Firmware Update Instructions for The B3 Motherboards

USER'S GUIDE

Revision 1.0

The information in this user's guide has been carefully reviewed and is believed to be accurate. The manufacturer assumes no responsibility for any inaccuracies that may be contained in this document and makes no commitment to update or to keep current the information in this user's guide, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this user's guide, please see our website at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this user's guide at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL SUPER MICRO COMPUTER, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING, OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in an industrial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".

WARNING: This product can expose you to chemicals including lead, known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to www.P65Warnings.ca.gov.

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.

User's Guide Revision 1.0

Release Date: June 17, 2021

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2021 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Preface

The Intended Audience

This user's guide is written for system integrators, IT technicians, and knowledgeable end users. It provides firmware update instructions for the Supermicro B3 motherboards.

About This User's Guide

This user's guide provides hands-on, practical instructions on how to update the firmware used in the B3 motherboards. This user's guide focuses on the BIOS/BMC/CPLD firmware update using the Baseboard Management Controller (BMC) via WebGUI (Graphical User Interface), which is a flexible management system that allows an IT administrator to arrange the contents, page layouts, and features of a web page based on the user's skill set and needs in an effort to enhance user interface experience and maximize platform utility.

To best utilize our products, please bear in mind that all Supermicro products are intended to be installed, configured, and serviced by professional technicians only. For processor/memory updates, please refer to our website at http://www.supermicro.com/products/.

Conventions Used in the Manual

Special attention should be given to the symbol below to properly configure your BIOS settings and to avoid causing damage to your system or injury to yourself:

Note: Important Information is given for proper system setup or for proper firmware configuration.

Warning! Indicates important information is given to avoid possible damages to the system or injuries to yourself.

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc.
	980 Rock Ave.
	San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information)
	support@supermicro.com (Technical Support)
Website:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V.
	Het Sterrenbeeld 28, 5215 ML
	's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information)
	support@supermicro.nl (Technical Support)
	rma@supermicro.nl (Customer Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc.
	3F, No. 150, Jian 1st Rd.
	Zhonghe Dist., New Taipei City 235
	Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Website:	www.supermicro.com.tw

Table of Contents

Preface

Chapter 1 Firmware Update Instructions

1.1 Using the BMC for Firmware Updates 6

1.1.1 How to Update Your Firmware Using the BMC 6

1.1.2 Accessing the Remote BMC via WebGUI 6

1.2 Updating the BMC Firmware 8

1.2.1 Selecting the Type of Firmware (BMC) for Update 8

1.2.2 Selecting an Image File for Firmware (BMC) Update 9

1.2.3 Updating the BMC to a Different Version of BMC 10

1.3 Updating the BIOS Firmware 12

1.3.1 Selecting the Type of Firmware (BIOS) for Update 12

1.3.2 Selecting an Image File for Firmware (BIOS) Update 13

1.4 Updating the CPLD Firmware 15

1.4.1 Selecting the Type of Firmware (CPLD) for Update 15

1.4.2 Selecting an Image File for Firmware (CPLD) Update 16

Chapter 1

Firmware Update Instructions

This chapter provides hands-on, practical instructions on how to perform firmware updates for Supermicro B3 motherboards using the BMC (Baseboard Management Controller) firmware via WebGUI (Graphical User Interface). Section 1.1 provides the overview of firmware updates using the BMC. Section 1.2 provides instructions on how to update the BMC firmware used in a server. Section 1.3 provides instructions on how to update the BIOS firmware. Section 1.4 provides instructions on how to update the CPLD (Complex Programmable Logic device) firmware.

1.1 Using the BMC for Firmware Updates

There are different methods that can be used for firmware updates in a remote server. This user's guide focuses on how to update your firmware by using the remote BMC. Although considered "out-of-band", using BMC WebGUI to update the firmware may be the easiest way for manual firmware updates on certain remote servers.

1.1.1 How to Update Your Firmware Using the BMC

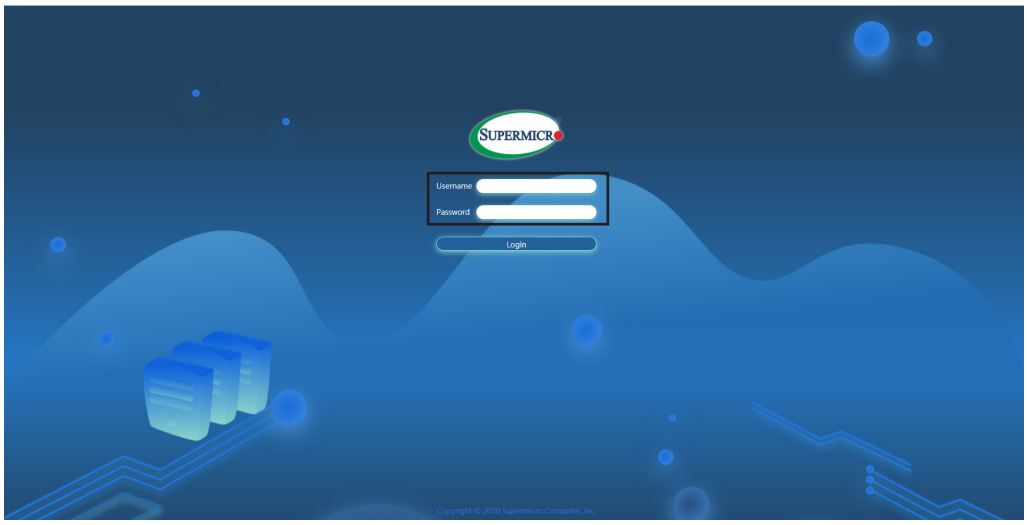
To update the firmware installed in a remote server, which is the host server, using the remote BMC, you will need to have a client browser that can be used to connect to the BMC WebGUI.

1.1.2 Accessing the Remote BMC via WebGUI

To access the remote BMC via WebGUI for firmware updates, follow the steps below.

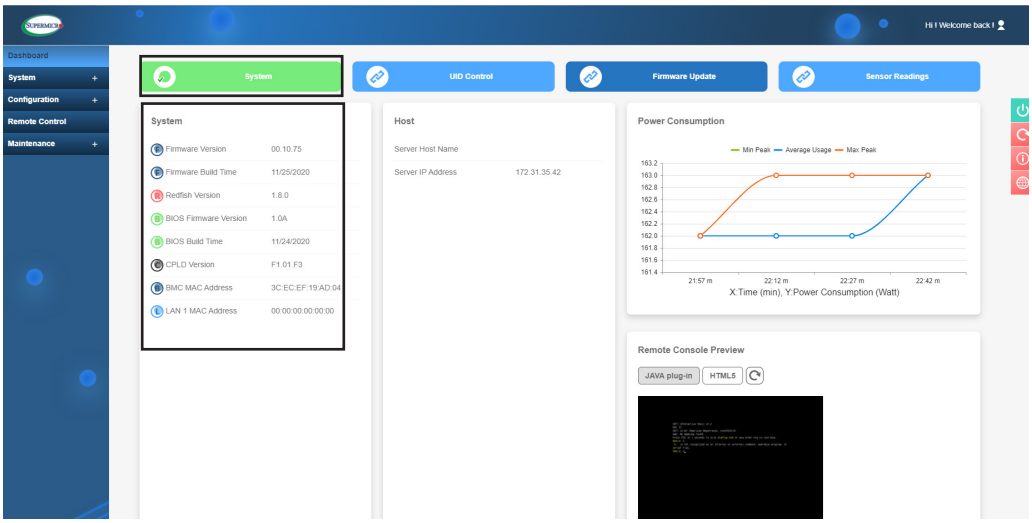
1. Connect a client browser that supports the BMC WebGUI to the remote BMC.
2. Obtain the BMC IP address of the remote server whose firmware you want to update by using a Static IP address that you know of, or by obtaining an IP address using the Dynamic Host Configuration Protocol (DHCP).

3. Enter the IP address of the server that contains the remote BMC in the address bar of the (client) browser you are using to update the firmware, and press <Enter>. The BMC Login screen will display as shown below.



4. Enter your username and your unique password* (See the note below.) in the username and password fields.

5. Click ***Login*** to enter the BMC home page as shown below.



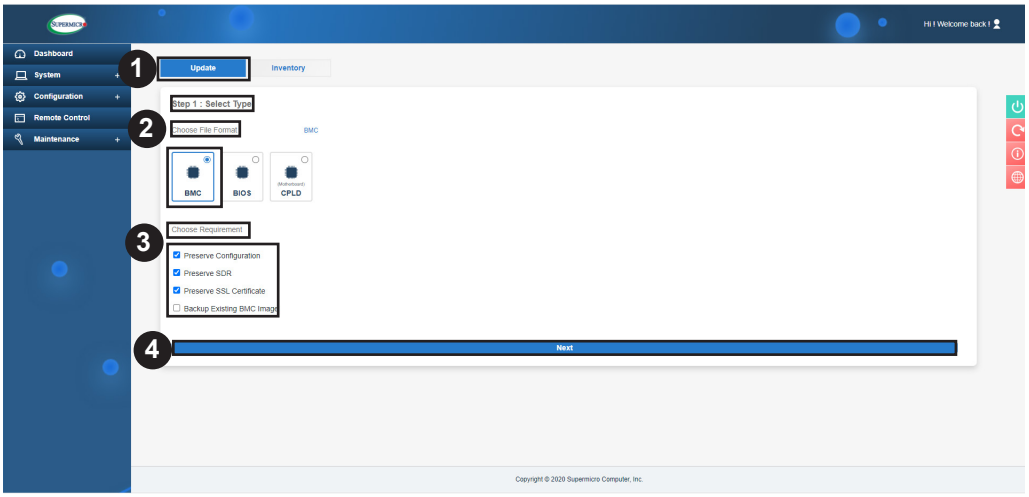
6. Click on the **System** section to check the system information and confirm the updated firmware version, making sure that it is the correct version you want to use.

Note: Every SMCI's standard product is shipped with a unique password for the BMC ADMIN user. This password can be found on a label on the motherboard. When logging in to the BMC for the first time, please use the unique password provided by Supermicro to log in. You can change the unique password to a password of your choice for subsequent logins. *For more information regarding BMC passwords, please visit our website at http://www.supermicro.com/bmcpassword.*

1.2 Updating the BMC Firmware

Follow the instructions given on Section 1.1.2 to access the BMC Login page. Click ***<Login>*** and enter the BMC home page as shown on the screen below.

1.2.1 Selecting the Type of Firmware (BMC) for Update



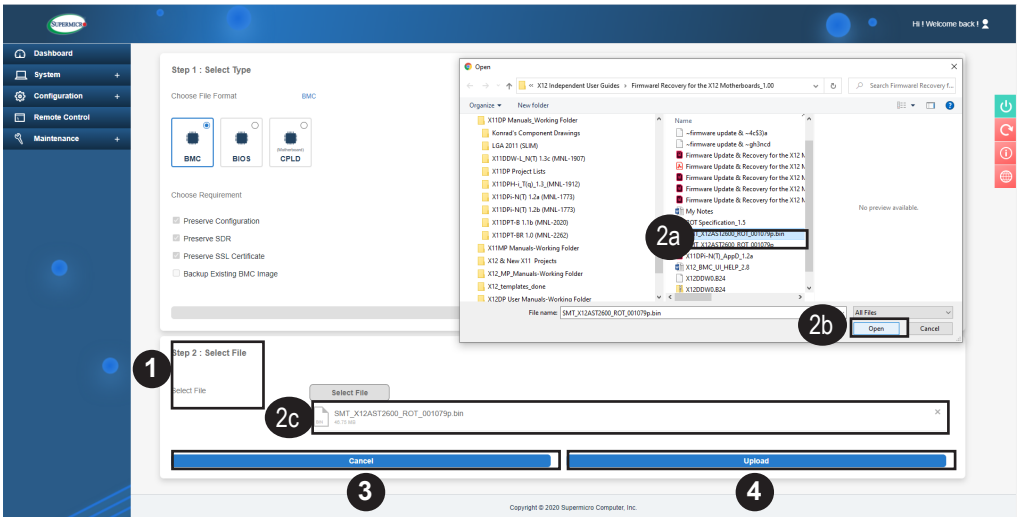
The screen above allows you to update the BMC, BIOS, or CPLD firmware used in your machine. To update your BMC, please follow the instructions below:

1. Select ***Update*** on top of the menu bar for firmware update as shown above.
2. Under *Step 1: Select Type*, choose ***BMC*** as your file format for update as shown above.
3. The screen above also allows you to choose your update requirements. Click on the box in front of a requirement item to choose it. The following items are available for you to choose from:

- Preserve Configuration
- Preserve SDR
- Preserve SSL Certificate
- Backup Existing BMC Image

4. Once you've made the selections, click ***Next*** and the following screen will display.

1.2.2 Selecting an Image File for Firmware (BMC) Update



The screen above allows you to choose an image file for your firmware (BMC) update. To update your BMC to a desired BMC version, follow the instructions below.

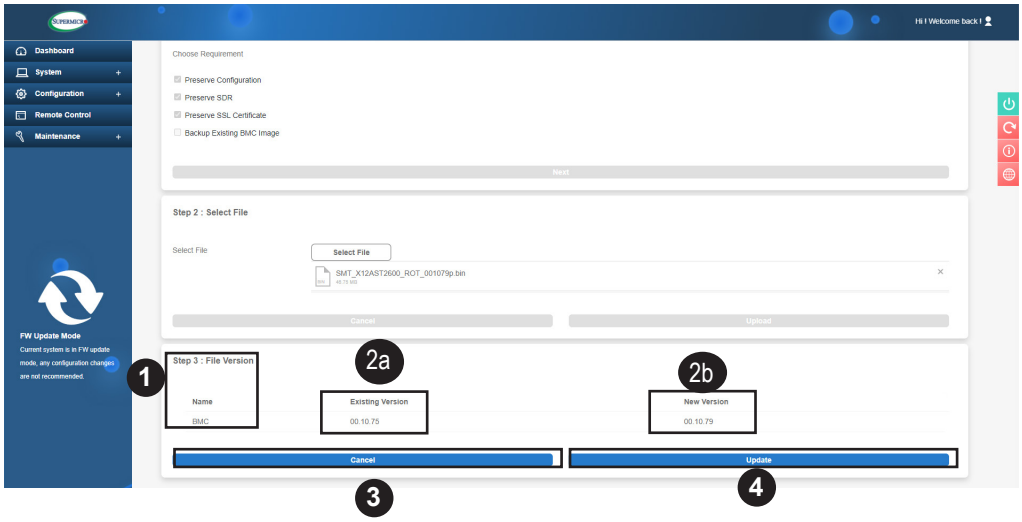
1. Click ***Select File*** 1 to browse the files that are available to you, including the files stored in your local hard drives.

2. Select the file that you want to use for the BMC update 2a and click ***Open*** 2b. The file you've selected will appear on the Select File field 2c as shown above.

3. To cancel your selection, click ***Cancel*** 3 to de-select the file and choose another image file for your BMC update.

4. Once you've finalized your selection, click ***Upload*** 4 to update your BMC using the selected image file.

1.2.3 Updating the BMC to a Different Version of BMC



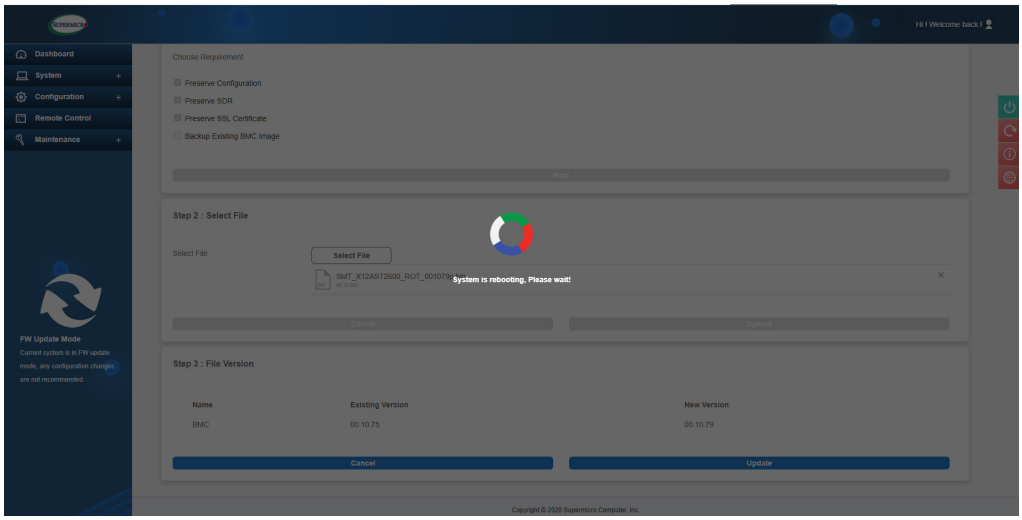
To update your BMC to a different version of BMC, follow the instructions below.

1. After you've uploaded the file you want to use for the BMC update as shown in the previous section, you are ready to update your BMC firmware to the version of your choice. (1)

2. The existing version will display as shown in the box indicated by (2a), and the desired version that you want to update to will appear in the box indicated by (2b).

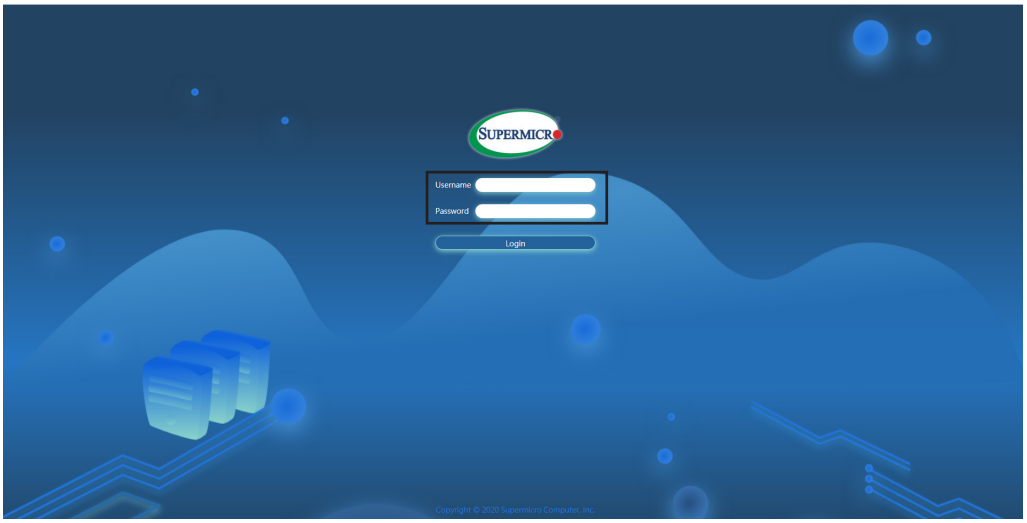
3. To de-select the file that you've just chosen for BMC update, click ***Cancel*** (3) which will allow you to select another file for your BMC update.

4. Once you've finalized your selection, click ***Update*** (4) to update your BMC using your selected image file. Once BMC update is complete, the BMC will be reset accordingly.



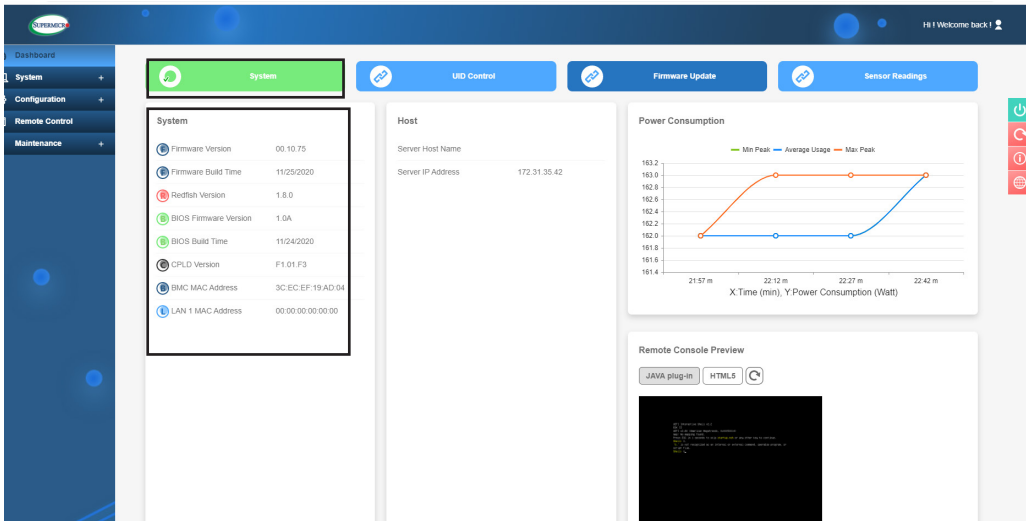
Warning! After BMC upgrading is complete, the BMC firmware will reset itself.

5. The system will display the BMC Login page as shown below.



6. Enter your username and password in the appropriate boxes.

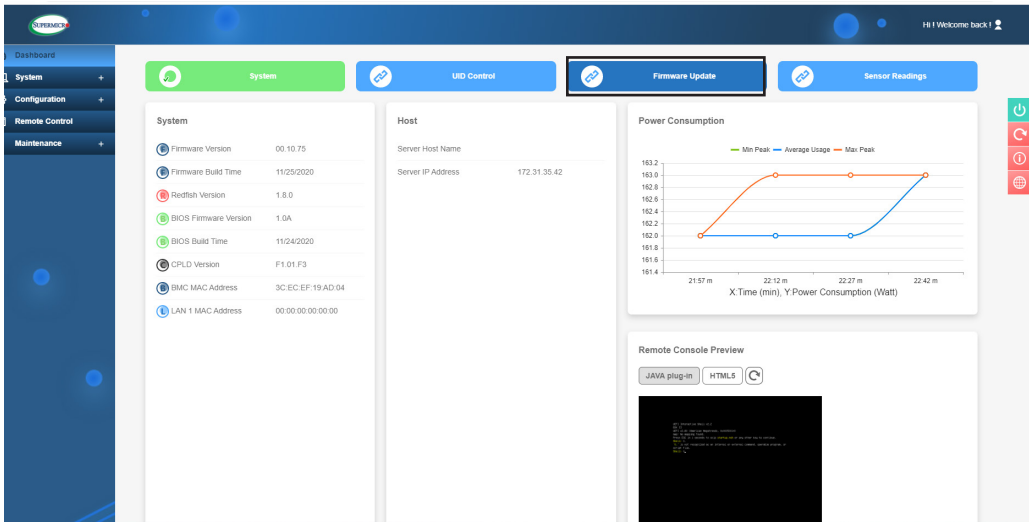
7. Click ***Login*** to enter the BMC home page as shown below.



8. Click on the **System** section to check the system information and confirm the updated firmware version, making sure that it is the correct version you want to use.

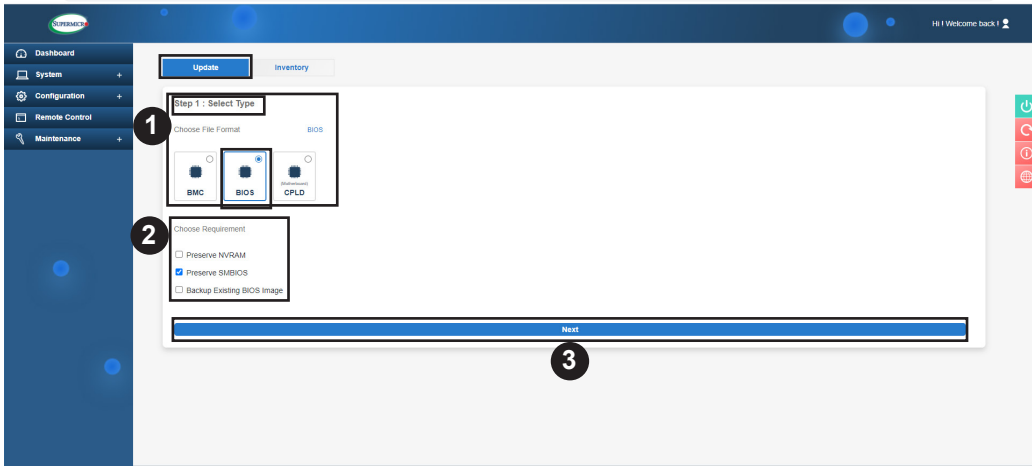
1.3 Updating the BIOS Firmware

Follow the instructions given on Section 1.1.2 to access the BMC Login page. Click ***<Login>*** and enter the BMC home page as shown on the screen below.



When the screen above displays, select Firmware Update and press <Enter>. The following screen will display.

1.3.1 Selecting the Type of Firmware (BIOS) for Update



To update your BIOS utility, please follow the instructions below:

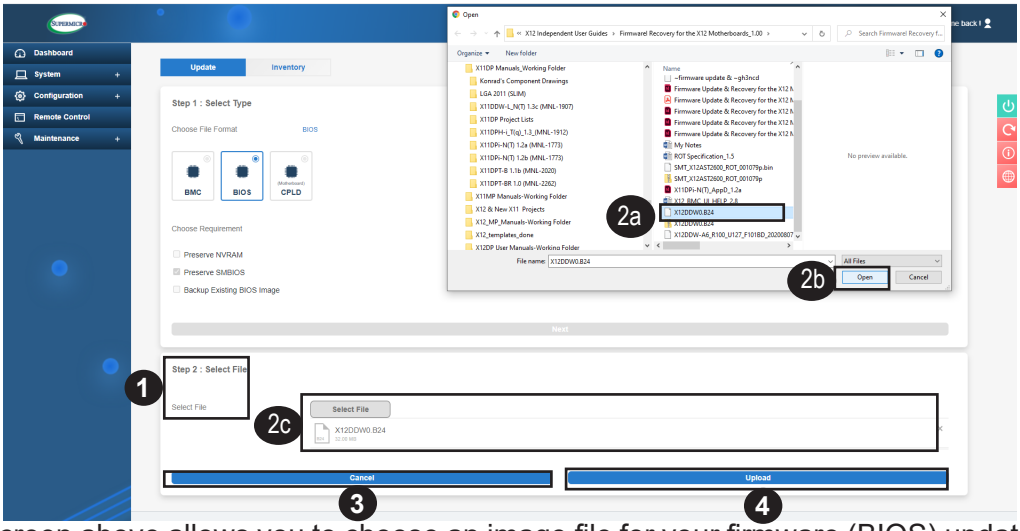
1. Select ***Update*** and choose ***BIOS*** as your file format for update as shown above.

2. To select your requirements for the BIOS update, click the box in front of an item to select it. The following items are available for your use.

- Preserve NVRAM
- Preserve SMBIOS
- Backup Existing BIOS Image

3. Once you've made the selections, click ***Next***, and the following screen will display.

1.3.2 Selecting an Image File for Firmware (BIOS) Update



The screen above allows you to choose an image file for your firmware (BIOS) update. Follow the instructions below to update your BIOS to a desired BIOS version.

1. Click ***Select File*** 1 to browse the files that are available to you, including the files stored in the hard drives of your machine used to update the BIOS for the host server.

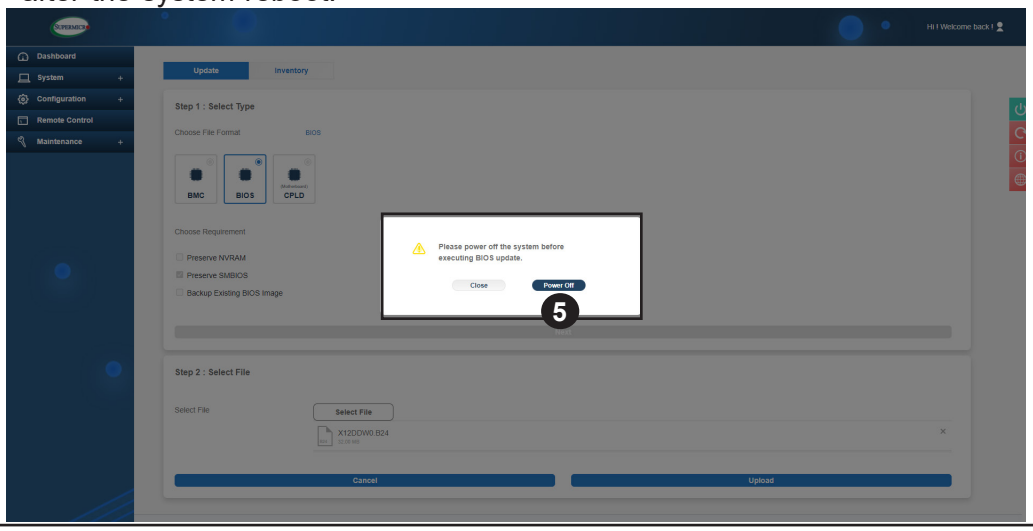
2. Select the file that you want to use for the BIOS update 2a and click ***Open*** 2b. The file you've selected will appear on the Select File field 2c as shown above.

3. To de-select the file that you've just chosen for BIOS update, click ***Cancel*** 3 which will allow you to select another image file for your BIOS update.

4. Once you've finalized your selection, click ***Upload*** 4 to update your BIOS using your selected image file.

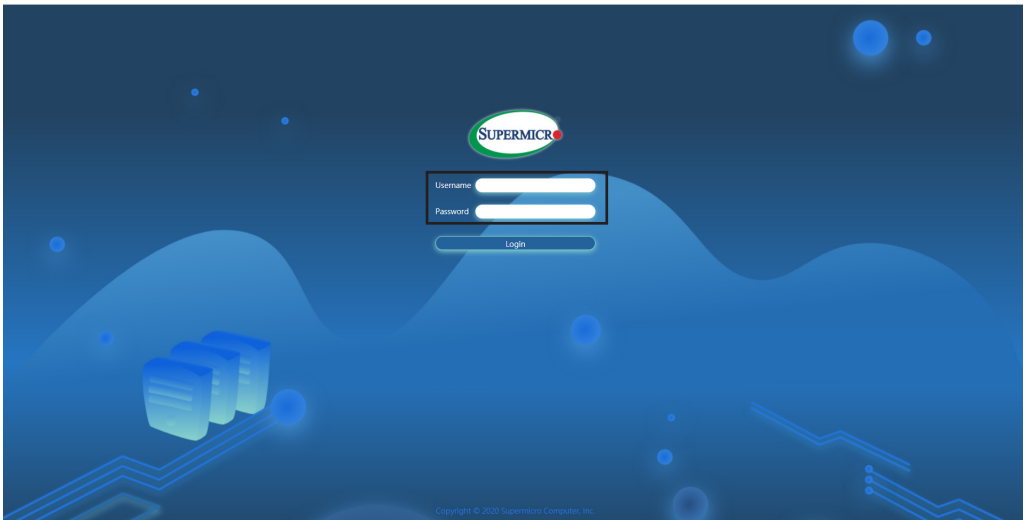
5. A warning will display asking you to power off the system before you proceed with BIOS update as shown below. Click ***Power Off*** before updating your BIOS.

Warning! Be sure to power off your system before updating your BIOS! After BIOS upgrading is complete, the system will reboot, and the new BIOS utility will take effect after the system reboot.



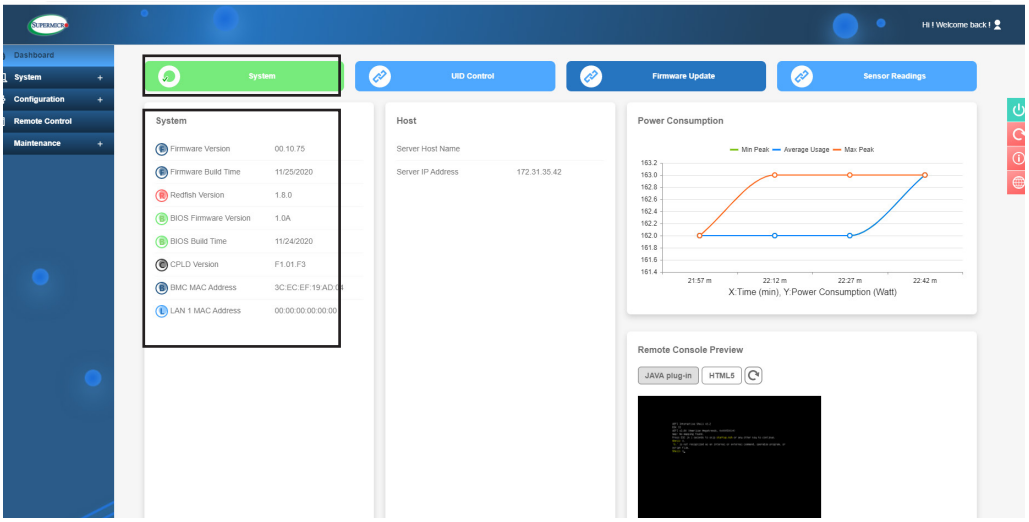
6. When BIOS upgrading is complete, the system will reboot.

7. After the system reboots, the BMC Login page will display as shown below.



8. Enter your username and password in the appropriate boxes on the BMC Login page.

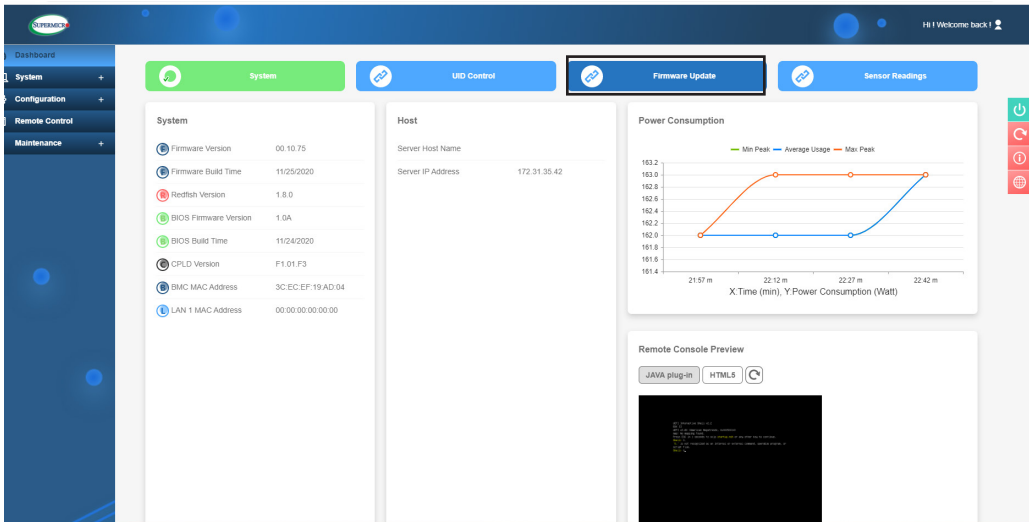
9. Click ***Login*** to enter the BMC home page as shown below.



10. Click on the **System** section to check the system information and confirm the updated firmware version, making sure that it is the correct version you want to use.

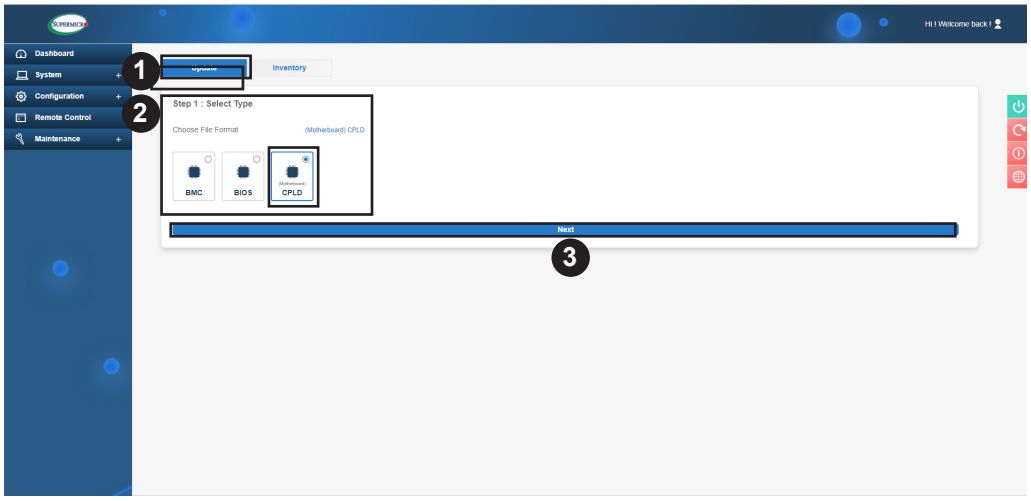
1.4 Updating the CPLD Firmware

Follow the instructions given on Section 1.1.2 to access the BMC Login page. Click ***<Login>*** and enter the BMC home page as shown on the screen below.



When the screen above displays, select Firmware Update and press <Enter>. The following screen will display.

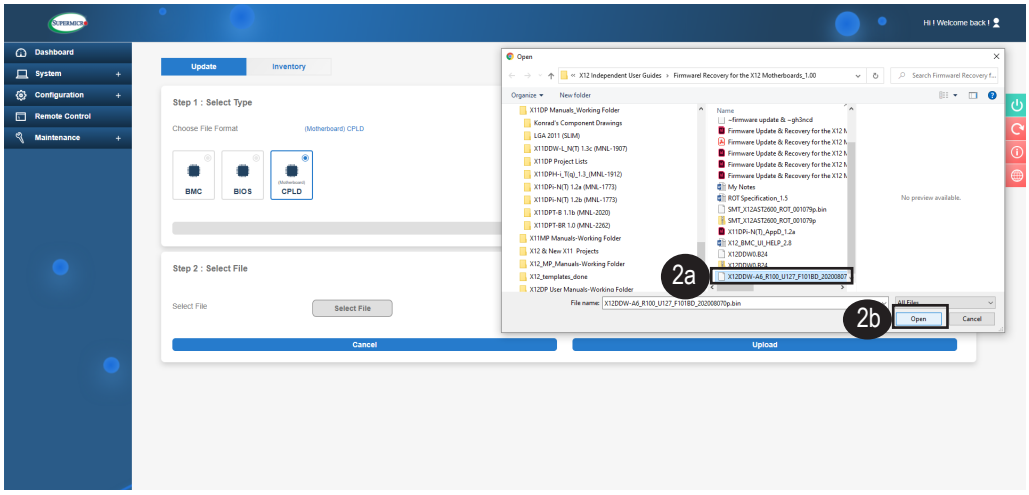
1.4.1 Selecting the Type of Firmware (CPLD) for Update



To update the CPLD (Complex Programmable Logic Device), follow the steps below.

1. Select ***Update*** on top of the menu bar for firmware update as shown above.
2. Under *Step 1: Select Type*, choose ***CPLD*** as your file format for update as shown above.
3. Once you've selected CPLD for firmware update, click ***Next*** and the following screen will display.

1.4.2 Selecting an Image File for Firmware (CPLD) Update

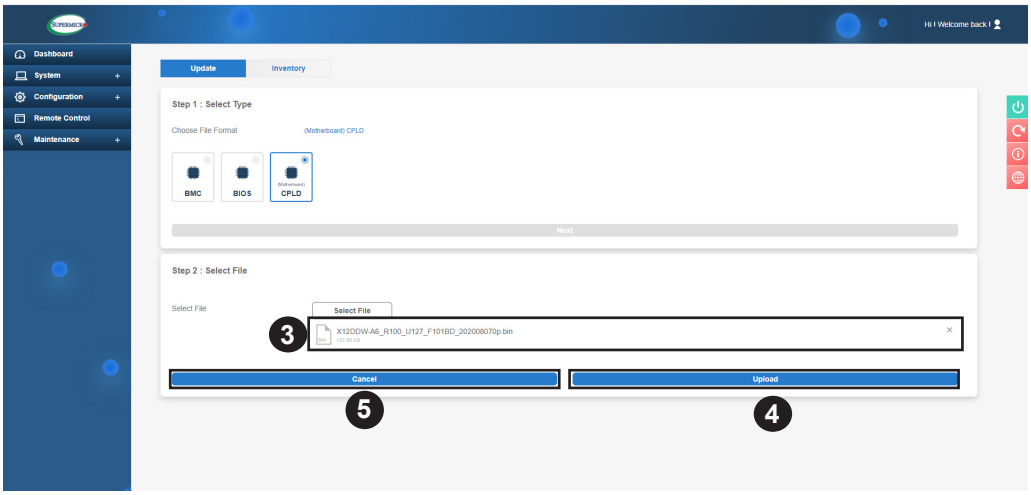


Follow the steps below to select an image file to update your Complex Programmable Logic Device (CPLD) to a desired firmware version.

1. Click ***Select File*** 1 to browse the files that are available to you, including the files stored in the hard drives of the local machine which you use to update the CPLD firmware for the remote server.

2. From the screen as shown above, select the file that you want to use for your CPLD update 2a and click ***Open*** 2b.

3. The file you've selected will appear on the Select File field 3 as shown below.

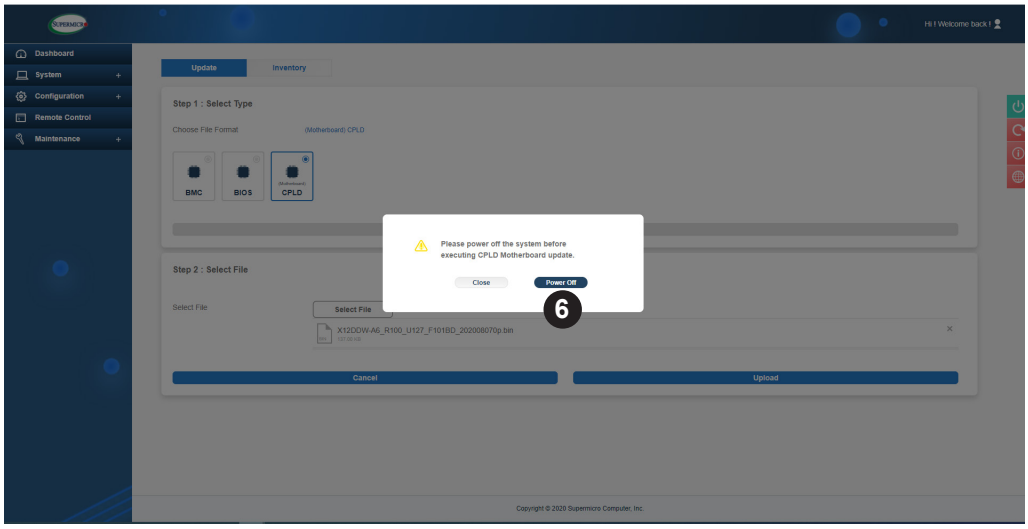


4. To de-select the file that you've just chosen for CPLD update, click ***Cancel*** 4 which will allow you to select another file to update your CPLD firmware.

5. Once you've finalized your selection, click ***Upload*** 5 to update your CPLD using the selected image file.

6. A warning will display asking you to power off the system for CPLD update. Click ***Power Off*** as shown below.

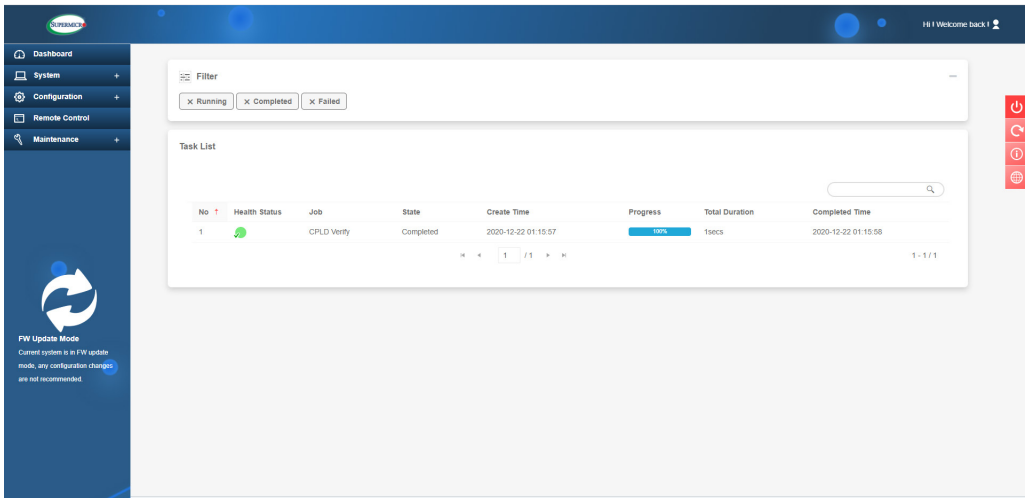
Warning! Be sure to power off your system before you start to update your CPLD with the image file that you've just uploaded to the system!



7. When the CPLD update is complete, the system will reboot as indicated by a warning statement displayed on the screen.

Warning! After CPLD upgrading is complete, the system will reboot for the new CPLD firmware to take effect!

8. After the system reboot, the health status of the system will display as shown below.



9. To go back to the BMC Login page, please re-load the web-page by following the instructions given in Section 1.1.2 to access the remote BMC via WebGUI on page 6.

10. Click on the **System** section (on the left side of the screen) to check the system information and confirm the updated firmware version, making sure that it is the correct version you want to use.