Troubleshoot "Invalid FRU" Errors in UCS Manager

Contents

Introduction

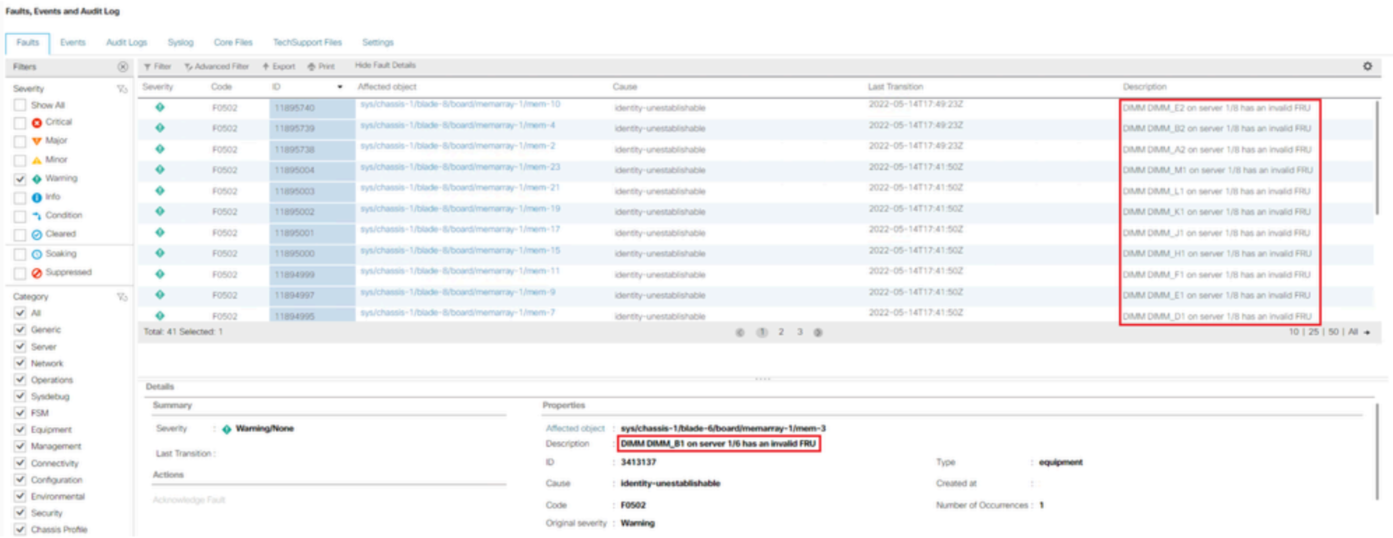
This document describes how to troubleshoot the "Invalid FRU" error message and address it within the UCS Manager.

Background Information

A Field Replaceable Unit (FRU), describes a part that can be replaced in the field, without requiring complex tools or procedures. Within Cisco Unified Computing System (UCS), all the components have a specific part ID (PID), and all the officially supported PIDs are contained within the Capability Catalog.

The Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configuration of components such as newly qualified DIMMs and disk drives for servers. The catalog is divided by hardware components, such as the chassis, CPU, local disk, and I/O module to view the list of providers available for that component. There is one provider per hardware component. Each provider is identified by the vendor, model (PID), and revision.

The "Invalid FRU" error messages usually appear after replacing or newly installing a part/server. Most often the fix for these is to update the capability catalog in UCSM. There is no impact on the catalog update, catalogs are backward compatible in the same major release (for example: 3.2(3i) is compatible with all previous 3.2 versions).



Severity	Code	ID	Affected object	Cause	Last Transition	Description
◆	F0502	11895740	sys/chassis-1/blade-8/board/memarray-1/mem-10	identity-unestablishable	2022-05-14T17:49:23Z	DIMM DIMM_E2 on server 1/8 has an invalid FRU
◆	F0502	11895739	sys/chassis-1/blade-8/board/memarray-1/mem-4	identity-unestablishable	2022-05-14T17:49:23Z	DIMM DIMM_B2 on server 1/8 has an invalid FRU
◆	F0502	11895738	sys/chassis-1/blade-8/board/memarray-1/mem-2	identity-unestablishable	2022-05-14T17:49:23Z	DIMM DIMM_A2 on server 1/8 has an invalid FRU
◆	F0502	11895004	sys/chassis-1/blade-8/board/memarray-1/mem-23	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_M1 on server 1/8 has an invalid FRU
◆	F0502	11895003	sys/chassis-1/blade-8/board/memarray-1/mem-21	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_L1 on server 1/8 has an invalid FRU
◆	F0502	11895002	sys/chassis-1/blade-8/board/memarray-1/mem-19	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_K1 on server 1/8 has an invalid FRU
◆	F0502	11895001	sys/chassis-1/blade-8/board/memarray-1/mem-17	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_J1 on server 1/8 has an invalid FRU
◆	F0502	11895000	sys/chassis-1/blade-8/board/memarray-1/mem-15	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_H1 on server 1/8 has an invalid FRU
◆	F0502	11894999	sys/chassis-1/blade-8/board/memarray-1/mem-11	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_F1 on server 1/8 has an invalid FRU
◆	F0502	11894997	sys/chassis-1/blade-8/board/memarray-1/mem-9	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_E1 on server 1/8 has an invalid FRU
◆	F0502	11894995	sys/chassis-1/blade-8/board/memarray-1/mem-7	identity-unestablishable	2022-05-14T17:41:50Z	DIMM DIMM_D1 on server 1/8 has an invalid FRU

Total: 41 Selected: 1

1 2 3

Details

Summary

Severity : ◆ Warning/None

Last Transition :

Actions

Properties

Affected object : sys/chassis-1/blade-6/board/memarray-1/mem-3
Description : DIMM DIMM_B1 on server 1/6 has an invalid FRU
ID : 3413137
Cause : identity-unestablishable
Code : F0502
Original severity : Warning
Type : equipment
Created at :
Number of Occurrences : 1

Updates to the Capability Catalog

The Cisco UCS Infrastructure Software Bundle includes capability catalog updates. Unless otherwise instructed by the Cisco Technical Assistance Center (TAC), you only need to activate the capability catalog update after you have downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

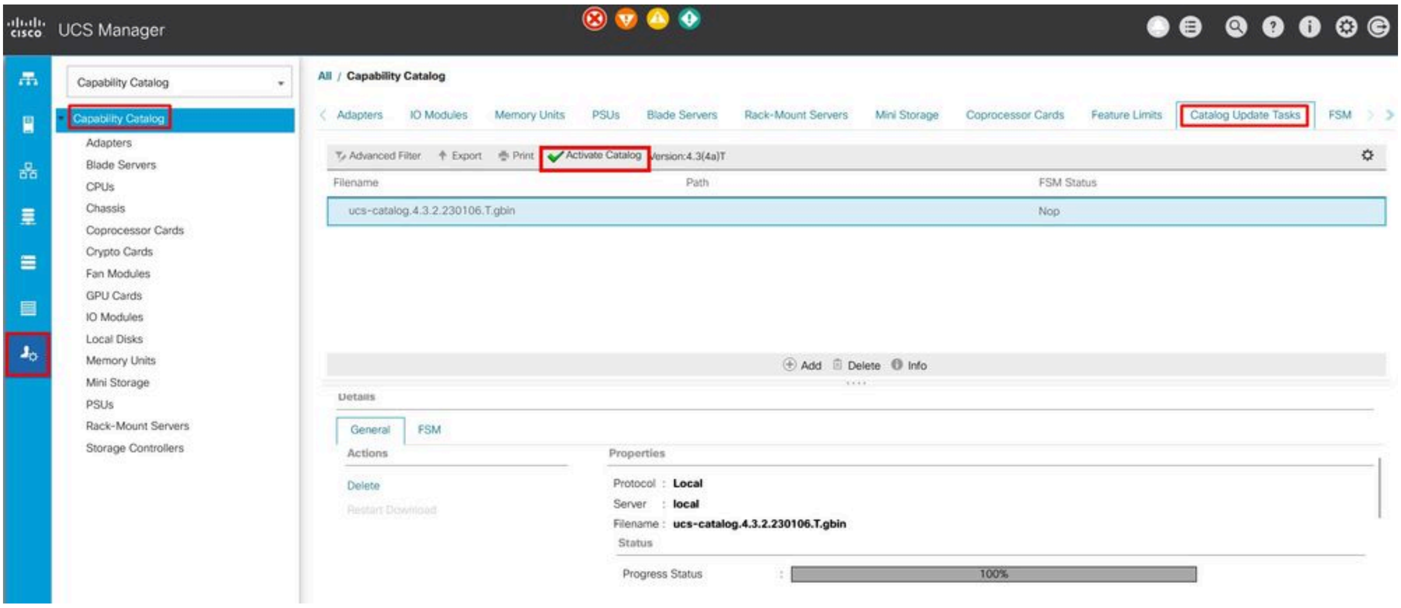
As soon as you activate a capability catalog update, Cisco UCS immediately updates to the new baseline catalog. You do not have to perform any further tasks. Updates to the capability catalog do not require you to reboot or reinstall any component in a Cisco UCS domain.

Each Cisco UCS Infrastructure Software Bundle contains a baseline catalog. Under some circumstances, Cisco releases an update to the capability catalog between Cisco UCS releases and makes it available on the same site where you download firmware images.

Configuration Steps

Activating a Capability Catalog Update.

Step 1. In the Navigation pane, click **Admin**.
Step 2. Expand **All > Capability Catalog.**
Step 3. Click **Capability Catalog node**.
Step 4. In the Work pane, click **Catalog Update Tasks** tab.
Step 5. Click **Activate Catalog**.
Step 6. In the Activate Catalog dialog box, choose the **Capability Catalog Update** that you want to activate from the version to be Activated drop-down list.
Step 7. Click **OK**.



Version:4.3(4a)T

Filename	Path	FSM Status
ucs-catalog.4.3.2.230106.T.gbin		Nop

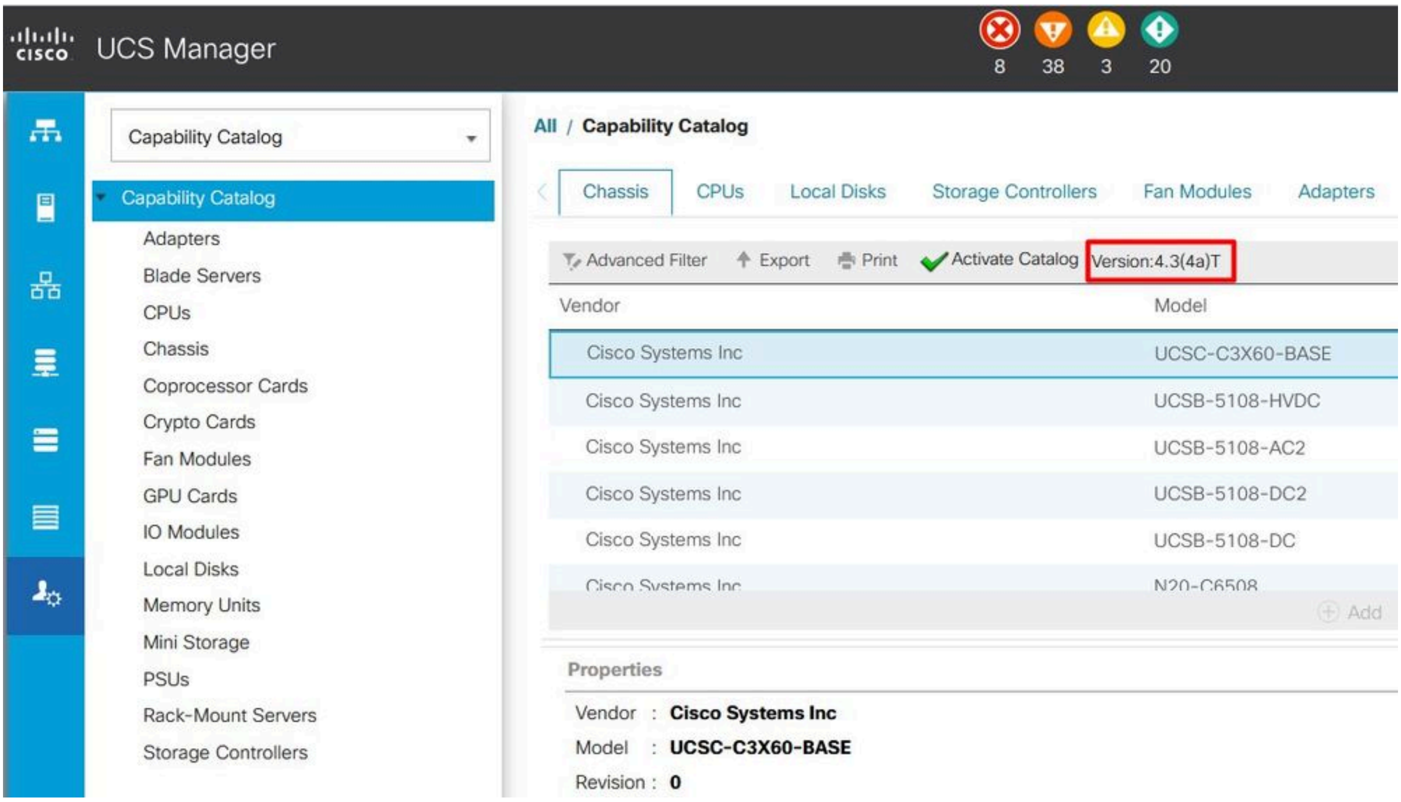
Protocol : Local
Server : local
Filename : ucs-catalog.4.3.2.230106.T.gbin

Progress Status : 100%

Verify

Verify that the Capability Catalog Is current.

Step 1. In the Navigation pane, click **Admin**.
Step 2. Expand **All > Capability Catalog**.
Step 3. Click **Capability Catalog node**.
Step 4. In the Work pane, click **Catalog Update Tasks** tab. The current version of the capability catalog is located on the upper right of that tab.



Version:4.3(4a)T

Vendor	Model
Cisco Systems Inc	UCSC-C3X60-BASE
Cisco Systems Inc	UCSB-5108-HVDC
Cisco Systems Inc	UCSB-5108-AC2
Cisco Systems Inc	UCSB-5108-DC2
Cisco Systems Inc	UCSB-5108-DC
Cisco Systems Inc	N20-C6508

Vendor : Cisco Systems Inc
Model : UCSC-C3X60-BASE
Revision : 0

Step 5. On Cisco website, determine the most recent release of the capability catalog available. For more information about the location of capability catalog updates, review the Troubleshooting section under Obtaining Capability Catalog Updates from Cisco.

Step 6. If a more recent version of the capability catalog is available, update the capability catalog with that version.

Troubleshooting

Obtaining Capability Catalog Updates from Cisco.

Step 1. In a web browser, navigate to the Cisco website.
Step 2. Under **Support**, click **All Downloads**.
Step 3. In the center pane, click **Unified Computing and Servers**.
Step 4. If prompted, enter your **Cisco.com username** and **password** to log in.
Step 5. In the right pane, click Cisco **UCS Infrastructure and UCS Manager Software > Unified Computing System (UCS) Manager Capability Catalog**.
Step 6. Click the link for the latest release of the Capability Catalog
Step 7. Choose one of the options available.

Download Now — Allows you to download the catalog update immediately.
Add to Cart — Adds the catalog update to your cart to be downloaded at a later time.

Step 8. Complete the download of the catalog update.

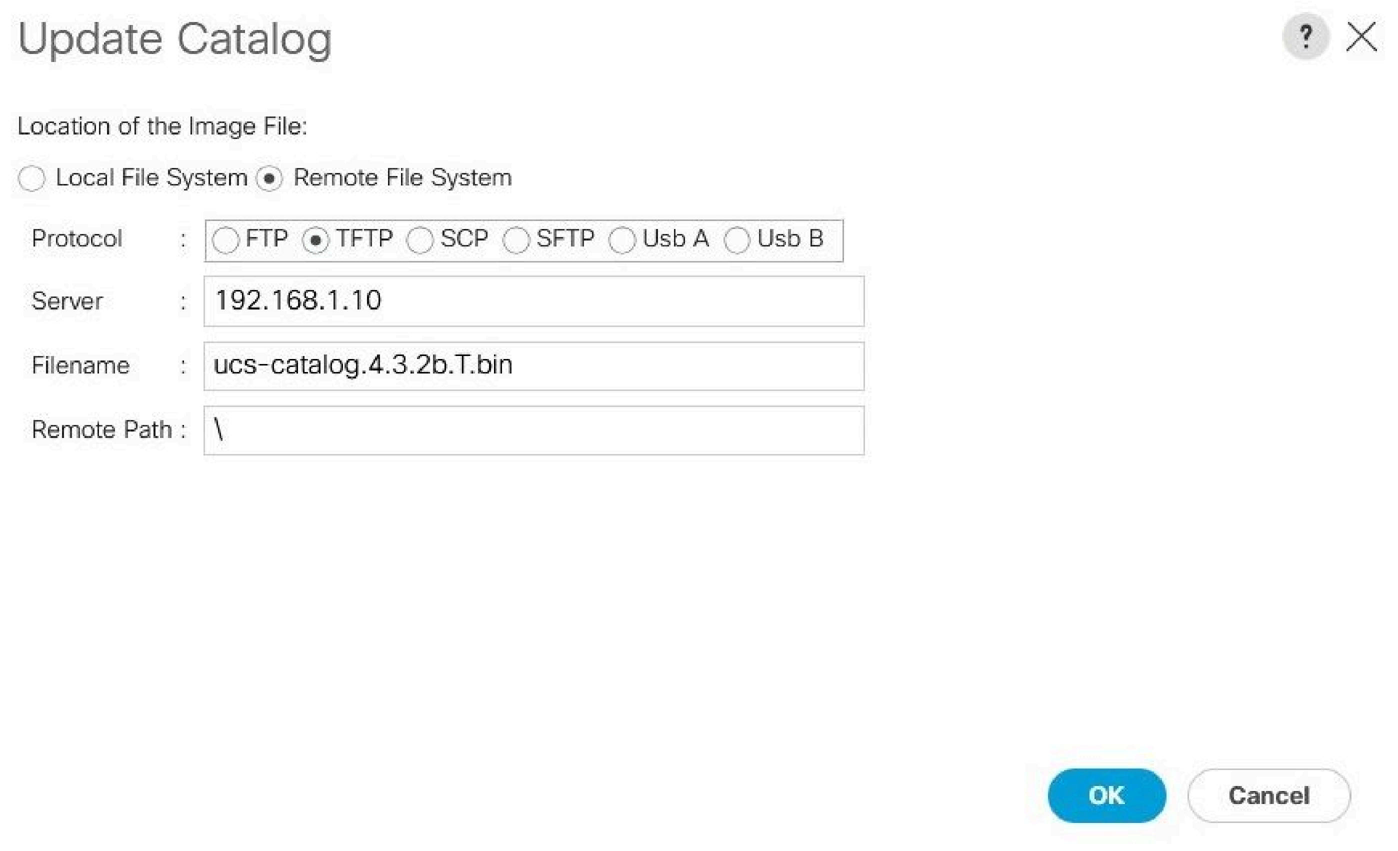
Updating the Capability Catalog from a Remote Location.

You cannot perform a partial update to the Capability Catalog. When you update the Capability Catalog, all components included in the catalog image are updated.
A B-series server bundle includes the Capability Catalog update for that server. You do not need to download a separate Capability Catalog update. You only need to activate the Capability Catalog update.

Step 1. In the Navigation pane, click **Admin**.
Step 2. Expand **All > Capability Catalog**.
Step 3. Click the **Capability Catalog node**.
Step 4. In the Work pane, click the **Catalog Update Tasks** tab.
Step 5. Click **Add**, to open the **Update Catalog** prompt.

Step 6. In the **Update Catalog** dialog box, click **Remote File System** radio button in the Location of the Image File field and fill in the required fields.
Step 7. Click **OK**.

Example using TFTP.



Update Catalog

Location of the Image File:

○ Local File System ● Remote File System

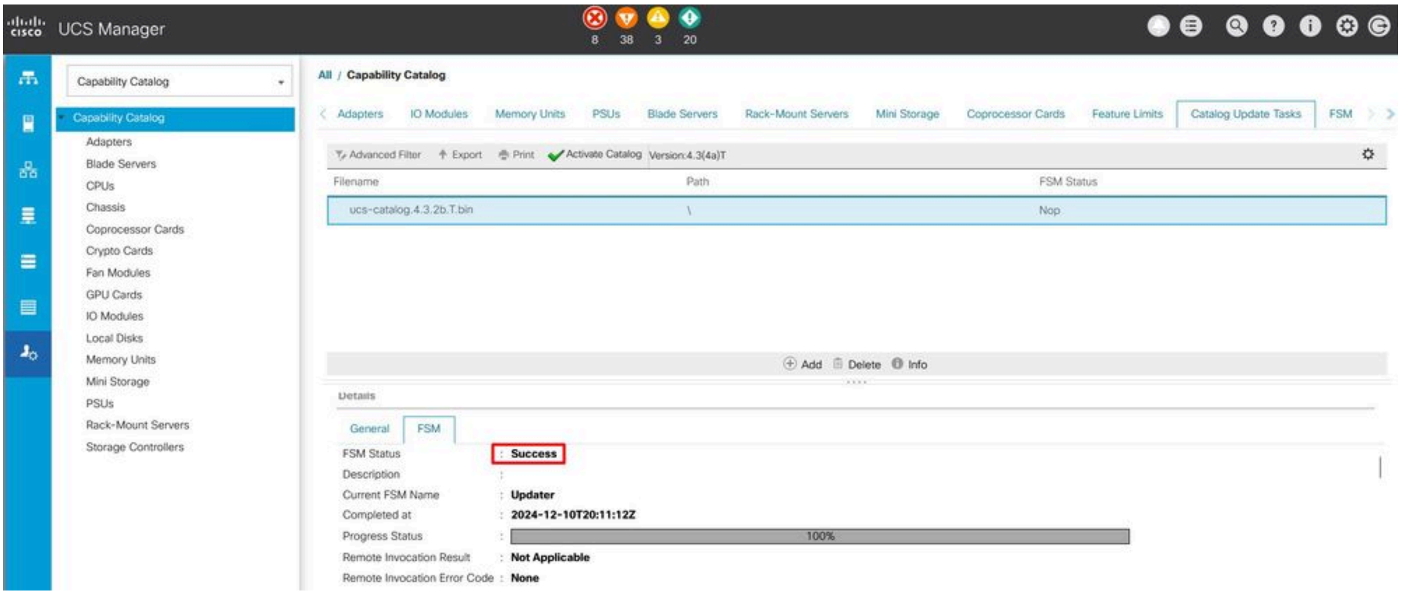
Protocol : ○ FTP ● TFTP ○ SCP ○ SFTP ○ Usb A ○ Usb B

Server : 192.168.1.10

Filename : ucs-catalog.4.3.2b.T.bin

Remote Path : \

Cisco UCS Manager downloads the image and updates the Capability Catalog. You do not need to reboot any hardware components.



All / Capability Catalog

Version:4.3(4a)T

Filename	Path	FSM Status
ucs-catalog.4.3.2b.T.bin	\	Nop

Details

FSM Status : Success

Description :

Current FSM Name : Updater

Completed at : 2024-12-10T20:11:12Z

Progress Status : 100%

Remote Invocation Result : Not Applicable

Remote Invocation Error Code : None

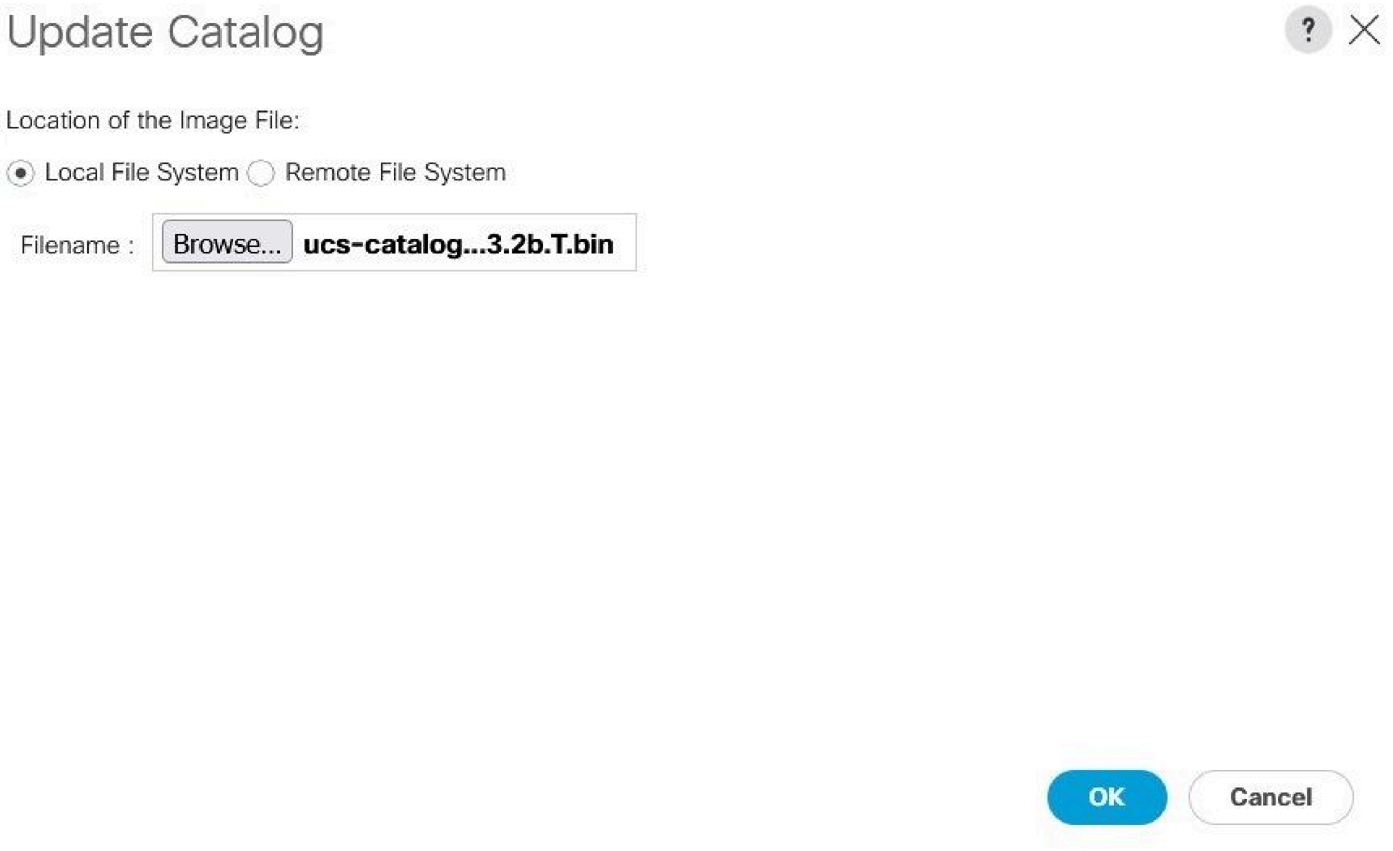
Updating the Capability Catalog from the Local File System

You cannot perform a partial update to the Capability Catalog. When you update the Capability Catalog, all components included in the catalog image are updated.

A B-series server bundle includes the Capability Catalog update for that server. You do not need to download a separate Capability Catalog update. You only need to activate the Capability Catalog update.

Step 1. In the Navigation pane, click **Admin**.
Step 2. Expand **All > Capability Catalog**.
Step 3. Click **Capability Catalog node**.
Step 4. In the Work pane, click **Catalog Update Tasks** tab.
Step 5. Click **Add**, to open the **Update Catalog** prompt.
Step 6. In the Download Firmware dialog box, click the **Local File System** radio button in the Location of the Image File field.
Step 7. In the **Filename** field, type the **full path** and **name** of the image file. If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.
Step 8. Click **OK**.

Cisco UCS Manager downloads the image and updates the Capability Catalog. You do not need to reboot any hardware components



Update Catalog

Location of the Image File:

● Local File System ○ Remote File System

Filename : Browse... ucs-catalog...3.2b.T.bin

After the capability catalog is updated, the server must go through a rediscovery so all the FRU PIDs are rediscovered and checked against the new capability catalog. You can accomplish this by doing a reacknowledgment of the server. This is impactful as the server reboots during the process. Also, be mindful if you have any local disk scrub policies assigned as a decommission, and re-acknowledge can trigger during those if applied.

If the "Invalid FRU" error messages persist after the Compatibility Catalog update, and the server re-acknowledges, validate these items:

- All components are correctly installed/seated.
- The components installed are genuine with a valid Cisco PID.
- For DIMMs, validate that the correct population rules are being followed as documented on the server spec sheet.
- For Converged Network Adapters, such as VIC or MLOMs, NIC Adapters, and HBA Adapters, validate the card is in the correct slot and that it is supported for the intended server.

Related Information

- Capability Catalog Download from Cisco.com
- Cisco UCS X-Series Modular System - Datasheets
- UCS C-Series Rack Servers - Datasheets
- UCS B-Series Blade Servers - Datasheets