



Intel® Active System Console and Intel® Multi-Server Manager Replacement

White Paper

Rev 1.0

March 2020

<Blank page>

Document Revision History

Date	Revision	Changes
March 2020	1.0	Initial release.

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

© Intel Corporation

Table of Contents

1. Overview.....	6
2. Intel® Active System Console.....	7
2.1 Integrated BMC Web Console.....	7
2.2 Comparing Intel® Active System Console (IASC) to the Integrated BMC Web Console	7
2.3 Configuring the Integrated BMC Web Console	8
2.3.1 BIOS Setup.....	8
3. Intel® Multi-Server Management (MSM).....	12
3.1 Intel® Data Center Manager (DCM).....	12
3.2 Comparing Intel® MSM to Intel® DCM	12
3.3 Configuring the Intel® DCM with the Intel® SDPTool Plugin	13
Appendix A. Glossary	17

List of Figures

Figure 1. BIOS setup screen.....	8
Figure 2. Server Management screen	9
Figure 3. BMC LAN Configuration screen	9
Figure 4. User Configuration screen.....	10
Figure 5. Integrated BMC Web Console home screen.....	11
Figure 6. BMC FRU screen.....	13
Figure 8. SDPTool setup and config location	14
Figure 9. Permit policy file.....	15
Figure 10. DCM console showing firmware versions	15
Figure 11. Firmware update screen.....	16

List of Tables

Table 1. Comparing Intel® Active System and BMC EWC features.....	7
Table 2. Comparing Intel® MSM to Intel® DCM	12

1. Overview

In January 2020, Intel announced the end of life of the Intel® Active System Console and Intel Multi-Server Manager. This whitepaper discusses replacement options and instructions for how to set up these replacement options.

This whitepaper focuses on Intel® Xeon® Scalable Processors with Intel® C620 Series Chipsets based Intel® Server Boards (formerly Purley) and Intel® Xeon® Processor E5-2600 v3/v4 Family based Intel® Server Boards (formerly Grantley) products. Instructions below are for Purley products, but the steps should be very similar on Grantley.

- Purley
 - Intel Server Board S2600WF Family
 - Intel Server Board S2600BP Family
 - Intel Server Board S2600ST Family
 - Intel Server Board S2600WK Family
- Grantley
 - Intel Server Board S2600WT Family
 - Intel Server Board S2600KP Family
 - Intel Server Board S2600TP Family
 - Intel Server Board S2600CW Family
- Single Socket
 - Intel Server Board S1200SP Family

2. Intel® Active System Console

The following sections explain the Integrated Baseboard Management Controller (BMC) Web Console, compares the feature differences between the Integrated BMC Web Console and the Intel® Active System Console, and gives instructions for configuring the Integrated BMC Web Console.

2.1 Integrated BMC Web Console

The best replacement for the Intel Active System Console is to use the embedded web console in the BMC. Both the Intel Active System Console and BMC EWS are designed to manage the hardware on a single system only. Both can be accessed by opening a web browser on the client and setting the URL to the IP address of the remote system. The BMC EWS contains more functionality than the Intel Active System Console with only a slightly different user experience. The BMC EWS can be put on the dedicated management network, a recommended security option.

2.2 Comparing Intel® Active System Console (IASC) to the Integrated BMC Web Console

The following table shows the high-level differences between the IASC and the Integrated BMC Web Console.

Table 1. Comparing Intel® Active System and BMC EWC features

Features	Intel® Active System Console	Integrated BMC Web Console
Remote Access over Web console	Yes	Yes
Local Access via GUI	Yes	
IP address	Same as host	Isolated from host
Agentless		Yes
Access when operating system is down or system is off		Yes
Health Information	Sensor and SEL	Sensor and SEL
Email Alerting	Yes	Yes
SNMP Alerting	Yes	Yes
BMC User Management	Yes	Yes
Node Manager Settings	Yes	Yes
System and FRU Information	Yes	Yes
Diagnostics	Report generation for Asset Info, BMC Settings, Sensor & SEL	Debug Log (Asset, Settings, Sensor, SEL, Registers, Power Supply Info), POST Codes
Identify LED	Yes	Yes
Power Actions		Yes
Launch SOL or KVM		Yes
Virtual Media Redirection		Yes
BMC Configuration		Yes
Firmware Update		Yes
BIOS Configuration		Yes

2.3 Configuring the Integrated BMC Web Console

Users can use the same network cable on either LAN 1 or LAN 2 on the motherboard as they use for the host, or they can use a separate cable connected to the dedicated management network. For security reasons, Intel recommends using the dedicated management network.

There are multiple ways that users can configure the Integrated BMC Web Console. They can use the Intel SysCfg utility in the Extensible Firmware Interface (EFI) shell or in the operating system. They can also use the IPMItool from most Linux operating systems. However, the easiest way to configure is using the BIOS setup. This whitepaper only lists BIOS setup instructions.

2.3.1 BIOS Setup

1. While booting up the system press <F2> to go into BIOS setup.

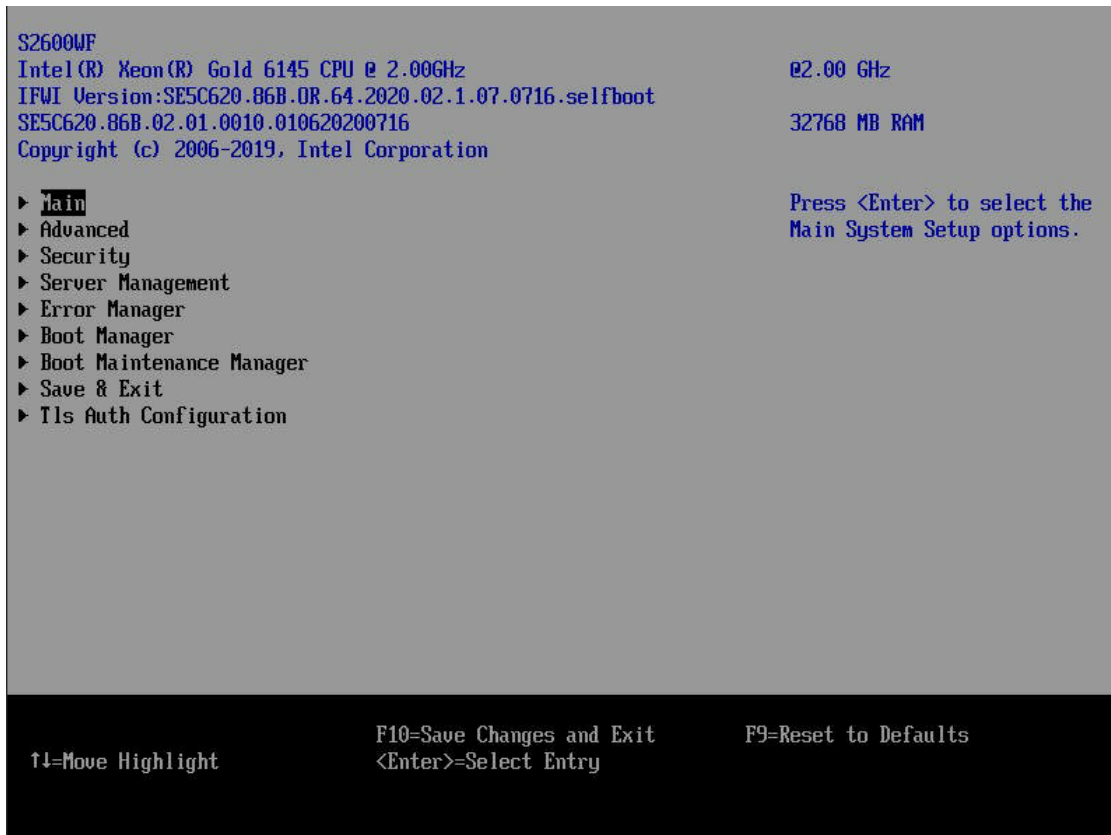


Figure 1. BIOS setup screen

2. Select **Server Management**.

The Server Management screen opens.

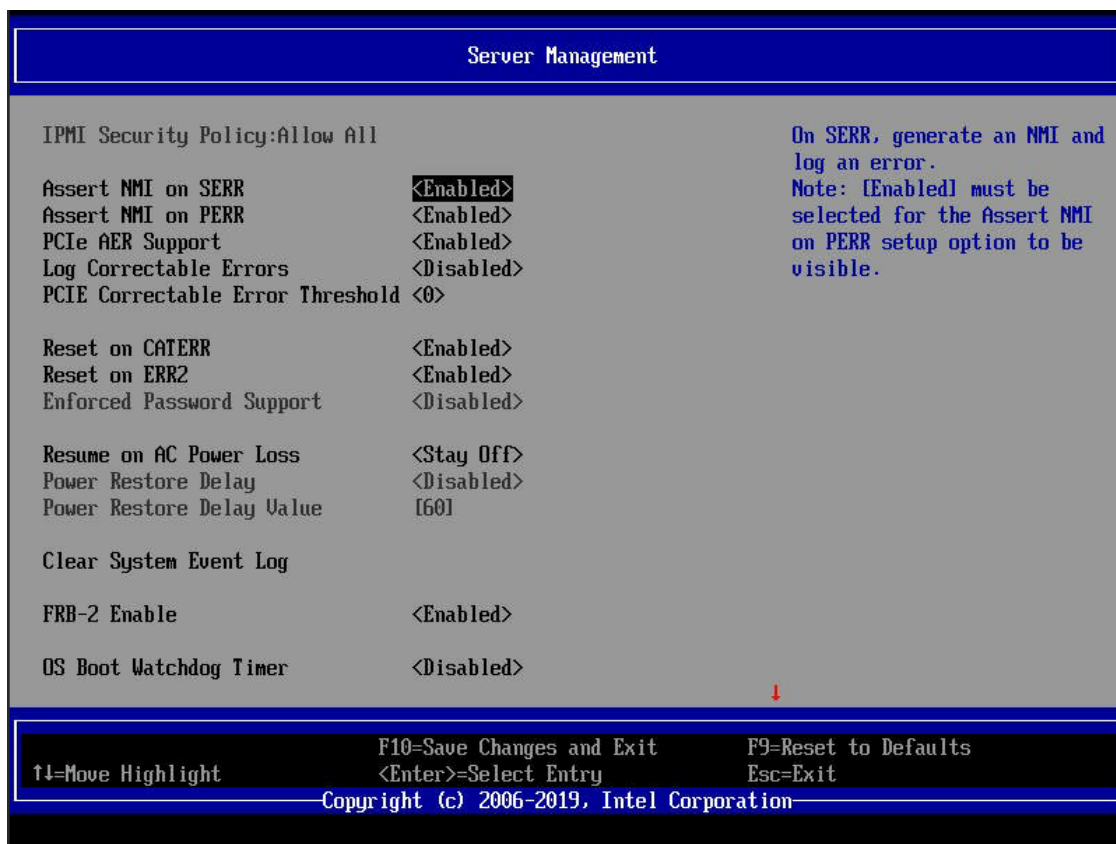


Figure 2. Server Management screen

3. Scroll to the BMC LAN Configuration.

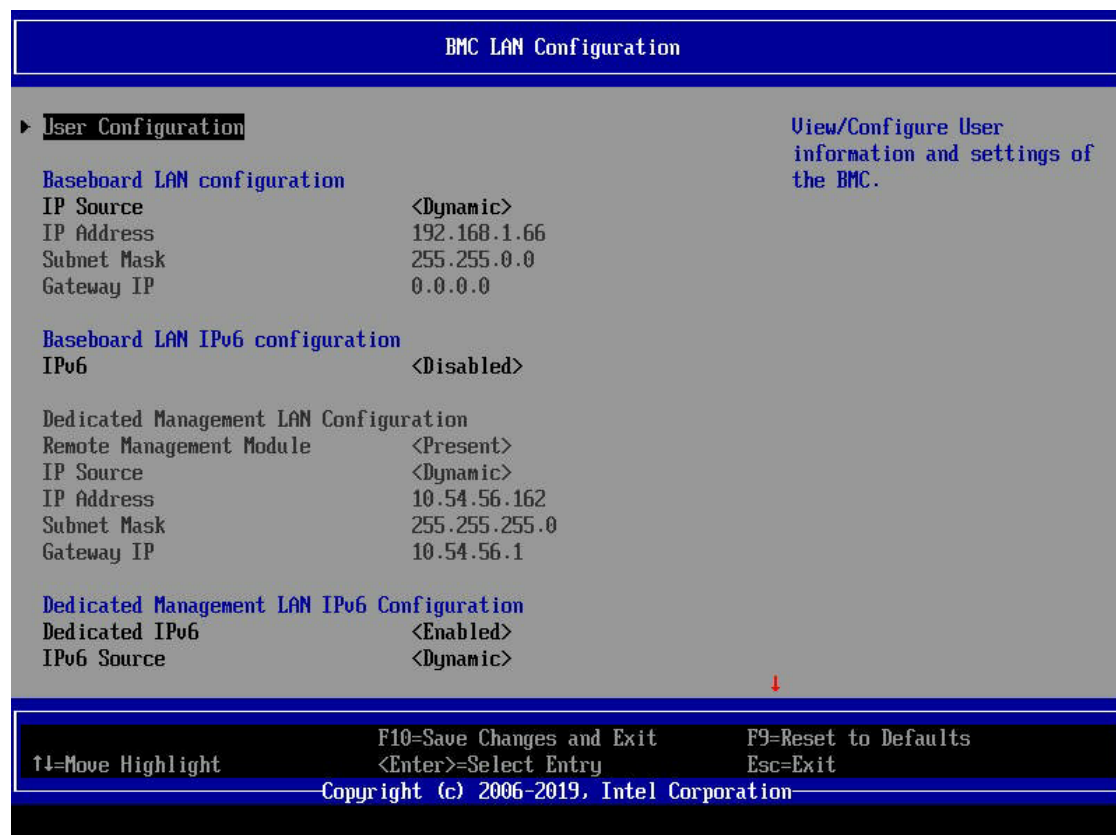


Figure 3. BMC LAN Configuration screen

4. Select **User Configuration** to setup a user account.

User Configuration		
Enable Complex Password	<Disabled>	Press <Enter> to edit User Name. User Name is a string of 1 to 16 alpha-numeric characters or '.', '_' or '-', and must begin with alpha-numeric character or '_'. User Name cannot be changed for User1 (anonymous).
User ID	anonymous	
Privilege	<No Access>	
User Status	<Disabled>	
User Password		
User ID	User2	
Privilege	<Administrator>	
User Status	<Enabled>	
User Name	admin	
User Password		
User ID	User3	
Privilege	<Administrator>	
User Status	<Enabled>	
User Name	admin	
User Password		
User ID	User4	
Privilege	<Operator>	
User Status	<Enabled>	

↓

F10=Save Changes and Exit F9=Reset to Defaults
 ↑↓=Move Highlight <Enter>=Select Entry Esc=Exit
 Copyright (c) 2006-2019, Intel Corporation
 Configuration changed

Figure 4. User Configuration screen

For security reasons, Intel recommends not enabling anonymous user.

5. Select a user from 2-4.
6. Set Privilege to **Administrator** and User Status to **Enabled**.
7. Create a username and password.
8. Return to the BMC LAN Configuration screen (see Figure 3).
9. If using a shared NIC with the host on NIC 1, use Baseboard LAN Configuration.
10. Either set the IP Source to **Dynamic** to get a DHCP address, or **Static** and fill out the IP Address, subnet mask, and gateway IP.
11. If using the dedicated management NIC, configure the Dedicated Management LAN Configuration and set it to either **Dynamic** or enter a static address.
12. Press **<F10>** to save the changes and exit.
13. If using the dynamic/DHCP: after rebooting, go back into the BIOS setup to see the IP address issued, or check the DHCP server.
14. Go to any client machine that has access to that network, open a web browser, and type in the issued IP address.
15. Login with the username and password that was created.

The Integrated BMC Web Console home screen opens (Figure 5).

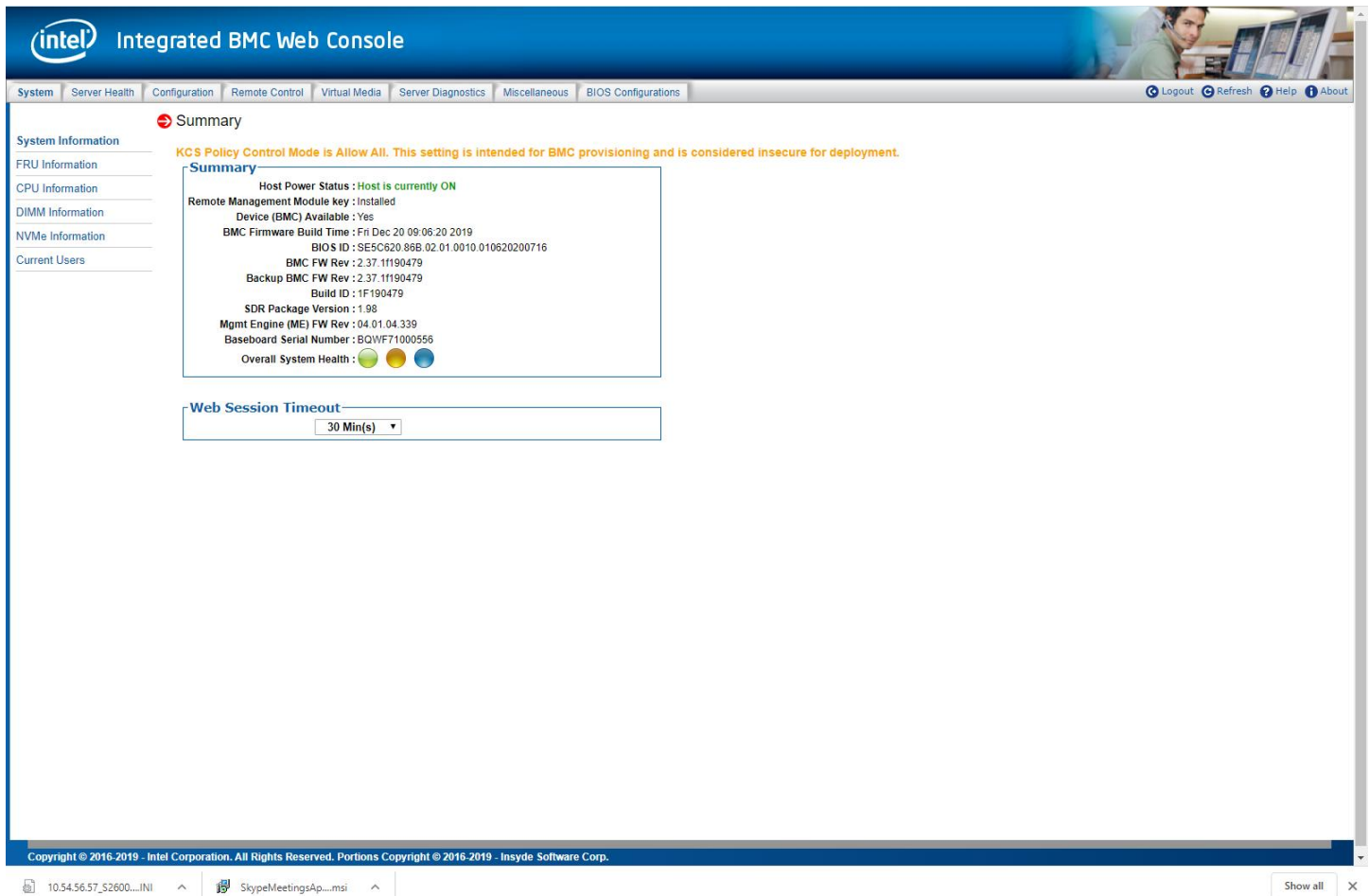


Figure 5. Integrated BMC Web Console home screen

The Integrated BMC Web Console allows customers to monitor the individual server's health, view sensors, event logs, and other diagnostics, configure BMC settings, provide remote access, and configure BIOS settings.

3. Intel® Multi-Server Management (MSM)

The following sections explain the Intel® Data Center Manager (DCM), compares the features between the Multi-Server Management (MSM) and the DCM, and gives instructions for configuring the DCM using the Intel SDPTool plugin.

3.1 Intel® Data Center Manager (DCM)

The best replacement for the Intel Multi-Server Manager is to use the Intel Data Center Manager with the Intel Server Debug and Provisioning Tool (Intel SDPTool) Plugin. This provides all the functionality that was provided from Intel MSM, but with a much better user experience. The Intel MSM was command line only, whereas the Intel DCM has options for a full GUI or Software Development Kit (SDK). In addition to most of the functionality provided by Intel MSM, the Intel DCM also provides an extensive thermal and power set of management capabilities. Finally, the Intel MSM had a command line tool that requires extra scripting or the use of the Nagios open source software to refresh information that it was collecting, whereas, the DCM automatically refreshes all the data that displays on the screen.

3.2 Comparing Intel® MSM to Intel® DCM

The following table compares the Intel MSM and Intel DCM features.

Table 2. Comparing Intel® MSM to Intel® DCM

Features	Intel® Multi-Server Manager	Intel® Data Center Manager
GUI	Requires Nagios	Yes
SDK/Command Line	Yes	Yes
OS Support	Linux only	Windows and Linux (Linux only for SDPTool plugin where noted by ** below)
Cost	Free	30-day free trial and then software license is required for a fee
SNMP & Email Alerting	Yes	Yes
Discovery and Grouping	Yes	Yes
Consistency Check	Yes	
Health Monitoring	Yes	Yes
Firmware Update	Yes	Yes **
Custom Deploy*	Yes	Yes **
BMC Configuration	Yes	Yes **
BIOS Configuration	Yes	Yes **
Power & Thermal Statistics	Yes	Yes
Power Actions	Yes	Yes
Virtual Media		Yes **
RAID Configuration	Yes (limited)	
RAID Health	Yes (inband only)	
SSD Health	Yes (inband only)	Yes (inband only)
Firmware Versions	Yes	Yes **
Node Manager		Yes
Energy Management		Yes
Data Center Infrastructure Management		Yes
Asset Inventory		Yes

* The Custom Deploy feature allows users to build a custom package that performs any task possible from the EFI shell.

** These items require an intel® SDPTool plugin. For steps on how to install the Intel® SDPTool and connect to the DCM, follow the steps in the next section.

3.3 Configuring the Intel® DCM with the Intel® SDPTool Plugin

If using the Intel® SDPTool plugin, users must install on a supported Linux operating system.

To download the Intel DCM and user guide, which contains instructions for installing the Intel DCM, go to: <https://downloadcenter.intel.com/download/28894> and follow the installation instructions.

For help with installation and support, contact dcmsupport@intel.com.

After the install is complete, download and install the Intel Server Debug and Provisioning Tool on the same server as the Intel DCM from the following link:

<https://downloadcenter.intel.com/download/29257/Intel-Server-Debug-and-Provisioning-Tool?wapkw=SDPTool>.

The following steps are for connecting the Intel SDPTool to the DCM and enabling all features designated in Table 2 footnote **.

1. Create a configuration file called SDPTool_Config.xml for all platform types that firmware updates or BIOS configurations will be done on. An example XML file can be found in the folder where DCM was installed (e.g. /opt/intel/datacentermanager) under the Samples folder.
 - a. Copy the file to any location on the DCM server (e.g. /usr/local/SDPTool).
 - b. For each server model managed by DCM, the configuration file should have an entry with the board product name and path where the firmware package will be located. To get the board product name, look it up in the Integrated BMC Web Console, shown below.

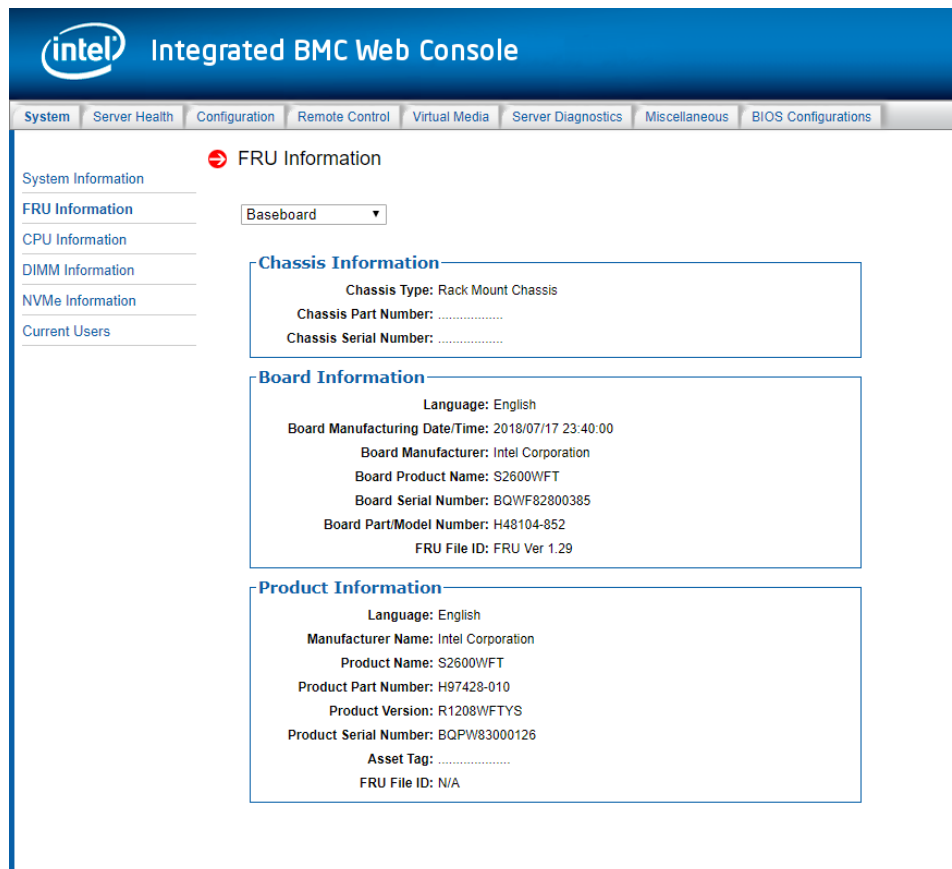


Figure 6. BMC FRU screen

- Download the System Update Package from the Intel website and unzip it into the DCM server folder for each platform type specified in the XML file above.
- Copy the file: FirmwareProvisioningConfig.xml found in the samples folder (/opt/intel/datacentermanager/samples) to the conf folder (/opt/intel/datacentermanager/conf).
- Change the owner of the FirmwareProvisioningConfig.xml to dcm by issuing the following command:

```
chown dcm
/opt/intel/datacentermanager/conf/FirmwareProvisioningConfig.xml
```

- Edit the FirmwareProvisioningConfig.xml and set the right value for **SDPTool_SetupLocation** and **SDPTool_ConfigLocation** in this configuration file. Typically, this would be /usr/local/SDPTool and /usr/local/SDPTool/SDPTool_Config.xml, as shown in the figure below.

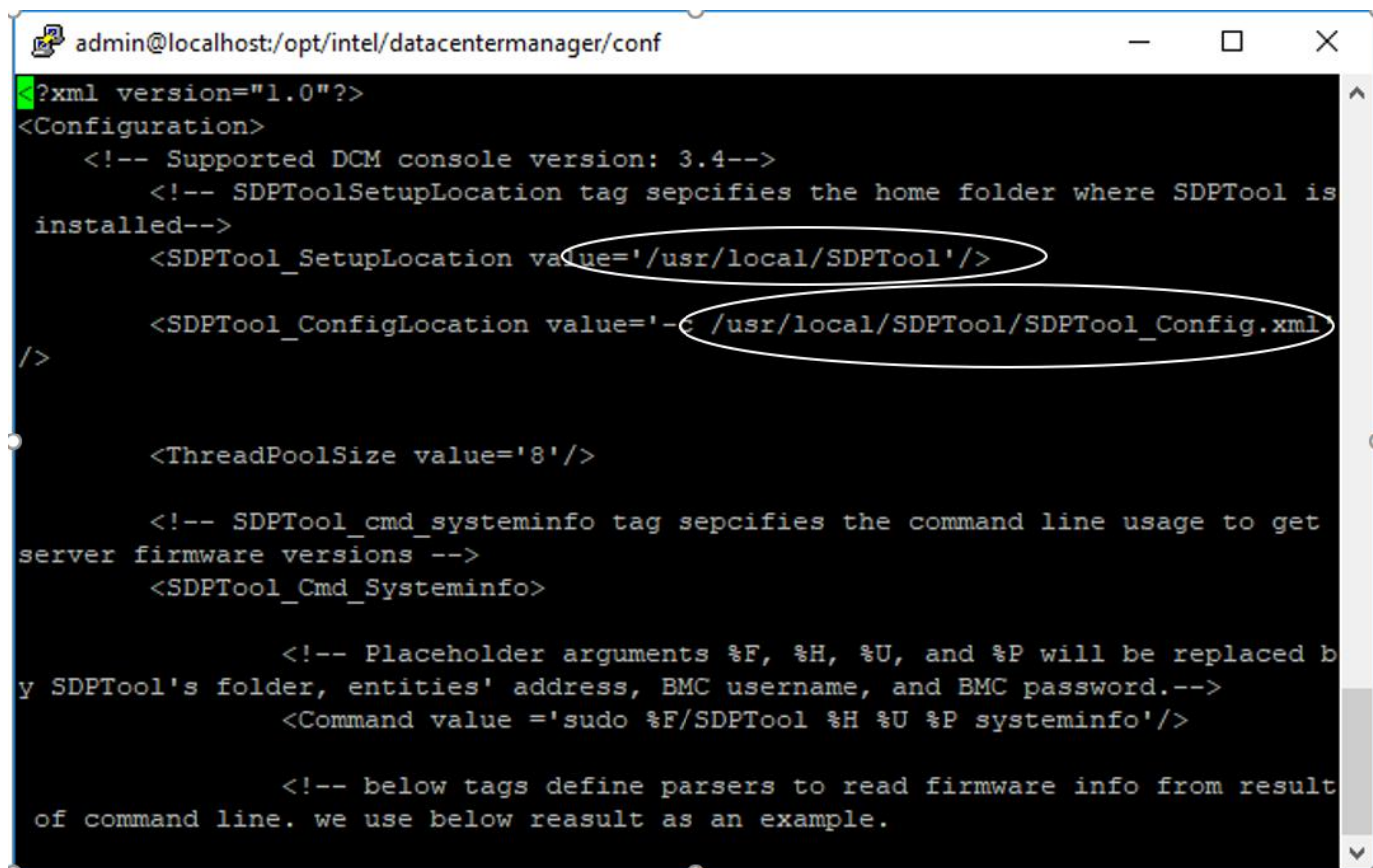


Figure 7. SDPTool setup and config location

- Run GrantExternalTool.sh (as root) from the Intel DCM console to configure the correct access for the following files. To do this, first change directory (cd) into the DCM folder and then issue each command below.

```
cd /opt/intel/datacentermanager/bin
./GrantExternalTool.sh add dcm /usr/local/SDPTool dcm
./GrantExternalTool.sh add dcm /bin/cp
./GrantExternalTool.sh add dcm /bin/chmod
```

The items below should be added to the file /etc/sudoers.


```
dcm ALL=(ALL) NOPASSWD:/usr/local/SDPTool/SDPTool
dcm ALL=(ALL) NOPASSWD:/bin/cp
dcm ALL=(ALL) NOPASSWD:/bin/chmod
```

7. Append into the file /opt/intel/datacentermanager/bin/allpermit.policy;
permission java.io.FilePermission "<<ALL FILES>>", "execute"; (shown in figure below).

```
[root@ftaol-desk11 bin]# vi /etc/sudoers
[root@ftaol-desk11 bin]# vi /opt/intel/datacentermanager/bin/allpermit.policy

permission java.net.URLPermission "http:*", "*:*";
permission java.net.URLPermission "https:*", "*:*";
permission java.net.URLPermission "file:*", "*:*";

permission org.osgi.framework.AdminPermission "*", "lifecycle,class,execute,extensionLifecycle,listener,metadata,resolve,resource,startlevel,context";
permission org.osgi.framework.ServicePermission "*", "register,get";
permission org.osgi.framework.BundlePermission "*", "provide,require,host,fragment";
permission org.osgi.framework.PackagePermission "*", "export,import";
permission org.osgi.framework.AdaptPermission "*", "adapt";

permission org.eclipse.equinox.log.LogPermission "*", "log";

permission java.util.logging.LoggingPermission "control";
permission javax.management.MBeanServerPermission "*";
permission javax.management.MBeanPermission "*", "*";
permission java.lang.management.ManagementPermission "monitor";
permission java.io.FilePermission "<<ALL FILES>>", "execute";
};
```

Figure 8. Permit policy file

8. To avoid exposing sensitive information, mount /proc with hidepid option.
 - cd /opt/intel/datacentermanager/bin
 - mount -o remount,rw,hidepid=2 /proc
9. Restart DCM services:
 - /opt/intel/datacentermanager/startdcm.sh restart
10. Log into the DCM Console, go to Devices, hover the mouse over the BMC version and verify all other versions are shown, similar to the following figure.

Device List						
Selected Devices: 1 Total Devices: 1						
	Name	Address	Device Type	Protocol	Derated Power	Firmware Version
<input checked="" type="checkbox"/>	Wolf Pass	10.239.172.235	Server	IPMI	400	BMC: 2.22
						BMC: 2.22 BIOS: SE5C620.86B.02.01.0009.0 92820190230 ME: 04.01.04.323 SDR: 01.96

Figure 9. DCM console showing firmware versions

11. For a firmware update, select one or more systems and click **Provisioning** in the upper right-hand corner of the screen.
12. Follow the instructions on the screen.

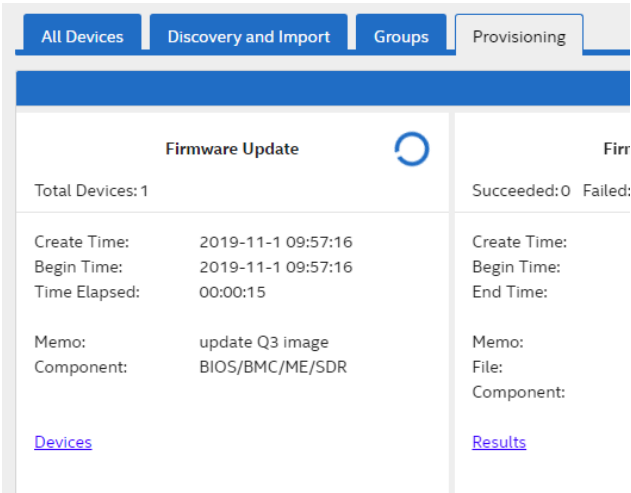


Figure 10. Firmware update screen

If the update is successful, users can go to the provisioning screen and monitor the progress and see the results of the update.

A successful update indicates that the plugin was installed correctly.

Appendix A. Glossary

This appendix contains important terms used in the preceding chapters.

Terms	Definitions
BMC	Baseboard Management Controller
BMC EWS	BMC Embedded Web Server
DCM	Intel® Data Center Manager
DHCP	Dynamic Host Configuration Protocol
FRU	Field Replacement Units
FW	Firmware
IASC	Intel® Active System Console
KVM	Keyboard Video Mouse
MSM	Intel® Multi-Server Manager
SDK	Software Development Kit
SDPTool	Intel® Server Debug and Provisioning Tool
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN