Manage UCS C-Series M3 and M4 Servers that Do Not Support HTML5 After Flash Deprecation

Contents

[Introduction](#)
[Requirements](#)
[Components Used](#)
[Background Information](#)
[Problem](#)
[Solutions](#)
[Direct Link to Launch the vKVM while the CIMC is Inaccessible](#)
[Use XML API to Launch vKVM](#)
[Update the CIMC from the Command Line](#)
[Related Information](#)

Introduction

This document describes the different procedures to access and upgrade the Cisco Integrated Management Console (CIMC) or Virtual Keyboard Video Mouse (vKVM) with the firmware that does not support HTML5. Post-Flash Deprecation.

Requirements

Cisco recommends that you have knowledge of these topics.

- CIMC
- vKVM
- Cisco UCS C Series Rack Server

Components Used

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

However, the information in this document is based on these software and hardware versions for demonstration only.

- UCSC-C220-M4S
- CIMC Version 2.0(13g) and 3.0(3f)

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

By Adobe's End-of-Life announcement, Adobe plans to deprecate Flash-based content and software after 2020-12-31.

Problem

The Web User Interface (WebUI) of Cisco Integrated Management Controller (IMC) software releases which are Java-based might not function after the deprecation of Adobe Flash on 2020-12-31. Field Notice: FN - 72014

> **Note**: For M3 Platform Server's HTML5-based Web UI interface for Cisco IMC is not available on any software releases. Refer to the Cisco bug ID CSCvs11682.

> **Note**: UCS M4 C-Series servers do have an HTML5-based WebUI with Cisco IMC 3.0(x), hence the M4 servers are not impacted. However, any 2.(x) or lesser server firmware is affected for all UCS C series M3/M4 servers.

Solutions

Methods to access CIMC for M3 for M4 Platform Servers.

One can access the CIMC if they still have the older versions of the browser or any third-party browser which still supports the flash in it.

However, due to multiple security factors, Cisco does not recommend this method.

Direct Link to Launch the vKVM while the CIMC is Inaccessible

- Please ensure that you have a compatible Java version installed on your computer or VM.
- If the CIMC version is 2.x or 1.x then you need to downgrade the java version to the java7 u21 or Java7 u56 version if it fails with the current java version.
- Users must allow the CIMC's IP to launch the vKVM in the Java's settings.

Link's Format:

```
https://x.x.x.x/kvm.jnlp?cimcAddr= x.x.x.x &tkn1=admin&tkn2=password
```

1. Replace <x.x.x.x> with the CIMC IP in both locations of the link (this is used twice in the link).

2. Replace <CIMC Username with the CIMC username (usually admin) change only it is other than admin.

3. Replace <password> with the current CIMC password.

Example:

```
https://172.16.10.20/kvm.jnlp?cimcAddr=172.16.10.20&tkn1=admin&tkn2=cisco@123
```

Paste the formatted link with specific info into a browser **Save/Keep** the JNLP file and open it up **Accept/Continue/Yes** to all the pop-ups, once the KVM is launched then please run an HUU or upgrade the OS version with the ISO.

Use XML API to Launch vKVM

It is recommended that PowerShell and Java be installed on the workstation.

Modify the **$cimcIP/$cimcUsername/$cimcPassword** variables and paste the script into the PowerShell CLI to launch the KVM via XML API:

#Powershell Script to Launch Java KVM on Cisco IMC:

```
$cimcIP = "XX.XX.XX.XX"
$cimcUsername = "admin"
$cimcPassword = "password"
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Auth = @{uri = "https://$cimcIP/nuova";
                  Method = 'POST';
                                    Body = "<aaaLogin inName='$cimcUsername'
inPassword='$cimcPassword'></aaaLogin>";
                                }
[xml]$AuthXML = Invoke-WebRequest @Auth -UseBasicParsing $AuthCookie =
$AuthXML.aaaLogin.outCookie $GetComputeAuthTokens = @{uri = "https://$cimcIP/nuova";
                  Method = 'POST';
                                    Body = "<aaaGetComputeAuthTokens cookie='$AuthCookie'/>";
                                }
[xml]$GetComputeAuthTokensXML = Invoke-WebRequest @GetComputeAuthTokens -UseBasicParsing
$Token = $GetComputeAuthTokensXML.aaaGetComputeAuthTokens.outTokens -replace ",", "&tkn2="
$KVMurl = "https://$cimcIP/kvm.jnlp?cimcAddr=$cimcIP&cimcName=KVM&tkn1=$Token"
javaws "https://$cimcIP/kvm.jnlp?cimcAddr=$cimcIP&cimcName=KVM&tkn1=$Token"
```

The full IMC API can be found here: Cisco IMC XML API Programmer's Guide.

Update the CIMC from the Command Line

You can upgrade the CIMC firmware with the CLI (for M4s only).

Then, you can launch vKVM and run the HUU as normal.

Step 1. Use the CLI Configuration Guide found at the embedded link and check Step 11. of the section **Obtaining Firmware from Cisco** for steps to extract the file.

Step 2. Add the **CIMC.BIN** into the **tftp/SCP/FTP** server on your system.

Step 3. SSH to the server with the IP address of the CIMC. Then run the shared commands:

```
C-Series-III# scope cimc
C-Series-III /cimc# scope firmware
C-Series-III /cimc/firmware# update tftp172.16.10.29 /cimc.bin

Format :- update protocol IP /Path/Filename
```

Step 4. Then verify the upgrade status by the command **#Show detail**.

```
C-Series-III /cimc/firmware # show detail

Firmware Image Information:
Update Stage: DOWNLOAD  <<<<<<<<<<<<<<===============
Update Progress: 5              <<<<<<<<<<<<<===============
Current FW Version: 2.0(13n)<<<<<<<<<<<<<===============
FW Image 1 Version: 4.0(2h) <<<<<<<<<<<<<===============
FW Image 1 State: BACKUP INACTIVATED
FW Image 2 Version: 2.0(13n)
FW Image 2 State: RUNNING ACTIVATED
Boot-loader Version: 2.0(13n).36
Secure Boot: ENABLED
```

Step 5. Run the **#show detail** command again once the download is completed.

```
C-Series-III /cimc/firmware # show detail
Firmware Image Information:
Update Stage: NONE             <<<<<<<<<<<<<===============
Update Progress: 100           <<<<<<<<<<<<<===============
Current FW Version: 2.0(13n)<<<<<<<<<<<<<===============
FW Image 1 Version: 3.0(3f)  <<<<<<<<<<<<<=============== (This is the new image which is added
by the TFTP server)
FW Image 1 State: BACKUP INACTIVATED
FW Image 2 Version: 2.0(13n)
FW Image 2 State: RUNNING ACTIVATED
Boot-loader Version: 2.0(13n).36
Secure Boot: ENABLED
```

Step 6. Then type **activate**.

```
C-Series-III /cimc/firmware # activate
This operation activates firmware 2 and reboot the BMC.
Continue?[y|N] Y
```

Step 7. Now, the server is expected to reboot, and the connectivity is restored in 5 minutes. You will be able to verify the upgrade with the same command:

```
C-Series-III /cimc/firmware # show detail
Firmware Image Information:
Update Stage: NONE
Update Progress: 100
Current FW Version: 3.0(3f)  <<<<<<<<<<<<<=============== (Firmware got update from 2.0(13n) to
3.0(3f).
FW Image 1 Version: 3.0(3f)
FW Image 1 State: RUNNING ACTIVATED
FW Image 2 Version: 2.0(13n)
FW Image 2 State: BACKUP INACTIVATED
Boot-loader Version: 3.0(3f).36
Secure Boot: ENABLED
C-Series-III /cimc/firmware #
```

Step 8. You can log in to CIMC and Launch the vKVM and then update the firmware with the Host upgrade utility.

> **Tip**: This is not necessary to update the BIOS from CLI to achieve the CIMC upgrade for M4 Servers. But once CIMC is updated and accessible from the browser. Please ensure to run the HUU and update all the components.

For more details, please refer to the Cisco IMC Firmware Management guide: CLI Configuration Guide.

Related Information

- **FN - 72012 - Specific Releases of UCS Manager Affected by Adobe Flash End-of-Life - Software**
- **FN - 72014 - (Cisco IMC) for UCS M3 Rack Servers Affected by Adobe Flash End-of-Life**
- **Technical Support & Documentation - Cisco Systems**