



Disabling the USB Port on Cisco ACI-Mode Switches

[New and Changed Information](#) 2

[About Disabling the USB Port on Cisco ACI-Mode Switches](#) 2

[Guidelines and Limitations for Disabling the USB Port on Cisco ACI-Mode Switches](#) 2

[Disabling the USB Port on All Cisco ACI-Mode Switches in the Fabric Using the GUI](#) 3

[Disabling the USB Port on Specific Cisco ACI-Mode Switches in the Fabric Using the GUI](#) 3

[Disabling the USB Port on Cisco ACI-Mode Switches in the Fabric Using the REST API](#) 4

[Disabling the USB Port on a Specific Cisco ACI-Mode Switch in the Fabric Using the REST API](#) 4

Revised: April 7, 2022

New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Table 1: New Features and Changed Information

Cisco APIC Release	Feature	Description
5.2(3)	The ability to disable the USB port on Cisco ACI-mode switches was introduced.	--

About Disabling the USB Port on Cisco ACI-Mode Switches

Beginning in the Cisco Application Centric Infrastructure (ACI) 5.2(3) release, you can disable the USB port on a Cisco ACI-mode switch. If you have disabled the USB port, then when the switch is rebooted, the switch boots using the last known operating system image in the bootflash instead of using an image on a connected USB device. This feature provides an extra layer of protection in the event that someone power cycles the switch to try to boot the switch from a USB image that contains malicious code.

The USB port is enabled by default. You can configure a switch-level policy to disable the USB port on specific switches, or update the default USB configuration policy to disable USB port on all switches.

You can verify if someone tried to boot from the USB port by running the following command:

```
leaf1# show system reset-reason
***** module reset reason (1) *****
0) At 2021-09-01T12:04:10.165-07:00
Reason: reset-due-to-no-boot-from-usb-policy
Service:module reloaded
Version: 15.2(3a)
```

In this example output, the reason shows that someone tried to boot from the USB port, but because the USB port was disabled, the switch instead booted automatically with the last known good image in the bootflash.

Guidelines and Limitations for Disabling the USB Port on Cisco ACI-Mode Switches

The following guidelines and limitations apply for disabling the USB port on Cisco ACI-mode switches:

- If you downgrade to a release that is earlier than the 5.2(3) release, any disabled USB ports will become enabled.
- The contents of a USB drive that is plugged into the USB port will not be accessible if the USB port has been disabled due to the USB boot disable policy.
- On a dual supervisor spine switch, a USB configuration policy can disable the USB port on both the active and standby supervisor.

Disabling the USB Port on All Cisco ACI-Mode Switches in the Fabric Using the GUI

The following procedure uses the Cisco Application Policy Infrastructure Controller (APIC) GUI to disable the USB port on all Cisco ACI-mode switches in the fabric, except the switches that are controlled by a specific USB boot configuration policy.

For information about specific USB boot configuration policies, see [Disabling the USB Port on Specific Cisco ACI-Mode Switches in the Fabric Using the GUI, on page 3](#).

Procedure

- Step 1** On the menu bar, choose **Fabric > Access Policies**
- Step 2** In the Navigation pane, choose **Policies > Switch > USB Configuration > default**.
- Step 3** In the Work pane, put a check in the **Disable USB Port** check box.
This disables the USB port on all switches in the Cisco ACI fabric.
- Step 4** Click **Submit**.
-

Disabling the USB Port on Specific Cisco ACI-Mode Switches in the Fabric Using the GUI

The following procedure uses the Cisco Application Policy Infrastructure Controller (APIC) GUI to disable the USB port on specific Cisco ACI-mode switches in the fabric. The procedure assumes that you have not already created a USB configuration policy, switch policy group, or switch profile.

Procedure

- Step 1** On the menu bar, choose **Fabric > Access Policies**
- Step 2** In the Navigation pane, choose **Policies > Switch > USB Configuration**.
- Step 3** Right-click **USB Configuration** and choose **Create USB Configuration Policy**.
- Step 4** In the dialog, perform the following actions:
- a) In the **Name** field, enter a name.
 - b) Put a check in the **Disable USB Port** check box.
This disables the USB port on any switch that uses this policy, regardless of the configuration in the default USB configuration policy.
 - c) Click **Submit**.
- Step 5** In the Navigation pane, choose **Switches > Leaf Switches > Policy Groups** or **Switches > Spine Switches > Policy Groups** as appropriate.
- Step 6** Right-click **Policy Groups** and choose **Create Access Switch Policy Group** or **Create Spine Switch Policy Group** as appropriate.

- Step 7** In the dialog, perform the following actions:
- In the **Name** field, enter a name.
 - For the **USB Configuration Policy** drop-down list, choose the policy that you created.
 - Fill out the remaining fields as necessary.
 - Click **Submit**.
- Step 8** In the Navigation pane, choose **Switches > Leaf Switches > Profiles** or **Switches > Spine Switches > Profiles** as appropriate.
- Step 9** Right-click **Profiles** and choose **Create Leaf Profile** or **Create Spine Profile** as appropriate.
- Step 10** In the dialog, perform the following actions:
- In the **Name** field, enter a name.
 - For the **Leaf Selectors** or **Spine Selectors** section (as appropriate), click the +.
 - Enter a name for the selector, choose the switches for which you want to disable the USB port, and choose the policy group that you created, then click **Update**.
 - Click **Next**.
 - Create any interface selector profiles as necessary.
 - Click **Finish**.
-

Disabling the USB Port on Cisco ACI-Mode Switches in the Fabric Using the REST API

The following example XML post uses the REST API to disable the USB port on all Cisco ACI-mode switches in the fabric:

```
POST https://apic_name_or_ip/api/node/mo/uni/infra/usbconfigprofilepol-default.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="1">
  <topoctrlUsbConfigProfilePol disabled="yes" userdom="all"/>
</imdata>
```

- *apic_name_or_ip*: Replace this with the hostname or IP address of your Cisco APIC.
- *usbconfigprofilepol-default*: This specifies the default USB port policy, which applies to all switches.

Disabling the USB Port on a Specific Cisco ACI-Mode Switch in the Fabric Using the REST API

The following example XML post uses the Cisco Application Policy Infrastructure Controller (APIC) REST API to disable the USB port on a specific Cisco ACI-mode switch in the fabric:

```
POST https://apic_name_or_ip/api/node/mo/uni/infra/usbconfigprofilepol-usb_policy.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="1">
  <topoctrlUsbConfigProfilePol disabled="yes" userdom="all"/>
</imdata>
```

- *apic_name_or_ip*: Replace this with the hostname or IP address of your Cisco APIC.

- `usbconfigprofilepol-usb_policy`: This specifies the USB port policy. Replace *usb_policy* with the policy's name.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.