

# Run UCSM Health and Pre-Upgrade Check Tool

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[When to Use](#)

[How to Use](#)

[Windows OS](#)

[MacOS](#)

[Understand Outputs/Checks Performed](#)

[Checks Performed by UCSM HealthCheck](#)

[Sample UCSM Tool Output Number](#)

[Analyze Tool Output - Next Steps](#)

[CLI Commands](#)

## Introduction

This document describes the process to run Unified Computing System Manager (UCSM) Health and Pre-Upgrade check tool.

## Prerequisites

### Requirements

Cisco recommends that you have Python 3.6 or later installed on the system.

---

**Note:** If you are running Windows OS, you can have Python installed and configured the Environment path.

---

---

**Note:** Do not open a TAC case for Python issues/Script failed to run. Refer the CLI commands section to manually identify the issue and open TAC case per identified issue

---

### Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

The UCSM Check Tool is a utility to perform pro-active self-checks on UCSM to ensure its stability and resiliency. It helps automate a list of health and pre-upgrade checks on UCS systems to save time when the

UCS infrastructure upgrade and maintenance operations take place.

---

**Note:** Always download and use the latest version of the tool. Since the tool is enhanced frequently, when you use an older version, it can miss important checks.

---

**Note:** This script is a best effort, free to use, and cannot identify all possible issues.

---

## When to Use

- Before UCS infrastructure upgrades
- UCS Health Check before and after Maintenance Activity
- When you work with Cisco TAC
- Proactive Health Check anytime

## How to Use

### Windows OS

Step 1. Download the latest version of Python from [Python Downloads](#)

Step 2. Use the normal installation process and click **Install Now** (the recommended one), to download the setup.

---

**Note:** Ensure to check **Add Python to PATH**.

---

Python 3.10.0 (64-bit) Setup



## Install Python 3.10.0 (64-bit)

Select Install Now to install Python with default settings. Customize to enable or disable features.



### Install Now

C:\Users\akmalla\AppData\Local\Programs\Python\Python310

Includes IDLE, pip and documentation  
Creates shortcuts and file associations



Customize installation  
Choose location and features

Install launcher for all users (recommended)

Add Python 3.10 to PATH

Step 3. Navigate to the directory in which Python was installed on the system.

Step 4. Open the command prompt and type the command **Python** to verify the python installation.

Command Prompt - python

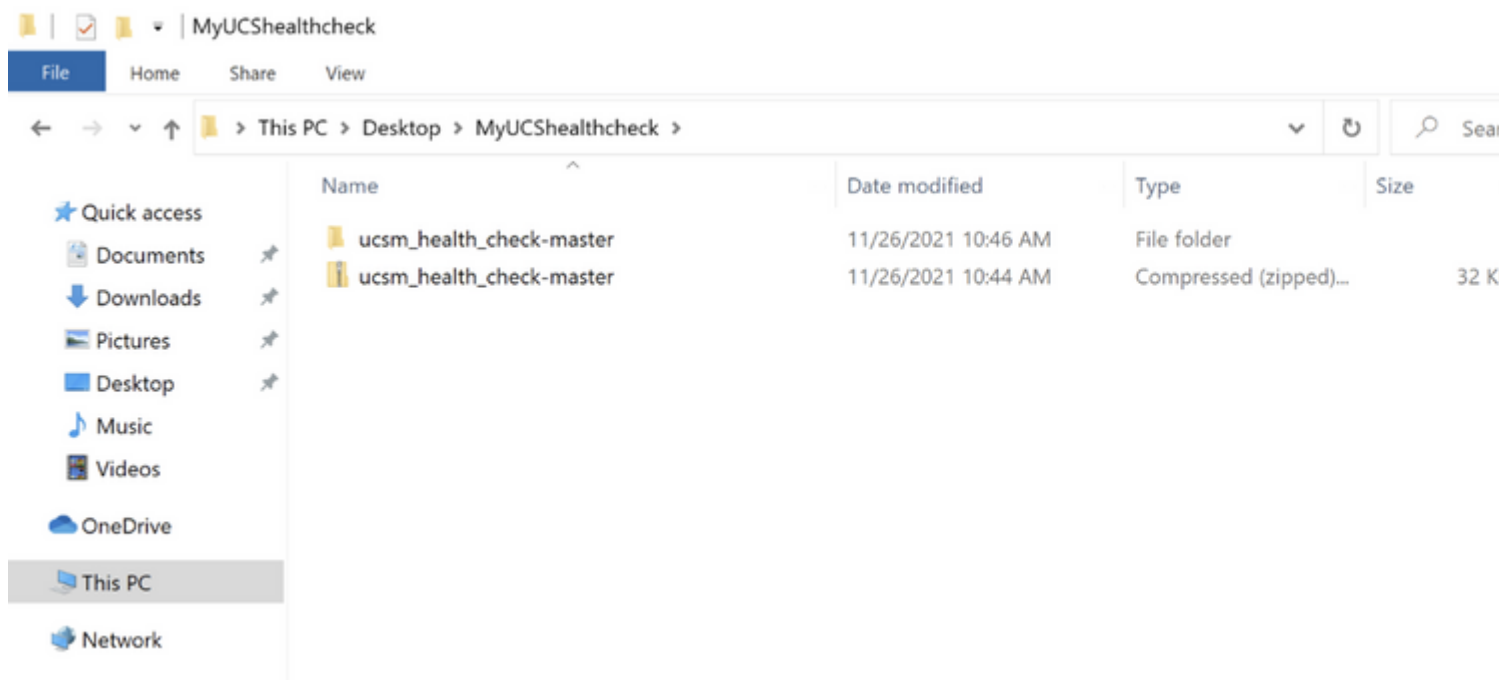
```
Microsoft Windows [Version 10.0.19043.1288]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\akmalla>python
```

```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct 4 2021, 19:00:18) [MSC v.1929 64 bit (AMD64)] on  
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>>
```

Step 5. Download the latest version of the health check script from [here](#) and save it to a folder. Now, extract the compressed file, as shown in the image.



Step 6. **Download** and **save** the latest UCSM technical support logs to the folder created, as shown in the image. Click this link to find the steps to download UCSM log bundle; [Generating UCSM technical support.](#)

Step 7. Open CMD and cd to the folder where UCSMTool.py is located and run **UCSMTool.py** as shown in the image.

C:\> Select Command Prompt - UCSMTool.py

```
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\[redacted]>cd akash
```

```
C:\Users\[redacted]>cd ucsm_health_check-mast
```

```
C:\Users\[redacted]\ucsm_health_check-master>
```

```
UCS Health Check Tool 1.1
```

```
Enter the UCSM file path: █
```

Step 8. Enter the file path where the UCSM technical support file is located and choose **desired option**.

1. UCSM Health Check
2. PreUpgrade Check

```
C:\[REDACTED]\Akash\ucsm_health_check-master>UCSMTool.py

UCS Health Check Tool 1.1

Enter the UCSM file path: \Akash\ucsm

Press 1 for UCSM Health Check
Press 2 for PreUpgrade Check
Enter your choice (1/2): 1
Invalid file path: \Akash\ucsm

C:\[REDACTED]\Akash\ucsm_health_check-master>UCSMTool.py

UCS Health Check Tool 1.1

Enter the UCSM file path: C:\[REDACTED]\Akash\UCSM.tar

Press 1 for UCSM Health Check
Press 2 for PreUpgrade Check
Enter your choice (1/2): 1

Log Extraction: [#####] COMPLETED
```

## MacOS

Step 1. MacOS comes with default python installed, verify the installed python version as shown here:

```
[MacBook-Pro:~ gakumari$ python --version
Python 2.7.16
[MacBook-Pro:~ gakumari$
[MacBook-Pro:~ gakumari$ python3 --version
Python 3.9.9
```

---

**Note:** In case the python version is lower than 3.6, please upgrade to 3.6 and later releases.

---

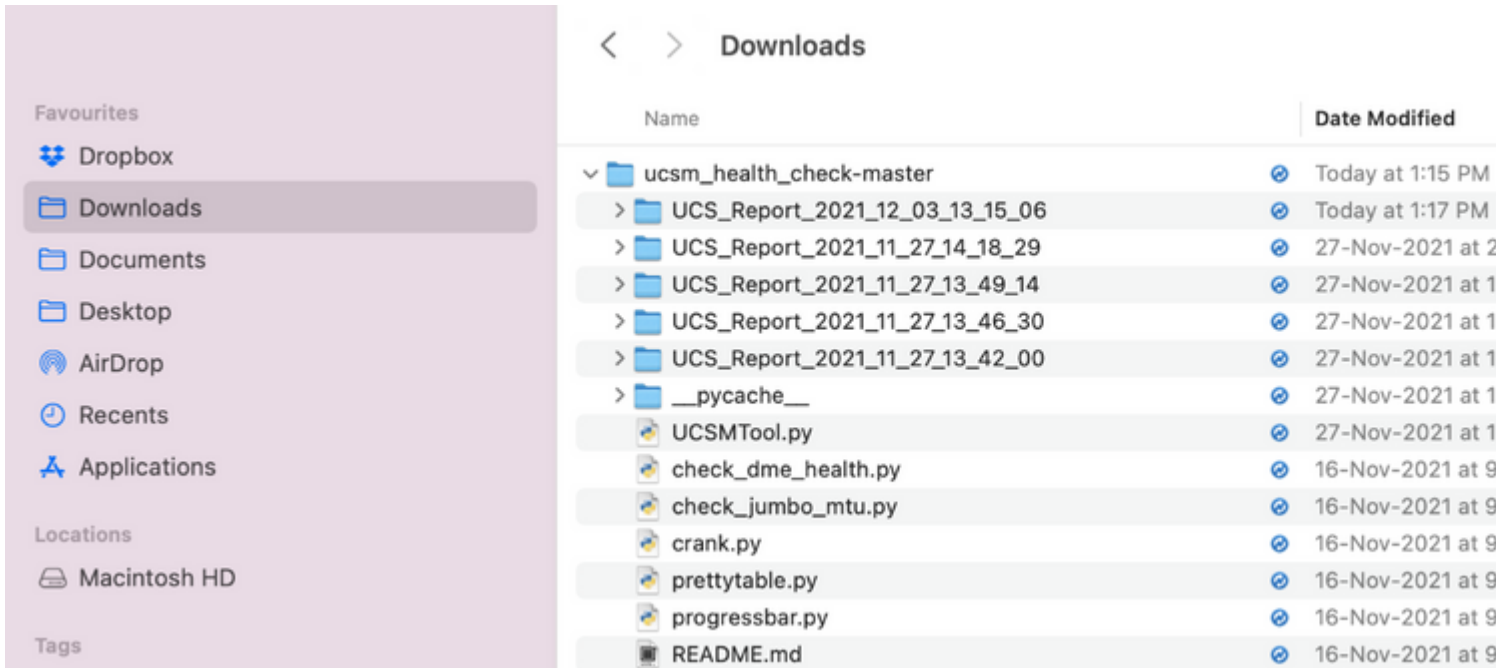
**Note:** If the python version is 3.6 or later, jump to Step 5 otherwise, jump to Step 2.

---

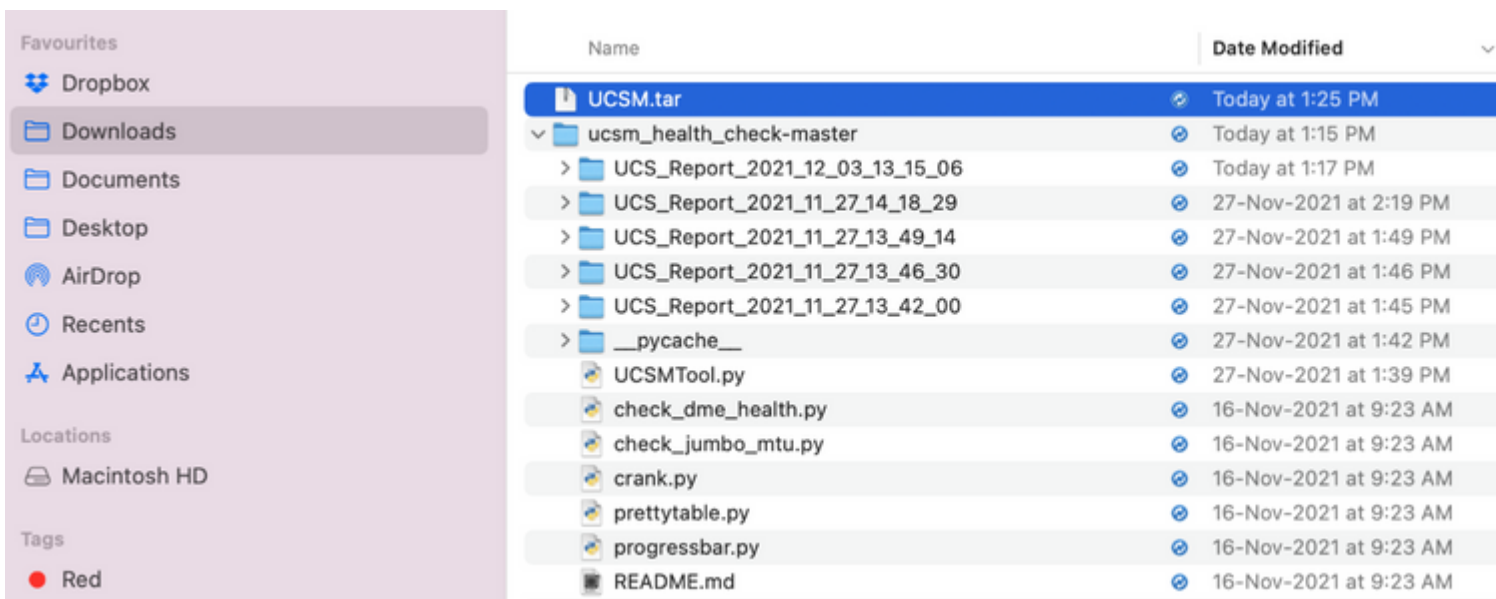
Step 2. Download the latest version of Python from <https://www.python.org/downloads/macos/>.

Step 3. Use the normal installation process to complete/upgrade the python installation.

Step 4. **Download** the latest version of the health check script from [here](#) and **save** it to a folder. Now, extract the compressed file, as shown in this image.



Step 5. **Download** and **save** the latest UCSM technical support logs to the folder created, as shown in this image. Click the link to find the steps to download UCSM log bundle; [Generating UCSM technical support.](#)



Step 6. Open the terminal, browse to the directory where you have the health check script downloaded, run `python UCSMTool.py` or `python3UCSMTool.py` as shown here.

```

[MacBook-Pro:~ gakumari$ cd Downloads
[MacBook-Pro:Downloads gakumari$ cd ucsm_health_check-master/
[MacBook-Pro:ucsm_health_check-master gakumari$ /usr/local/bin/py

```

Step 7. Enter the file path where the UCSM technical support file is located and choose **desired option** to execute the script.

1. UCSM Health Check
2. PreUpgrade Check

```
MacBook-Pro:ucsm_health_check-master gakumari$ /usr/local/bin/
UCS MU Tool 1.1
Enter the UCSM file path: /Users/gakumari/Downloads/UCSM.tar
Press 1 for UCSM Health Check
Press 2 for PreUpgrade Check
Enter your choice (1/2): 1
Log Extraction: [#####] COMPLETED
```

## Understand Outputs/Checks Performed

### Checks Performed by UCSM HealthCheck

These checks are performed by UCSM-Healthchecktool:

**UCSM HA Cluster State:** Displays the cluster state of fabric interconnects.

**PMON Process State:** Displays the state of all processes in Cisco UCS Manager.

**File System Mount:** Displays the mount table.

**Check for /var/ sysmgr size issue:** Checks /var/ sysmgr usages.

**Check for /var/ tmp size issue:** Checks if /var/ tmp usages.

**6296 FI unresponsive after a power cycle, HW revision update:** Verify Fabric interconnect module and its HW revision number.

**Faults with Severity Major or Severity Critical:** Reports if you have any Major or Critical Alert in UCS Manager.

**Check Backup Available:** Verify if Backup is Available in UCS Manager.

**Keyring Cert Check:** Check if the keyring is expired or valid.

**Safeshut Workaround Needed or Not:** Check if shafeshut workaround is needed or not by verifying the FI model and its version.

**Deprecated Hardware in Cisco UCS Manager Release 4.x:** Check for any deprecated Hardware in Cisco UCS Manager 4.x Release.

**Deprecated HW found for 3.1.x onwards:** Check for any deprecated Hardware in Cisco UCS Manager 3.x Release

**Check for B200M4 reboot due to blank MRAID12G fields:** Check if B200M4 server has a blank



S/N of MRAID12G RAID controller.

**UCSM 3.1 Change in max power allocation causes blade discovery failure:** Verifies the power policy configured in the UCS Manager.

**Existence of bootflash corruption fault code F1219:** Check the existence of bootflash corruption.

**Check for httpd fail to start when the default keyring is deleted:** Check if the default keyring is deleted.

**3rd GEN FIs has unclean file system states-"Filesystem state: clean with errors":** Check for file system error.

**Check for Server Auto-Install to 4.0(4b) Fails to Activate SAS Controller:** Verify the host Firmware version and the SAS Expander version

**Check for C-Series firmware upgrade stays long in process "perform an inventory of server" PNU OS Inventory:** It verifies the server Model and its version to identify if you hit this issue.

**Check UCSM Authentication Domain that uses a Period or Hyphen:** Verify if Authentication Domain name is configured with a period or hyphen characters.

**Local or fallback Authentication failure:** Check for authentication method configured for a particular FI model and verifies its version as well.

**Health check between UCSM and UCS central:** Verify if UCSManager is registered with UCS Central

**LAN and SAN Pin Groups:** Check the lan/san pinning configuration in your cluster and highlight to review your configuration before upgrade/any MW activity

**Checking Pending Activities Present in UCSM:** Verify if there are any pending Activities in your UCS Manager Domain.

**Health Check for IOM:** Check overall health of the IO Modules.

**Core Files available in UCSM Check:** Verify if any Core File is found within 60 days.

**Disjoint L2 potential misconfiguration:** Verify if there is any misconfiguration in case Disjoint L2 is configured.

**VIC 1400 and 6400 Link Flap issue:** Check for conditions present in this defect

**Check 2304 IOMs disconnect and re-connect during firmware update:** Verify the Fabric Interconnect and IO module model and identify if there is any potential issue.

**DME Health Check:** Verify the health of the Data Management Engine (DME) database.

**Number of Interface up and Flogi Matching on FI:** Verify number of interfaces and flogiâ€™s session

**Jumbo or Standard MTU Check:** Identify the MTU configuration.

## Sample UCSM Tool Output Number

```
afrahmad@AFRAHMAD-M-C3RS ucsm_health_check-master $ python UCSMTool.py
```

Enter the UCSM file path: /Users/afrahmad/Desktop/20190328180425\_fabric-5410-1k08\_UCSM.tar

Press 1 for UCSM Health Check

Press 2 for PreUpgrade Check

Enter your choice (1/2): 2

Enter the UCS Target Version [Ex:4.1(1x)]: 4.2(1i)

Log Extraction: [#####] COMPLETED

UCSM Version: 3.2(3h)A

Target Version: 4.2(1i)

Upgrade Path: 3.2(3) ==> 4.2(1i)

Summary Result:

SlNo	Name	Status	Comments
1	UCSM HA Cluster State	PASS	
2	PMON Process State	PASS	
3	File System Mount	PASS	
4	Check for /var/sysmgr size issue	Not Found	
5	Check for /var/tmp size issue	Not Found	
6	6296 FI unresponsive after power cycle, HW revision update	Not Found	
7	Faults with Severity Major or Severity Critical	Found	Review the faults
8	Check Backup Available	No Backup	Please ensure backup is available. Refer this link: <a href="http://go2.cisco.com">http://go2.cisco.com</a>
9	Keyring Cert Check	PASS	
10	Safeshut Workaround Needed or Not	Not Needed	
11	Deprecated Hardware in Cisco UCS Manager Release 4.x	Found	Review the release notes. Refer this link: <a href="http://go2.cisco.com">http://go2.cisco.com</a>
12	Deprecated HW found for 3.1.x onwards	Not Found	
13	Check for B200M4 reboot due to blank MRAID12G fields	Found	Contact TAC
14	UCSM 3.1 Change in max power allocation causes blade discovery failure	Not Found	
15	Existence of bootflash corruption fault code F1219	Not Found	
16	Check for httpd fail to start when default keyring is deleted	Not Found	
17	3rd GEN FIs has unclean file system states-"Filesystem state: clean with errors"	Not Found	
18	Check for Server Auto-Install to 4.0(4b) Fails to Activate SAS	Not Found	

	Controller		
19	Check for C-Series firmware upgrade stays long in process "perform inventory of server" PNU OS Inventory	Not Found	
20	Check UCSM Authentication Domain using a Period or Hyphen	Not Found	
21	Local or fallback Authentication failure	Not Found	
22	Health check between UCSM and UCS central	Not Found	UCS Manager is
23	LAN and SAN Pin Groups	Not Found	
24	Checking Pending Activities Present in UCSM	Not Found	
25	Health Check for IOM	PASS	
26	Core Files available in UCSM Check	Not Found	No core files
27	Disjoint L2 potential misconfiguration	Not Found	
28	VIC 1400 and 6400 Link Flap Issue	Not Found	
29	Check 2304 IOMs disconnect and re-connect during firmware update step	Not Found	
30	Number of Interface up and Flogi Matching on FI	---	Primary: FC Port Trun Eth up Port: Flogi Count: Secondary: FC Port Trun Eth up Port: Flogi Count:
31	Jumbo or Standard MTU Check	NOT_FOUND	

#### Faults with Severity Major:

F0207: Adapter ether host interface 3/3/1/2 link state: down  
F0207: Adapter ether host interface 3/3/1/4 link state: down  
F0207: Adapter ether host interface 3/3/1/3 link state: down  
F0283: ether VIF 1153 on server 3 / 3 of switch B down, reason: Admin config change  
F0479: Virtual interface 1153 link state is down

We would recommend Customers should complete the below prior to an upgrade:

- Review firmware release notes
- Review compatibility
- Upload required images
- Generate/Review UCSM show tech
- Determine vulnerable upgrade bugs and complete pro-active workaround
- Verify FI HA and UCSM PMON status
- Generate all configuration and full state backups (right before upgrade)
- Verify data path is ready (right before upgrade)
- Disable call home (right before upgrade)

#### NOTE:

- All reports and logs will be saved in the same location from where the script was executed.
- Please visit the Summary Report/ Main Report to view all the Major and Critical Fault alerts.

## Analyze Tool Output - Next Steps

- The tool automates the process of running manual commands on UCS Systems.
- If the tool runs **OK** and gives **PASS/NOT FOUND** on all tests. The UCS system is good for all the checks which the script has performed.
- In situations where the tool **FAIL/FOUND** on some checks or does not run successfully, you can use the CLI commands (listed here) to perform the same checks on UCS System/Fabric interconnect as done by the script Manually.
- The tool DOES NOT check for any old/new/open/resolved caveats and hence it is highly recommended to review UCS Release Notes and Upgrade Guides before any upgrade or maintenance activity.

---

**Tip:** For a general health check of your UCS environment, Cisco TAC does not provide this service. Cisco's CX Customer Delivery Team (formerly known as Advanced Services) does have a bug scrub/risk analysis it offers. If you require this type of service, contact your Sales/Account Team.

---

## CLI Commands

SSH to both Fabric Interconnects:

```
# show cluster extended-state, verify HA status is ready.
# connect local-mgmt ; # show pmon state, Verify the services are in running status.
# connect nxos ; # show system internal flash, Verify free size in /var/sysmgr and /var/tmp
# connect nxos ; # show module, verify HW revision number for 6296 fabric interconnects.
# show fault detail | include F1219, verify this fault code for bootflash corruption
# show iom health status, displays health of IOM
# show server status, verify the status of server.
# scope monitoring; # scope sysdebug; # show cores , verify if there are any core files.
# scope security; # scope keyring default; #show detail, verify details for default keyring, expiry etc
# connect nxos; # show int br | grep -v down | wc -l, verify the number of active Ethernet interfaces
# scope security; # show authentication, review the authentication type.
# connect nxos; # show flogi database, review the flogi database.
```