Table of Contents .................................................................1

1. Introduction ........................................................................2
   1.1 Terminologies ....................................................................2
   1.2 What’s new – IMM2 ............................................................2

2. Important Notes ......................................................................2
   2.1 Minimum AMM Firmware levels (BladeCenter Only) ..................2
   2.2 Mandatory UEFI configuration .............................................3
   2.3 Firmware Image Compatibility with IMM .................................3
   2.4 Backup IMM2 Bank ............................................................3
   2.5 Important Notice for Updating all firmware ..............................3

3. Requirements for updating firmware ........................................4
   Recommended firmware update methods .......................................4
   Requirements for updating firmware via ToolCenter UpdateXpress System Pack Installer (UXSPI) or ToolCenter Bootable Media Creator (BoMC) .................................................................5
   Requirements for updating imm2, uefi, dsa firmware via IMM WEB interface .................................................................5
   Requirements for Updating IMM2 and UEFI firmware via the AMM (BladeCenter only) .................................................................5
1. INTRODUCTION

1.1 TERMINOLOGIES

IMM – Integrated Management Module
IMM2 – Second Generation of Integrated Management Module
UEFI – Unified Extensible Firmware Interface
pDSA – preboot Dynamic System Analysis
UXSP – UpdateXpress System Pack
UXSPI – UpdateXpress System Pack Installer
AMM – Advanced Management Module

1.2 WHAT’S NEW – IMM2

IMM2 is the new generation of Integrated Management Module that provides advanced server management capability. The IMM2 includes features such as following:

- Single firmware image for IMM across the product set.
- Ability to remotely configure IMM and UEFI settings without the server powered on.
- Standards based interfaces including IPMI and SNMP.
- Upward integration with IBM Systems Director.

Compared to the previous generation of integrated management module, IMM2 brings additional improvement:

- Advanced processor that increase system performance and response speed
- Enhanced user interface that improve user experience
- Dual IMM2 banks for recovery in the unlikely event of a primary bank firmware failure

IBM is changing the supported methods to deploy firmware updates to new IBM System x and BladeCenter servers starting in 2011. Detailed changes can be found in IBM System X update tools transition.

2. IMPORTANT NOTES

2.1 MINIMUM AMM FIRMWARE LEVELS (BLADECENTER ONLY)

AMM firmware Version 3.62O (Build ID BPET62O) or higher is required to support the new blade server HS23.
2.2 **MANDATORY UEFI CONFIGURATION**

To enable firmware update, the LAN over USB interface must be enabled.

To enable the LAN over USB interface on a rack server, ensure that in the UEFI menu, the option "Commands on USB interface" is enabled (default setting). This can be found in the UEFI menu:

- systems settings -> Integrated Management Module -> Commands on USB Interface Preference -> Commands on USB interface. You can also enable it via the menu in the IMM WEB interface.
- Go to System -> IMM Control -> System Settings, and at the bottom of the page in the Miscellaneous section, ensure that Allow commands on USB interface is set to Enabled.

To enable the LAN over USB interface on a blade server, from the AMM WEB interface, click on the “Configuration link” under “Blade Tasks”. Scroll down and click on the “Advanced Blade Policy Settings” link at the bottom of the page. Under the “Service Processor’s Ethernet over USB interface” section, ensure the status is “Enabled”. If any are disabled, select the checkbox next to the disabled blade(s), and press the “Enable” button. This can also be done using the AMM “ethoverusb” CLI command.

2.3 **FIRMWARE IMAGE COMPATIBILITY WITH IMM**

IMM2 firmware is not compatible with the previous generation of IMM firmware.

2.4 **BACKUP IMM2 BANK**

IMM2 provides dual banks (primary and backup) of isolated IMM2 firmware image to improve system availability and to provide system recovery function. During normal operation, IMM2 always boots from the primary bank. Backup bank provides system recovery function in the event of a firmware failure in primary bank.

The backup IMM bank is not an exact copy of the primary bank and should only be used for recovering the primary bank in the event of a firmware failure. The backup bank firmware level may be older than the primary and the configuration settings will be different as well. You should not run from the backup bank for an extended period of time, only long enough to update and recover the primary bank.

You should periodically update the backup banks of both the IMM and UEFI firmware. The best practice would be to update the backup bank to the currently running firmware level before updating the primary bank to newer firmware level.

When using UXSPI and WEB to perform flashing, user is allowed to select either bank of IMM2 to perform firmware update.

2.5 **IMPORTANT NOTICE FOR UPDATING ALL FIRMWARE**

- When updating through the AMM, after the IMM update is complete, wait at least 15 minutes before you initiate any further firmware updates.
- It is recommended that all firmware are updated together as a matched set. The best practice is to use the UpdateXpress System Pack Installer (UXSPI) for a system. If a firmware fails to update, the best practice is to attempt the firmware update again before rebooting the system.
- Operating systems with link-local IP address support (such as Windows) assigns 169.254.xxx.xxx address to any interface in the system that is configured for DHCP but cannot reach a DHCP server. If any LAN interface is assigned a 169.254.xxx.xxx address, it will prevent the firmware update from completing. Assign an address or disable the interface.
- Updated firmware version numbers will not be visible in SMBIOS tables until after the operating system is
rebooted.

- The IMM must be reset after updating its firmware before configuration changes can be made. Note that when updating via UXSPI, BoMC, or individual update packages, the IMM will automatically be reset after updating its firmware.
- Do not remove AC power or remove the blade from the chassis after an IMM update until the IMM has completed rebooting. Doing so could result in unpredictable behavior. The location LED in front panel will blink to indicate the activation is still in progress.
- UEFI can only be updated when the server is powered off or if the operating system has completely loaded. Any update attempts when the server is booting, sitting in the UEFI F1 setup menu, or when the operating system is loading will be rejected.
- Do not remove AC power or remove the blade from the chassis when updating UEFI. If the UEFI is being updated by IMM WEB or AMM when the server is power off, the power LED in the control panel will fast blink to indicate the event.

3. REQUIREMENTS FOR UPDATING FIRMWARE

IBM ToolsCenter UpdateXpress System Pack Installer (UXSPI) can help reduce your cost of computing by providing an effective and simple way to update device drivers, server firmware and firmware of supported options contained within the server on most of your System x and BladeCenter products. UXSPI can apply individual updates to the system as well as UpdateXpress System Packs which are a group of drivers and firmware updates tested as a bundle to verify that they work together without issues.

UXSPI provides both a GUI interface and a command line (CLI) interface to allow for both attended, easily customized updates and for scripted updates. It can acquire updates from a local path, a network shared folder, or directly from ibm.com.

After acquiring the updates, UXSPI will use the metadata in each updates associated xml file to apply the updates in unattended mode, in the correct order, with any necessary reboots or delays included.

Bootable Media Creator (BoMC) provides firmware updating capabilities on a bootable media such as a CD, DVD, USB key, or PXE files for a network boot. It leverages UXSPI to perform the update by bundling the UXSPI utility onto the bootable media. Since BoMC creates bootable media that runs independent of any OS installed on a system, it is unable to perform device driver updates. Updates supporting multiple systems can be contained on a single bootable media image.

RECOMMENDED FIRMWARE UPDATE METHODS

There are multiple methods with unique and individual procedures for performing firmware updates. The preferred methods to perform firmware updates are to use the ToolsCenter UpdateXpress System Pack Installer (UXSPI) or Bootable Media Creator (BoMC). These tools are able to:

- Display an inventory of installed firmware and drivers
- Download firmware and drivers from ibm.com
- Download an UXSP from ibm.com
- Update all of the firmware and drivers in your system, including RAID, HDD, NIC, and Fibre Channel devices
- Apply updates in the correct order to completely update a system with the fewest reboots
- Create a bootable CD/DVD/USB key/PXE image to perform firmware updates (BoMC)

For updating firmware on VMware OS, the recommended method is to use Bootable Media Creator (BoMC).
REQUIREMENTS FOR UPDATING FIRMWARE VIA TOOLCENTER UPDATEEXPRESS SYSTEM PACK INSTALLER (UXSPI) OR TOOLCENTER BOOTABLE MEDIA CREATOR (BOMC)

ToolsCenter Bootable Media Creator (BoMC)
• If the BoMC .ISO image that is created will be remote mounted via the IMM, it will require a remote access license on the x3550M4/x3650M4 server to utilize that functionality.
• 8677 BladeCenter – E (1xx, 2xx and 3xx --non-refresh models) may require an HS22/HS22V USB port speed configuration change. See RETAIN Tip H163233 for details.

ToolsCenter UpdateXpress System Pack Installer (UXSPI)
• Requires an operating system to be installed on the server prior to execution of the package.
• Requires the device driver for the LAN over USB interface to be installed and configured.

IMM2 firmware update on Vmware ESXi/vSphere
• For VMWARE 4.x, you must execute the following command to disable the firewall:
o esxcfg-firewall -o 623,udp,out,USBLan
• For VMWare vSphere 5.0, you must turn off the firewall. To do this:
  1. SSH into the vSphere system.
  2. Issue this command: escd li network firewall set -d true
• On VMWare ESXi/vSphere systems, do not select usb0 when configuring network adapters.
• To determine whether the IMM2 has completed initialization, ssh into the ESXi/vSphere system and run this command: cat /etc/cim/ibm/imm_fw_schema.
• Check "%SYSTEMDRIVE%\IBM_Support\fupbdebug.txt" in ESXi/vSphere system when encountering IMM2 update error, or "/tmp/fupbdebug.txt" if above file does not exist.

Notes
• The online firmware update utilities use the Ethernet (LAN) over USB interface to communicate with the IMM2. BoMC and UXSPI will automatically enable and configure this interface if it is not already configured.
• When encountering such problems as LAN-over-USB undetected or pinging IP of IMM failed, ensure the LAN Over USB interface is configured properly:
  Run ifconfig or ipconfig and verify the LAN Over USB interface (usb0 on Linux, RNDIS on Windows) is enabled and has an IP address in the range or 169.254.95.xxx.

REQUIREMENTS FOR UPDATING IMM2, UEFI, DSA FIRMWARE VIA IMM WEB INTERFACE

Updating IMM2, UEFI, DSA via IMM2 WEB interface is used as the recovery method.

Detailed instruction can be found in IMM2 WEB update whitepaper document.

REQUIREMENTS FOR UPDATING IMM2 AND UEFI FIRMWARE VIA THE AMM (BLADECENTER ONLY)

Note: When updating IMM and UEFI firmware via the AMM Command Line Interface (Telnet/SSH), set the inactivity timer to zero (0) during the update process. Run the following command after logging in via Telnet/SSH: telnetcfg -t 0 -T system:mm[1]
where 1 is the active advanced management module bay. After the update completes, reset the timer to the previous value.
• Ensure that all blades have been discovered and VPD is correctly displayed with no errors in the AMM event log.
• A network switch must be installed in I/O bay 1 of the chassis.
- The Copper Pass-thru Module (CPM) and Optical Pass-thru Module (OPM) do not support updating IMM2, UEFI firmware.
- When using an Intelligent Copper Pass-Thru Module (iCPM), the external port of the iCPM that corresponds to the blade that is being updated must be connected and have a link to an upstream switch.
- No special configuration is needed when using the Ethernet switches at default settings.
- Ensure VLAN 4095 is enabled (this is default).

- The AMM TFTP server must be enabled.
  - This can be done under MM Control – Network Protocols or Command Line (ports -tftp on)
- Do not remove AC power or remove the blade from the chassis when blade is being discovered after IMM is updated.
- The blade should not be rebooted during the UEFI update process.
- The UEFI should only be updated via the AMM when the blade is powered on with the operating system fully loaded, or powered off completely
- If the server is powered off when the UEFI update starts, do not power on the server until the update has completed.
- Note that DSA Preboot can not be updated via the AMM. Use ToolsCenter UpdateXpress System Pack Installer (UXSPI) or ToolsCenter Bootable Media Creator (BoMC) to update the DSA Preboot firmware.
- Note: The BladeCenter HX23 Problem Determination and Service Guide contains an example script for updating firmware via the AMM CLI.