Overview Cisco UCS Host Upgrade Utility (Standalone & Non Interactive)

Jeff Foster
Technical Marketing Engineer

The Cisco C-Series Cisco Integrated Management Controller (CIMC) software delivers many new features and capabilities including enhancements to the Host Upgrade Utility (HUU). The Host Upgrade Utility enables users to update their CIMC, BIOS, LOM, RAID Controllers, PCI adapters and Cisco VIC cards from a single interface. In previous versions of HUU, an interactive menu-driven command line interface was the only option provided to update system BIOS, CIMC, adapter firmware, and LAN on Motherboard (LOM).

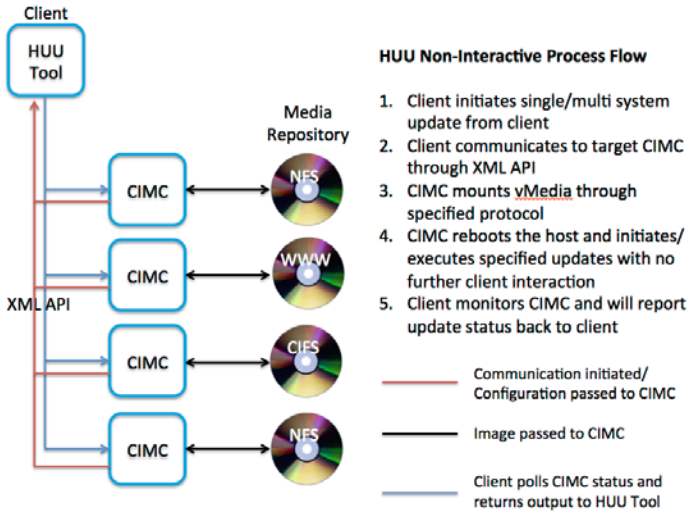
Enhancements to HUU include adding an interactive graphical user interface to HUU and adding non-interactive update capabilities for single-system and multiple-system updates for no touch upgrades of Cisco C-Series Server firmware. Updates can be applied using the bootable image in the HUU ISO which can be mounted via vMedia to boot host to HUU and triggered through the KVM using an interactive update interface.

The Host Update Utility (HUU) is a tool that helps users to update the various levels of firmware running on their system including:

- CIMC
- BIOS
- LAN on Motherboard (LOM)
- RAID Controllers
- PCI Adapters
- Cisco Virtual Interface Cards (VIC)

These components should be updated together using 'Update All', however the tool will accept user-defined update combinations as long as the CIMC is at the same or later release version than the BIOS.

The utilities discussed in this paper are run on the client system denoted in the graphic below. This client is used to pass configuration information to the CIMC for execution. The tools discussed in this paper will monitor the progress of the updates initiated and at the completion of the update activity will show a status output for each system in the interface where the tool is running. The graphic below outlines the connection, update, and reporting flow used by these tools.



Highlights for the Single System (Interactive) include:
- HUU Graphical Interface
- Display table of current/update firmware versions
- Update Verification

Highlights for the Python Tool:
- Single system or multi-system Non-Interactive update capabilities
- Supports NFS, CIFS, or WWW protocols
- Supports updating one, many or all <firmware> updates for target systems
- Supports updates of multiple platform types concurrently
- Supports for different version updates for each target system
- Supports upgrade/downgrade of <firmware>
- Support for the password encryption/masking for configuration files & logs

Note: The Host Update Utility requires that systems are taken offline to complete updates. All of the procedures discussed in the paper require that the systems are shut down (ie the host OS is shut down), and updates are applied while these systems are offline.

This paper has been broken into 3 sections with each section representing a different tool or update method as follows:

Section #1: Interactive Update User Interface (Single System)
The interactive single system update tool is packaged in the HUU ISO and is an evolution of the update utility that has been available in previous versions of CIMC.

This tool is ideal for customers that want to update a single system and understand both current and future code versions prior to executing the update.

Section #2: Non-Interactive Update (Single System) – Python Tool
This section will outline the steps required to update a single system using the Python tool. The tool can be downloaded from the Cisco C-Series Standalone Management page at the Cisco CDN site.

The python update tool has been designed for Linux/UNIX environments where administrators want support for single system or multi-system non-interactive updates of Cisco C-Series Standalone systems.

Section #3: Non-Interactive Update (Multi-System) – Python Tool:
This section will outline the steps required to update multiple systems using the Python tool using a save configuration file and encrypting passwords using this tool. The Python HUU Utility can be downloaded from the Cisco C-Series Standalone Management page at the Cisco CDN site.

The python update tool has been designed for Linux/UNIX environments where administrators want support for single system or multi-system non-interactive updates of Cisco C-Series Standalone systems.

Appendix #1: Updating a System CIMC from 1.4 to 1.5 to enable support for HUU Non-Interactive capabilities.
Because these features outlined in Sections #2-4 rely on a Cisco CIMC running version 1.5 to full leverage the tools discussed in this document, the appendix will walk users through the steps of updating CIMC code through the Cisco CIMC GUI to enable the HUU features discussed in the Sections #2-4.

Appendix #2: Determining appropriate update options for Python update tool (by system model)
This section will provide users the tools they need to determine the update modules applicable to the system(s) being updated.

The following sections of this paper include step-by-step illustrations, recommendations and requirements for using the Host Update Utility update interfaces.

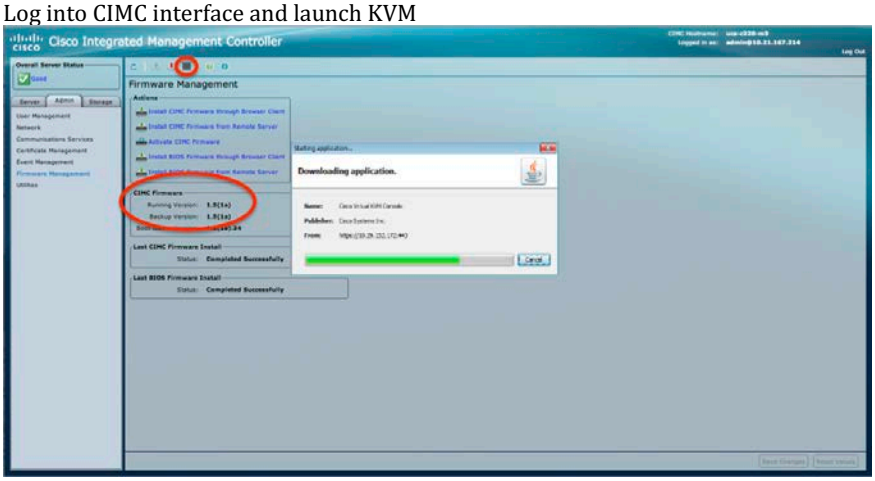
Please direct any comments or suggestions regarding this document to jeffoste@cisco.com.

Section #1:
Interactive Update User Interface (Single System)

The single system HUU update utility is packaged in update ISO and is an evolution of the update utility that has been available in previous versions of CIMC. This tool is ideal for customers that want to update a single system and understand both current and future code versions before executing the update.

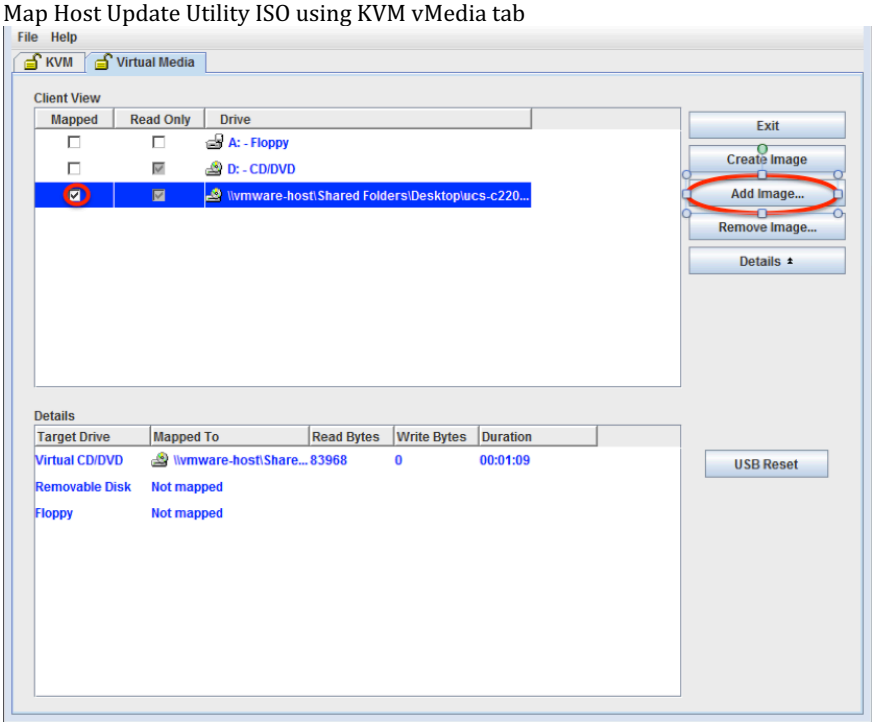
Steps for using this tool include:

Step 1:
Log into CIMC interface and launch KVM



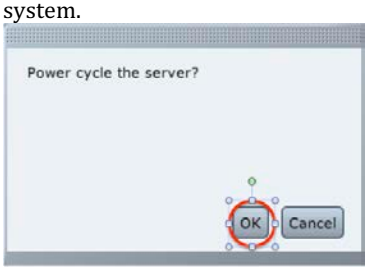
Note: The current CIMC version can be found on the login screen and on the 'Server → Summary' screen. A more detailed summary of firmware running on the system is available in the 'Admin → Firmware Management' menu.

Step 2:
Map Host Update Utility ISO using KVM vMedia tab

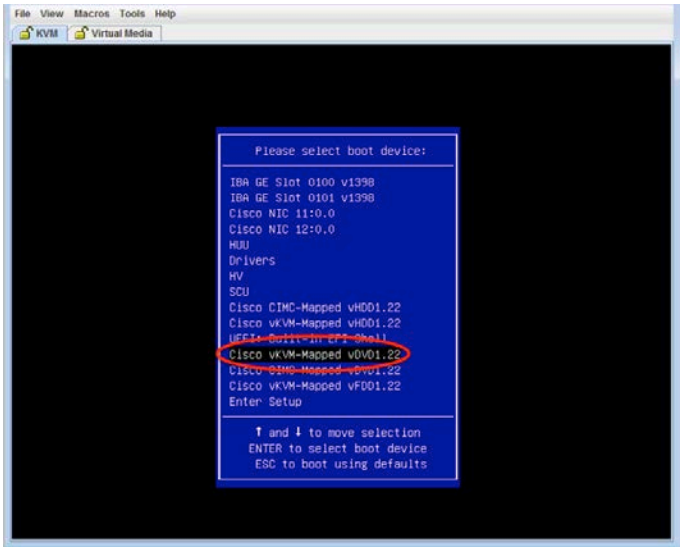


To map vMedia, click on 'Add Image' button, select the proper image and check the 'Mapped' checkbox as shown above.

Step 3:
Shutdown operating system and reboot system. Note this action will power cycle the system.



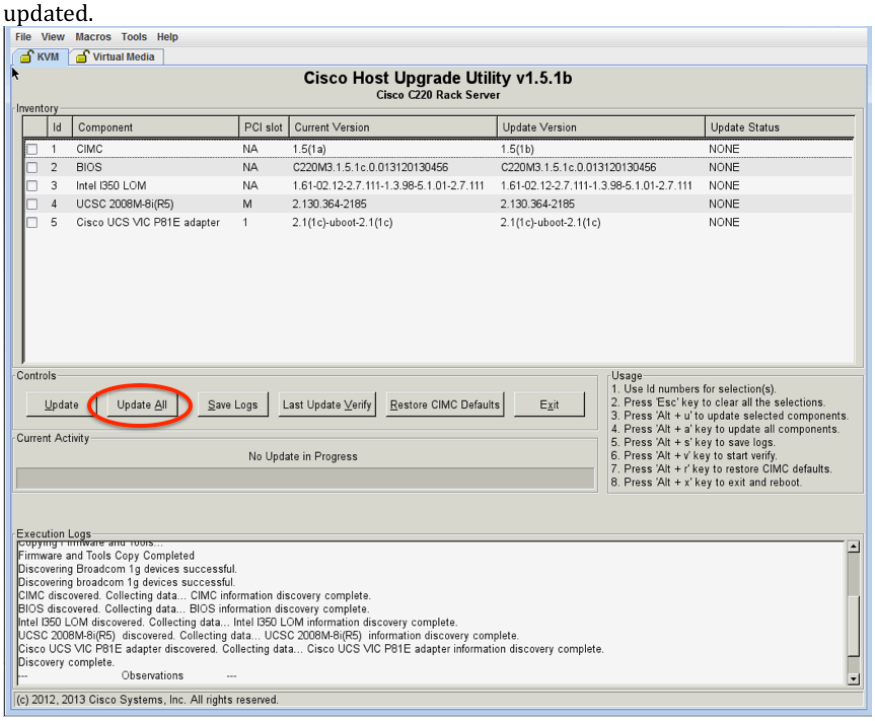
Step 4:
Enter BIOS boot menu (F6) and select appropriate boot source. In this scenario we will select 'Cisco vKVM-Mapped vDVD'



Step 5:
Accept the License Agreement

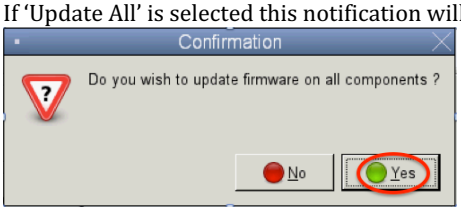
Accepting the license agreement will take you to the HUU Interactive menu system.

Step 6:
Select appropriate update options and select 'Update' or if 'Update All' is selected then none of the specific modules need to be checked since all modules will be updated.

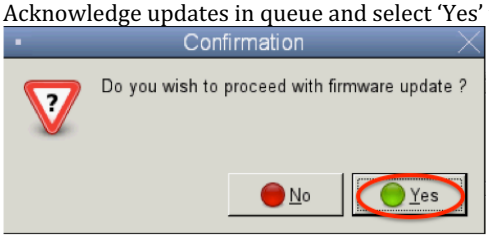


Note: The system will update components in the order listed with the exception of the BIOS. The BIOS will be the last component updated.

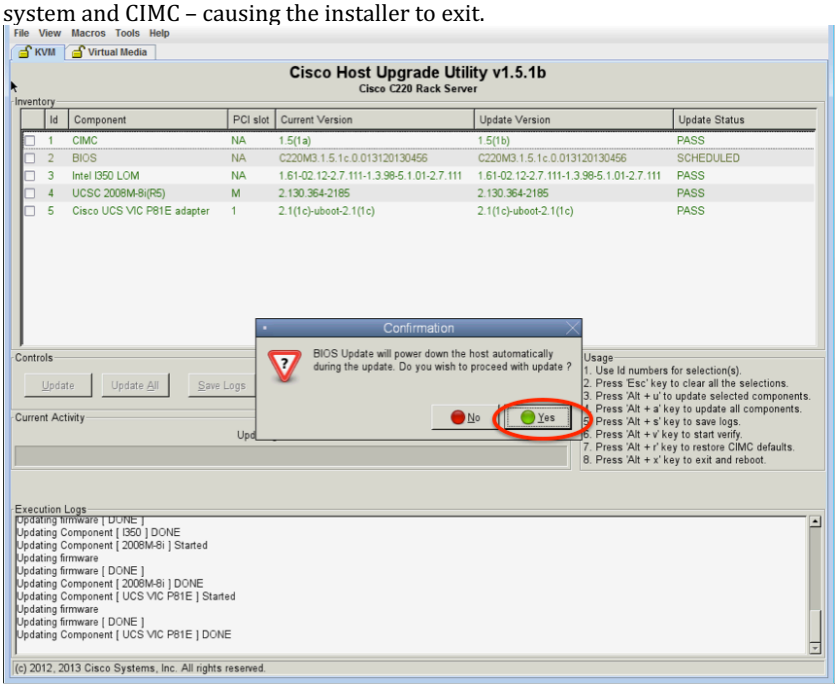
Step 7:
If 'Update All' is selected this notification will need to be acknowledged.



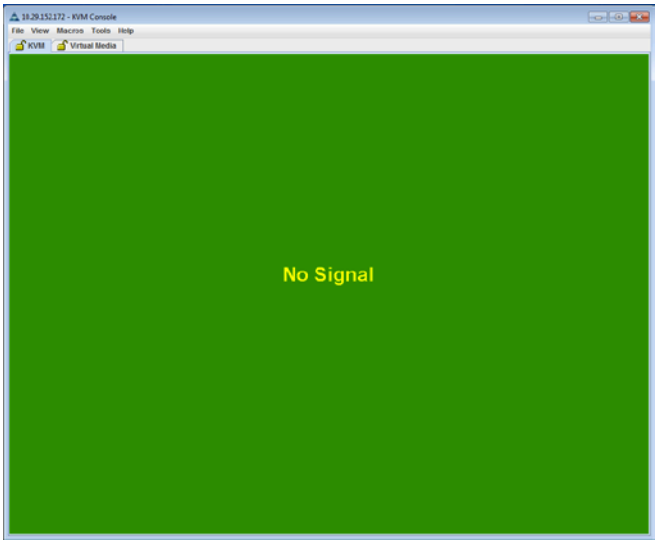
Step 8:
Acknowledge updates in queue and select 'Yes' to proceed.



Step 9:
Once all updates (except BIOS) are applied, the system will prompt user a finale time for acknowledgement of BIOS update and system reboot. Once this acknowledgement happens the tool will complete the BIOS update and reboot the system and CIMC – causing the installer to exit.

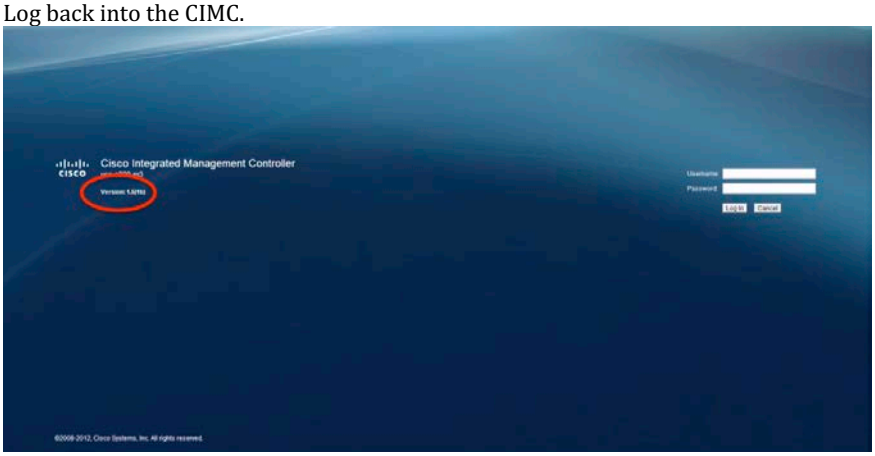


Note: The update status is provided for the modules as they are updated.



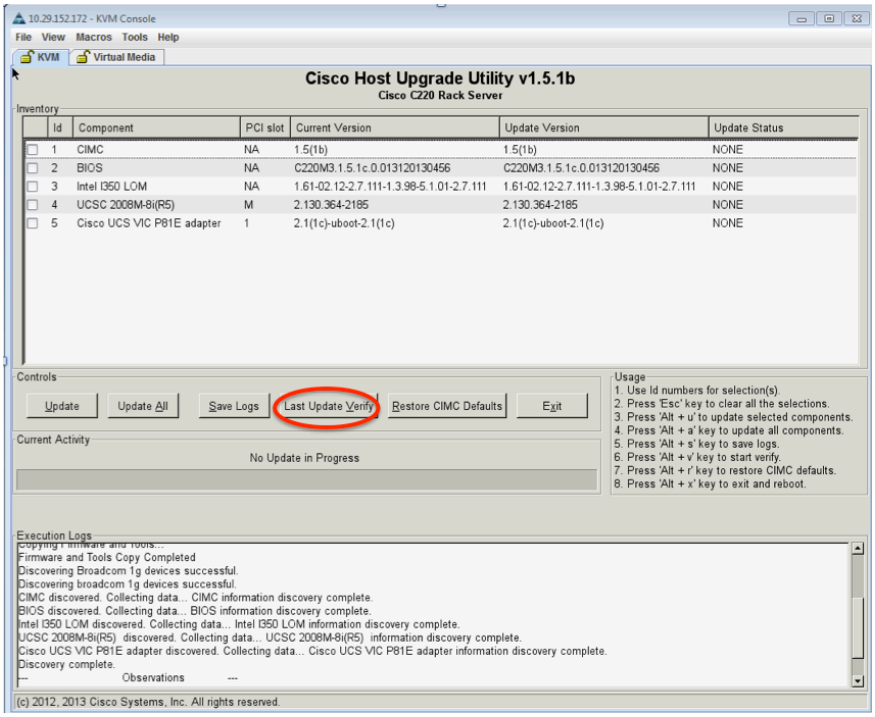
Note: The system will power-cycle and the CIMC will reboot on updated version of software. This will cause the KVM session to disconnect. This is normal.

Step 10:
Log back into the CIMC.

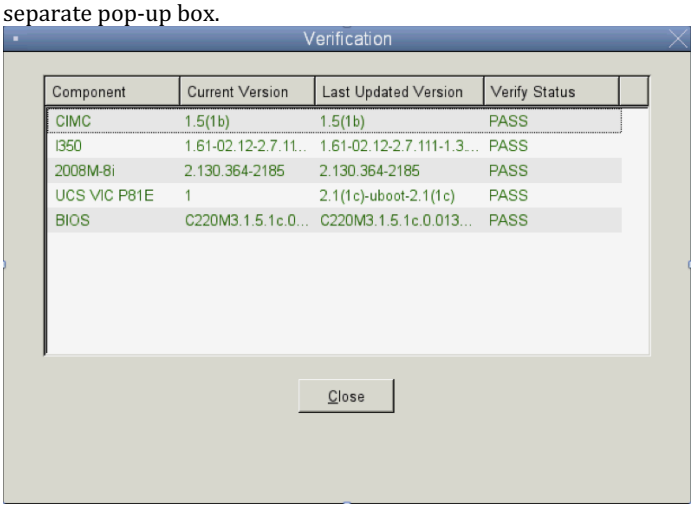


Note: Note that the CIMC is now reporting that it is running on the newly updated version.

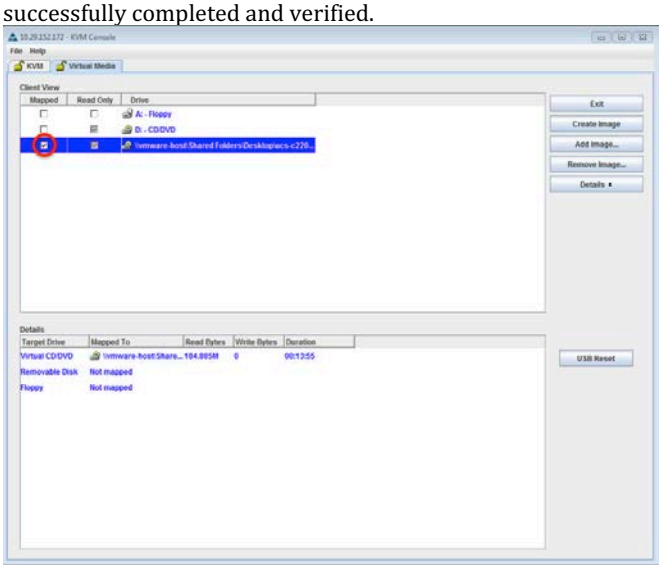
Step 11:
(Optional) To verify that all components were updated properly, please repeat Steps 1-5. In the HUU Utility, select the 'Last Update Verify' option. This will initiate a verification of the updates that were applied during steps 6-9 above.



Note: The verification process will complete and a status will be reported in a separate pop-up box.



Step 11a:
If the verification step was completed successfully, click on the 'Virtual Media' tab, uncheck the 'Mapped' image box, and remove image. This update has been successfully completed and verified.



Section #2
Non-Interactive Update (Single System) – Python Tool

There is a single Python tool that supports both single system and multi-system non-interactive updates. The system can be downloaded from the Cisco C-Series Standalone Management page at the Cisco CCO site.

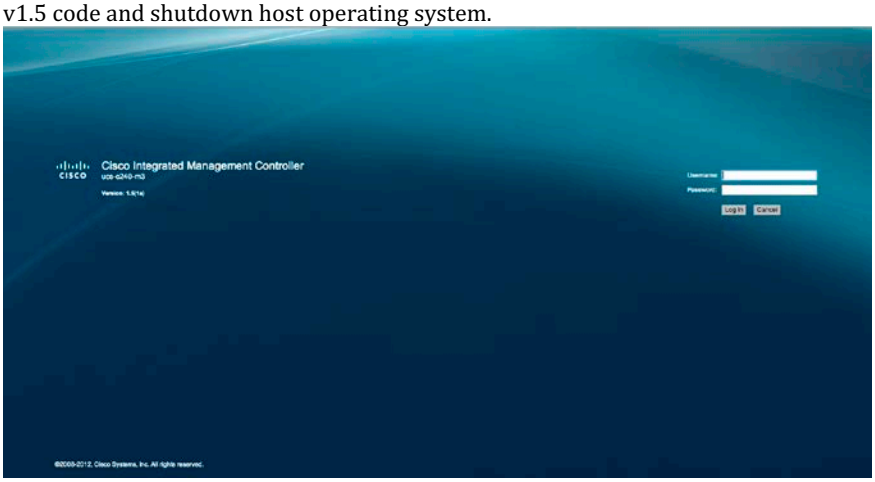
The Python update tool has been designed for Linux/UNIX environments where administrators want support for single system or multi-system non-interactive updates of Cisco C-Series Standalone systems.

This Python tool can be run from any system that meets the following criteria:
1. Minimum python version 2.6
2. Python-multiprocessing package installed
3. (Optional) Minimum pycrypto-2.6 installed
– Not applicable to single system update since credentials are entered in command string. This module is used to support the multi-system update capability where the CIMC and remote share passwords are encrypted in the configuration file and a key is required at the time the utility is run to decrypt passwords.

Step 1:
Download the update_firmware.py utility to the client system where the system update will be initiated. An overview of usage, including available flags and options can be printed with the –help option as shown below.

```
$ ./update_firmware.py -help
Usage: update_firmware.py [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit

  Single server options:
    This options to be used while upgrading a single server firmware

    -a a.b.c.d, --address=a.b.c.d
                        CIMC IP address
    -u USERNAME, --user=USERNAME
                        Username of the CIMC admin user
    -p PASSWORD, --password=PASSWORD
                        Password of the CIMC admin user
    -m ucs-c240-huu-146.iso, --imagefile=ucs-c240-huu-146.iso
                        HUU iso image file name
    -i a.b.c.d, --remoteshareip=a.b.c.d
                        IP address of the remote share
    -d /data/image, --sharedirectory=/data/image
                        Directory location of the image file in remote share
    -t cifs/nfs/www, --sharetype=cifs/nfs/www
                        Type of remote share
    -r REMOTESHAREUSER, --remoteshareuser=REMOTESHAREUSER
                        Remote share user name
    -w REMOTESHAREPASSWORD, --remotesharepassword=REMOTESHAREPASSWORD
                        Remote share user password
    -y COMPONENTLIST, --componentlist=COMPONENTLIST
                        Component List
    -f LOGFILE, --logrecordfile=LOGFILE
                        Log file name where log data will be saved

  Multiple server update options:
    This options to be used while upgrading multiple servers firmware

    -c CONFIGFILE, --configfile=CONFIGFILE
                        Name of the file with the list of CIMC IP address and
                        other data
    -l LOGFILE, --logfile=LOGFILE
                        Log file name where the log data will be saved
    -s USESECURE, --secure=USESECURE
                        Use HTTPS. Default is yes. Options yes/no
    -e INFILE, --encrypt=INFILE
                        Public key file.
    -g, --generatekey   Generate public and private keys
$
```

Step 2:
(Recommended) Verify the system to be updated is running a version of Cisco CIMC v1.5 code and shutdown host operating system.



Step 3:
Run update_firmware.py utility with appropriate flags/options.

Note: In the update below, the following command was provided:
./update_firmware.py -a 192.168.1.3 -u admin -p password -m ucs-c240-huu-1.5.1b.iso -i 192.168.1.2 -d /FW_Repos/ -t nfs -r Administrator -w password -y all

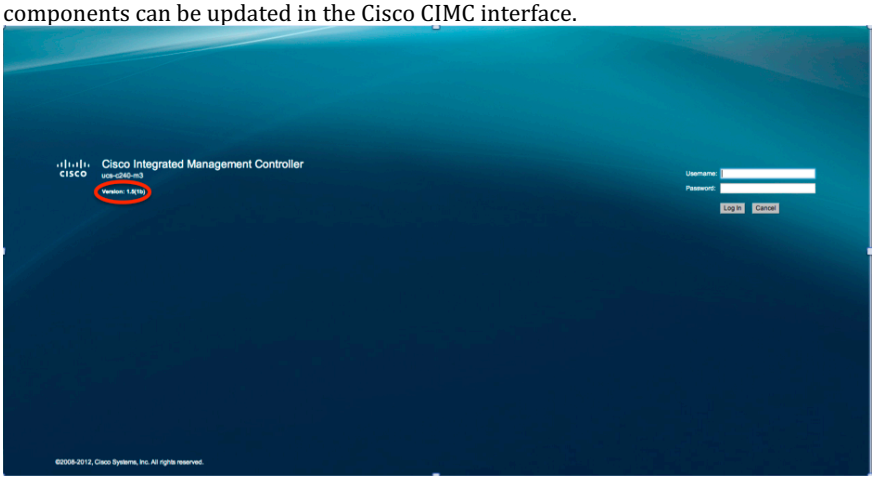
This command will update the target (192.168.1.3) using the authentication provided. It will mount the 1.5(1b) ISO via NFS and update all applicable modules.

This update process will provide no intermediate status updates on the console screen where the update was initiated, however if an administrator is interested in following along with the update, a KVM session can be opened to monitor the update process.

Step 4:
The tool reports back the status of the update. In this case we see that the firmware update completed successfully.

```
$ cd /Utilities/Python
$ ls
cimc.pass           multiserver_config.txt      update_firmware.py
keys.pem            password.key                update_huu.log
keys.pub            remshare.pass
$

$ ./update_firmware.py -a 192.168.1.3 -u admin -p password -m ucs-c240-huu-1.5.1b.iso -i 192.168.1.2 -d /ISO_Repos/ -t nfs  -r Administrator -w password -y

Total of 1 servers firmware to be updated.

Updating firmware.....


Update Summary:
---------------

Firmware update successful for CIMC - 192.168.1.3

$
```

Administrators can verify the CIMC has been updated on the login screen. Other components can be updated in the Cisco CIMC interface.



Section #3
Non-Interactive Update (Multi-System) – Python Tool:

There is a single Python tool that supports both single system and multi-system non-interactive updates. This tool can be downloaded from the Cisco C-Series Standalone Management page at the Cisco CCO site.

The python update tool has been designed for Linux/UNIX environments where administrators want support for single system or multi-system non-interactive updates of Cisco C-Series Standalone systems.

This Python tool can be run from any system that meets the following criteria:
1. Minimum python version 2.6
2. python-multiprocessing package installed
3. (Reccommended) Minimum pycrypto-2.6 installed

Step 1:
Download the update_firmware.py utility and the multiserver_config file to the client system where the system update will be initiated.

```
$ ./update_firmware.py -help
Usage: update_firmware.py [options]

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit

  Single server options:
    This options to be used while upgrading a single server firmware

    -a a.b.c.d, --address=a.b.c.d
                        CIMC IP address
    -u USERNAME, --user=USERNAME
                        Username of the CIMC admin user
    -p PASSWORD, --password=PASSWORD
                        Password of the CIMC admin user
    -m ucs-c240-huu-146.iso, --imagefile=ucs-c240-huu-146.iso
                        HUU iso image file name
    -i a.b.c.d, --remoteshareip=a.b.c.d
                        IP address of the remote share
    -d /data/image, --sharedirectory=/data/image
                        Directory location of the image file in remote share
    -t cifs/nfs/www, --sharetype=cifs/nfs/www
                        Type of remote share
    -r REMOTESHAREUSER, --remoteshareuser=REMOTESHAREUSER
                        Remote share user name
    -w REMOTESHAREPASSWORD, --remotesharepassword=REMOTESHAREPASSWORD
                        Remote share user password
    -y COMPONENTLIST, --componentlist=COMPONENTLIST
                        Component List
    -f LOGFILE, --logrecordfile=LOGFILE
                        Log file name where log data will be saved

  Multiple server update options:
    This options to be used while upgrading multiple servers firmware

    -c CONFIGFILE, --configfile=CONFIGFILE
                        Name of the file with the list of CIMC IP address and
                        other data
    -l LOGFILE, --logfile=LOGFILE
                        Log file name where the log data will be saved
    -s USESECURE, --secure=USESECURE
                        Use HTTPS. Default is yes. Options yes/no
    -e INFILE, --encrypt=INFILE
                        Public key file.
    -g, --generatekey   Generate public and private keys
$
$
$
```

Step 2:
Edit the multiserver_config file as appropriate.

```
# Use this flag use_http_secure to toggle between https and http protocol
use_http_secure=yes
# Firmware update should complete within this many minutes. This value will be
# sent along with the firmware update XML request to the CIMC
update_timeout=60
# Should the firmware update process stop the update once an error is encountered?
update_stop_on_error=no
# Is it required to verify the update by rebooting to the same HUU image after the update
# gets completed?
update_verify=no
# List of components to be updated. Check the HUU release note for the list of
# supported components. Multiple components should be comma separated.
#update_component=9266-8i
#update_component=9266-8i, BIOS, CIMC, I350
update_component=all

# IP address of the remoted share (cifs/nfs/www) holding the HUU image for booting
remoteshareip=192.168.1.2
# Directory within the share where the HUU image is being kept
sharedirectory=/ISOS/HUU/
# Type of share (nfs/cifs/www)
sharetype=nfs
# Username of the remote share to login to
remoteshareuser=Administrator
# Password corresponding to the remote user
#remotesharepassword=

# Password file for remoteshare. If this option is provided, then the above option (remotesharepassword) should not be giver
remoteshare_passwordfile=/Users/user1/Documents/C-Series/Management/Python/remshare.pass

#Common CIMC password --> The password provided below along with CIMC information will be ignored.
#cimc_password_file=/Users/user1/Documents/C-Series/Management/Python/cimc.pass


# Enter the list of CIMC ip addresses where the firmware needs to be updated
address=192.168.1.3, user=admin, password=, imagefile=ucs-c460-huu-1.5.1a.iso
address=192.168.1.4, user=admin, password=, imagefile=ucs-c220-huu-1.5.1a.iso
address=192.168.1.5, user=admin, password=, imagefile=ucs-c220-huu-1.5.1a.iso
address=192.168.1.6, user=admin, password=, imagefile=ucs-c240-huu-1.5.1a.iso
address=192.168.1.7, user=admin, password=, imagefile=ucs-c260-huu-1.5.1b.iso
address=192.168.1.8, user=admin, password=, imagefile=ucs-c420-huu-1.5.1b.iso
address=192.168.1.9, user=admin, password=, imagefile=ucs-c22-huu-1.5.1b.iso
address=192.168.1.10, user=admin, password=, imagefile=ucs-c24-huu-1.5.1b.iso
```

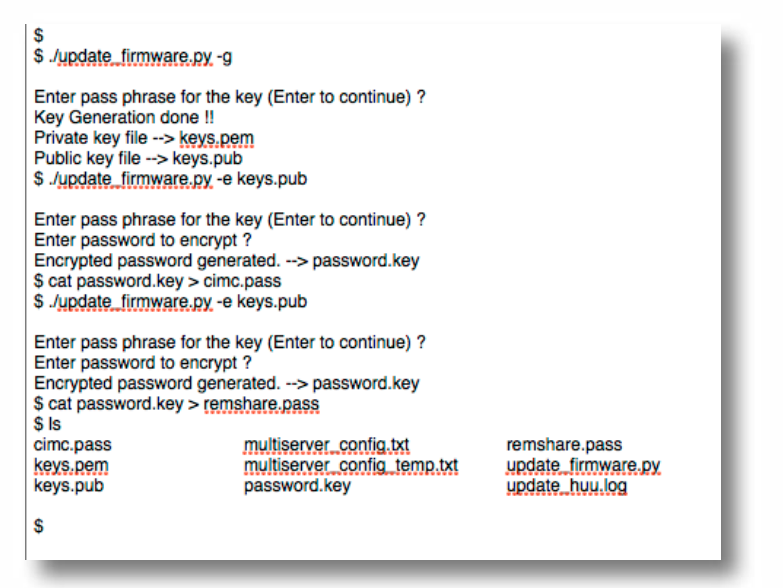
Note: A number of configuration options are available including:
use_http_secure=yes
update_timeout=60
update_stop_on_error=no
update_verify=no
update_component=<List components or 'all'>
remoteshareip=<IP Share>
sharedirectory= <loction of update>
sharetype= <nfs, cifs, or www>
remoteshareuser=<username>
remotesharepassword=<password> Populate only when not encrypting passwords

Optional options listed below if encrypting passwords with pycrypto:
Use either remotesharepassword OR remoteshare_passwordfile (Not Both)
Use either CIMC passwords (below) or a common encrypted password file (Not both)

#remoteshare_passwordfile=/<file structure>/remshare.pass
#cimc_password_file=/<file structure>/cimc.pass

Systems should be entered as follows: (one system per line)
# Enter the list of CIMC ip addresses where the firmware needs to be updated
address=<IP>, user=<admin>, password=<password> (or blank if 'cimc_password_file' is specified above), imagefile=<file.iso>

Step #3: (Optional)
If encryption for the CIMC and/or remote share passwords is desired, complete this step. Enter the following at the system console of the platform where the updates will be initiated:



1. Type './update_firmware.py –g' from the directory where the file resides
This will create two files: keys.pem and keys.pub.
Enter: Encryption passphrase (remember this!)

2. Type './update_firmware.py -e keys.pub'
Enter: Encryption passphrase (from above) and also string to be encrypted

This will create a file called password.key.

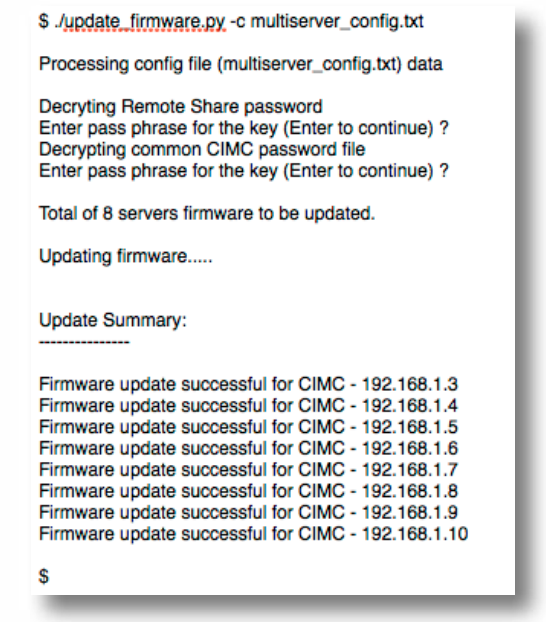
3. Change the name of the password.key file (or dump contents) to a file specified in the multiserver_config file. We have used the default naming convention cimc.pass.

4. Repeat these steps for the remoteshare_passwordfile.

Step 4:
Check to ensure all required/optional files are available. In this example I will be using the following files:

- update_firmware.py
- multiserver_config
- cimc.pass (optional)
- remshare.pass (optional)

Step 5:
Initiate the update using the –c flag and providing a pointer to the proper configuration file.



Note: Status for each system update will be reported in the console of the system initiating the update. The update progress can be monitored by opening a KVM session on these target systems.

FAQ Concerning the Host Update Utility:

1. What is the minimum version CIMC required to run these tools?
A. The Python Non-Interactive utilities require the system is running Cisco CIMC version 1.5 at a minimum. The interactive GUI utility can be used to update a system to version 1.5 and this update can be made directly from version 1.3.X or 1.4.X

2. Which tools store my passwords?
A. The multi-system non-interactive tool require that passwords be provided at the time that the updates are initiated. Customers have the option of which fields they want to save to this file where a file can be saved without any passwords specified (so they can be entered at the time the tool is run). The Python multi-system update tool can encrypt passwords for the remote share and for the Cisco CIMC provided that all target CIMC passwords. This encryption requires that the pycrypto 2.6 module is installed.

The single-system interactive tool does not require any further authentication once the admin logs into the Cisco CIMC. The single system non-interactive tool does require that passwords be passed in the command at the time that it is executed and those passwords are removed from the log files.

3. Do I need to encrypt my passwords?
A. Encryption of passwords are available with the python tool if the pycrypto 2.6 module is installed on the system where the updates are being initiated.

4. What are the client prerequisites to run these tools?
Requirements for these tools is as follows:
Targets – A minimum of Cisco CIMC version 1.5 on targets for all non-interactive updates
Hosts – A host used to initiate an update must have the proper utility loaded. These can be downloaded from the Cisco C-Series Standalone CCO page.
Python Update Tool: Python tool requires the following two files for usage python 2.6 and python-multiprocessing package
Python Update Tool: Python tool requires the following one package for encryption pycrypto-2.6

Note: The client used to initiate these updates should have sufficient CPU cores to handle multi-threading associated with number of targets being updated simultaneously.

5. Is there any way to verify the remote share configuration?
A. Users can map the ISO through the CIMC scriptable vMedia interface (CIMC CLI) on one server, verify boot into HUU and ensure that there are no issues in the environment.

6. Is there anything that should be done on the host to prepare for an update?
A. Complete an ordered shutdown of the host OS before doing this update. The CIMC will trigger a host reboot when update is started, but it is safer to do a shutdown prior to initiating the update from one of the utilities listed above. . After update is complete the CIMC will take care of booting up the host to the previously configured boot order.

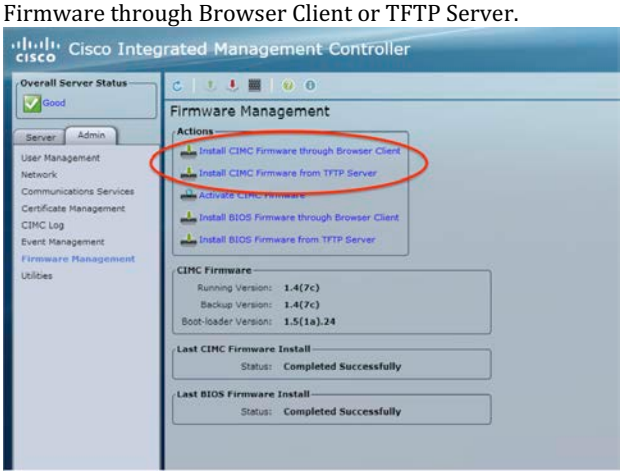
Appendix #1: Updating a System CIMC from 1.4 to 1.5 to enable support for HUU Non-Interactive capabilities.

Comment [JF1]: Check with Tony V. to see if this is a generally supported or if we should use this mechanism on a case by case basis.

The new features and update procedures outlined in Sections #2-4 require a system running CIMC 1.5. This document will walk users through the steps of updating only a systems CIMC code through the CIMC GUI to enable the HUU Non-Interactive features discussed in the companion file.

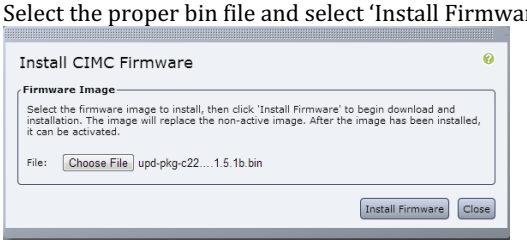
Please note that these steps must be followed closely and these instructions are intended to put the system in a state that will support the Non-Interactive HUU Utilities. Do not attempt to update platform BIOS in a similar fashion as BIOS updates require that CIMC updates are applied either prior to or with these updates.

In our example, we will start with a C220 M3 running 1.4.7a.1.
Step 1: Navigate to 'Admin → Firmware Management' and select install CIMC Firmware through Browser Client or TFTP Server.

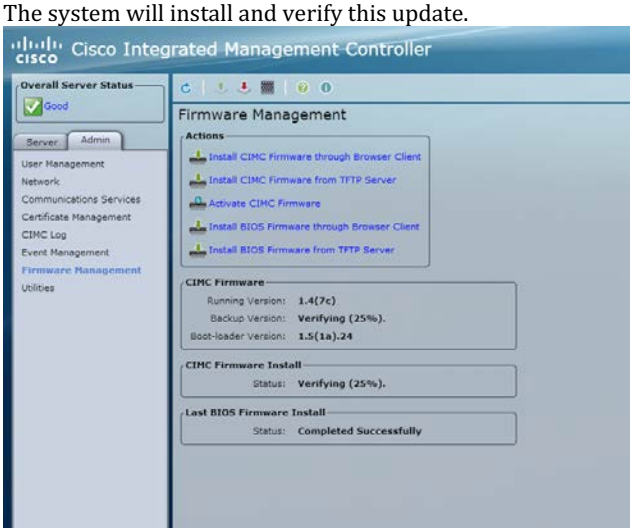


Note: The CIMC bin file can be found on the HUU Update ISO in the CXX0-MX-1.5.1b.zip file → 1.5.1b Folder → cimc → CXX0-MX-cimc-1.5.1b.zip file. In this case, we have selected the upd-pkg-c220-m3-cimc.1.5.1b.bin file.

Step 2:
Select the proper bin file and select ‘Install Firmware’

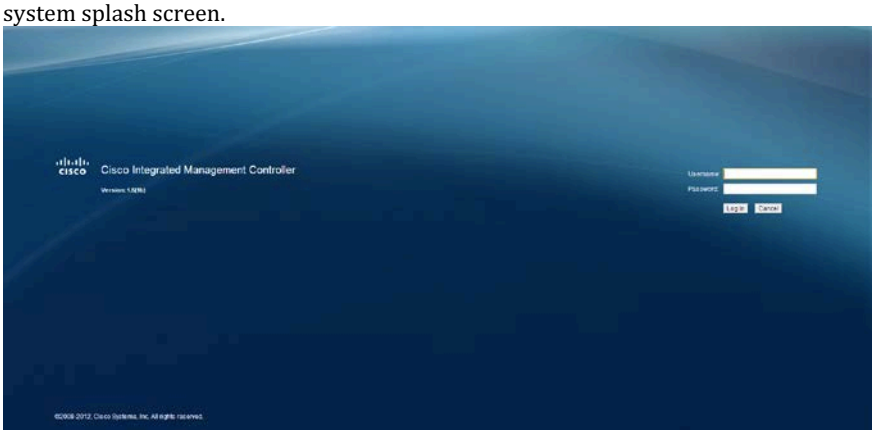


The system will install and verify this update.



Step 3:
Activate the newly installed (v1.5.1b) version of firmware. Note this will reboot the CIMC.

Upon reboot the system should reflect the newly activated CIMC version in the system splash screen.



At this point the system can be updated using the HUU Utilities discussed in the companion papers that can be downloaded from the C-Series Standalone page on the Cisco Developer Network.

Appendix #2: Identifying the relevant update modules for update using Python tool.

Venkata – Please help with this. I was hoping to provide users two options for identifying the modules to be updated using the Python tool:

1. Querying the XML API (I could not find a decoder ring in a single place in the API) – does such a query exist with output that can be reasonably interpreted?
2. Do we have a static list of the standard/optional components for each system that we could embed in this appendix?