Upgrading or Downgrading with APIC Release 5.1 or Later Using the GUI

Note Ensure that you check and follow these guidelines:

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric

- Pre-Upgrade/Downgrade Checklists

- Guidelines and Limitations for Upgrading or Downgrading

- Starting from release 5.1, ACI firmware upgrade using the GUI does not provide an option to set a scheduler for the upgrade. Instead, the benefits from using a scheduler such as image pre-download on switches are all built-in the native workflow.

- You must decommission an unsupported leaf switch that is connected to the Cisco APIC and move the cables to the other leaf switch that is part of the fabric before you upgrade the image.

Accessing the Dashboard

You can access the dashboard, which shows you the firmware status of the APIC nodes and switches in your fabric, by navigating to **Admin** > **Firmware** > **Dashboard**.

The dashboard also shows the usage of firmware repository on each APICs.

Downloading APIC and Switch Images on APICs

This procedure downloads firmware images of the Cisco Application Policy Infrastructure Controllers (APICs) and Cisco Application Centric Infrastructure (ACI)-mode switches into the Cisco APIC's firmware repository from an external file server or from your local machine.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Note In the Cisco APIC release 6.0(2) and later, download both the 32-bit and 64-bit Cisco ACI-mode switch images to the Cisco APIC. Downloading only one of the images may result in errors during the upgrade process. For more information, see Guidelines and Limitations for Upgrading or Downgrading.

In the Cisco ACI-mode switch 16.0(3d), 16.0(3e), 16.0(4c), and 16.0(5h) releases, the 64-bit switch software has the same image name as the 32-bit software when installed on the switch. To verify which version is running on the switch, use the **md5sum** command against the image file on switch. Compare this md5sum hash to the switch image contained in the `/firmware/fwrepos/fwrepo` directory of the Cisco APIC. On subsequent upgrades, the 64-bit and 32-bit image names are differentiated on the switch.

Procedure

Step 1 Download the desired target version from the Cisco Software Download site (for example, 5.2(1g) release) to your file server or local machine.

Step 2 On the menu bar, choose **Admin** > **Firmware**.
The **Dashboard** window appears, which provides general information one the controllers and the leaf and spine switches (nodes).

Step 3 Click **Images** in the left navigation bar.
The **Image** window appears, which shows the images that you downloaded previously.

Step 4 Click the **Actions** icon and select **Add Firmware** from the scrolldown menu.
The **Add Firmware Image** popup window appears.

Step 5 Determine if you want to import the firmware image from a local or a remote location.

- If you want to import the firmware image from your computer, in the **Location** field, click the **Local** radio button. Click the **Choose File** button, then navigate to the folder on your local system with the firmware image that you want to import. Go to .

- If you want to import the firmware image from a remote location, click either **Secure copy** or **HTTP**, depending on the method that you want to use to import the firmware image from the remote location:

  - If you selected the **Secure copy** radio button, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image:

    a. In the **URL** field, enter the URL from where the image will be downloaded.

    The format for the SCP source is:

    `<SCP server IP or FQDN>:/<path>/<filename>`

An example URL is `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso`.

b. In the **Username** field, enter your username for secure copy.

c. In the **Authentication Type** field, select the type of authentication for the download. The type can be:

- **Password**

- **Ssh Public Private Files**

The default is **Password**.

- If you selected **Password**, in the **Password** field, enter your password for secure copy.

- If you selected **Ssh Public Private Files**, enter the following information:

    - **Ssh Key Contents**: The SSH private key content.

    - **Ssh Key Passphrase**: The SSH key passphrase that is used for generating the SSH private key.

Note	Based on the provided SSH private key, the Cisco APIC internally creates a temporary SSH public key just for this transaction to establish a connection with the remote server. You must ensure that the remote server has the corresponding public key as one of the "authorized_keys". After the authentication check is performed, the temporary public key on the Cisco APIC is deleted.

      You can generate an SSH private key (`~/.ssh/id_rsa`) and a corresponding SSH public key (`~/.ssh/id_rsa.pub`) on one of the Cisco APICs by entering the following:

      ```
      ssh-keygen -t rsa -b 2048 -C "<username>@<apic_name>"
      ```

      Or you can generate them on another machine. For either method, you need to provide the generated private key for each download configuration.

- If you selected the **HTTP** radio button, enter the http source that you want to use to download the software image.

  The format for the HTTP source is:

  ```
  <HTTP server IP or FQDN>:/<path>/<filename>
  ```

  An example URL is `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso`.

Step 6   Click **Submit**.

The Cisco APICs begins downloading the specified firmware images from the configured source. The download progress is shown in the **Download Status** column

Upgrading or Downgrading the Cisco APIC From Releases 5.1x or Later

Use these GUI-based upgrade or downgrade procedures to upgrade the software on the Cisco APICs in your fabric.

If you are not able to upgrade the software on the Cisco APICs in your fabric using these GUI-based upgrade procedures for some reason (such as if you received a Cisco APIC through a new order or Product Returns & Replacements (RMA), and the version is old and not able to join the fabric to perform an upgrade using the GUI), you can perform a clean installation of the software on the Cisco APICs through the CIMC instead to upgrade your Cisco APIC software. See Installing Cisco APIC Software Using Virtual Media for those procedures. Or, if your Cisco APIC cluster is running the Cisco APIC 6.0(2) release or newer, the new Cisco APIC is automatically upgraded or downgraded to the same version of the existing cluster using Auto Firmware Update on APIC discovery.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric

- Pre-Upgrade/Downgrade Checklists

- Guidelines and Limitations for Upgrading or Downgrading

- If you are upgrading from a Cisco APIC release earlier than 5.0 to a 5.0 or later release and you have an IPv4 host route (/32) or IPv6 host route (/128) that is learned using MP-BGP, if those host routes overlap with a local attached non-pervasive subnet, such as an L3Out SVI subnet, the forwarding information base (FIB) process skips the hardware programming for those host routes. This behavior is intentional. You can avoid this situation by using one of the following workarounds:

    - Do not advertise in the /32 or /128 host route that overlaps with an L3Out interface subnet.

    - Advertise using any subnet other than /32 or /128.

    - Peer directly from the border leaf switches to the same peers as the original nodes where there is peering.

Procedure

Step 1   On the menu bar, choose **Admin** > **Firmware**.
The **Dashboard** window appears, which provides general information one the controllers and the leaf and spine switches (nodes).

Step 2   In the left navigation window, click **Controllers**.
The **Controllers** window appears, which provides firmware information for the controllers.

Step 3   Click the **Setup Update** button.

The **Version Selection** step of the **Setup Controller Firmware Upgrade** window appears, showing all of the software images that you have downloaded onto your system.

Note   If you see the following error message instead:

```
No firmware images available. Please check the Images tab.
```

Then you do not have a image available to use for the upgrade. Add an image to use for the upgrade using the procedures provided in Downloading APIC and Switch Images on APICs, on page 2.

Step 4   Select an image that you want to use for the firmware update, then click **Next**.

The **Validation** step appears.

Step 5   Review the information provided in the **Validation** screen.

Beginning with release 5.1(1), certain validation checks are performed and displayed in the **Validation** screen, with a message showing whether each validation check passed or failed.

For any validation check that has failed, we recommend that you address those faults or issues before proceeding with the upgrade.

Once you have addressed the faults or issues raised in the **Validation** window, click **Next** to go to the **Confirmation** window.

Step 6   In the **Confirmation** window, verify that the information is correct, then click **Begin Install**.

The **Controllers** window appears again, and the status of the upgrade or downgrade is displayed.

The Cisco APICs are upgraded or downgraded serially so that the controller cluster is available during the upgrade or downgrade. Once a controller image is upgraded or downgraded, it drops from the cluster, and it reboots with the newer version while the other Cisco APICs in the cluster are still operational. Once the controller reboots, it joins the cluster again. Then the cluster converges, and the next controller image starts to upgrade or downgrade. If the cluster does not immediately converge and is not fully fit, the upgrade or downgrade waits until the cluster converges and is fully fit. During this period, a **Waiting for Cluster Convergence** message is displayed in the **Update Status** column for each Cisco APIC as it upgrades or downgrades.

When the Cisco APIC that the browser is connected to is upgraded or downgraded and it reboots, the browser first displays an error message, then you will not be able to see anything in the browser that you used to log into this Cisco APIC. However, you can log into any of the remaining Cisco APICs in the cluster to continue to monitor the progress of the upgrade or downgrade process, if you want.

Additional information may be provided on the status of the upgrade process for the controllers. See **Understanding APIC Upgrade and Downgrade Stages** for a complete description of the different stages for Cisco APIC upgrades or downgrades.

Note   The actual upgrade or downgrade process remains the same with release 5.1(1) as it was with previous releases. However, starting with release 5.1(1), additional information is now provided that shows you the stage that you are in during the upgrade or downgrade process.

Step 7   In the browser URL field, enter the URL for the Cisco APIC that has already been upgraded, and sign in to the Cisco APIC as prompted.

Step 8   Wait for all the Cisco APICs to complete the upgrade or downgrade and become **Fully Fit**.

Upgrading or Downgrading the Leaf and Spine Switches Through APIC Running Release 5.1x or Later

Pre-Download Images to the Leaf and Spine Switches

This procedure describes how to download switch images to leaf and spine switches from APIC's firmware repository at your own timing without starting the actual upgrade (i.e. software installation) or downgrade. This is called pre-download. Prior to APIC release 5.1(1), this operation had to be triggered through a scheduler. But starting from APIC release 5.1(1), the native GUI workflow allows you to create switches update groups and perform pre-download.

During this operation, switches will remain up and no reboot will be performed.

If you are downgrading the software on the Cisco APICs, the process is identical to the process for upgrading the software, except that the target release that you choose will be earlier than the currently installed release. The text for dialogs, fields, buttons, and other controls in the Cisco APIC GUI specify "upgrade" even though you are downgrading the software.

Before you begin

Ensure that you check and follow these guidelines:

- Wait until all the controllers are upgraded or downgraded to the new firmware version before proceeding to upgrade or downgrade the switch firmware.

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric

- Pre-Upgrade/Downgrade Checklists

- Guidelines and Limitations for Upgrading or Downgrading

Procedure

Step 1	On the menu bar, choose **Admin** > **Firmware**. The **Dashboard** window appears, which provides general information one the controllers and the leaf and spine switches (nodes).
Step 2	In the left navigation window, click **Switches**. The **Switches** window appears, which provides firmware information for the upgrade groups of leaf and spine switches.
Step 3	Click the **Actions** icon and select **Create Update Group** from the scroll down menu.
Step 4	In the **Setup Switch Update Group** window appears, enter a name for the **Upgrade Group Name**.
Step 5	In the **Switch Selection** step, click the **Add Switches** button, then select the switches that need to be upgraded / downgraded and then click **OK**, then click **Next**.
Step 6	In the **Version Selection** step, select an **Update Type**, then in the **Select Firmware** section select an image that you want to upgrade/downgrade.
Step 7	(Optional) If you need any of the advanced options listed below, click **Advanced Settings** to bring up the **Advanced Settings** window.

Note that typically there is no need to set these advanced options. We recommend that you disable the options or use the default values.

In the **Advanced Settings** window, perform any of the following actions if needed:

- In the **Compatibility Check** field, leave the setting in the default **Enforced** setting, unless you are specifically told to disable the compatibility check feature.

Note	A compatibility check verifies if an upgrade path from the currently running version of the system to a specific newer version is supported or not based on catalog that is embedded in Cisco APIC image. If you choose to disable the compatibility check feature by entering a check mark in the box next to the **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.

- **Graceful Upgrade (Graceful Check)**

  Enable this option to perform a **Graceful Upgrade** when the firmware installation is triggered. By default, this setting is **Unenforced**.

  See Graceful Upgrade or Downgrade of ACI Switches for details and make sure to follow the guidelines when enabling this option. Otherwise, your upgrade may fail.

- In the **Run Mode** field, choose the run mode to proceed automatically to the next set of nodes after the set of nodes has gone through the maintenance process successfully.

  The options are:

  - **Pause Upon Upgrade Failure**: The update group does not approve further switch upgrades if there is an upgrade failure in one of the switches, or if the APIC cluster status becomes not Fully Fit, which may happen (for example, when all APIC-connected leaf switches are upgraded at the same time, which is not recommended in Guidelines for ACI Switch Upgrades and Downgrades).

  - **Do not pause on failure and do not wait on cluster health**: The update group does not stop switch upgrades of the entire group just because one of the switches had an upgrade failure or a temporary APIC cluster issue.

  We recommend that you choose **Do not pause on failure and do not wait on cluster health** because it is recommended to group switches that should be upgraded at the same time in one update group instead of letting each update group to dynamically decide which set of switches within the same group to be upgraded (for instance, with the concurrent capacity setting). When following such best practices, **Pause Upon Upgrade Failure** does not provide much value.

Click **Done** when you have finished performing any of the actions in the **Advanced Settings** window. You are then returned to the main **Firmware** page.

Step 8   When you have verified that everything in the **Version Selection** step is correct, click **Next**.
The **Validation** step appears.

Step 9   Review the information provided in the **Validation** step.

Any faults or issues that might affect your upgrade are displayed in this page. We recommend that you address any faults or issues that you see displayed before proceeding with the upgrade.

See the Pre-Upgrade/Downgrade Checklists for items that are checked by the APIC pre-upgrade validator in your version and other items you should check through the AppCenter pre-upgrade validator, either using a script or manually.

After you have addressed the faults or issues raised in the **Validation** step, click **Next** to go to the **Confirmation** step.

Step 10 In the **Confirmation** step, verify that the information is correct, then click **Begin Download**.

The system begins downloading the software to all of the nodes that you selected in the previous screen, and displays the download status for each node.

Note If you are upgrading from a release prior to Cisco APIC release 4.2(6), the download status will show as `downloading` but will not progress to the next stage showing that the download has completed. This is a known issue when upgrading from a release prior to Cisco APIC release 4.2(6) and is expected behavior. Follow the instructions in Installing Images to the Leaf and Spine Switches, on page 9 so that the software installation process will begin after the download is completed.

Note If you are upgrading nodes in different upgrade groups from a pre-5.1x release using the instructions provided in Upgrading or Downgrading the Leaf and Spine Switches Through a Cisco APIC Running Releases 4.x or 5.0 and you made the following selections previously:

- **Now** in the **Upgrade Start Time** field

- **unlimited** in the **Maximum Running Time** field

Then you might see the following behavior:

- **First upgrade group**: When you click on **Begin Download** in these procedures, the software begins the image download and then automatically installs the software on the nodes in the first upgrade group after the image download is complete. This is unexpected behavior.

- **Second upgrade group**: When you click on **Begin Download** in these procedures, the software begins the image download but does not automatically install the software on the nodes in the second upgrade group after the image download is complete. This is expected behavior - you will install the software using the information in Installing Images to the Leaf and Spine Switches, on page 9 in these procedures.

While the behavior for the first upgrade group is unexpected, it is not harmful. Be aware that the nodes in the first upgrade group will reboot as part of the software installation process that happens automatically in this scenario.

Step 11 Verify that the download was completed successfully for all of the nodes that you want to upgrade in the group.

If any nodes are shown as **Failed** in the Status column, you have several options:

- Click **Retry All** at the bottom of the page to retry the download for all the nodes in the upgrade group.

- Click **Cancel All** at the bottom of the page to cancel the downloads for the nodes in the upgrade group.

- If you want to manually remove the failed nodes from this upgrade group so that you can move forward with the upgrade for the nodes that were successful in the download phase, click the pencil icon next to any node that you want to manually remove from this upgrade group and click **Remove**.

See Common Reasons for Download Failure for troubleshooting.

When you see the status of **Download Complete** for all the nodes in your group, you will see **Ready to Install** at the top of the screen.

Installing Images to the Leaf and Spine Switches

After the pre-download on all switches is done and their upgrade status show **Ready to Install**, you can perform the procedure to trigger the upgrade, which will install the firmware and reboot the switches.

Typically, you would perform a pre-download hours or days before this procedure. Make sure that you did not violate any validations since the pre-upgrade validations were performed at the time of pre-download. If you want to perform pre-upgrade validations again at this point, use the App Center Pre-Upgrade Validator or the script because the APIC built-in pre-upgrade validator will result in the re-downloading of the switch image.

Before you begin

Ensure that you check and follow these guidelines:

- Workflow to Upgrade or Downgrade the Cisco ACI Fabric

- Pre-Upgrade/Downgrade Checklists

- Guidelines and Limitations for Upgrading or Downgrading

You must first finish the pre-download procedures in Pre-Download Images to the Leaf and Spine Switches, on page 6.

Procedure

Step 1　When you have a maintenance window where you are able to have the nodes reboot as part of the upgrade process, click **Actions**, then **Begin Install** to begin the software installation.

You can monitor the progress of the upgrade for the nodes in the upgrade group in the **Node Firmware Update** window. You can also close this window and click **Nodes** in the left navigation window to check the overall status of the upgrade group in the **Status** column in the table.

Step 2　When all of the nodes are shown with a status of **Completed**, click **Done** and proceed with the next update group.

Understanding App Installation Behavior

Certain Apps are available to install on APICs and are available to download through the App Center (https://dcappcenter.cisco.com/). These Apps fall into two categories:

- **User-installed Apps**: Apps that you download manually from the App Center and then upload to the APIC.

- **Pre-packaged Apps**: Apps that are installed on an APIC automatically by the plugin-handler.

You can install an App using the REST API or the APIC GUI:

- To install an App using the REST API, send a post with XML such as the following examples. The protocol that you choose while triggering a download task depends on the file server hosting the App image. The following post shows an example where the protocol is SCP:

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
    <fabricInst>
        <firmwareRepoP>
            <firmwareOSource name="MY-APP" proto="scp" url="URL:PATH-TO-APP-IMAGE"
user="MY-USER-NAME" password="MY-PASSWORD"/>
        </firmwareRepoP>
    </fabricInst>
</polUni>
```

  The following example shows a similar post where the protocol is HTTP:

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
    <fabricInst>
        <firmwareRepoP>
            <firmwareOSource name="httpuploadapp" proto="http"
url="{{downloadserver}}/{{filename}}" status="created,modified"/>
        </firmwareRepoP>
    </fabricInst>
</polUni>
```

- To install an App using the APIC GUI:

  - For APIC releases prior to 5.2:

    1. Click **Admin** > **Downloads**.

       The **Downloads** screen appears.

    2. Click the **Task** icon (✕▾) on the far-right side of the **Downloads** work pane and select **Add File to APIC**.

       The **Add File to APIC** dialog appears.

    3. Enter the name of the download file in the **Download Name** field.

    4. In the **Protocol** field, choose **Secure Copy**.

    5. In the **URL** field, enter the path to the download file image location.

    6. Enter your username and password in the **Username** and **Password** field and click **Submit**.

    7. Click the **Operational** tab and then click the **Refresh** icon (↻) on the far-right side of the **Downloads** work pane to check the status.

       The application will automatically install after downloaded. This could take approximately five minutes to complete.

  - For APIC release 5.2 or later:

    1. Click **Apps** > **Downloads**.

The **Downloads** screen appears.

2. Click the **Task** icon (✕▾) on the far-right side of the **Downloads** work pane and select **Add File to APIC**.

The **Add File to APIC** dialog appears.

3. Enter the name of the download file in the **Download Name** field.

4. In the **Protocol** field, choose **Secure Copy**.

5. In the **URL** field, enter the path to the download file image location.

6. Enter your username and password in the **Username** and **Password** field and click **Submit**.

7. Click the **Operational** tab and then click the **Refresh** icon (↻) on the far-right side of the **Downloads** work pane to check the status.

The application will automatically install after downloaded. This could take approximately five minutes to complete.

When you install an App from App Center on an APIC, the behavior around that App installation varies, depending on several factors:

- Whether the App is a **user-installed App** or a **pre-packaged App**
- Whether this is a fresh installation, an upgrade, or a downgrade for the App on the APIC

User-Installed Apps

If you are manually installing an App that doesn't normally come pre-installed on an APIC, the behavior around that installation varies, depending on the following situations:

- If you do not already have this App installed on your APIC, then this is considered a fresh installation and the App is installed on your APIC in the normal fashion.

- If you already have this App installed on your APIC and the App currently installed on your APIC is an **earlier** version of the App, then the upload of this later version of the App to your APIC triggers an upgrade of the App on your APIC.

- If you already have this App installed on your APIC and the App currently installed on your APIC is a **later** version of the App, then the upload of this earlier version of the App to your APIC triggers a downgrade of the App on your APIC.

Pre-Packaged Apps

When you upgrade or downgrade all of the APICs in a cluster to a new APIC image, the plugin-handler checks for pre-packaged Apps images that come with that new APIC image.

- If the plugin-handler finds that an App is available in the new APIC image but that App is not currently installed on your APICs, then the plugin-handler triggers the installation of that App on your APICs.

- If the plugin-handler finds that an App is available in the new APIC image and that App is already installed on your APICs, the plugin-handler then checks if the App that is available in the new APIC image is an earlier or later release than the App currently installed on your APICs:

- If the version of the App in the new APIC image is a **later** release than the App currently installed in your APICs, then the plugin-handler triggers an upgrade or downgrade for that App on your APICs. Beginning with release 5.2(3), pre-packaged Apps get upgraded or downgraded to whatever App images are bundled in the APIC image after all of the APICs are upgraded or downgraded in a setup, regardless of what version of those Apps were running on that setup before the APICs got upgraded or downgraded.

- If the version of the App in the new APIC image is an **earlier** release than the App currently installed in your APICs, then the plugin-handler takes no action with the App on your APICs. The plugin-handler does not downgrade the App on your APICs to that earlier version that is available in the new APIC image. This is done so that you can install newer versions of an App, where the version of an App that you install might be later than the version that comes pre-packaged with an APIC image, and the plugin-handler won't automatically overwrite the later version of that App currently on your APICs with an earlier version.

For example, assume the APICs in a cluster are running on release version 1.2(3), and the pre-packaged App **AcmeApp** is available for APIC release 1.2(3), where 4.5(6) is the version of AcmeApp that is normally pre-packaged on APICs running on release 1.2(3).

Assume that you want to upgrade the AcmeApp at some later date and the latest version of AcmeApp, the 4.6(1) version of AcmeApp, is available at the App Center. You then manually download and install that latest version of AcmeApp so that the APICs and the AcmeApp are at the following versions:

- The APICs in the cluster are still running on APIC release 1.2(3)

- The AcmeApp on these APICs is now updated to AcmeApp version 4.6(1)

Now assume that you decide to upgrade the APIC from release 1.2(3) to release 1.2(4) at another date later on. However, for APICs running on 1.2(4), the version of AcmeApp that is normally pre-packaged is version 4.5(7). In that case, the plugin-handler would not make any changes to the version of AcmeApp running on your APIC, because your APIC already has a version of AcmeApp running on it [version 4.6(1)] that is later than the 4.5.(7) version that would normally come pre-packaged with APIC release 1.2(4).

Note that you can change the Apps policy for pre-packaged Apps:

- Through the REST API, you can change the Apps policy for pre-packaged Apps by modifying the `apPrepackagedPlugins` MO using one of the following three options:

  - **install-all**: This is the default value. This option installs or upgrades pre-packaged Apps in the manner that is described above.

    ```
    POST {{apic-url}}/api/policymgr/mo/.xml

    <polUni>
      <apPluginPolContainer>
          <apPrepackagedPlugins PrepackagedAppsAction="install-all"/>
      </apPluginPolContainer>
    </polUni>
    ```

  - **remove-all**: This option removes all pre-packaged Apps from APIC.

    ```
    POST {{apic-url}}/api/policymgr/mo/.xml

    <polUni>
      <apPluginPolContainer>
          <apPrepackagedPlugins PrepackagedAppsAction="remove-all"/>
    ```

```
        </apPluginPolContainer>
    </polUni>
```

- **skip-installation**: This option disables the plugin-handler from automatically installing or upgrading pre-packaged Apps in future APIC image upgrades.

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
  <apPluginPolContainer>
      <apPrepackagedPlugins PrepackagedAppsAction="skip-installation"/>
  </apPluginPolContainer>
</polUni>
```

- Through the APIC GUI:

  1. Navigate to **Apps** > **Installed Apps**.

     The **Apps** page is displayed.

 2. Click on the **Settings** icon (⚒▾), then choose **Change Prepackaged Apps Policy**.

     The **Change Prepackaged Apps Policy** page appears.

  3. Choose one of the following options (see the options descriptions above in the REST API information):

     - Install All

     - Remove All

     - Skip Installation

Working with Hidden Pre-Packaged Apps

For any App that you install, whether it is a user-installed App or a pre-packaged App, you can usually see that App displayed in the **Apps** window in the APIC GUI, which you can view by navigating to **Apps** > **Installed Apps**.
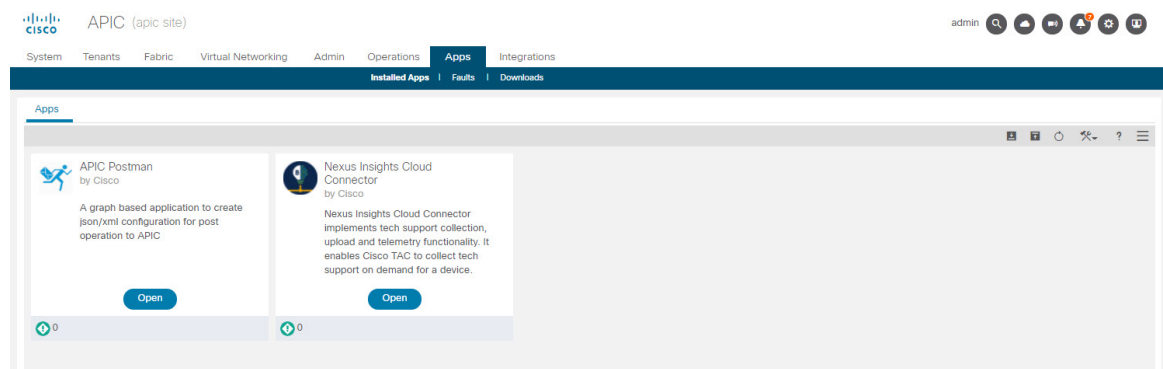
You can perform certain actions for Apps displayed in this window, such as opening, enabling, or deleting those Apps.

However, there are certain pre-packaged Apps that might be installed on your APICs but are not displayed in the **Apps** window in the APIC GUI, such as the ApicVision App that became available beginning with

release 5.2(1). While these hidden Apps won't appear in the **Apps** window, they might appear in the **Faults** window if there is an issue with that App (**Apps** > **Faults**).

✎

Note   The pre-packaged ApicVision App that became available with release 5.2(1) is not available for download through the App store, so do not make changes to or delete the ApicVision App. Contact Cisco TAC support if you have any issues or faults with the pre-packaged ApicVision App.

You can locate and work with these hidden pre-packaged Apps through Visore, the APIC Object Store Browser that you can use to directly query Managed Objects (MOs). For more information on Visore, see *Application Policy Infrastructure Controller Visore Tool Introduction*.

You can access Visore by appending `/visore.html` to the URL that you would normally use to log into your APIC GUI:

https://<APIC or Switch IP ADDRESS>/visore.html

After you have logged into Visore, the Object Store window is displayed.

From there, you can query the MO for any Apps installed on your APICs by entering `apPlugin` in the **Class or DN or URL** field and clicking **Run Query**. Visore returns output showing the number of objects found for this MO, which is the total number of Apps that are installed on your APICs, including hidden Apps that aren't displayed in the **Apps** window in the normal APIC GUI.
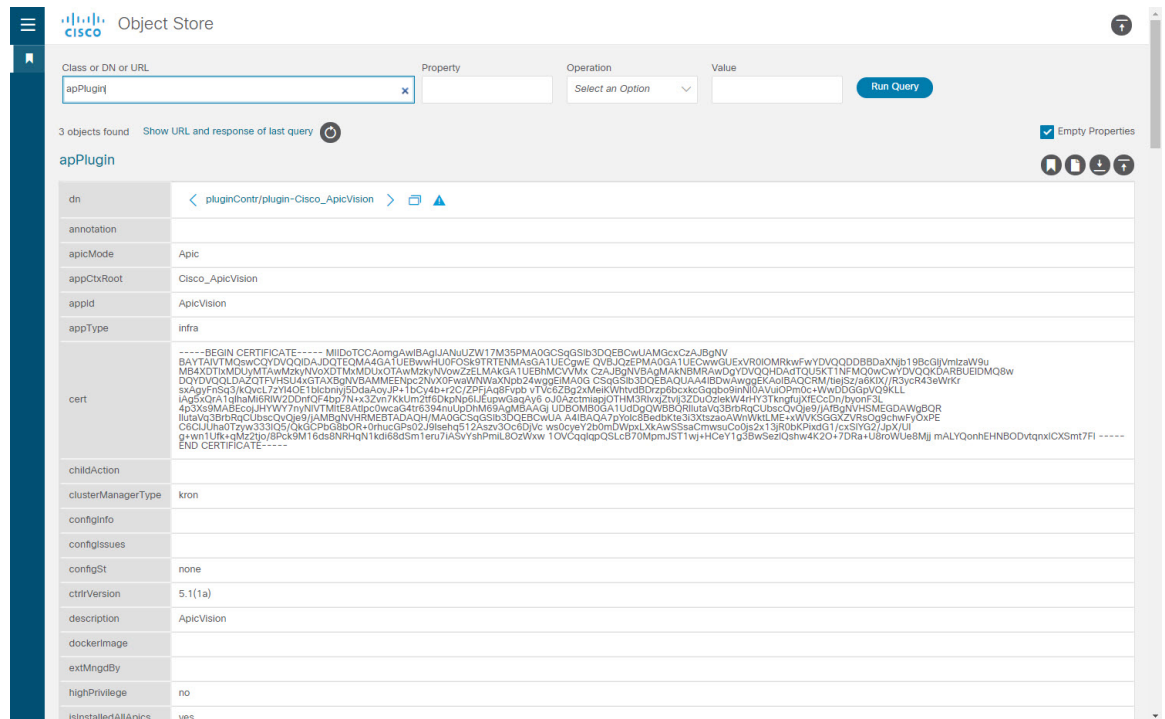
For example, the information provided in the **Apps** window in the example above shows two Apps installed, whereas the information returned from the `apPlugin` query in Visore shows three objects found for the Apps MO. Comparing the two lists of Apps, you can see that the ApicVision App is not shown in the **Apps** window in the normal APIC GUI but is displayed in the Visore output, so that means that the ApicVision App is a hidden pre-packaged App.

You can now get more information on this hidden pre-packaged App through certain fields displayed in the Visore output, such as the **pluginSt** field that shows your desired state for the App and the **operSt** field that shows the operational state for the App.

For example, you could verify that an App is up and running if you see the following for an App:

- No faults are shown for this App in the **Faults** window (**Apps** > **Faults**)

- The state in the **operSt** field is shown as `active`

- The state in the **pluginSt** field is shown as `active`

In addition, you should pick a security domain when you enable an App, and the **securityDomains** field is populated with that value when you enable an App as described below (when you set the **pluginSt** field to `active` for an instance of an apPlugin MO). Note that the plugin-handler selects `all` as the security domain for infra Apps (for Apps that are set to `infra` in the **appType** field in the apPlugin MO instance).

Because you can't view these hidden Apps in the **Apps** window in the normal APIC GUI, you are not able to perform certain actions such as opening, enabling, or deleting the hidden Apps through the APIC GUI. However, you can perform these actions on a hidden App through the REST API:

- To enable a hidden App, send a post with XML such as the following example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/plgnhandler/mo/.xml -->
<apPluginContr>
    <apPlugin appCtxRoot="{{vendordomain}}_{{appid}}" pluginSt="active"
securityDomains="{{security-domains}}"/>
</apPluginContr>
```

Where the `pluginSt` is `active`.

- To disable a hidden App, send a post with XML such as the following example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/plgnhandler/mo/.xml -->
<apPluginContr>
    <apPlugin appCtxRoot="{{vendordomain}}_{{appid}}" pluginSt="inactive"/>
</apPluginContr>
```

Where the `pluginSt` is `inactive`.

Note the following:

- The security domain is not needed when disabling a hidden App.

- To find the `appCtxRoot` value for an App for either of the posts shown above, query for instances of the apPlugin MO and use the entry in the `appCtxRoot` field in the instance of the apPlugin MO that corresponds to your App of interest.

  To get this information, log in to your APIC through ssh as an admin user and enter the `moquery -c apPlugin | grep appCtxRoot` command:

  ```
  # moquery -c apPlugin | grep appCtxRoot
  appCtxRoot          : Cisco_NIBASE
  appCtxRoot          : Cisco_ApicVision
  ```

- To delete a hidden App, send a post with XML such as the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/node/mo/.xml -->
<firmwareRepo>
    <firmwareFirmware name="{{vendordomain}}_{{appid}}" deleteIt="true"/>
</firmwareRepo>
```