



Pre-Upgrade/Downgrade Checklists

- [Check Basic Information on Your Fabric, on page 1](#)
- [Check Configurations and Conditions That May Cause An Upgrade or Downgrade Failure, on page 2](#)
- [Download Both the 32-bit and 64-bit Cisco ACI-Mode Switch Images \(6.0\(2\) and later\), on page 2](#)
- [Deprecated Managed Objects, on page 2](#)
- [Checklists for Downgrade, on page 3](#)
- [Examples of Pre-Upgrade Validator \(APIC\), on page 6](#)

Check Basic Information on Your Fabric

Check some basic information on your fabric to ensure that you have everything that you need for a smooth upgrade. Specifically, it is critical that you clear all faults. Although some faults are described as specific issues in [Check Configurations and Conditions That May Cause An Upgrade or Downgrade Failure, on page 2](#), you should always clear any faults before performing an upgrade except for the faults that are expected due to configurations in staging phase.

- Clear all your faults
- Perform a configuration export with AES Encryption
- Verify access to out-of-band IP addresses of all your ACI nodes (all your APIC nodes and switch nodes)
- Verify CIMC access for all your APICs
- Verify console access for all your switches
- Understand **Changes in Behavior** in Release Notes of both [APIC](#) and [ACI switches](#) for versions between the target and current version
- Understand **Open Issues** and **Known Issues** in Release Notes of both [APIC](#) and [ACI switches](#) for the target version

Check Configurations and Conditions That May Cause An Upgrade or Downgrade Failure

There are three different tools to perform pre-upgrade validation for Cisco Application Centric Infrastructure (ACI):

- **Pre-Upgrade Validator (APIC):** A validator embedded in the Cisco Application Policy Infrastructure Controller (APIC) Upgrade Configuration. This is automatically performed when configuring an update group for the Cisco APIC or switches.
- **Pre-Upgrade Validator (App Center app):** A validator that can be installed on the Cisco APICs as an app that can be downloaded through dcappcenter.cisco.com. After the app is installed, the app enables you to download the latest validation script from Cisco Cloud. This can be run on demand and is supported on release 5.2 and later.
- **Script:** For any feature not currently implemented in the Pre-Upgrade Validator, you can run a standalone script directly on the Cisco APIC to validate any existing issues prior to upgrading. The script supports all versions of software. **We strongly recommend that you use this tool.** See <https://github.com/datacenter/ACI-Pre-Upgrade-Validation-Script> for more details about the script.

See <https://datacenter.github.io/ACI-Pre-Upgrade-Validation-Script/validations/> for the list of validations supported by the script along with comparisons with the other tools (Pre-Upgrade Validator (APIC, App Center app)).

Download Both the 32-bit and 64-bit Cisco ACI-Mode Switch Images (6.0(2) and later)

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](#).

Deprecated Managed Objects

The Pre_Upgrade checker script checks for the existence of the following deprecated managed objects on the running version of the software and blocks the upgrade, if they exist in the configuration. You must update your script or code to use the new managed object.

- **Class: config:RsExportDestination**
- **Class: config:RsImportSource**
- **Class: fabric:RsResMonFabricPol**
- **Class: infra:RsResMonInfraPol**
- **Class: fabric:RsResMonCommonPol**
- **Class: trig:Triggered**

- **Class: trig:TriggeredWindow**
- **Class: fv:CCg**
- **Class: fv:RsToCtrct**
- **Class: mgmt:RsOobEpg**
- **Class: mgmt:RsInbEpg**
- **Class: vns:RsCifAtt**
- **Class: fault:RsHealthCtrlrRetP**
- **Class: fv:PndgCtrctCont**
- **Class: vz:RsAnyToCtrct**
- **Class: fv:PndgCtrctEpgCont**
- **Class: fv:AREpPUpd**
- **Class: vns:Chkr**
- **Class: aaa:RsFabricSetup**
- **Class: ap:PluginPol**
- **Class: tag:ExtMngdInst**
- **Class: telemetry:Server**
- **Class: telemetry:FltPolGrp**
- **Class: telemetry:FilterPolicy**
- **Class: telemetry:FlowServerP**
- **Class: pol:RsFabricSelfCAEp**
- **Class: fabric:PodDhcpServer**
- **Class: fabric:SetupAllocP**
- **Class: fabric:AssociatedSetupP**
- **Class: cloud:AEPgSelector**
- **Class: fv:VmmSelCont**

Checklists for Downgrade

In general, the same checklists as upgrades should be applied to downgrades. On top of that, you need to pay attention to the new features that may not yet be supported on older versions. If you are using such features, you should disable or change the configurations prior to the downgrade. Otherwise, some functionality will stop working after downgrades.

The following lists some of the example features that you should pay attention to prior to downgrades. However, note that the following list is not complete and we highly recommend that you check the Release Notes or Configuration Guides to confirm that features that you are using are supported on older releases as well.

- The ability to use the DUO application as an authentication method when logging in to Cisco Application Policy Infrastructure Controller (APIC) was introduced as part of the Cisco APIC release 5.0(1). If you are running release 5.0(1) and you have DUO set up as your default authentication method, but then you decide to downgrade from release 5.0(1) to a previous release where DUO was not supported as an authentication method, we recommend that you change the default authentication method from DUO to an option that was available prior to release 5.0(1), such as Local, LDAP, RADIUS, and so on. If you do not change the default authentication method before downgrading in this situation, you will have to log in using the fallback option after the downgrade, then you will have to change the authentication method to an option that was available prior to release 5.0(1) at that point.

Navigate to **Admin > AAA > Authentication**, then change the setting in the **Realm** field in the **Default Authentication** area of the page to change the default authentication method before downgrading your system. You will also have to manually delete the DUO login domain after the downgrade.

- Beginning in the 4.2(6) release, SNMPv3 supports the Secure Hash Algorithm-2 (SHA-2) authentication type. If you are running on Cisco APIC release 4.2(6) or later and you are using the SHA-2 authentication type, and then downgrade from Cisco APIC release 4.2(6) to a previous release, the downgrade will be blocked with the following error message:

```
SHA-2authentication type is not supported.
```

You can choose to either change the authentication type to MD5 or delete the corresponding SNMPv3 users to continue.

- Changing the container bridge IP address on Cisco APIC is supported only on Cisco APIC release 4.2(1) or later. If the container bridge IP address on Cisco APIC for AppCenter is configured with a non-default IP address, change it back the default 172.17.0.1/16 prior to downgrading to the older versions than 4.2(1).
- A static route (MO:**mgmtStaticRoute**) for Inband and/or Out-of-band EPG under **Tenants > mgmt > Node Management EPGs** is supported only on Cisco APIC release 5.1 or later. Delete this configuration and ensure the required service is still reachable via other means prior to the downgrade.
- Newly added microsegment EPG configurations must be removed before downgrading to a software release that does not support it.
- Downgrading the fabric starting with the leaf switch will cause faults such as policy-deployment-failed with fault code F1371.
- If you must downgrade the firmware from a release that supports FIPS to a release that does not support FIPS, you must first disable FIPS on the Cisco ACI fabric and reload all the switches in the fabric for the FIPS configuration change.
- If you have Anycast services configured in your Cisco ACI fabric, you must disable the Anycast gateway feature and stop Anycast services on external devices before downgrading from Cisco APIC 3.2(x) to an earlier release.
- CiscoN9K-C9508-FM-E2 fabric modules must be physically removed before downgrading to releases earlier than Cisco APIC 3.0(1). The same applies to any new modules for their respective supported version.

- If you are downgrading from Cisco APIC release 4.0(1) or later to release 3.2(x) or earlier, you may encounter a minor traffic drop in the fabric due to a difference in QoS classes supported between the releases. For more information, see [CSCwa32037](#).
- If you have remote leaf switches deployed, and you downgrade the Cisco APIC software from release 3.1(1) or later to an earlier release that does not support the remote leaf switches feature, you must decommission the nodes before downgrading. For information about prerequisites to downgrading Remote Leaf switches, see the *Remote Leaf Switches* chapter in the *Cisco APIC Layer 3 Networking Configuration Guide*.
- If the following conditions are met:
 - You are running the 5.2(4) release and the Cisco APIC created one or more system-generated policies.
 - You downgrade the Cisco APIC from the 5.2(4) release, then later upgrade back to the 5.2(4) release.

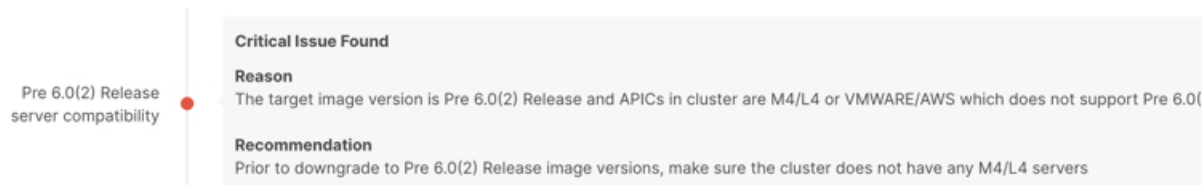
Then, one of the following behaviors will occur:

- If the Cisco APIC finds a policy with the same name and parameters as a system-generated policy that it is trying to create, then the Cisco APIC will take ownership of the policy and you cannot modify the policy. This occurs if you did not modify the policy after downgrading from the 5.2(4) release.
- If the Cisco APIC finds a policy with the same name as a system-generated policy that the Cisco APIC is trying to create, but the parameters are different, then the Cisco APIC will consider the policy to be a custom policy and you can modify the policy. This occurs if you modified the policy after downgrading from the 5.2(4) release.

Because of this behavior, you should not modify the system-generated policies after you downgrade from the 5.2(4) release.

- If you are downgrading from a Cisco APIC release that supports the Transport Layer Security (TLS) version 1.3, you enabled TLS 1.3 in a management access policy, and the target Cisco APIC release does not support TLS 1.3, then you must disable TLS 1.3 and instead enable TLS 1.2.
- 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 downgrade the image.
- In the Cisco APIC 6.0(2) release or later, if the cluster's discovery mode is set to "strict" and you want to downgrade to any 4.2 release or earlier, you must first change the discovery mode "permissive."
- The APIC-M4/L4 server is supported in the Cisco APIC 6.0(2) release and later and 5.3(1) release and later. However, if you downgrade from the 6.0(2) or 6.0(3) release to a 5.3 release, you see a pre-upgrade validation warning that the APIC-M4/L4 server is not supported. In this case, you can ignore the warning.

The following screenshot shows an example of this pre-upgrade validation warning:



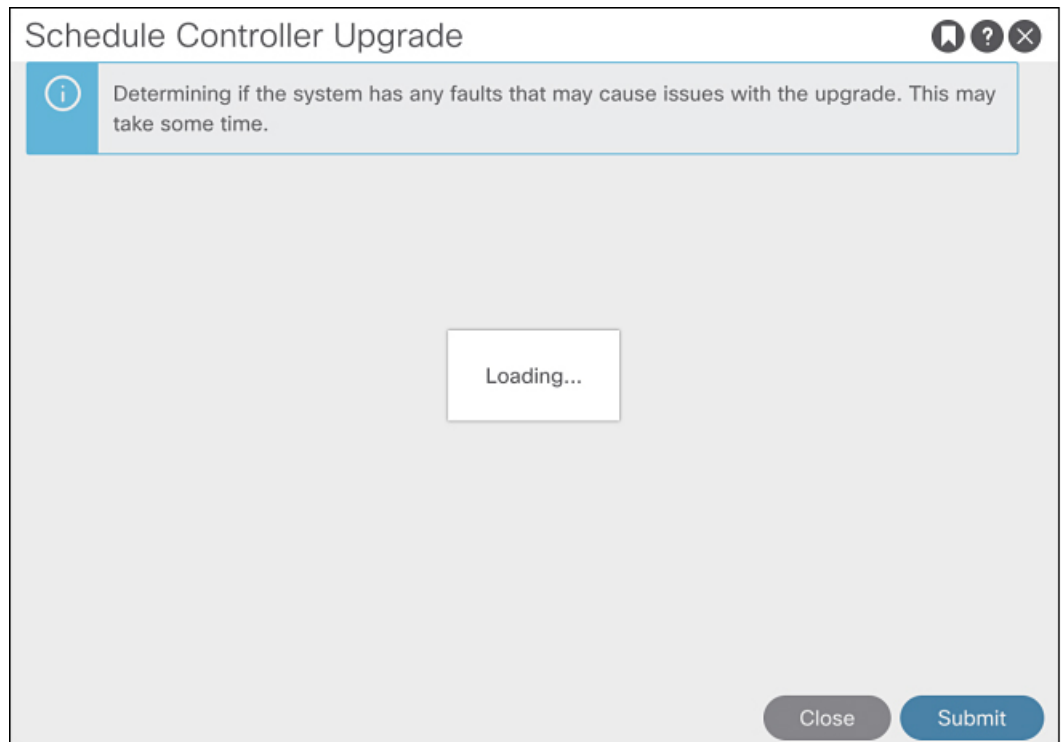
Examples of Pre-Upgrade Validator (APIC)

- [Example Error Messages and Override Options Through the GUI with APIC Release 4.2\(5\), on page 6](#)
- [Example Error Messages and Override Options Through the NX-OS Style CLI, on page 8](#)

Example Error Messages and Override Options Through the GUI with APIC Release 4.2(5)

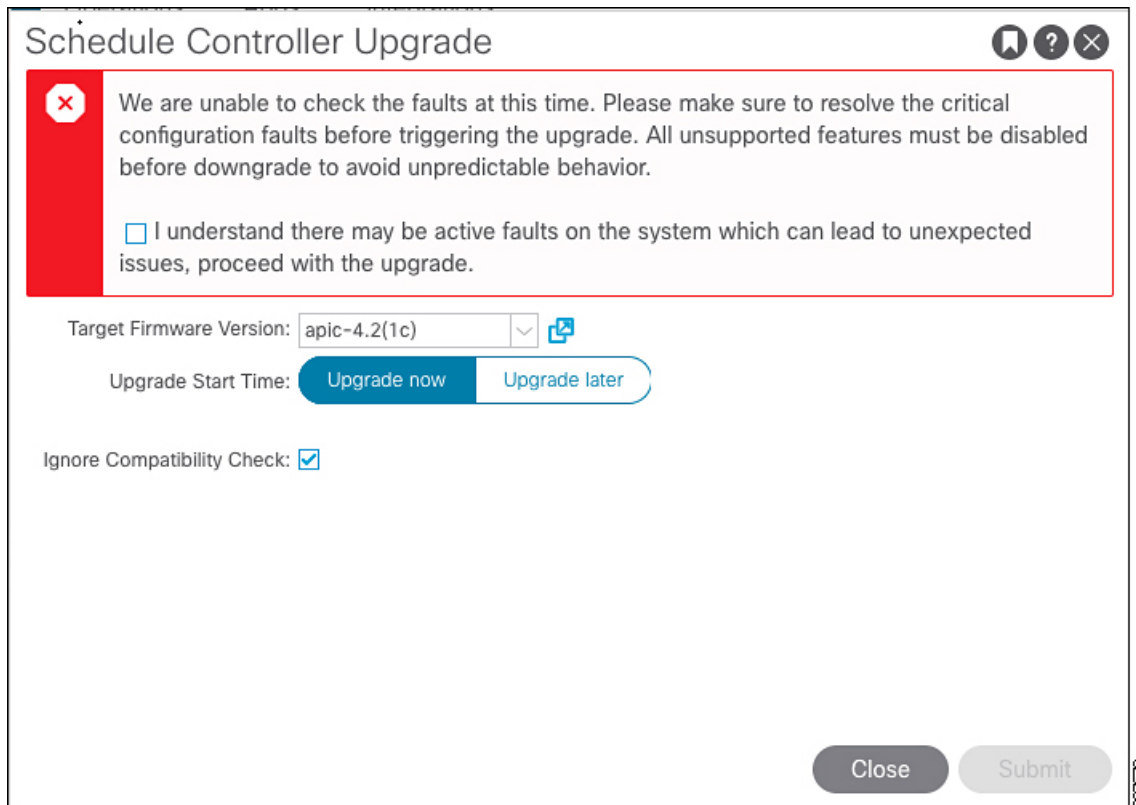
There are three situations where warning messages might appear through the GUI:

- While the query is loading, where you might see a message similar to the following:



This might occur because it sometimes takes a bit of time to load the data from a query. In this situation, be patient and wait for the system to finish loading the data from the query.

- If the query fails for some reason, you might see a message similar to the following:



Schedule Controller Upgrade

We are unable to check the faults at this time. Please make sure to resolve the critical configuration faults before triggering the upgrade. All unsupported features must be disabled before downgrade to avoid unpredictable behavior.

I understand there may be active faults on the system which can lead to unexpected issues, proceed with the upgrade.

Target Firmware Version:

Upgrade Start Time:

Ignore Compatibility Check:

This warning will appear if the query failed for some reason (for example, there might be so many faults that the system is overloaded). In this case, it is up to you to verify if there are any faults that might cause an issue with the upgrade.

However, if you want to override the block and proceed with an upgrade or downgrade without addressing the issue with the failed query, check the box next to the **I understand there may be active faults on the system which can lead to unexpected issues, proceed with the upgrade** field. This allows you continue with the upgrade or downgrade process without addressing the issue with the failed query.

- After the fault query is complete, where you might see a message similar to the following:

Schedule Controller Upgrade

Migration cannot proceed due to 1 active critical config faults. Ack the faults to proceed. It's recommended that these faults are resolved before performing a controller upgrade. All unsupported features must be disabled before downgrade to avoid unpredictable behavior. [Click Here](#) for more info.

I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade.

Target Firmware Version:

Upgrade Start Time:

Ignore Compatibility Check:

This warning message will appear when the fault query is complete and the system has found one or more faults. In this situation, click the **Click Here** link to get more information on the faults that the system found.

If possible, we recommend that you resolve the issue that was raised in the fault before proceeding with the upgrade or downgrade process. For more information on these faults and the recommended action for each, see the [Cisco APIC System Faults/Events Search Tool](#) and the [Cisco ACI System Messages Reference Guide](#).

However, if you want to override the block and proceed with an upgrade or downgrade without addressing the issue that was raised in the fault, check the box next to the **I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade** field. This allows you continue with the upgrade or downgrade process without addressing the faults that were detected.

Example Error Messages and Override Options Through the NX-OS Style CLI

When you attempt to upgrade the software through the NX-OS style CLI:

```
apic# firmware upgrade controller-group
```

You might see an error message similar to the following if faults on the fabric are detected:

```
Error: Migration cannot proceed due to 23 active critical config faults. Resolve the faults to proceed
```

If possible, we recommend that you resolve the issue that was raised in the fault before proceeding with the upgrade or downgrade process. For more information on these faults and the recommended action for each, see the [Cisco APIC System Faults/Events Search Tool](#) and the [Cisco ACI System Messages Reference Guide](#).

However, if you want to override the block and proceed with an upgrade or downgrade without addressing the issue that was raised in the fault, use the `ignore-validation` option to proceed with the upgrade:

```
apic# firmware upgrade controller-group ignore-validation
```

