to see the release date for that release

For example, if you are downgrading to Cisco Cloud APIC Release 5.0(2i):

1. Determine the release date for Cisco Cloud APIC Release 5.0(2i) using the information in [Cloud Application Policy Infrastructure Controller](#) in the Software Download site (in this case, 25-Sep-2020), then go to [Multi-Site Software](#) in the Software Download site to find the equivalent or later release of the Cisco Nexus Dashboard Orchestrator software (in this case, Multi-Site Release 3.0(2k), which was released on 02-Oct-2020).
2. First downgrade the Cisco Cloud APIC software to the Cloud APIC Release 5.0(2i) using the instructions in this document.
3. After you have downgraded the Cisco Cloud APIC software, then downgrade the Cisco Nexus Dashboard Orchestrator software to the Multi-Site Release 3.0(2k). See [Multi-Site Orchestrator Installation and Upgrade Guide, Release 3.1\(x\)](#) for those instructions.

Downgrading the Software

These procedures describe how to downgrade the software.

These procedures assume the following scenario:

1. At some point previously, you were running one version of the software, such as release 5.2(1), and you decided to upgrade to a later release, such as release 25.0(2). Before you performed that upgrade, however, you backed up your existing configuration and saved that backed-up configuration file, as described in [Backing Up Your Existing Configuration, on page 8](#).
2. You then performed the software upgrade and, at some pointer later on, decided to revert back to that previous release again.

These procedures describe how to revert back to that previous release, but you will need that backed-up configuration file for that previous release in order for these downgrade procedures to work.

Step 1 Verify that you have the backed-up configuration file for the previous release, as described in [Backing Up Your Existing Configuration, on page 8](#).

Do not use these procedures to downgrade your software if you do not have that backed-up configuration file from the previous release available. You will need that backup configuration file for these downgrade procedures.

Step 2 Download the recovery template for Cisco Cloud APIC.

Contact Cisco TAC to get the recovery template:

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Step 3 Deploy the 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 recovery template (for example, `template-521-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 recovery template in [Step 2, on page 23](#).

h) Using a text editor, open the 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 recovery template is added to the **Templates** page. If you do not see the new recovery template in the **Templates** page, click **Refresh** to refresh the page.

Step 4 Use the recovery template to deploy the Cisco Cloud APIC VM in the same resource group.

- a) In the **Templates** page, click the new 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 6](#).
- **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 6](#).
- **Location:** Select the same region that you used when you first deployed your Cisco Cloud APIC, as described in [Location, on page 6](#).

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 7](#).
- **Vm Size:** Select the size for the VM.
- **Image Sku:** Select the appropriate image SKU (for example, 5_2_1_byol).
- **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 6](#).
- **Infra VNET Pool:** Enter the same infra subnet pool that was used previously, as described in [Infra VNET Pool, on page 8](#).
- **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 7](#). 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 8](#).

- **Virtual Network Name:** 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:** 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:** 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.

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-**. 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-Downgrade Procedures, on page 25](#).

Performing Post-Downgrade Procedures

Before you begin

Complete the procedures in [Downgrading the Software, on page 23](#) 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 [Understanding Tenants, Identities, and Subscriptions](#) and [Adding a Role Assignment for a Virtual Machine](#) for more information.

Step 2 If you are downgrading from release 25.0(3) to an earlier release, trigger a CCR downgrade to the older Cisco Cloud Services Router 1000v.

As part of the upgrade to 25.0(3), you also moved from the older Cisco Cloud Services Router 1000v to the newer Cisco Catalyst 8000V. Downgrading from 25.0(3) to an earlier release therefore requires downgrading the CCR back to the older Cisco Cloud Services Router 1000v.

When the downgrade is completed, the system will recognize that the CCRs are now incompatible with the Cisco Cloud APIC. You will see a message saying that the CCRs and the Cisco Cloud APIC are incompatible and that any new policies configured for the Cisco Cloud APIC will not be applied to the CCRs until you've downgraded the CCRs.

You can begin the process of triggering the CCR downgrade using either of the following methods. Note that while the menu option is shown as **Upgrade CCRs** in both methods, you are actually downgrading the CCRs in this situation by selecting this option.

- In the banner at the top of the screen when your first log into the Cisco Cloud APIC, click on the **Upgrade CCRs** link, or
- Through the **CCRs** area in the **Firmware Management** page by navigating to:
Operations > Firmware Management
Click the **CCRs** tab, then choose **Upgrade CCRs**.

Step 3 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 [Backing Up Your Existing Configuration, on page 8](#), then click **Save** at the bottom of the window.

Step 4

Import the configuration that you backed up in [Backing Up Your Existing Configuration, on page 8](#).

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 [Backing Up Your Existing Configuration, on page 8](#).

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.

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 5](#) for those procedures.

Triggering an Upgrade of the CCRs

The following topics provide information and procedures for triggering an upgrade of the CCRs.

Triggering an Upgrade of the CCRs

Prior to Release 5.2(1), the CCRs are upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC. Beginning with Release 5.2(1), you can trigger upgrades to the CCRs and monitor those CCR upgrades, independent from the Cisco Cloud APIC upgrades. This is useful to reduce traffic loss by allowing you to split up the upgrades for the management plane (Cisco Cloud APIC) and the data plane (CCRs).

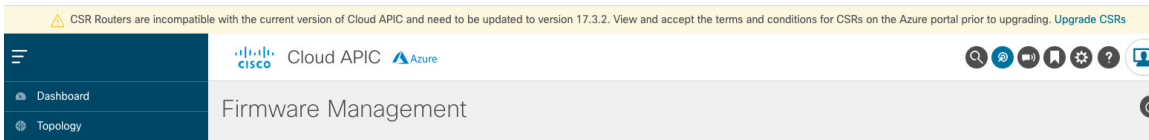
Beginning with Release 5.2(1), this feature is enabled by default, where the default assumption is that you will be triggering the upgrades to the CCRs after you trigger an upgrade to the Cisco Cloud APIC. You cannot disable this feature once it's enabled.

When this feature is enabled, the proper upgrade sequence for the Cisco Cloud APIC and the CCRs is as follows.



Note Following are upper-level steps to describe the overall process for triggering upgrades to the CCRs. For specific step-by-step instructions, see [Triggering an Upgrade of the CCRs Using the Cisco Cloud APIC GUI, on page 29](#).

1. Upgrade Cisco Cloud APIC using the instructions provided in this chapter.
2. Wait for the Cisco Cloud APIC upgrade process to complete. When that upgrade is completed, the system will recognize that the CCRs are now incompatible with the Cisco Cloud APIC. You will then see a message saying that the CCRs and the Cisco Cloud APIC are incompatible and that any new policies configured for the Cisco Cloud APIC will not be applied to the CCRs until you've upgraded the CCRs.



3. View and accept the terms and conditions for the CCRs on the Azure portal.
4. Trigger the CCR upgrade so that it is now at a compatible version as the Cisco Cloud APIC.

You can begin the process of triggering the CCR upgrade using either of these two methods:

- In the banner at the top of the screen, click on the **Upgrade CCRs** link, or
- Through the **CCRs** area in the **Firmware Management** page. Navigate to:

Operations > Firmware Management

Click the **CCRs** tab, then choose **Upgrade CCRs**.

You can also trigger the CCR upgrade through the REST API. See [Triggering an Upgrade of the CCRs Using the REST API, on page 30](#) for those instructions.

Guidelines and Limitations

- After you have upgraded the Cisco Cloud APIC, if you do not see the message saying that the CCRs and the Cisco Cloud APIC are incompatible, you might have to refresh the browser for that message to appear.
- Trigger an upgrade to the CCRs *after* you have upgraded the Cisco Cloud APIC. Do not trigger an upgrade to the CCRs before you have upgraded the Cisco Cloud APIC.
- Once you have triggered an upgrade to the CCRs, it cannot be stopped.
- If you see any errors after you trigger an upgrade to the CCRs, check and resolve those errors. The CCR upgrade will continue automatically once those CCR upgrade errors have been resolved.

Triggering an Upgrade of the CCRs Using the Cisco Cloud APIC GUI

This section describes how to trigger an upgrade to the CCRs using the Cisco Cloud APIC GUI. For more information, see [Triggering an Upgrade of the CCRs, on page 27](#).

Step 1

If the CCR software version is incompatible with the Cisco Cloud APIC software version, first view and accept the terms and conditions for the CCRs on the Azure portal.

- For releases prior to release 25.0(3), for the **Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL)**:

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 17.3.1a** 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**.

- For release 25.0(3) or later, for the **Cisco Catalyst 8000V Edge Software - Bring Your Own License (BYOL)**:

a) In the [Azure Marketplace](#) search text field, type *Cisco Catalyst 8000V Edge Software* and select the option that appears.

The **Cisco Catalyst 8000V Edge Software** option appears as a search suggestion.

b) Click the **Cisco Catalyst 8000V Edge Software** option.

You should be redirected to the **Cisco Catalyst 8000V Edge Software** 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 Catalyst 8000V Edge Software-BYOL-17.7.1** 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

Begin the process of triggering the CCR upgrade to a compatible CCR version.

You can begin the process of triggering the CCR upgrade using either of these two methods:

- In the banner at the top of the screen, click on the **Upgrade CCRs** link, or
- Through the **CCRs** area in the **Firmware Management** page. Navigate to:

Operations > Firmware Management

Click the **CCRs** tab, then choose **Upgrade CCRs**.

A warning appears after clicking **Upgrade CCRs**, stating that upgrading the CCRs will cause the CCRs to reboot, which may cause temporary disruption in traffic.

- Step 3** If this is a good time to upgrade the CCRs and have a temporary disruption in traffic, click **Confirm Upgrade** in the warning message.
- The CCR software upgrade begins. A banner appears at the top of the screen, saying that the CCR upgrade is in process. Click **View CCR upgrade status** in the message to view the status of the CCR upgrade.

- Step 4** Fix any faults that might occur during the upgrade of the CCRs.

If a fault occurs during the upgrade, you can get more information on the fault by navigating to:

Operations > Event Analytics > Faults

Triggering an Upgrade of the CCRs Using the REST API

This section describes how to trigger an upgrade to the CCRs using the REST API. For more information, see [Triggering an Upgrade of the CCRs, on page 27](#).

Set the value for the `routerUpgrade` field to `"true"` in the cloud template to trigger an upgrade to the CCRs through the REST API (`routerUpgrade="true"`).

```
<polUni>
<fvTenant name="infra">
  <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
    <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName" routerPassword="SomePass"
    routerUpgrade="true">
      </cloudtemplateProfile>
    <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
    <cloudtemplateIntNetwork name="default">
      <cloudRegionName provider="azure" region="westus"/>
      <cloudRegionName provider="azure" region="westus2"/>
    </cloudtemplateIntNetwork>
    <cloudtemplateExtNetwork name="default">
      <cloudRegionName provider="aws" region="us-west-2"/>
      <cloudtemplateVpnNetwork name="default">
        <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
        <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
        <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />
        <cloudtemplateOspf area="0.0.0.1"/>
      </cloudtemplateVpnNetwork>
      <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
    />
    </cloudtemplateExtNetwork>
  </cloudtemplateInfraNetwork>
```

```
</fvTenant>  
</polUni>
```
