UCS STP005 Firmware Component Activation

When a new release of UCS code is released you need to do a few things in sequence, and add these all together you get something called "UCS Upgrade Standard Operating Procedure".

STP001	Notification of Release
STP002	Research and Plan the Release
STP003	Download the Release
STP004	Firmware Core Activation
STP005	Firmware Component Activation
STP006	Backup the Release

Table 1 - List of Standard Technical Procedures in the UCS Upgrade Standard Operating Procedure"

This document describes how to execute STP005 Firmware Component Activation, which will result in your blade components (BMC, adapters and BIOS) being updated to a new release.

Contents

- **Location** – This document is on the web at https://supportforums.cisco.com/docs/DOC-8614
- **Prerequisites** - Before starting this procedure you should have completed steps 1-4 of the "UCS Upgrade Standard Operating Procedure" and have upgraded the core.
- **Author** – Steve Chambers, Unified Computing, Cisco Advanced Services, Europe.
- **Advanced Services** – Do it right, first time, every time, with Cisco.

Act 1: Plan the update

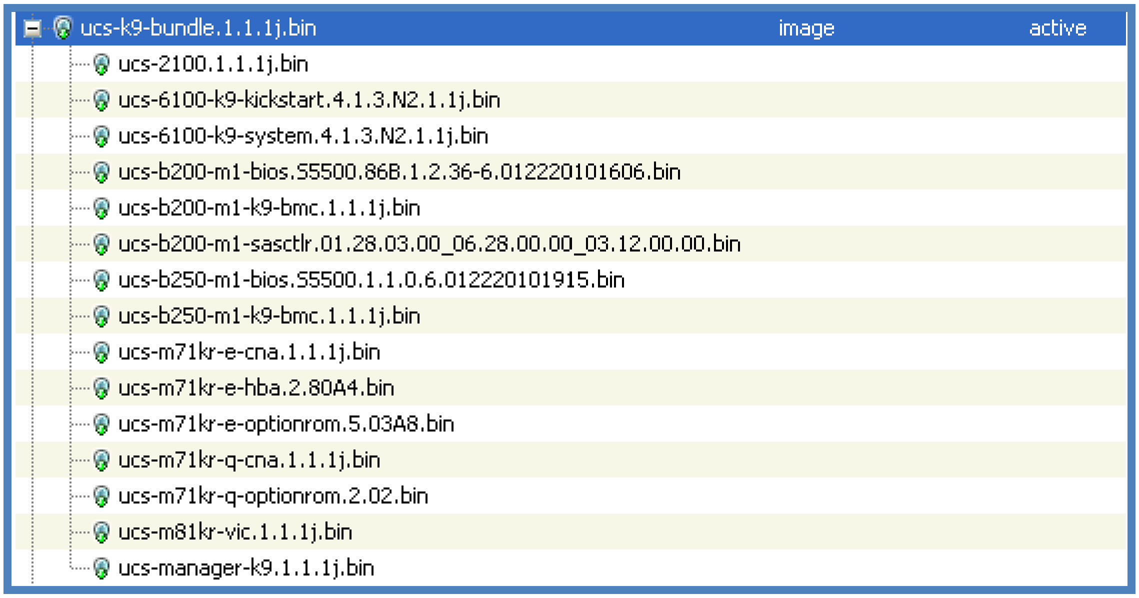
Summary: Work out what will be updated and how before you start.

A UCS blade has four major components – BMC, Adapter, BIOS and Disk controller.

Example ID	Component	Direct Update?	Policy that Updates	Description
BMC Controller	Baseboard Management Controller (BMC)	Yes	Management Firmware Policy	The IOM connects to the BMC.
N20-AQ0002	Converged Network Adapter (CNA)	Yes	Host Firmware Policy	This provides the VNIC and VHBA devices.
N20-AE0002	Host HBA (Emulex)	No	Host Firmware Policy	Emulex HBA
N20-AE0002	Host HBA Option ROM (Emulex)	No	Host Firmware Policy	Emulex HBA
N20-B6620-1	Server BIOS	No	Host Firmware Policy	Blade BIOS
LSI Logic	Internal Disk RAID Controller	No	Host Firmware Policy	Internel Disk Management

Table 2 - The updateable components in a blade

Which components need to be upgraded in this release? To find that out, you need to explore the Package from the Equipment → Installed Firmware screen.



```
ucs-k9-bundle.1.1.1j.bin                                   image          active
    ucs-2100.1.1.1j.bin
    ucs-6100-k9-kickstart.4.1.3.N2.1.1j.bin
    ucs-6100-k9-system.4.1.3.N2.1.1j.bin
    ucs-b200-m1-bios.S5500.86B.1.2.36-6.012220101606.bin
    ucs-b200-m1-k9-bmc.1.1.1j.bin
    ucs-b200-m1-sasctlr.01.28.03.00_06.28.00.00_03.12.00.00.bin
    ucs-b250-m1-bios.S5500.1.1.0.6.012220101915.bin
    ucs-b250-m1-k9-bmc.1.1.1j.bin
    ucs-m71kr-e-cna.1.1.1j.bin
    ucs-m71kr-e-hba.2.80A4.bin
    ucs-m71kr-e-optionrom.5.03A8.bin
    ucs-m71kr-q-cna.1.1.1j.bin
    ucs-m71kr-q-optionrom.2.02.bin
    ucs-m81kr-vic.1.1.1j.bin
    ucs-manager-k9.1.1.1j.bin
```

Figure 1 - Listing the Image files of a Package

The Image files in the Package map as follows:

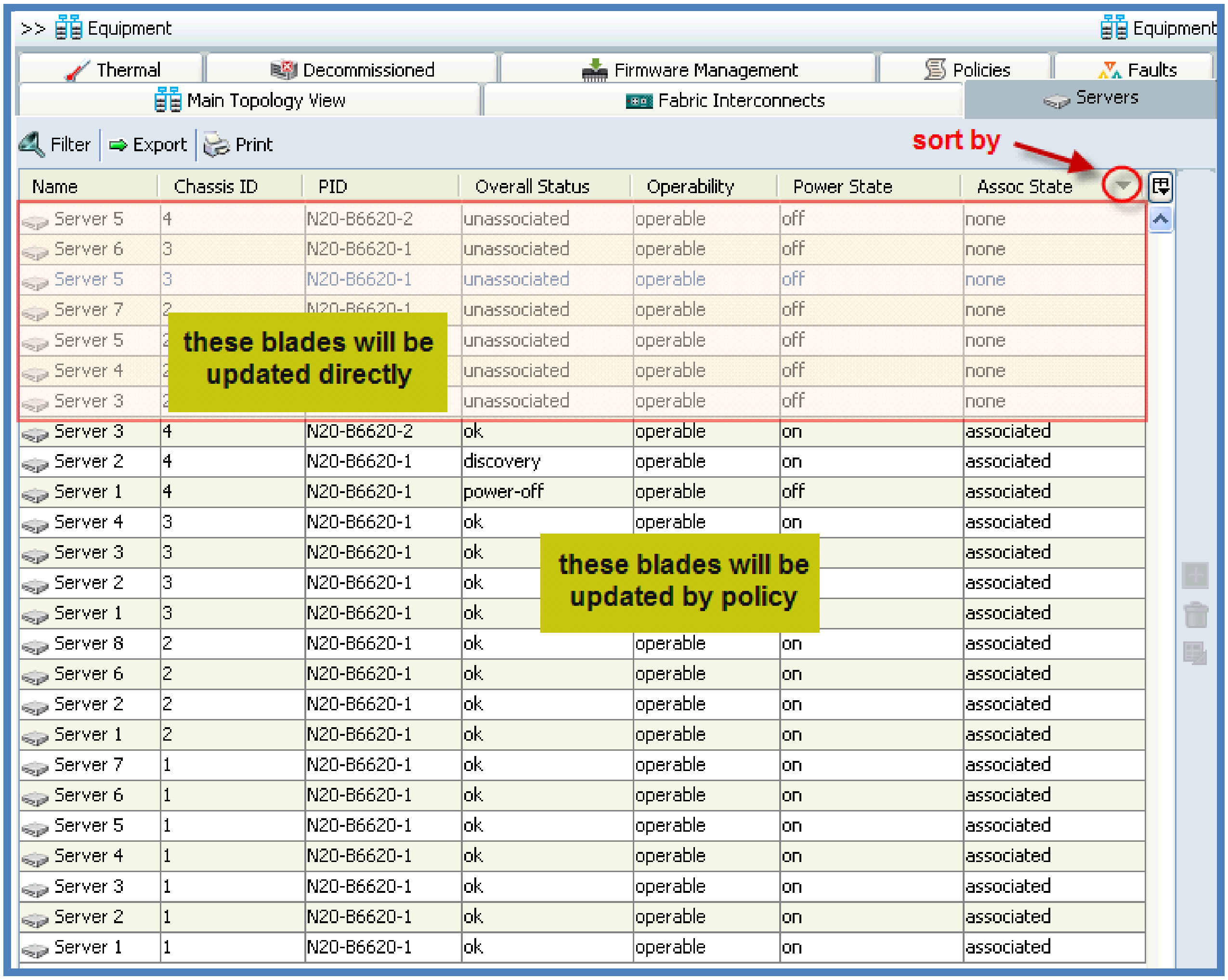
Image Filename	Component
ucs-2100	IOM
ucs-6100-k9-kickstart	Fabric Interconnect
ucs-6100-k9-system	Fabric Interconnect
ucs-b200-m1-bios	B200 BIOS
ucs-b200-m1-k9-bmc	B200 BMC
ucs-b200-m1-sasctlr	B200 RAID
ucs-b250-m1-bios	B250 BIOS
ucs-b250-m1-k9-bmc	B250 BMC
ucs-m71kr-e-cna	Emulex CNA
ucs-m71kr-e-hba	Emulex HBA
ucs-m71kr-e-optionrom	Emulex HBA ROM
ucs-m71kr-q-cna	QLogic CNA
ucs-m71kr-q-optionrom	QLogic CNA ROM
ucs-m81kr-vic	Cisco CAN
ucs-manager-k9	UCS Manager

Table 3 - Mapping Image filenames to components

The BMC and Adapter can be update either directly via the Installed Firmware screen, or via a policy. In practice, both methods are used for maximum efficiency. Direct update is immediately disruptive to a blade and is applied to stand-by/unused blades. You can update the BMC and Adapter via a Service Profile association for more operational control.

The HBA, BIOS and Disk components can only be updated via Policy.

So, the first step is to identify which blades will be updated by Direct or Policy methods. To do this, list the servers, sort by Association and choose unassociated servers as candidates for Direct updates, the rest will use a Policy.



Name	Chassis ID	PID	Overall Status	Operability	Power State	Assoc State
Server 5	4	N20-B6620-2	unassociated	operable	off	none
Server 6	3	N20-B6620-1	unassociated	operable	off	none
Server 5	3	N20-B6620-1	unassociated	operable	off	none
Server 7	2	N20-B6620-1	unassociated	operable	off	none
Server 5	2		unassociated	operable	off	none
Server 4	2		unassociated	operable	off	none
Server 3	2		unassociated	operable	off	none
Server 3	4	N20-B6620-2	ok	operable	on	associated
Server 2	4	N20-B6620-1	discovery	operable	on	associated
Server 1	4	N20-B6620-1	power-off	operable	off	associated
Server 4	3	N20-B6620-1	ok	operable	on	associated
Server 3	3	N20-B6620-1	ok			associated
Server 2	3	N20-B6620-1	ok			associated
Server 1	3	N20-B6620-1	ok			associated
Server 8	2	N20-B6620-1	ok	operable	on	associated
Server 6	2	N20-B6620-1	ok	operable	on	associated
Server 2	2	N20-B6620-1	ok	operable	on	associated
Server 1	2	N20-B6620-1	ok	operable	on	associated
Server 7	1	N20-B6620-1	ok	operable	on	associated
Server 6	1	N20-B6620-1	ok	operable	on	associated
Server 5	1	N20-B6620-1	ok	operable	on	associated
Server 4	1	N20-B6620-1	ok	operable	on	associated
Server 3	1	N20-B6620-1	ok	operable	on	associated
Server 2	1	N20-B6620-1	ok	operable	on	associated
Server 1	1	N20-B6620-1	ok	operable	on	associated

these blades will be updated directly

these blades will be updated by policy

Figure 2 - Dividing the blades by association to decide what is updated directly or by policy

Act 2: Direct update of BMC and CNA

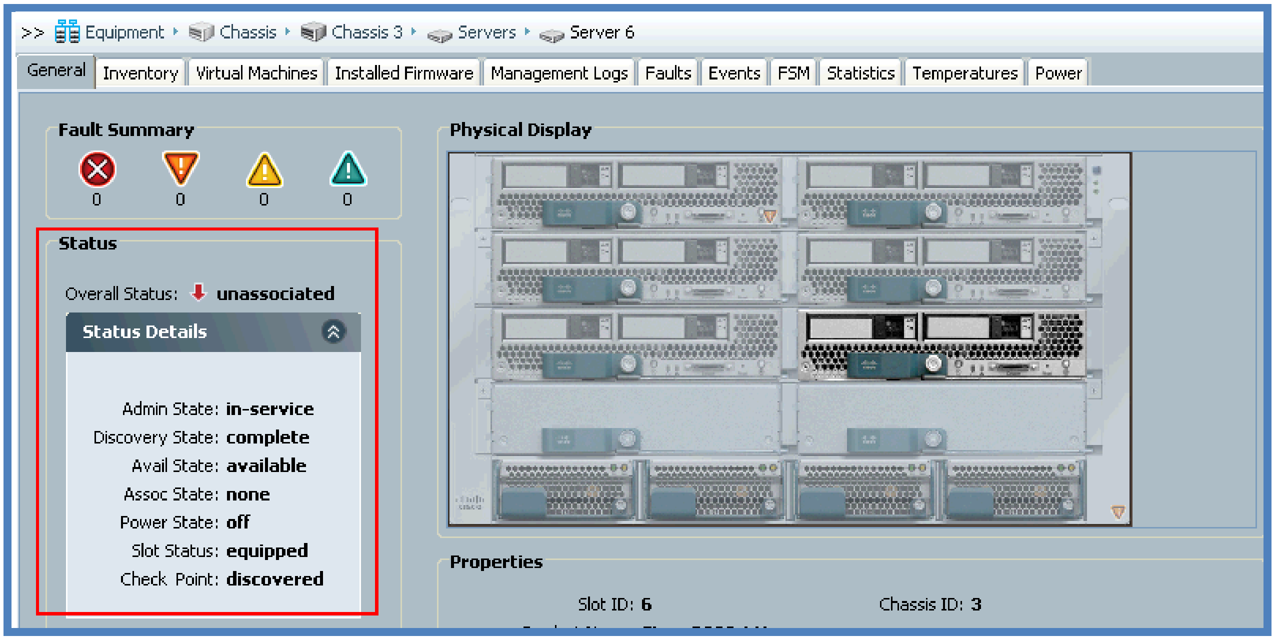
Summary: For unassociated blades, update the BMC and Adapter directly.

Work through your list of Servers to update, in our case it is:

Chassis	Server
2	3
2	4
2	5
2	7
3	5
3	6
4	5

Table 4 - List of servers to update BMC and Adapters directly

For this illustration we will update Chassis 3 / Server 6. First, confirm that the server is unassociated.



Status

Overall Status: **unassociated**

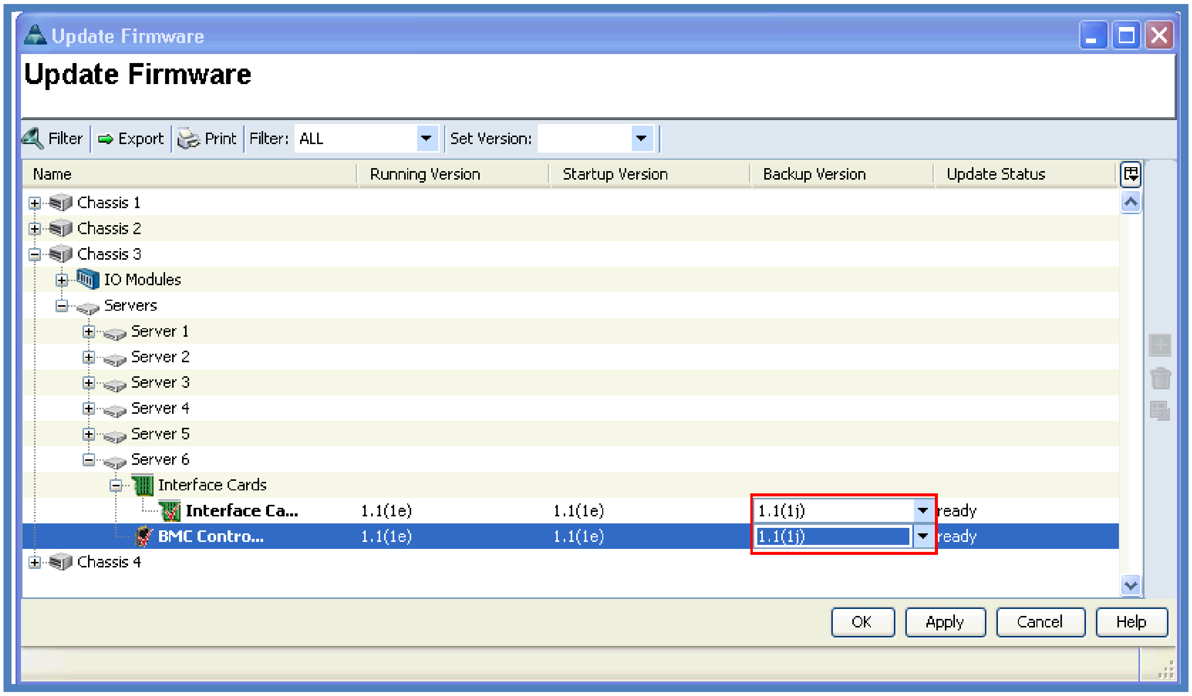
Status Details

Admin State: **in-service**
Discovery State: **complete**
Avail State: **available**
Assoc State: **none**
Power State: **off**
Slot Status: **equipped**
Check Point: **discovered**

Slot ID: **6**
Chassis ID: **3**

Figure 3 - Confirm the server status

To install the new release you need to Update then Activate the component via the Installed Firmware screen.



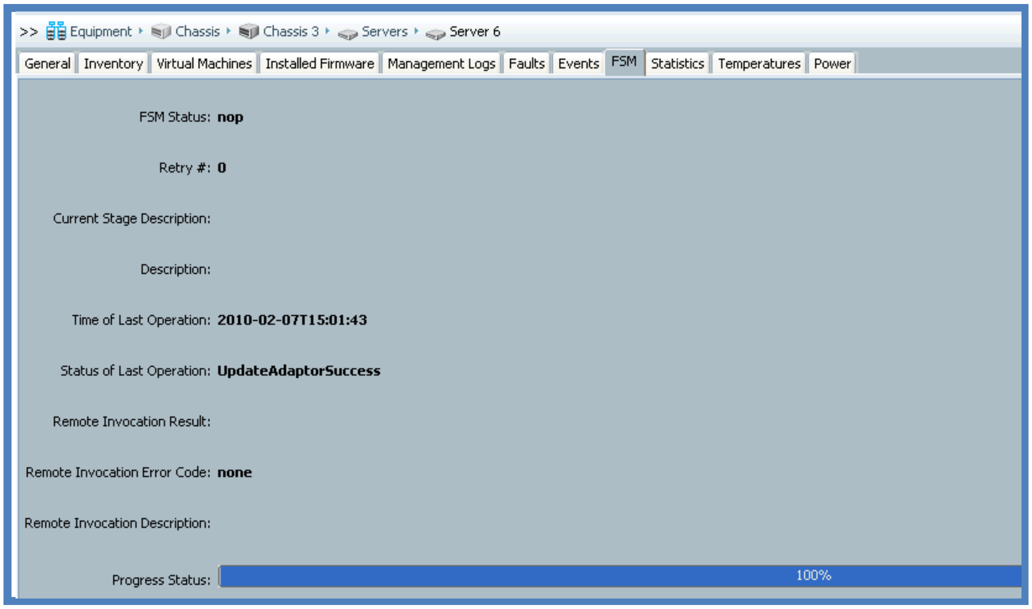
Update Firmware

Filter: ALL Set Version:

Name	Running Version	Startup Version	Backup Version	Update Status
Chassis 1				
Chassis 2				
Chassis 3				
IO Modules				
Servers				
Server 1				
Server 2				
Server 3				
Server 4				
Server 5				
Server 6				
Interface Cards				
Interface Ca...	1.1(1e)	1.1(1e)	1.1(1j)	ready
BMC Contro...	1.1(1e)	1.1(1e)	1.1(1j)	ready
Chassis 4				

Figure 4 - Directly updating the BMC and CNA of a blade

In the Server's FSM screen you can watch progress:



FSM Status: nop

Retry #: 0

Current Stage Description:

Description:

Time of Last Operation: 2010-02-07T15:01:43

Status of Last Operation: UpdateAdaptorSuccess

Remote Invocation Result:

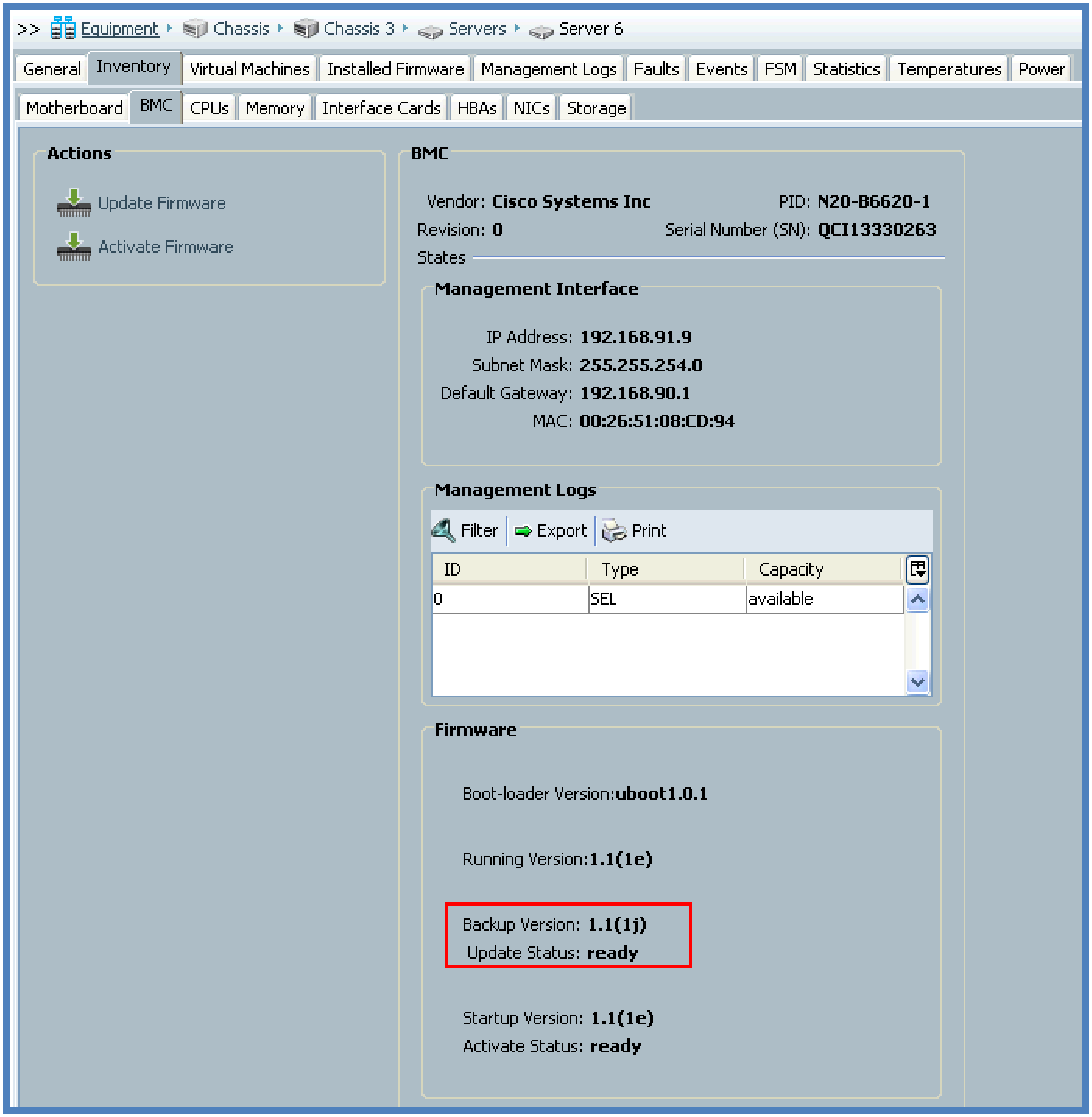
Remote Invocation Error Code: none

Remote Invocation Description:

Progress Status: 100%

Figure 5 - Watching a servers FSM apply changes

You can also look directly at the server's BMC (and this is another place to do Direct updates – there are many ways with UCS! That's a Good Thing ☺).



BMC

Vendor: **Cisco Systems Inc**
PID: **N20-B6620-1**
Revision: **0**
Serial Number (SN): **QCI13330263**
States

Management Interface

IP Address: **192.168.91.9**
Subnet Mask: **255.255.254.0**
Default Gateway: **192.168.90.1**
MAC: **00:26:51:08:CD:94**

Management Logs

ID	Type	Capacity
0	SEL	available

Firmware

Boot-loader Version:**uboot1.0.1**

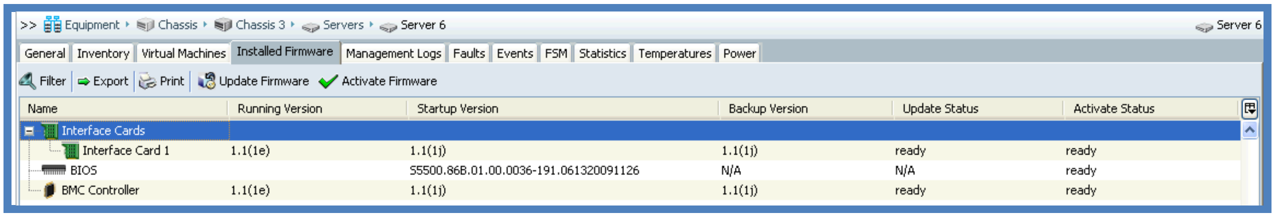
Running Version:**1.1(1e)**

Backup Version: **1.1(1j)**
Update Status: **ready**

Startup Version: **1.1(1e)**
Activate Status: **ready**

Figure 6 - Checking the update status

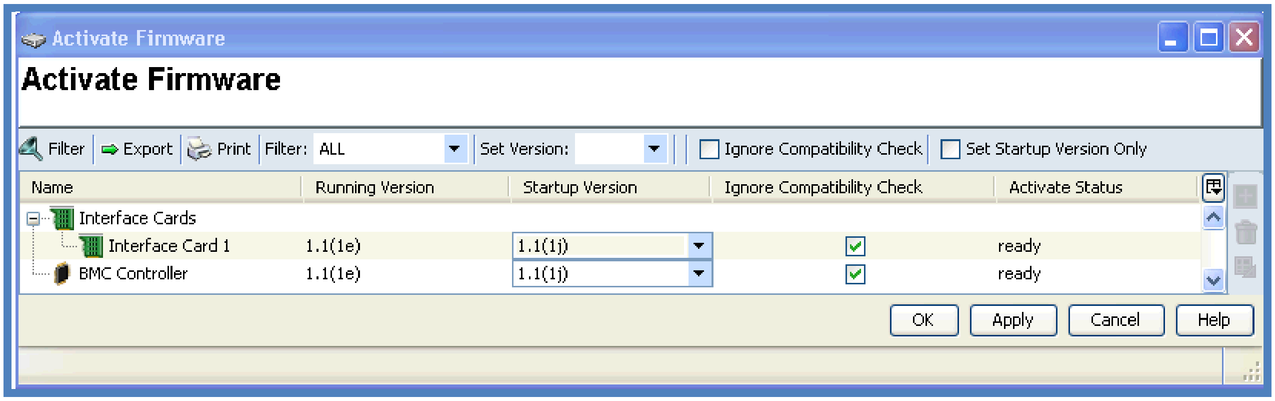
Navigating to Chassis 3 / Server 6 and click Installed Firmware we can see that the Update has completed (Backup Version is at 1.1(1j)) so we are ready to Activate the CNA and BMC updates by clicking Activate Software.


>> Equipment ▸ Chassis ▸ Chassis 3 ▸ Servers ▸ Server 6
Server 6
General | Inventory | Virtual Machines | Installed Firmware | Management Logs | Faults | Events | FSM | Statistics | Temperatures | Power
Filter | Export | Print | Update Firmware | Activate Firmware

Name	Running Version	Startup Version	Backup Version	Update Status	Activate Status
Interface Cards					
Interface Card 1	1.1(1e)	1.1(1j)	1.1(1j)	ready	ready
BIOS		S5500.86B.01.00.0036-191.061320091126	N/A	N/A	ready
BMC Controller	1.1(1e)	1.1(1j)	1.1(1j)	ready	ready

Figure 7 - The update is complete

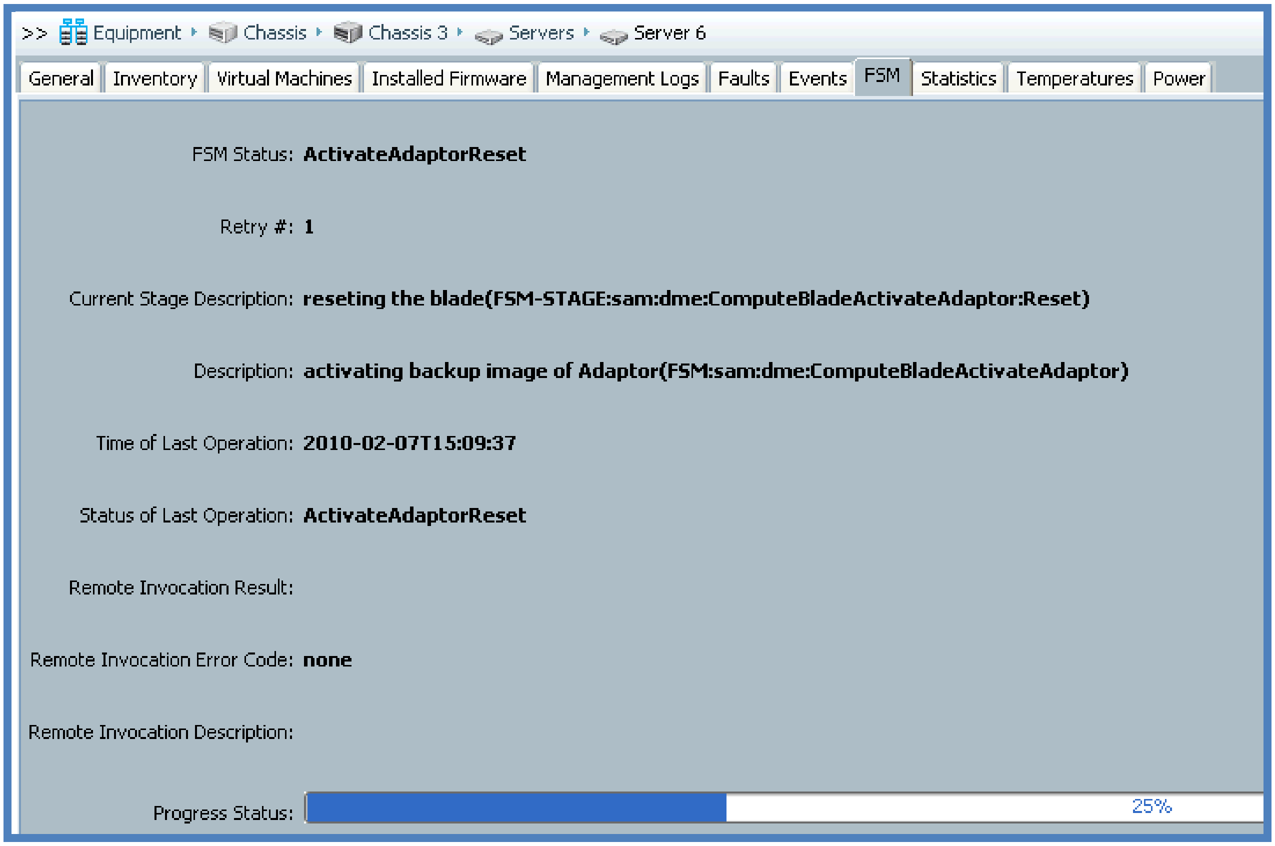
On the Activate Firmware pop-up, change the Startup Version to 1.1(1j), make sure both Ignore Compatibility Check and Set Startup Version are de-selected, then OK.


Activate Firmware
Activate Firmware
Filter | Export | Print | Filter: ALL | Set Version:
☐ Ignore Compatibility Check
☐ Set Startup Version Only
OK
Apply
Cancel
Help

Name	Running Version	Startup Version	Ignore Compatibility Check	Activate Status
Interface Cards				
Interface Card 1	1.1(1e)	1.1(1j)	☑	ready
BMC Controller	1.1(1e)	1.1(1j)	☑	ready

Figure 8 - Activating the firmware upgrade

You can watch the Server's FSM to monitor the activation progress as the server is reset and updated.



FSM Status: **ActivateAdaptorReset**

Retry #: **1**

Current Stage Description: **reseting the blade(FSM-STAGE:sam:dme:ComputeBladeActivateAdaptor:Reset)**

Description: **activating backup image of Adaptor(FSM:sam:dme:ComputeBladeActivateAdaptor)**

Time of Last Operation: **2010-02-07T15:09:37**

Status of Last Operation: **ActivateAdaptorReset**

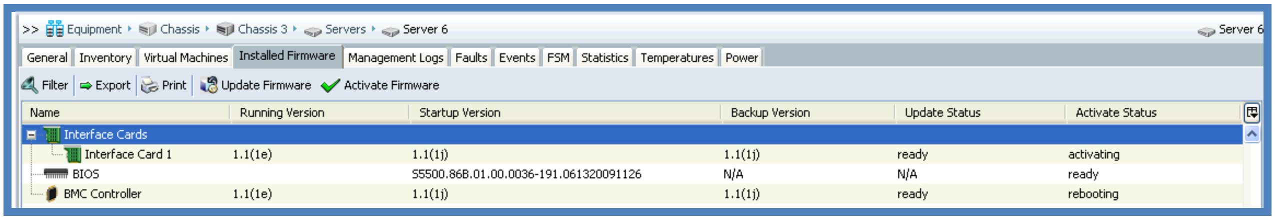
Remote Invocation Result:

Remote Invocation Error Code: **none**

Remote Invocation Description:

Progress Status: 25%

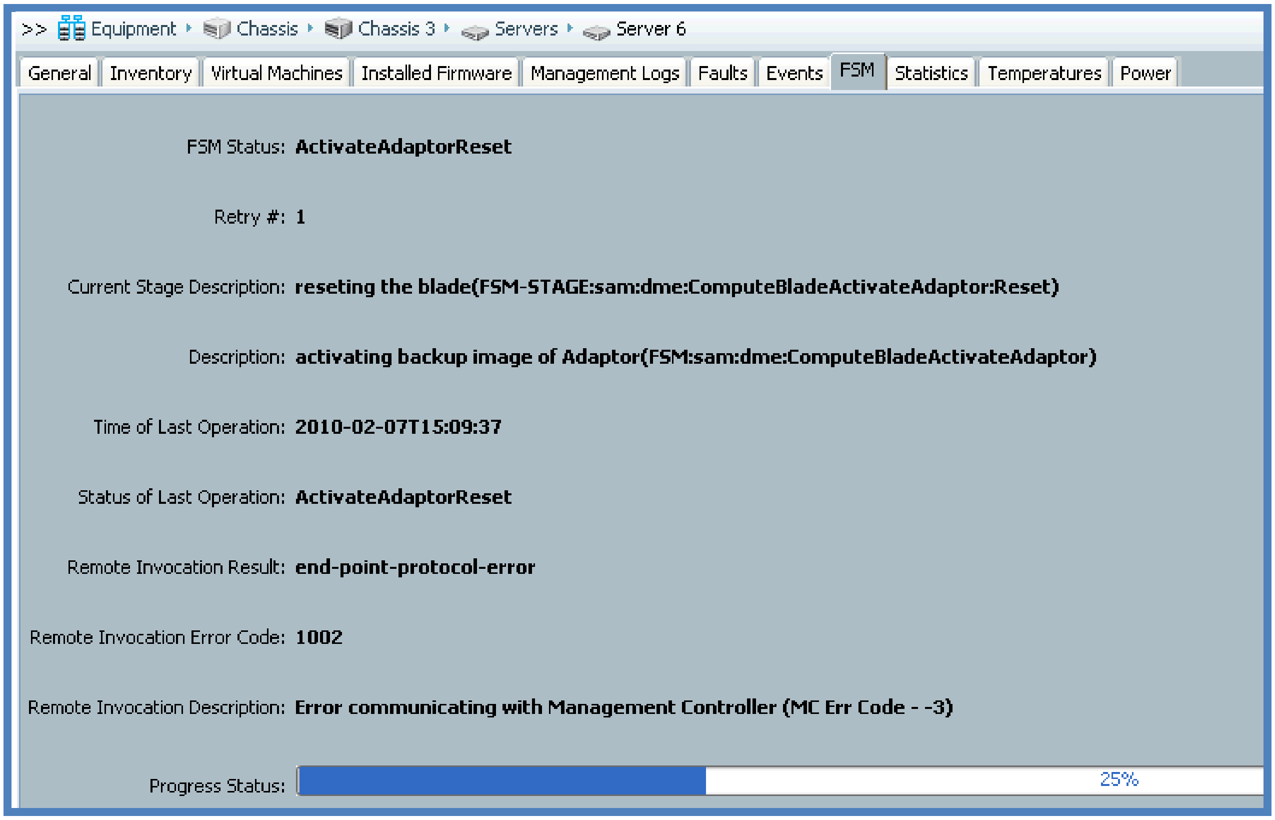
Figure 9 - Watching a server's FSM activate firmware



Name	Running Version	Startup Version	Backup Version	Update Status	Activate Status
Interface Cards					
Interface Card 1	1.1(1e)	1.1(1j)	1.1(1j)	ready	activating
BIOS		S5500.86B.01.00.0036-191.061320091126	N/A	N/A	ready
BMC Controller	1.1(1e)	1.1(1j)	1.1(1j)	ready	rebooting

Figure 10 - A firmware activation in-progress

Don’t worry if you get these errors: the BMC is being rebooted!



FSM Status: **ActivateAdaptorReset**

Retry #: **1**

Current Stage Description: **reseting the blade(FSM-STAGE:sam:dme:ComputeBladeActivateAdaptor:Reset)**

Description: **activating backup image of Adaptor(FSM:sam:dme:ComputeBladeActivateAdaptor)**

Time of Last Operation: **2010-02-07T15:09:37**

Status of Last Operation: **ActivateAdaptorReset**

Remote Invocation Result: **end-point-protocol-error**

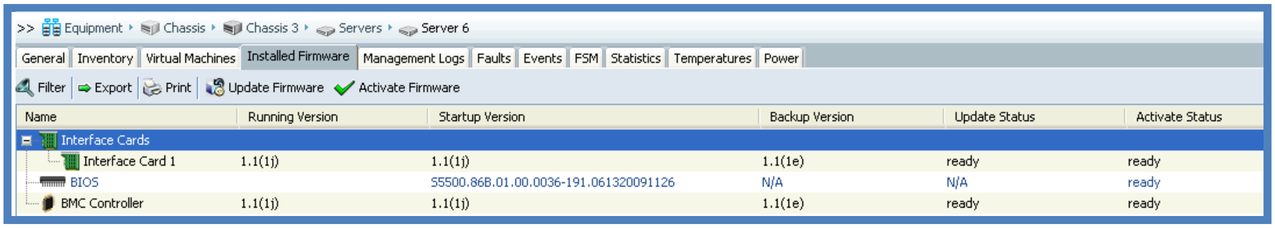
Remote Invocation Error Code: **1002**

Remote Invocation Description: **Error communicating with Management Controller (MC Err Code - -3)**

Progress Status: 25%

Figure 11 - The BMC is being updated and is unavailable which triggers these normal messages

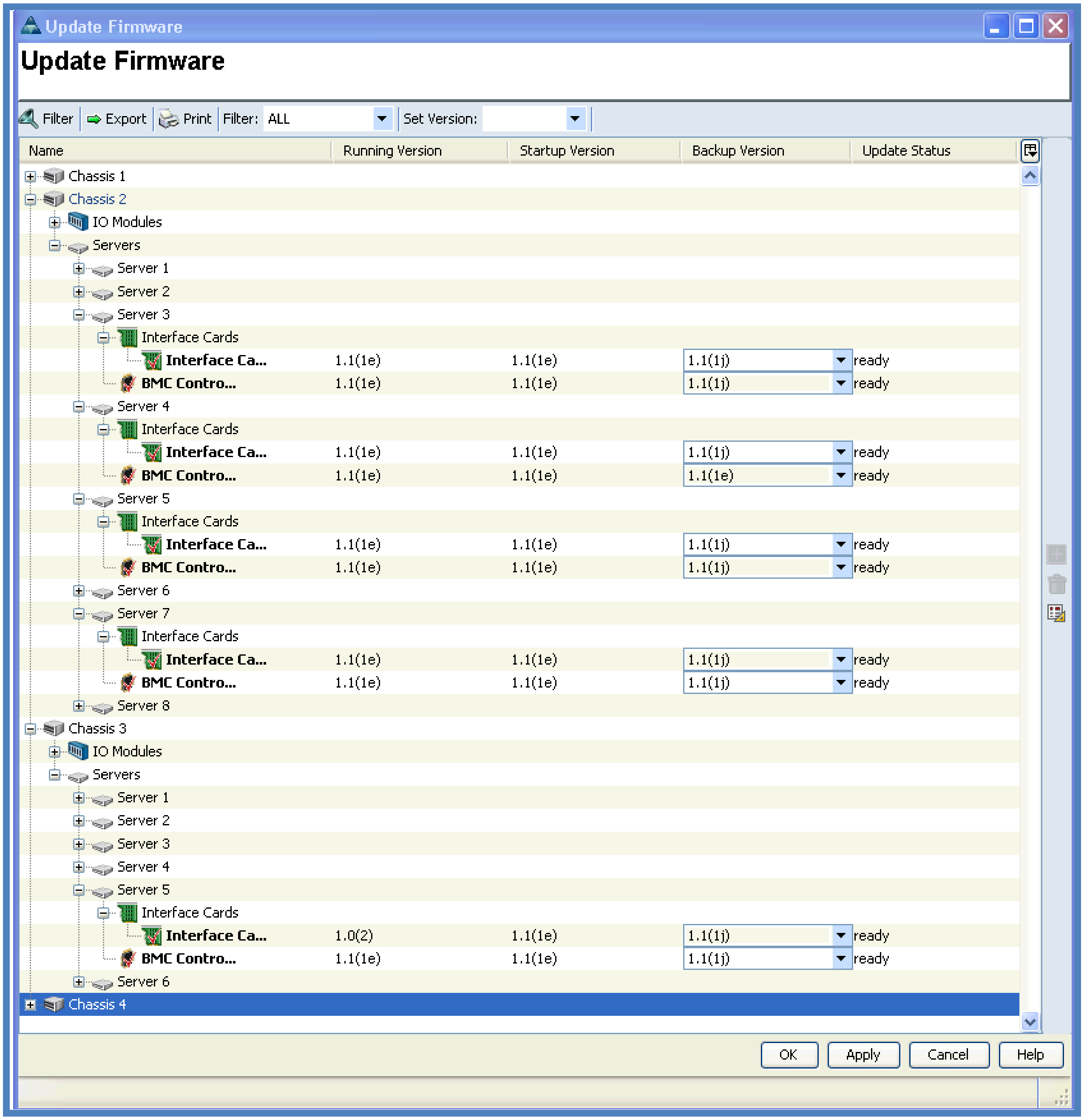
In three or four minutes, the activation is complete.



Name	Running Version	Startup Version	Backup Version	Update Status	Activate Status
Interface Cards					
Interface Card 1	1.1(1j)	1.1(1j)	1.1(1e)	ready	ready
BIOS		S5500.86B.01.00.0036-191.061320091126	N/A	N/A	ready
BMC Controller	1.1(1j)	1.1(1j)	1.1(1e)	ready	ready

Figure 12 - Firmware activation complete

We can directly update blades in bulk using the Equipment → Firmware Management tab.



Update Firmware

Filter: ALL Set Version:

Name	Running Version	Startup Version	Backup Version	Update Status
Chassis 1				
Chassis 2				
IO Modules				
Servers				
Server 1				
Server 2				
Server 3				
Interface Cards				
Interface Ca...	1.1(1e)	1.1(1e)	1.1(1j)	ready
BMC Contro...	1.1(1e)	1.1(1e)	1.1(1j)	ready
Server 4				
Interface Cards				
Interface Ca...	1.1(1e)	1.1(1e)	1.1(1j)	ready
BMC Contro...	1.1(1e)	1.1(1e)	1.1(1e)	ready
Server 5				
Interface Cards				
Interface Ca...	1.1(1e)	1.1(1e)	1.1(1j)	ready
BMC Contro...	1.1(1e)	1.1(1e)	1.1(1j)	ready
Server 6				
Server 7				
Interface Cards				
Interface Ca...	1.1(1e)	1.1(1e)	1.1(1j)	ready
BMC Contro...	1.1(1e)	1.1(1e)	1.1(1j)	ready
Server 8				
Chassis 3				
IO Modules				
Servers				
Server 1				
Server 2				
Server 3				
Server 4				
Server 5				
Interface Cards				
Interface Ca...	1.0(2)	1.1(1e)	1.1(1j)	ready
BMC Contro...	1.1(1e)	1.1(1e)	1.1(1j)	ready
Server 6				
Chassis 4				

Figure 13 - Bulk blade firmware upgrade

It took three minutes to update those five servers.

I’m now going to activate the BMC and CNAs on Chassis 2 only, simulating the operational situation of chassis 2 running a set of compute that I can update in a specific change window, whereas chassis 4 cannot be updated until another change window.

By selecting chassis 2 in the left hand navigation column, then clicking the Installed Firmware tab, I can confirm that servers 3, 4, 5 and 7 have been updated (Backup version is 1.1.1j) and now I can click Activate Firmware to complete the instalation.

Act 3: Update by Policy

Summary: This allows you to automatically update blades with Service Profiles.

For servers that are in-service and running workloads you will want to schedule a time when you can update the components. When that time comes you want to implement the change as efficiently as possible, using a proven practice, and that's what Host Management and Firmware Management policies allow you to do.

The Management Firmware policy takes care of the BMC update, and the Host Firmware policy does the rest of the components.

You create these policies ahead of time, attach them to a Service Profile and through associating this profile with a blade, the blades firmware will be upgrade.

If you attach the policies to a Service Profile that is already associated with a blade, that blade will be rebooted – you are warned first, so take heed of the notice! Don't attach a policy to a service profile unless you are managing that change properly: ie. you understand the impact, you have authorization and a change window.

This is part of the "Wire Once and Walk Away" design of UCS: you configure the policies once, then apply them multiple times. Simple.

Create the Host Management Policy first to take care of the Service Profile's blade BMC:

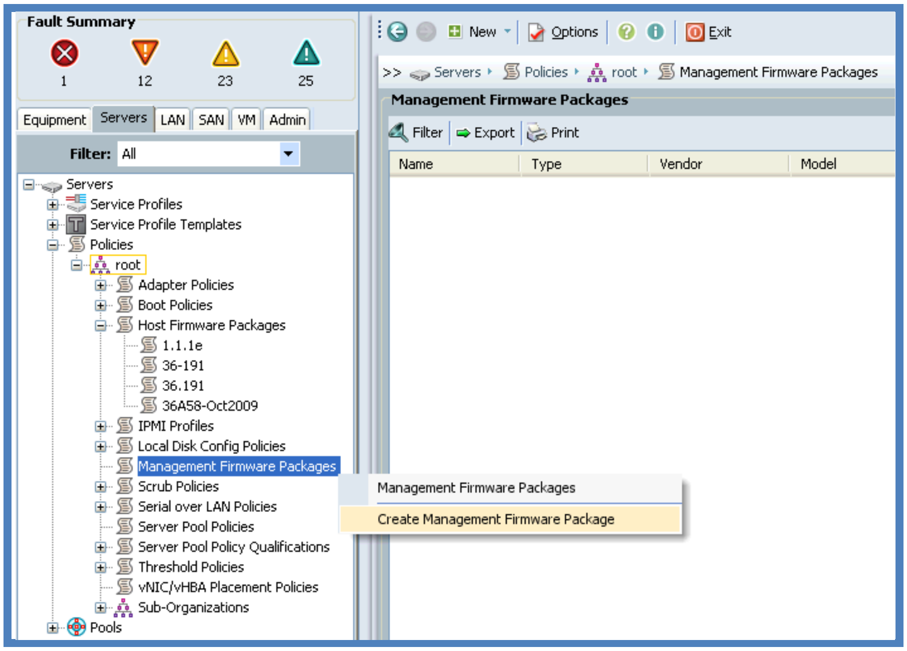
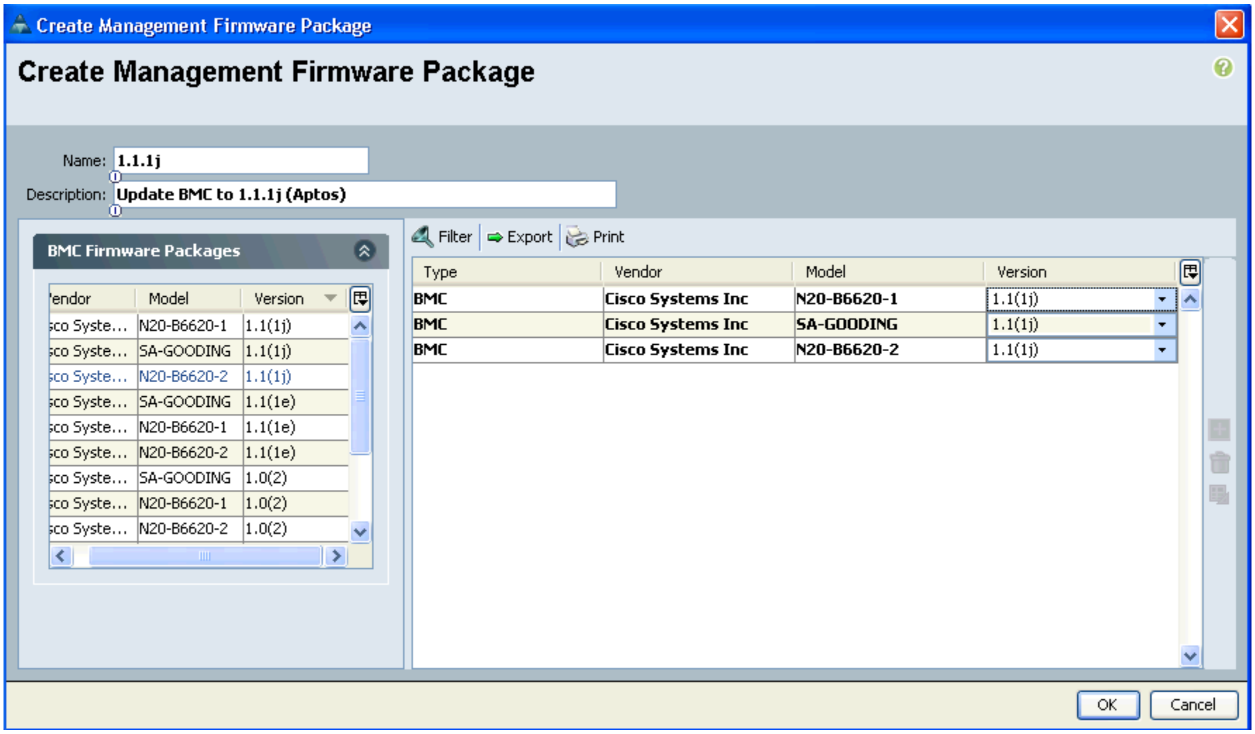


Figure 14 - Creating a Management Firmware package

I will title the policy to match the release (1.1.1j) and sort the BMC Firmware Packages by descending Version so that 1.1.1j images are at the top.

There are three images – so which do I choose? The answer is: all three. This policy will be attached to any Service Profile, even though the Service Profiles might run on different hardware. If the Service Profile runs on a B200 or a B250, this policy will still work if all of the images are in the policy. UCS takes care of selecting the correct image for the hardware so you don't have to.

If UCS didn't do this, you'd have to create a policy for each image which is clearly a less efficient way of working.



Create Management Firmware Package

Name: 1.1.1j

Description: Update BMC to 1.1.1j (Aptos)

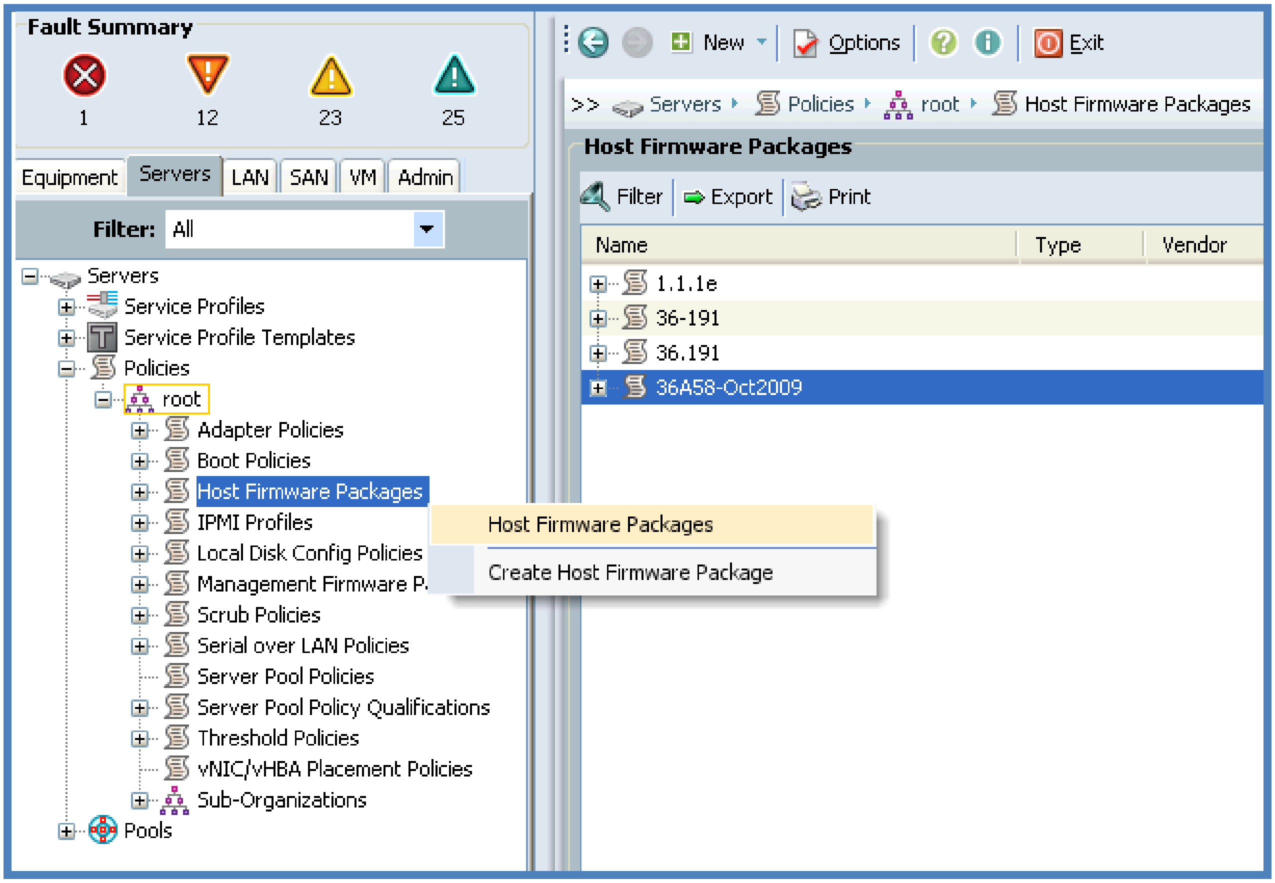
BMC Firmware Packages

endor	Model	Version
co Syste…	N20-B6620-1	1.1(1j)
co Syste…	SA-GOODING	1.1(1j)
co Syste…	N20-B6620-2	1.1(1j)
co Syste…	SA-GOODING	1.1(1e)
co Syste…	N20-B6620-1	1.1(1e)
co Syste…	N20-B6620-2	1.1(1e)
co Syste…	SA-GOODING	1.0(2)
co Syste…	N20-B6620-1	1.0(2)
co Syste…	N20-B6620-2	1.0(2)

Type	Vendor	Model	Version
BMC	Cisco Systems Inc	N20-B6620-1	1.1(1j)
BMC	Cisco Systems Inc	SA-GOODING	1.1(1j)
BMC	Cisco Systems Inc	N20-B6620-2	1.1(1j)

And we're done!

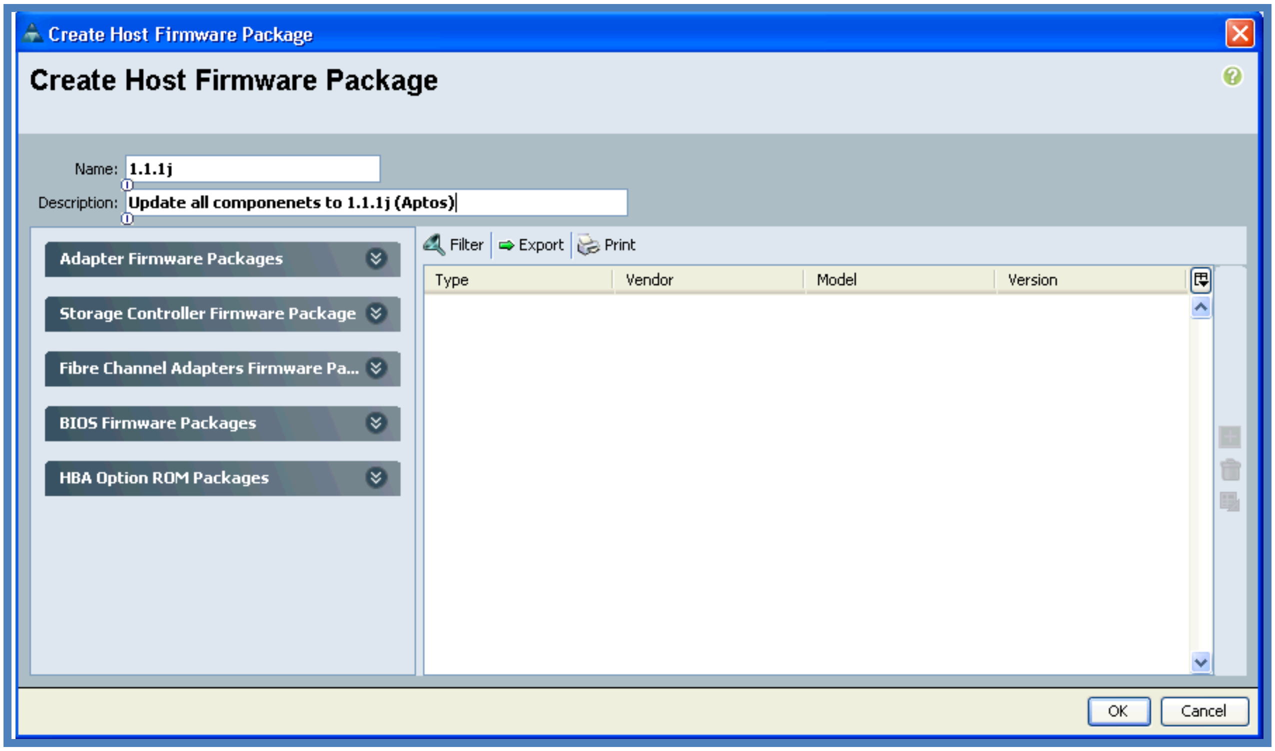
Now we can create the Host Firmware policy for the rest of the components, but all the same principles apply. Simple.



Filter: All

Name	Type	Vendor
1.1.1e		
36-191		
36.191		
36A58-Oct2009		

Figure 15- Creating a Host Firmware policy



Create Host Firmware Package

Name: 1.1.1j

Description: Update all componenets to 1.1.1j (Aptos)

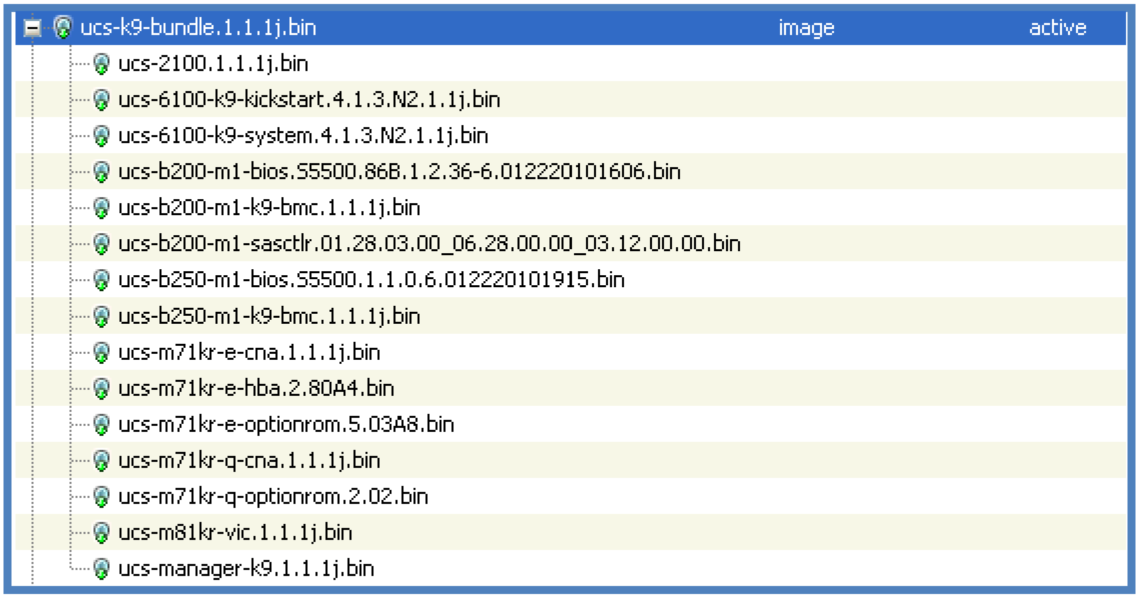
Create Host Firmware Package
Adapter Firmware Packages
Storage Controller Firmware Package
Fibre Channel Adapters Firmware Pa...
BIOS Firmware Packages
HBA Option ROM Packages
Filter
Export
Print
Type
Vendor
Model
Version
OK
Cancel

Figure 16 - Selecting the images to go into the policy

For the Adapter Firmware package I can add all the 1.1.1j images.

For the Storage Controller, Fibre Channel Adapter, BIOS Firmware and HBA Option ROM I want to pick specific images to keep my policy clear.

I need to know the image names from the 1.1.1j package so I pick the right ones, so I made notes from Equipment → Firmware Management → Packages



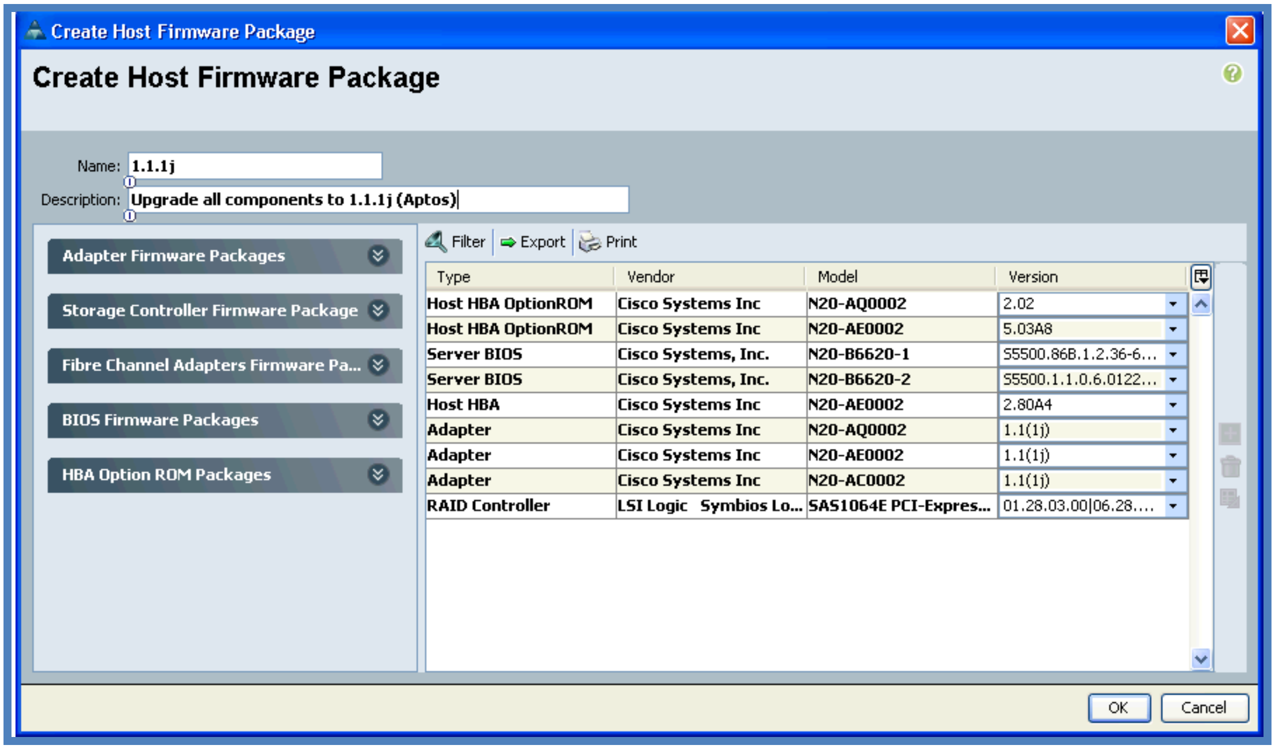
```
ucs-k9-bundle.1.1.1j.bin                                   image          active
    ucs-2100.1.1.1j.bin
    ucs-6100-k9-kickstart.4.1.3.N2.1.1j.bin
    ucs-6100-k9-system.4.1.3.N2.1.1j.bin
    ucs-b200-m1-bios.S5500.86B.1.2.36-6.012220101606.bin
    ucs-b200-m1-k9-bmc.1.1.1j.bin
    ucs-b200-m1-sasctlr.01.28.03.00_06.28.00.00_03.12.00.00.bin
    ucs-b250-m1-bios.S5500.1.1.0.6.012220101915.bin
    ucs-b250-m1-k9-bmc.1.1.1j.bin
    ucs-m71kr-e-cna.1.1.1j.bin
    ucs-m71kr-e-hba.2.80A4.bin
    ucs-m71kr-e-optionrom.5.03A8.bin
    ucs-m71kr-q-cna.1.1.1j.bin
    ucs-m71kr-q-optionrom.2.02.bin
    ucs-m81kr-vic.1.1.1j.bin
    ucs-manager-k9.1.1.1j.bin
```

Figure 17 - Listing the image filenames in the 1.1.1j package

Here's what I need in the table below. Note when you are dragging the images into your policy, the OK popup will give the full image name to match above

Adapter Firmware	All 1.1.1j files
Storage Controller Firmware	Version 01.28.03…
Fibre Channel Adapters Firmware	Pull all files
BIOS Firmware	Sort by descending version, I'ts the second-last one at the bottom for the b200. For the b250, find the two beginning with S5500.1 and pick the Cisco one.
HBA Option ROM	Sort by descending version, pick the first 5.03A8 and the first 2.02 version

One last step is to delete any items of your policy that have "MENLO", "PALO" and "GOODING" kind of names in them – these are duplicate packages.


Create Host Firmware Package
Adapter Firmware Packages
Storage Controller Firmware Package
Fibre Channel Adapters Firmware Pa...
BIOS Firmware Packages
HBA Option ROM Packages
Filter
Export
Print
OK
Cancel

Create Host Firmware Package

Name: 1.1.1j

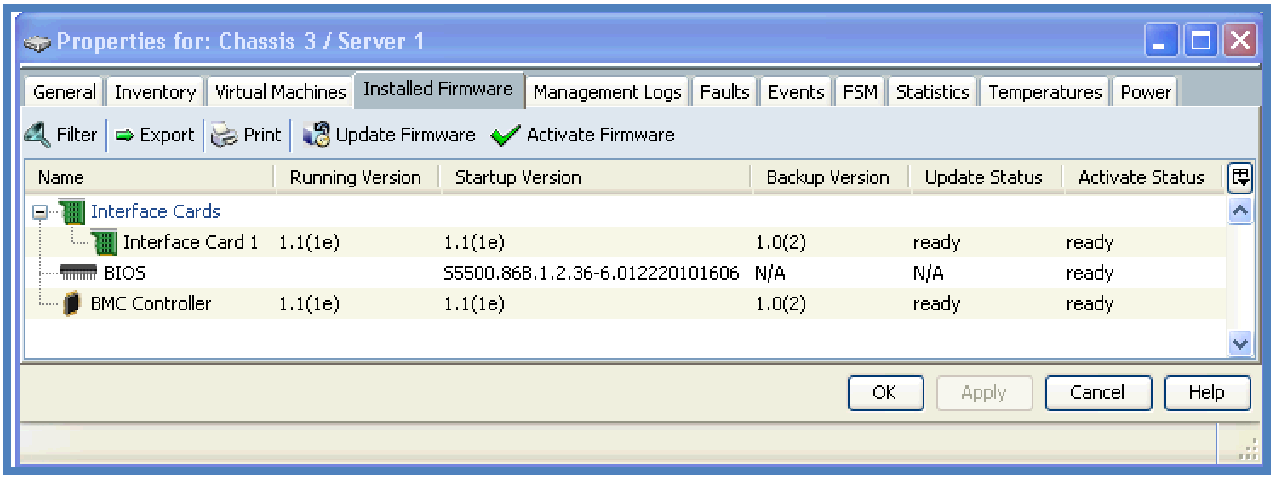
Description: Upgrade all components to 1.1.1j (Aptos)

Type	Vendor	Model	Version
Host HBA OptionROM	Cisco Systems Inc	N20-AQ0002	2.02
Host HBA OptionROM	Cisco Systems Inc	N20-AE0002	5.03A8
Server BIOS	Cisco Systems, Inc.	N20-B6620-1	S5500.86B.1.2.36-6...
Server BIOS	Cisco Systems, Inc.	N20-B6620-2	S5500.1.1.0.6.0122...
Host HBA	Cisco Systems Inc	N20-AE0002	2.80A4
Adapter	Cisco Systems Inc	N20-AQ0002	1.1(1j)
Adapter	Cisco Systems Inc	N20-AE0002	1.1(1j)
Adapter	Cisco Systems Inc	N20-AC0002	1.1(1j)
RAID Controller	LSI Logic Symbios Lo...	SAS1064E PCI-Expres...	01.28.03.00|06.28....

Figure 18 - A completed Host Firmware package

Now to try it out. I have a service profile called esx4i-a and it is currently associated with blade chassis-3/server-1.

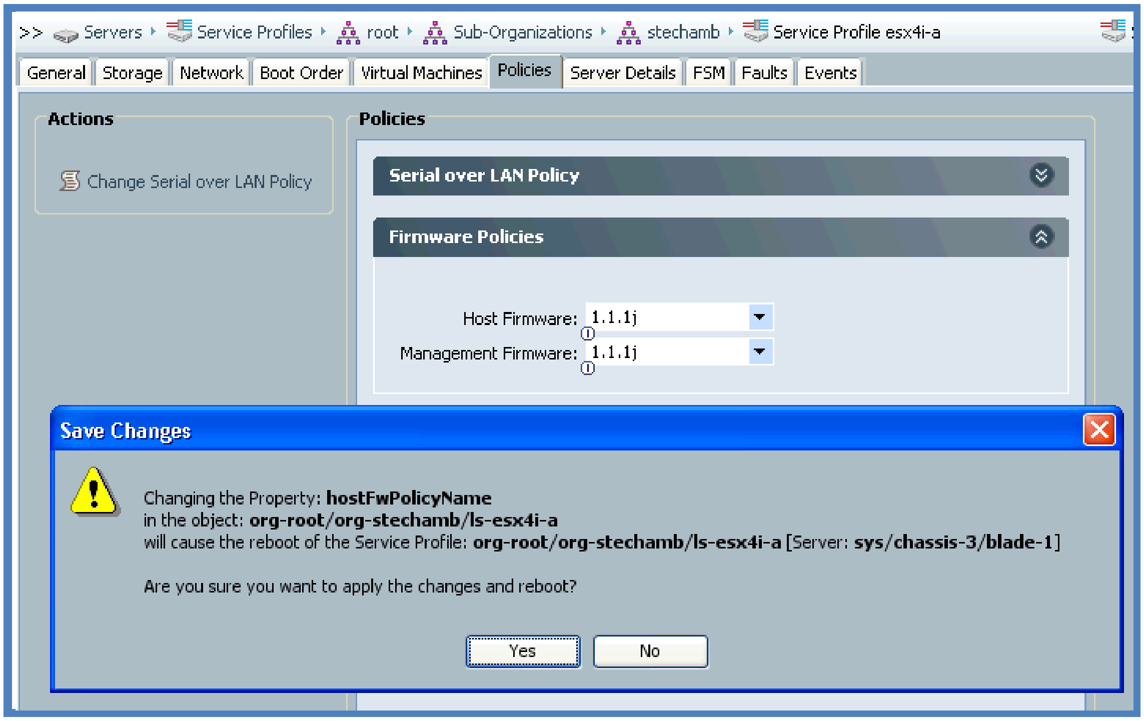
I know that this blade is running on old firmware:



Name	Running Version	Startup Version	Backup Version	Update Status	Activate Status
Interface Cards					
Interface Card 1	1.1(1e)	1.1(1e)	1.0(2)	ready	ready
BIOS		S5500.86B.1.2.36-6.012220101606	N/A	N/A	ready
BMC Controller	1.1(1e)	1.1(1e)	1.0(2)	ready	ready

Figure 19 - A blade running old firmware

My service profile doesn't have a Host Management nor Host Firmware policy attached, so if I wanted to upgrade the firmware I need to attach my new policies which will disrupt the blade.



Host Firmware: 1.1.1j

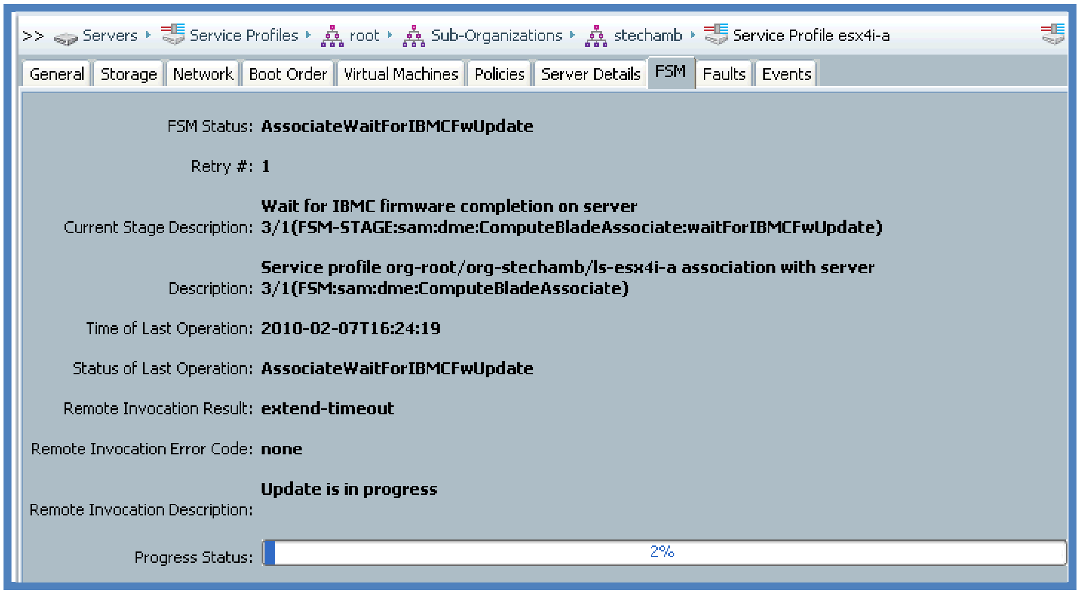
Management Firmware: 1.1.1j

Changing the Property: **hostFwPolicyName**
in the object: **org-root/org-stechamb/ls-esx4i-a**
will cause the reboot of the Service Profile: **org-root/org-stechamb/ls-esx4i-a** [Server: **sys/chassis-3/blade-1**]

Are you sure you want to apply the changes and reboot?

Figure 20 - Attaching the policies to the service profile

Watch the FSM apply the updates:


>> Servers ▸ Service Profiles ▸ root ▸ Sub-Organizations ▸ stechamb ▸ Service Profile esx4i-a
General
Storage
Network
Boot Order
Virtual Machines
Policies
Server Details
FSM
Faults
Events

FSM Status: **AssociateWaitForIBMCFwUpdate**

Retry #: **1**

Current Stage Description: **Wait for IBMC firmware completion on server 3/1(FSM-STAGE:sam:dme:ComputeBladeAssociate:waitForIBMCFwUpdate)**

Description: **Service profile org-root/org-stechamb/ls-esx4i-a association with server 3/1(FSM:sam:dme:ComputeBladeAssociate)**

Time of Last Operation: **2010-02-07T16:24:19**

Status of Last Operation: **AssociateWaitForIBMCFwUpdate**

Remote Invocation Result: **extend-timeout**

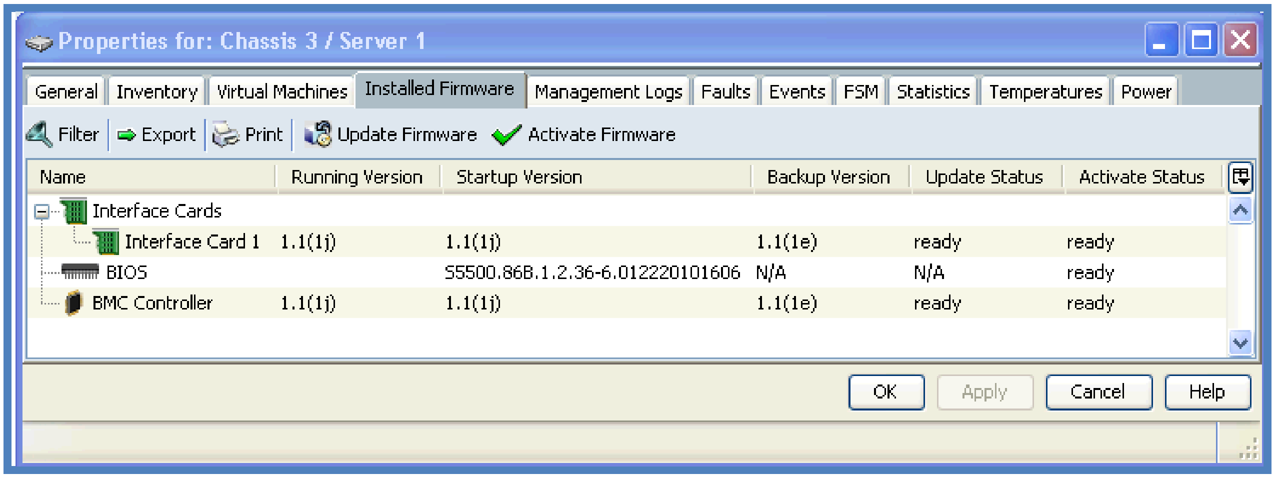
Remote Invocation Error Code: **none**

Remote Invocation Description: **Update is in progress**

Progress Status: 2%

Figure 21 - Watching the FSM update a blade

UCS will now reset the blade, implement all the images on the blade components, and bring the service profile back up, which in my case is an ESX4i instance.



Name	Running Version	Startup Version	Backup Version	Update Status	Activate Status
Interface Cards					
Interface Card 1	1.1(1j)	1.1(1j)	1.1(1e)	ready	ready
BIOS		S5500.86B.1.2.36-6.012220101606	N/A	N/A	ready
BMC Controller	1.1(1j)	1.1(1j)	1.1(1e)	ready	ready

Figure 22 - A blade that has had its firmware upgrade by policies

If you create a new service profile and these two firmware policies are attached, whatever blade is associated – no matter what CNA type, or blade type – will be running the latest 1.1.1j firmware because if the blade is running old firmware, the policy will update it. This update process takes less than five minutes so it doesn't impact service profile deployment times.