Hewlett Packard Enterprise

Configuring HPE Superdome Flex 280 Server

Abstract

Server configuration, operation, and administration procedures.

Part Number: 10-192002-Q221
Published: April 2021
Edition: 4

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

AMD and the AMD EPYC™ and combinations thereof are trademarks of Advanced Micro Devices, Inc.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.

Revision history

Part number	January 2021	Edition	Summary of changes
1012865453-CFG-0121A	January 2021	3	
1012865453-CFG-0121	January 2021	2	• Revise chassis depth details • Update chassis architecture diagrams
1012865453-CFG-1120	November 2020	1	First edition.

Contents

System overview

HPE Superdome Flex 280 Server is a 5U rackmounted system that uses in-memory computing technology to enable real-time transactional and analytical processing.

Every Superdome Flex 280 Server has a base chassis providing BaseIO, management interfaces, and boot support. One expansion chassis can be added to expand the system to eight processor sockets. The required base chassis provides platform management through an embedded Rack Management Controller (eRMC).

NOTE: Although the user or reader may encounter both RMC and eRMC terminology in displays and documentation, the preferred term is always RMC.

Key features of Superdome Flex 280 Server

For complete details of the server hardware and configuration options, see **HPE Superdome Flex 280 Server QuickSpecs**.

Features of HPE Superdome Flex 280 Server include:

- Supports 2, 4, 6, and 8 processor sockets with Intel Xeon 53xx, 63xx, and 83xx (Cooper Lake) processors in a two-chassis system (for example, when populated with 28-cores per processor this provides 224 processor cores in the system)
- Six Ultra Path Interconnect (UPI) links per socket providing unparalleled bandwidth and performance
- 48 DIMM slots per chassis (for example, when populated with 128 GB DIMMs this provides 6 TB of memory per chassis)
- Choice of I/O bays, including either 16 half-height I/O slots, or 8 full-height and 4 half-height I/O slots, per four-socket chassis
- Up to 10 drive bays per chassis
- Two 1GbE NIC ports, four USB ports
- Optional DVD
- Superdome Flex Analysis Engine for better diagnostics and mission-critical reliability

Each Superdome Flex 280 Server chassis may be configured with:

- Two or four Intel Xeon 53xx, 63xx, and 83xx (Cooper Lake) processors
- Up to 48 DDR4 DIMM slots (12 memory slots per processor)

- Up to 16 PCIe Gen 3 slots
- Eight fans
- Two or four power supplies
- BaseIO management, management USB port, and Ethernet ports (base chassis only)

UPI processor interconnections

A single-chassis configuration uses only internal UPI cables. Two-chassis configurations are connected with external UPI cables.

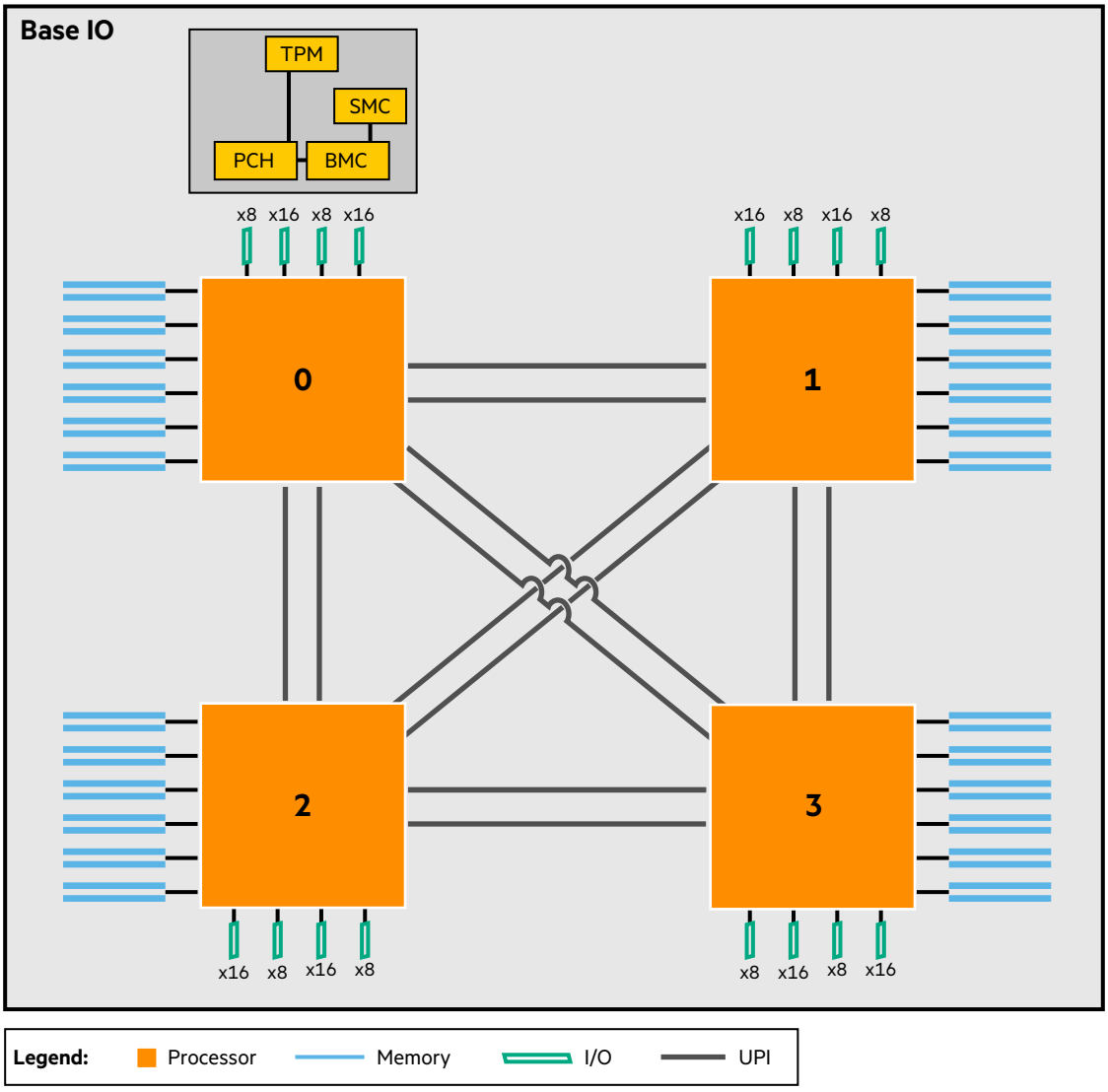


Figure 1: Superdome Flex 280 Server single-chassis system architecture

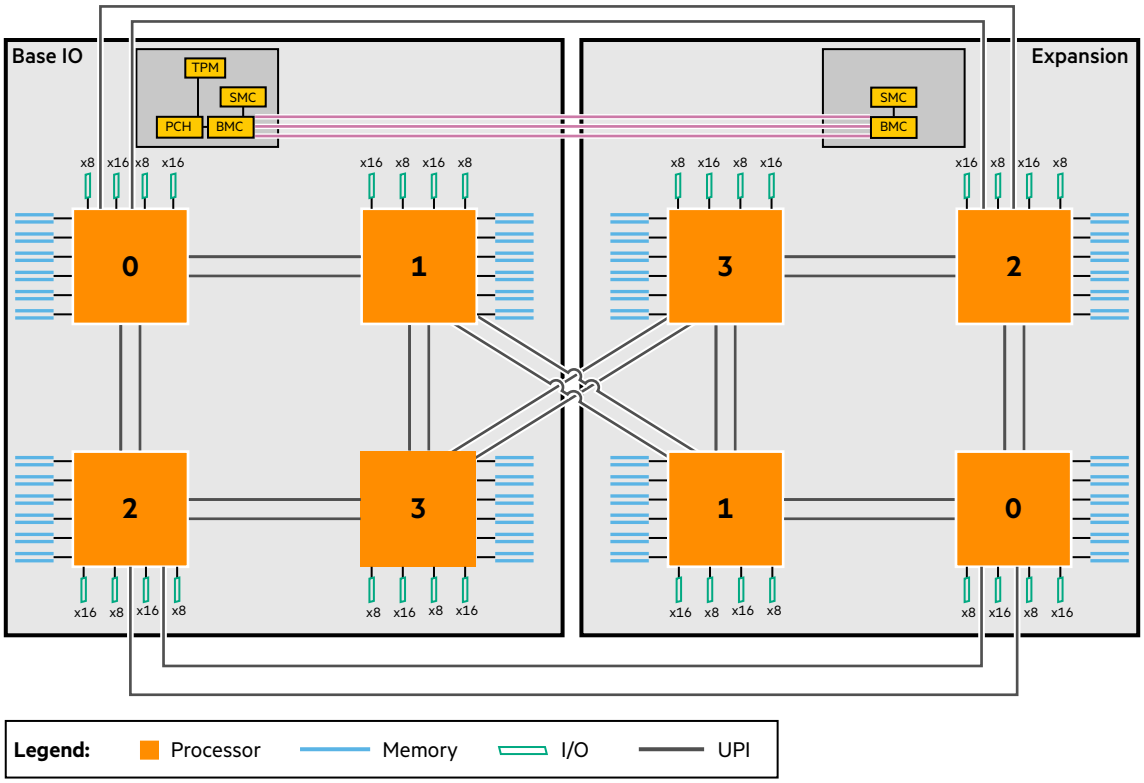


Figure 2: Superdome Flex 280 Server two-chassis system architecture

Logging in to the system

Logging in to the RMC Web GUI

The RMC web GUI provides a management interface accessible by a web browser.

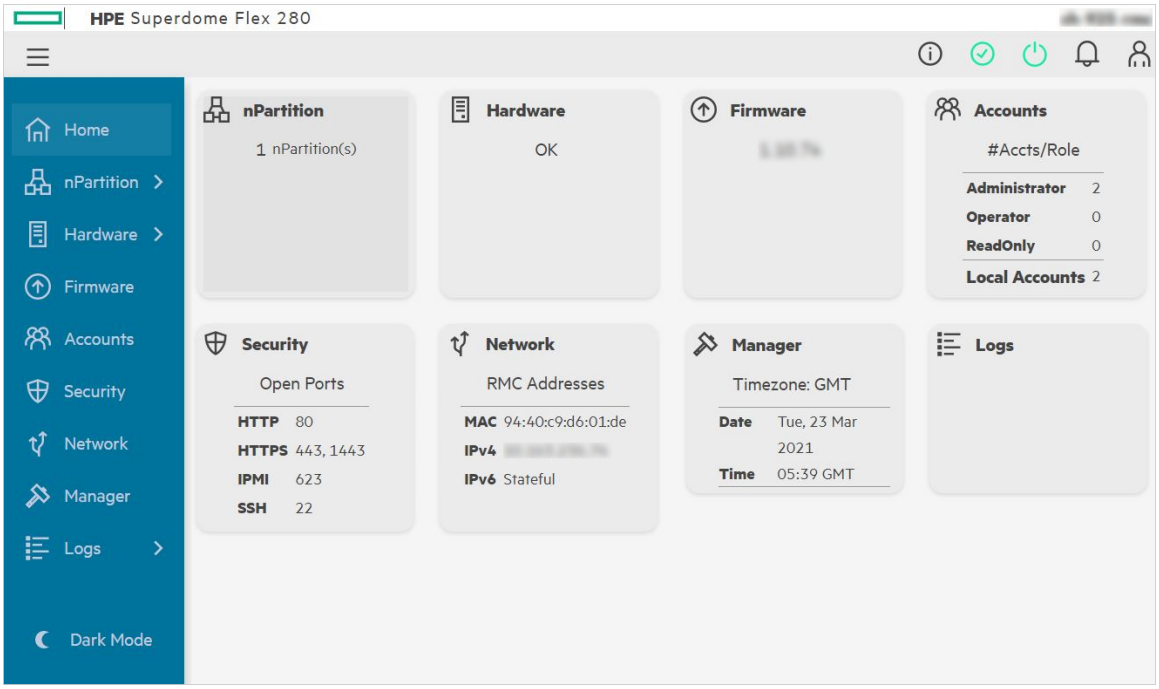
Prerequisites

- An Ethernet cable must be connected from the base chassis eRMC port to the manageability network.
- An IP address must be configured for the eRMC.

Procedure

1. Use a web browser to access the RMC web GUI at `https://`*`RMC-IP-ADDRESS`*.
2. Log in with an RMC user account and password.

   You can operate the RMC web GUI from a phone or desktop browser interface.



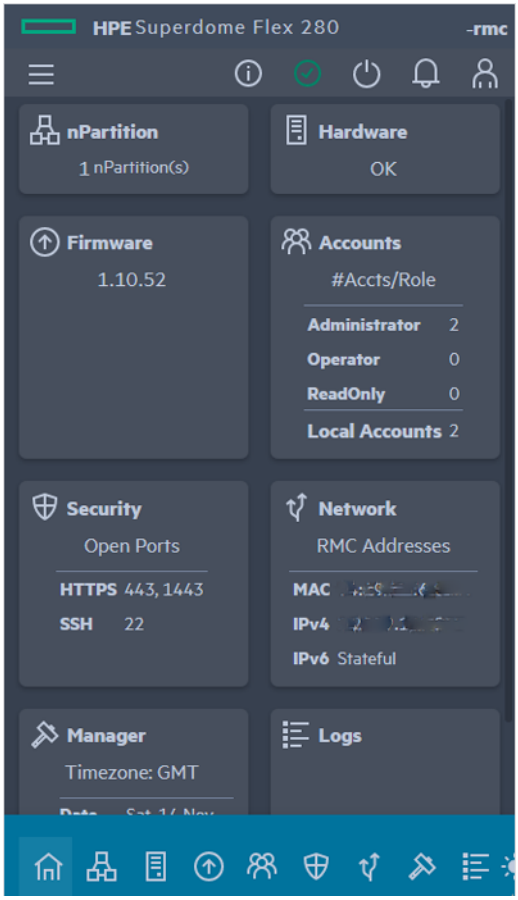


Figure 3: RMC web GUI phone view

Logging in to the RMC CLI through the CNSL port (Windows)

Prerequisites

The FT230X device driver must be installed. You can download the device driver and setup instructions from **https://www.ftdichip.com/Drivers/D2XX.htm**. Windows 10 systems do not have the FT230X driver installed by default.

NOTE: CNSL connection with Windows 7 and Windows 8 are not supported.

Procedure

1. Connect a mini-USB cable between the Windows laptop port and the base chassis CNSL port.

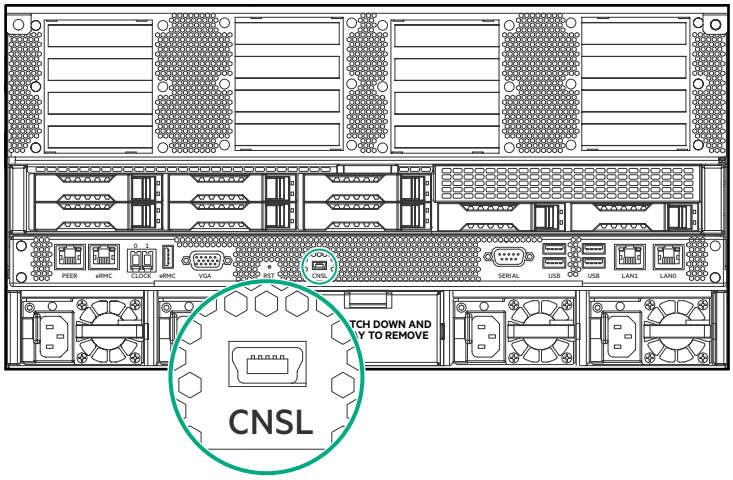


Figure 4: CNSL port on chassis rear

2. In Windows, use **Settings** > **Device Manager** > **Ports (COM & LPT)** to list the available COM ports.

3. Determine which COM port is assigned to the RMC. The BMC port enables RMC CLI access.

   In Windows, the Superdome Flex 280 Server port numbering can vary.

   Three COM ports represent the CNSL port. One COM port is the BMC port (RMC CLI), one is the SMC port (unused, no customer or service feature), and the other port also is unused.

4. Use PuTTY or another terminal program to connect to the COM port.

   Establish a serial connection at 115200 baud with 8 data bits, 1 stop bit, no parity, XON/XOFF flow control.

5. Press Enter to access the RMC CLI login prompt.

```
login as: USER_NAME
Pre-authentication banner message from server:
| #------------------------------------------------------------------------
| # WARNING: This is a private system.  Do not attempt to login unless you are
| # an authorized user.  Any access and use may be monitored and can result in
| # criminal or civil prosecution under applicable law.
| #------------------------------------------------------------------------
| #
| # Firmware Bundle Version: 1.xx.xxx
```

```
| #
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password: PASSWORD
End of keyboard-interactive prompts from server

HPE Superdome Flex 280 BMC,  Firmware Rev. 3.xx.xxx-xxxxxxxx_xxxxxx
(C) Copyright 2019-2021 Hewlett Packard Enterprise Development LP


================================================================================

Type "help" to see list of available commands.
Type "help <command>" to learn more about each command.

Enter <tab> to tab-complete a command.
Use cursor keys for command history.

HPE Rack Management Controller
(C) Copyright 2019-2021 Hewlett Packard Enterprise Development LP

================================================================================

example-rmc eRMC:r001u01c cli> help


Commands (type "help <command>" for more information):
======================================================
acquit   clear       deconfig  generate  ping        remove   show
add      collect     disable   help      ping6       restore  test
apropos  commands    download  indict    power       save     update
backup   connect     enable    ipmi      reallocate  search   upload
cancel   deallocate  exit      modify    reboot      set


example-rmc eRMC:r001u01c cli>
```

Logging in to the RMC through the CNSL port (Linux)

Prerequisites

The FT230X device driver must be installed. You can download the device driver and setup instructions from **https://www.ftdichip.com/Drivers/D2XX.htm**. Linux systems might have the FT230X driver installed by default.

Procedure

1. Connect a mini-USB cable between the laptop and the CNSL port on the base chassis.

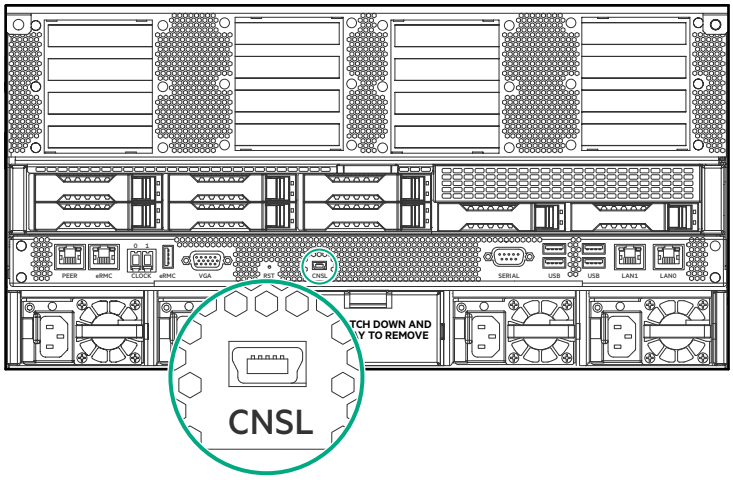


Figure 5: CNSL port on chassis rear

2. Use `cu` or `minicom` to connect to the `/dev/ttyACM1` device.

```
linux# minicom -D /dev/ttyACM1
```

   Connect at 115200 baud using 8 data bits, 1 stop bit, no parity, XON/XOFF flow control.

3. Press Enter to access the RMC CLI prompt.

Default RMC password location

An information pull-tab with the default network configuration for the Superdome Flex 280 Server RMC is on the rear of the base chassis. The default password for the default RMC administrator account is on the pull-tab. The base chassis is located in the lowest U-position in the rack.

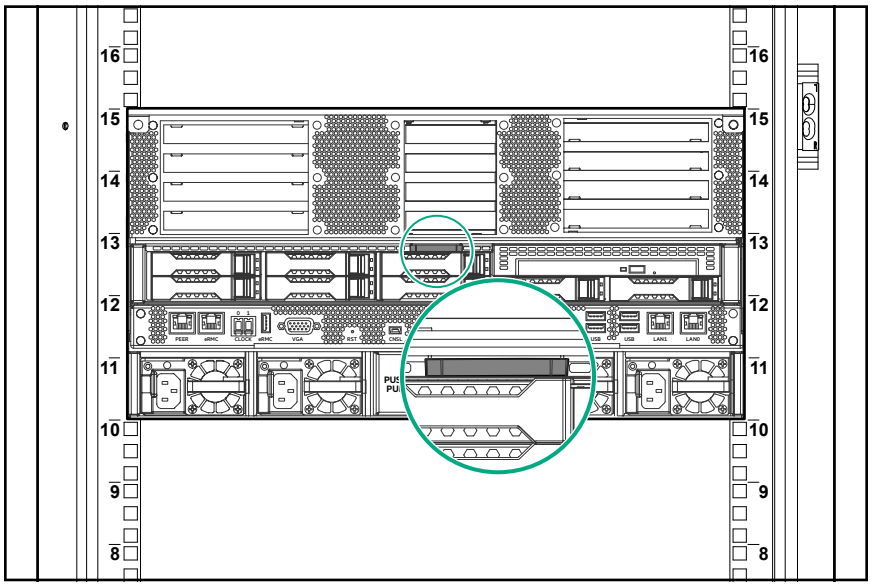


Figure 6: Information pull-tab location on chassis rear

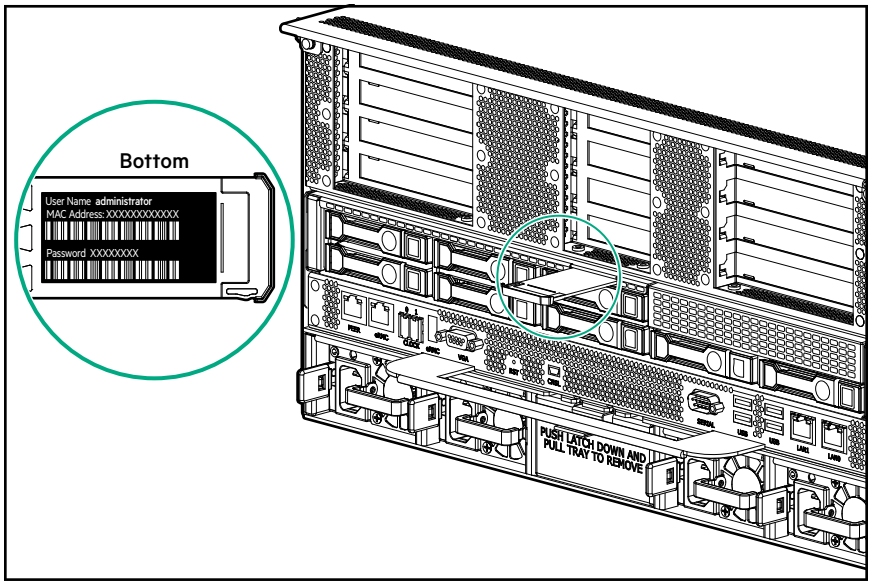


Figure 7: Information pull tab bottom: account, password, MAC address

Setting up the management network from the CLI

Prerequisites

- Laptop with drivers for direct connection
- USB-A to Mini-USB-B adapter cable
- Network configuration details for your management LAN
- RMC administrator account credentials

Procedure

1. Connect to the CNSL port on the back of the base chassis using the USB adapter cable.

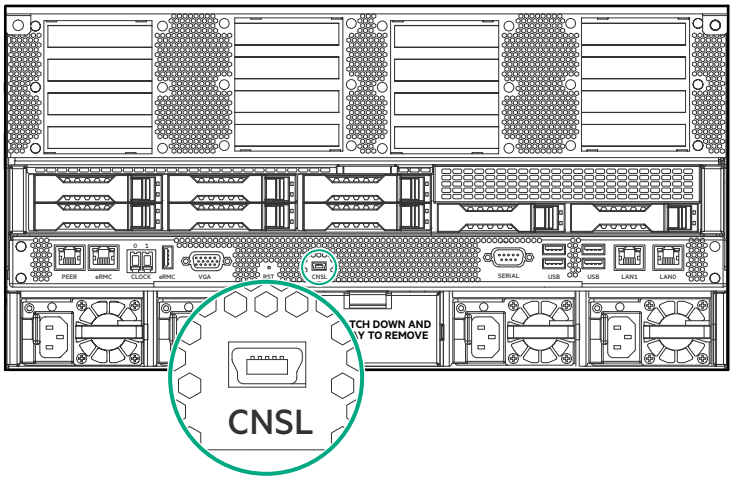


Figure 8: CNSL port location

2. Confirm access to the RMC using the default RMC administrator account.
3. Specify the network settings.

   Use the following command if the mehtod is static:

   ```
   set network addressing=METHOD gateway=GATEWAY_IP
   hostname=HOSTNAME ipaddress=HOST_IP
   netmask=SUBNETMASK
   ```

   Use the following command if the mehtod is DHCP:

   ```
   set network addressing=dhcp
   ```

4. Specify the NTP server for the Superdome Flex 280 Server.

   ```
   set ntp server=SERVER | FQDN of NTP
   ```

5. If the RMC will participate in name resolution, add DNS name servers and a domain name search list.

   ```
   RMC cli> add dns ipaddress=IPADDRESS1
   RMC cli> add dns ipaddress=IPADDRESS2
   RMC cli> add dns search=DOMAIN1
   RMC cli> add dns search=DOMAIN2
   ```

6. Specify your time zone.

a. Retrieve the list of time zone codes.

```
help set timezone str
```

b. Choose a location that is in your time zone and specify your time zone code.

```
set timezone str=CODE
```

For example:

```
RMC cli> set timezone str=America/Thunder_Bay
```

7. Reboot the RMC for the changes to take effect.

```
reboot rmc
```

8. To test new IP address and password for the RMC, open another terminal window (on Linux) or use a tool that supports SSH (on Windows) and enter the following command:

```
ssh administrator@NEW_RMC_IP_ADDRESS
```

For Windows, use the supported SSH tool.

9. To view the NTP server for the Superdome Flex 280 Server, enter the following command:

```
show ntp
```

10. To view and confirm the DNS configuration, enter the following command.

```
show dns
```

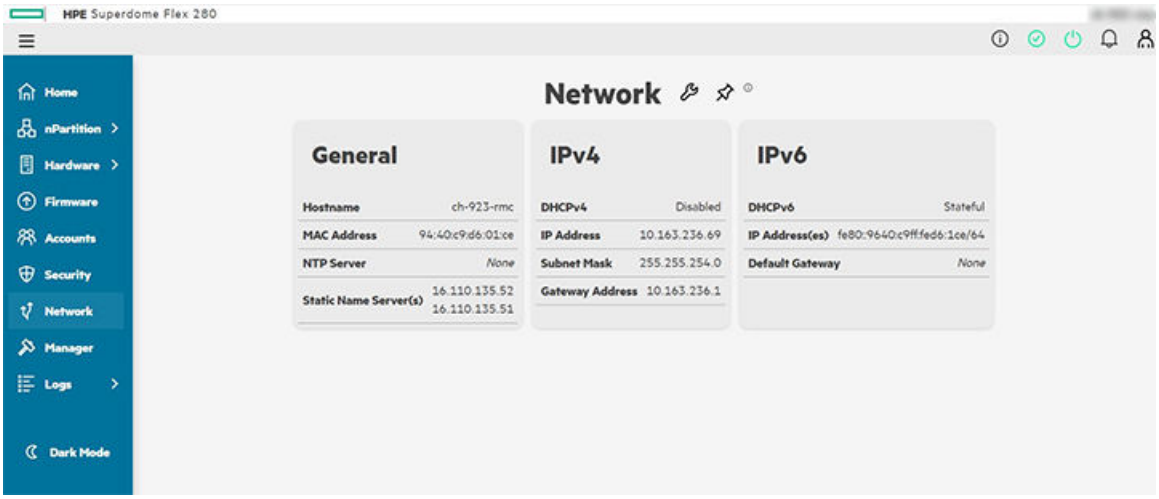
11. To display and make note of the RMC hostname and IP address, enter the following command.

```
show network
```

Setting up management network from the GUI

Procedure

1. Use a web browser to access the RMC web GUI at `https://`*`RMC-IP-ADDRESS`*.
2. Log in to the RMC web GUI.
3. Click **Network** on the main screen or the menu bar on the left.



4. Click the  icon next to **Network**.
5. Enter the required details.
6. To confirm the changes, click **Submit**.

Setting up users

The Superdome Flex 280 Server RMC can have a maximum of 30 local users, with specified roles that control access to the RMC. If configured using LDAP, there is no limit on LDAP users. User roles must be specified when creating a user account.

Procedure

1. Log in to the RMC.
2. Enter the `add user` command.

   ```
   add user name=USERNAME role={administrator,monitor,operator}
   ```

   The `add user` command has the following specifiers.

   name (*USERNAME*)

   Specify the name of the user that you want to add to the system.

   role

   Each role has a different level of privileges and are assigned when creating a user account.

RMC role name	Redfish role name	Privileges
administrator	Administrator	All privileges including ability to create, delete, and edit other user accounts
operator	Operator	Power control, setting a profile, and BIOS parameters
monitor	ReadOnly	Change own password, access read-only JViewer, and access read-only console

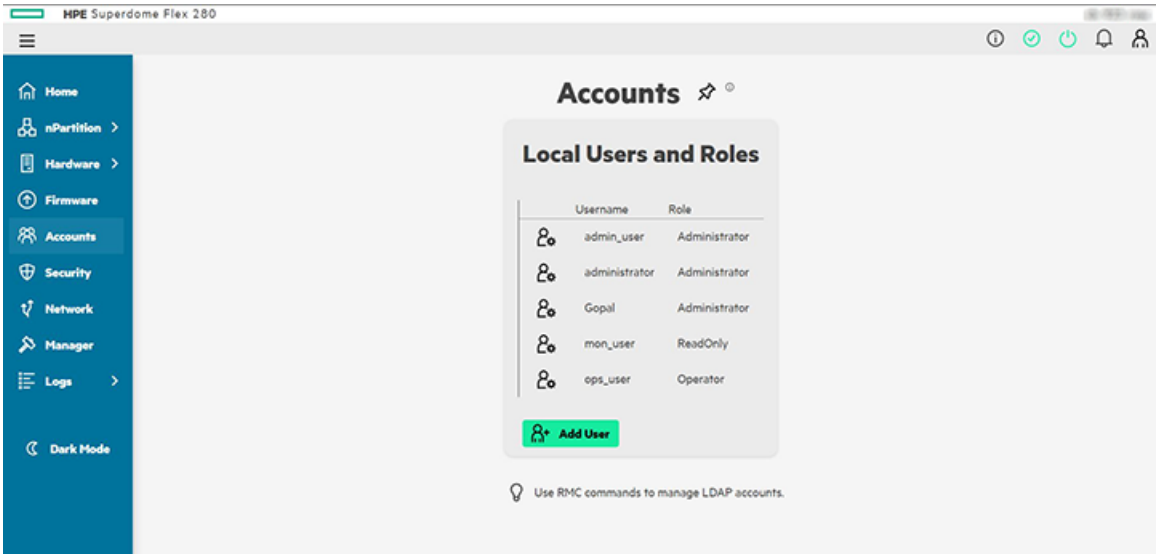
3. Enter a password for the user account. The password requirements are as follows.
   - Passwords may include combinations of these types of characters:
     - Upper case letters
     - Lower case letters
     - Numbers
     - Special characters, including `!@#$%^&*()`
   - Password length is dependent on the types of characters used. The minimum length is six characters, with the minimum length increased by two characters for each type not included. The maximum length is 40 characters.
     - Passwords only containing one type of character must be at least 12 characters.
     - Passwords containing two types of character must be at least 10 characters.
     - Passwords containing three types of character must be at least 8 characters.
     - Passwords containing all four types of characters must be at least 6 characters.
4. To verify the user list, enter the command `show user list`.

- To see details of the current user, enter the command `show user`.
- To delete an existing user, enter the command `remove user name=`*`USERNAME`*.

Setting up users from the GUI

Procedure

1. Use a web browser to access the RMC web GUI at `https://`*`RMC-IP-ADDRESS`*.
2. Log in to the RMC web GUI.
3. Click **Accounts** on the main screen or the menu bar on the left.



4. Click **Add User**.
5. Enter the user name and assign a role to the user.

RMC role name	Privileges
administrator	All privileges including ability to create, delete, and edit other user accounts
operator	Power control, setting a profile, and BIOS parameters
monitor	Change own password, access read-only JViewer, and access read-only console

6. To add the user, click **Submit**.

Setting up RMC SNMP alert monitoring

The Superdome Flex 280 Server RMC can be configured to send SNMP alerts to a specified IP address for remote monitoring.

Procedure

1. Log in to the RMC as an administrator.
2. Specify the destination IP address for SNMP alerts.

   ```
   set snmp forward_address=FORWARD_ADDRESS [port=FORWARD_PORT] [protocol=PROTOCOL]
   ```

   Where `forward_address` can be either IPv4, IPv6 address, or hostname.
3. Reboot the RMC.

   ```
   RMC cli> reboot rmc
   ```
4. To remove SNMP forwarding, enter the `remove snmp` command.

   ```
   remove snmp forward_address=FORWARD_ADDRESS
   ```

   where, `forward_address` is either IPv4 address, Ipv6 address, or hostname.

Configuring nPartition attributes

nPartition attributes control the nPartition configuration.

Attributes values are applied during the nPartition boot process. You can configure attributes either when the nPartition is powered off, or when it is booted (at UEFI or running an OS). Attribute changes that are made while an nPartition is booted are applied the next time it reboots.

Procedure

1. Access the server management interface.

   You can configure nPartition attributes from the RMC web GUI (**nPartition** > **Attributes**), or the RMC web GUI or the CLI `modify npar attributes` command or through Redfish APIs.

2. Set attributes to default values or configure custom attribute values.

   Setting an nPartition to default attributes configures all values and applies the default workload profile. The default attributes are:

   - Mission critical (MC)
   - High Performance Compute (HPC)
   - Virtualization
   - Custom

   Configuring an individual attribute or applying a workload profile applies specific values, but leaves other optional values unchanged.

```
example eRMC:r001u01c cli> modify npar attributes WorkloadProfile=HPC

SUCCESS

Partitions: 1


  Current:  Setting from most recent npar boot
  Pending:  Setting pending next npar boot
  Default:  Default setting.  Set all attributes to default using 'set npar default attributes'

Partition 0:

  Attribute
================================================================================
  BootSlots
      Current:    3,5,8
      Pending:    3,5,8
      Default:    3,5,8
--------------------------------------------------------------------------------
...

example eRMC:r001u01c cli> modify npar attributes HThread=Disabled

SUCCESS

Partitions: 1
...
```

3. Boot or reboot the nPartition.

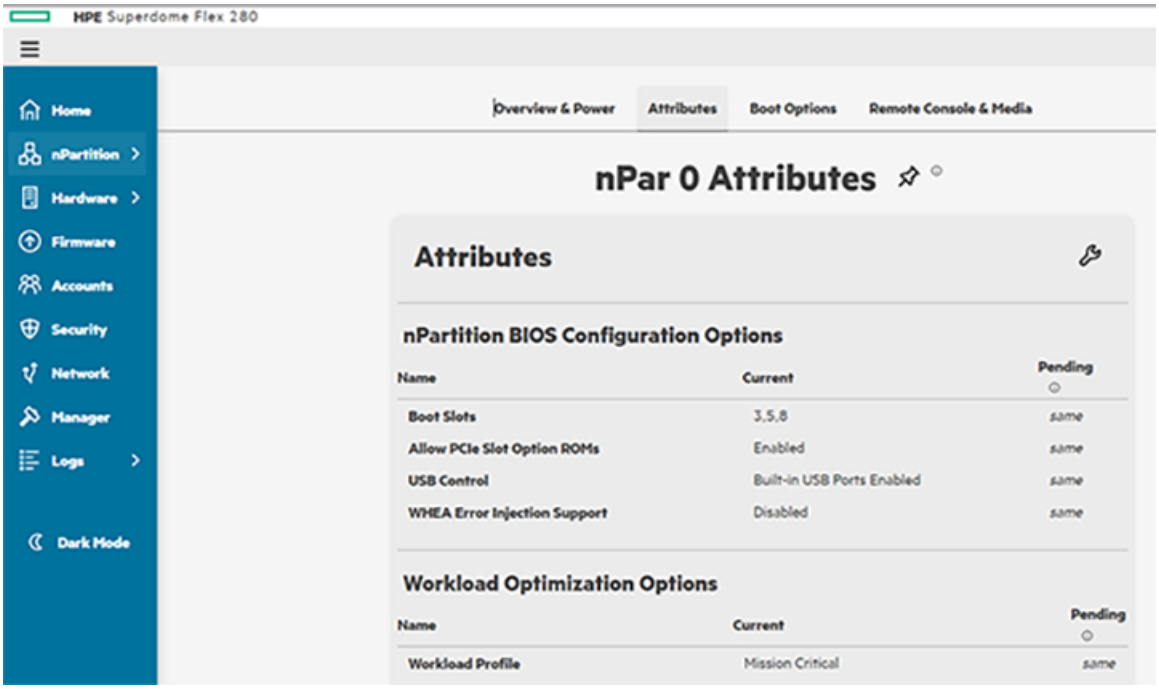
   nPartition attributes take effect the next time the nPartition boots.

   To view the current and pending nPartition attribute values, use the RMC web GUI (**nPartition** > **Attributes**) or the RMC `show npar attributes` command.

Configuring system nPartition attributes from the GUI

Procedure

1. Use a web browser to access the RMC web GUI at `https://`*`RMC-IP-ADDRESS`*.
2. Log in to the RMC web GUI.
3. Click **nPartition** on the main screen or the menu bar on the left.
4. Click the **Attributes** tab.



5. Click the  icon next to **Attributes**.
6.

Configuring the Custom workload profile

The Custom workload profile allows nearly all nPartition attributes to be configured with specific values.

Other workload profiles allow some attributes to be customized, and have specific settings for other attributes.

Procedure

1. Access the server management interface.

   To configure the Custom workload profile, use the RMC web GUI (**nPartition** > **Attributes**) or the RMC `modify npar attributes` command.

```
example eRMC:r001u01c cli> modify npar attributes WorkloadProfile=Custom

SUCCESS

Partitions: 1


  Current:  Setting from most recent npar boot
  Pending:  Setting pending next npar boot
  Default:  Default setting.  Set all attributes to default using 'set npar default attributes'

Partition 0:

  Attribute
================================================================================
  BootSlots
      Current:    3,5,8
      Pending:    3,5,8
      Default:    3,5,8
--------------------------------------------------------------------------------
  AllowPcieSlotOpRoms
      Current:    Enabled
      Pending:    Enabled
      Default:    Enabled
--------------------------------------------------------------------------------
  ErrorInjection
      Current:    Disabled
      Pending:    Disabled
      Default:    Disabled
--------------------------------------------------------------------------------
  WorkloadProfile
      Current:    MC
      Pending:    Custom[1]
      Default:    MC
--------------------------------------------------------------------------------
...
```

   [1] The Mission Critical (`MC`) workload profile is in effect now. The Custom workload profile will be in effect the next time the system boots.

2. Set nPartition attributes to custom values.

```
example eRMC:r001u01c cli> modify npar attributes AdvancedMemProtection=AdvancedEcc

SUCCESS

Partitions: 1

...
--------------------------------------------------------------------------------
  NumaGroupSizeOpt
      Current:    Clustered
      Pending:    Clustered
      Default:    Clustered
--------------------------------------------------------------------------------
  AdvancedMemProtection
      Current:    ADDDC
```

```
      Pending:    AdvancedEcc[1]
      Default:    ADDDC
--------------------------------------------------------------------------------
...
```

[1] The Adaptive Double Device Data Correction feature (`ADDDC` setting) is in effect now. Advanced ECC Support (`AdvancedEcc` setting) will be in effect the next time the system boots.

3. Boot or reboot the nPartition.

   nPartition attributes take effect the next time the nPartition boots.

   To view the current and pending nPartition attribute values, use the RMC web GUI (**nPartition** > **Attributes**) or the CLI `show npar attributes` command.

Setting default nPartition attributes

You can configure all nPartition attributes to the default values by setting workload profile to Mission critical (MC).

Procedure

1. Log in to the RMC web GUI or RMC CLI.
2. To set the nPartition attributes to default values, use the `set npar default attributes` RMC command or **nPartition** > **Attributes** > **Settings Icon** > **Reset Defaults** in pop-up in the RMC web GUI.

```
eRMC:r001u01c cli> set npar default attributes

Setting all attributes to default values for partition p0...
SUCCESS

eRMC:r001u01c cli>

eRMC:r001u01c cli> show npar attributes


Partitions: 1


  Current:  Setting from most recent npar boot
  Pending:  Setting pending next npar boot
  Default:  Default setting.  Set all attributes to default using 'set npar default attributes'

Partition 0:

  Attribute
================================================================================
  BootSlots
      Current:    3,5,8
      Pending:    3,5,8
      Default:    3,5,8
--------------------------------------------------------------------------------
...
```

3. Boot or reboot the nPartition.

   nPartition attributes take effect the next time the nPartition boots.

   To view the current and pending nPartition attribute values, use the RMC web GUI (**nPartition** > **Attributes**) or the RMC `show npar attributes` command.

Superdome Flex 280 Server workload profiles and attributes

Superdome Flex 280 Server supports the following nPartition system attributes and workload profiles.

For detailed descriptions of all attributes, see the RMC web GUI.

Table 1: Workload optimization options

Attribute	Mission Critical profile setting	High Performance Compute profile setting	Virtualization profile setting	Attribute name (CLI)	Valid setting/ Supported values (CLI)

Workload Profile	Mission Critical (default)	High Performance Compute	Virtualization	`WorkloadProfile`	`MC`
					`HPC`
					`Virtualization`
					`Custom`

Power Regulator	OS Control Mode	Static High Performance	X[1]	`PowerRegulator`	`StaticHighPerf` `OsControl`

Minimum Processor Idle Power Core C-State	C6 State	No C-states	X	`MinProcIdlePower`	`C6`
					`C1E`
					`NoCStates`

Minimum Processor Idle Power Package C-State	Package C6 (nonretention) State	No Package State	X	`MinProcIdlePkgState`	`C6Retention`
					`C6NonRetention`
					`NoState`

Energy/ Performance Bias	Balanced Performance	Maximum Performance	X	`EnergyPerfBias`	`MaxPerf`
					`BalancedPerf`
					`BalancedPower`
					`PowerSavingsMode`

Table Continued

Attribute	Mission Critical profile setting	High Performance Compute profile setting	Virtualization profile setting	Attribute name (CLI)	Valid setting/ Supported values (CLI)
Intel UPI Link Power Management	Enabled	Disabled	X	`IntelUpiPowerManagement`	`Enabled` `Disabled`
Intel Turbo Boost Technology	Enabled	Enabled	X	`ProcTurbo`	`Enabled` `Disabled`
Energy Efficient Turbo	Enabled	Disabled	X	`EnergyEfficientTurbo`	`Enabled` `Disabled`

Uncore Frequency Scaling	X (Auto)	Maximum	X	`UncoreFreqScaling`	`Auto`
					`Maximum`
					`Minimum`

Sub-NUMA Clustering	Disabled	Disabled	X	`SubNumaClustering`	`Enabled` `Disabled`
NUMA Group Size Optimization	Clustered	Clustered	X	`NumaGroupSizeOpt`	`Flat` `Clustered`
Advanced Memory Protection	Adaptive Double Device Data Correction (ADDDC)	Advanced ECC Support	X	`AdvancedMemProtection`	`ADDDC` `AdvancedEcc`
Intel NIC DMA Channels (IOAT)	Enabled	Enabled	X	`IntelNicDmaChannels`	`Enabled` `Disabled`
SR-IOV	X (Enabled)	Disabled	Enabled	`Sriov`	`Enabled` `Disabled`
Intel Virtualization Technology (Intel VT)	X (Enabled)	Disabled	Enabled	`IntelProcVt`	`Enabled` `Disabled`

Table Continued

Attribute	Mission Critical profile setting	High Performance Compute profile setting	Virtualization profile setting	Attribute name (CLI)	Valid setting/ Supported values (CLI)
Intel VT-d	X (Auto)	Auto	Enabled	`IntelProcVtd`	`Auto` `Enabled`
Processor x2APIC Support	Auto	Auto	X	`ProcX2Apic`	`Auto` `ForceEnabled`

[1] In the given profile, the setting can be changed to any value, that is floating and not forced.

Table 2: Power and performance options

Attribute	Mission Critical profile setting	High Performance Compute profile setting	Virtualization profile setting	CLI form	CLI options
Intel Hyper-Threading	X (Enabled)	X	X	`HThread`	`Enabled` `Disabled`
HW Prefetcher	Enabled	Enabled	X	`HwPrefetcher`	`Enabled` `Disabled`
Adjacent Sector Prefetch	Enabled	Enabled	X	`AdjSecPrefetch`	`Enabled` `Disabled`
DCU Stream Prefetcher	Enabled	Enabled	X	`DcuStreamPrefetcher`	`Enabled` `Disabled`
DCU IP Prefetcher	Enabled	Enabled	X	`DcuIpPrefetcher`	`Enabled` `Disabled`
LLC Prefetch	X (Disabled)	X	X	`LlcPrefetch`	`Enabled` `Disabled`
LLC Dead Line Allocation	X (Enabled)	X	X	`LlcDeadLineAlloc`	`Enabled` `Disabled`

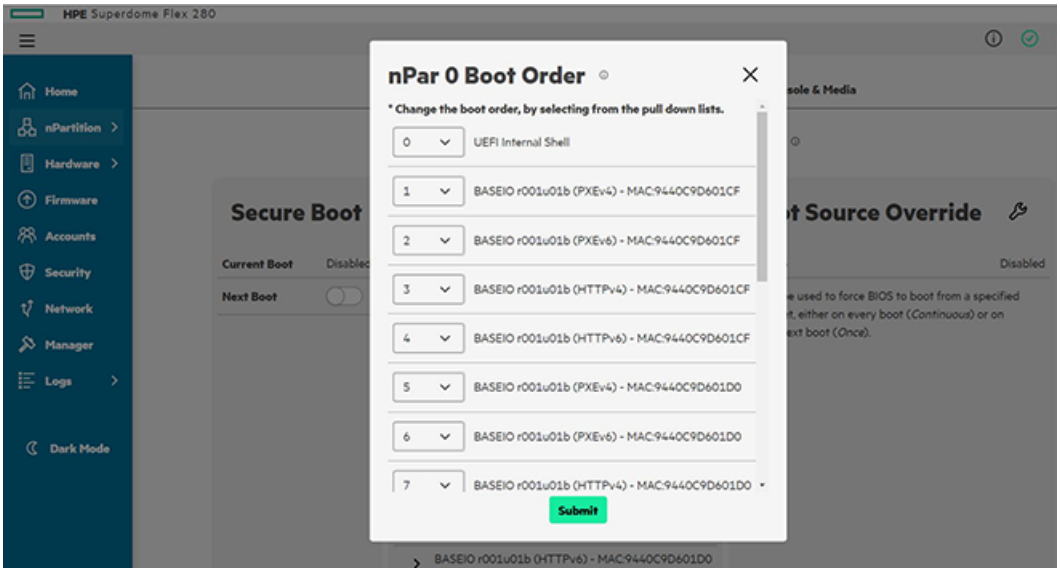
Table Continued

Attribute	Mission Critical profile setting	High Performance Compute profile setting	Virtualization profile setting	CLI form	CLI options
Local/Remote Threshold	Auto	Auto	X	LocalRemoteThreshold	Auto Manual
UPI RRQ Threshold	X (15)	X	X	UpiRrqThreshold	0-31
UPI IRQ Threshold	X (4)	X	X	UpiIrqThreshold	0-31
Snoop Throttle Configuration	X (Auto)	X	X	SnoopThrottleConfig	Auto Disabled Low Medium High
Enhanced Processor Performance	X (Disabled)	X	X	EnhancedProcPerf	Enabled Disabled
Intel DMI Link Frequency	Auto	Auto	X	IntelDmiLinkFreq	Auto DmiGen1 DmiGen2
Maximum Memory Bus Frequency	Auto	Auto	X	MaxMemBusFreqMHz	Auto MaxMemBusFreq2933 MaxMemBusFreq2667 MaxMemBusFreq2400 MaxMemBusFreq2133 MaxMemBusFreq1867
Memory Refresh Rate	X (Refreshx1)	X	X	MemRefreshRate	Refreshx1 Refreshx2
Memory Patrol Scrubbing	Enabled	Enabled	X	MemPatrolScrubbing	Enabled Disabled

Setting up boot order with the RMC web GUI

Procedure

1. Log in to the RMC web GUI.
2. Click **nPartition** on the main screen or the menu bar on the left.
3. Click the **Boot Options** tab.
4. To verify the system boot order, check the **Boot Order** heading.
5. Change the boot order.
   a. Click the  icon under the **Boot Order** heading.



   b. Choose the boot option you want to change and click the pull-down list.
   c. Select the position for the boot option from the list.
   d. To confirm the changes, click **Submit**.
6. Reverify the system boot order. The system uses the listed boot order during the next system boot.

Specifying boot options using the RMC CLI

The Superdome Flex 280 Server can be booted from multiple sources using RMC commands. The boot options can be specified during power on, power reset, or during reboot.

Procedure

1. Log in to the RMC CLI.
2. Verify the boot option required.
   The following boot options are available:
   - *None* - No boot option specified. Boots from default source.
   - *BiosSetup* - Boot to BIOS setup.
   - *Cd* - Boot from existing UEFI boot option entries that correspond to CD/DVD drives of any connection type (such as SATA and USB).
   - *Hdd* - Boot from existing UEFI boot option entries that correspond to local hard disk drives, excluding USB drives.
   - *Pxe* - Boot from existing UEFI boot option entries that correspond to PXE.
   - *RemoteDrive* - Boot from existing UEFI boot option entries that correspond to remote (FibreChannel or iSCSI) hard disk drives.
   - *SDCard* - Boot from existing UEFI boot option entries that correspond to SD cards.
   - *UefiShell* - Boot to UEFI Shell.
   - *UefiHttp* - Boot from existing UEFI boot option entries that correspond to HTTP boot.
   - *Usb* - Boot from existing UEFI boot option entries that correspond to USB disk drives.
3. Verify if you are powering on the server, resetting the power, or rebooting the server.
   - If you are powering on the server, enter the `power on` command.

     ```
     power on npar pnum=0 [bootopt=BOOTOPT]
     ```

   - If you are resetting the power or rebooting, enter the `power reset` or `reboot` command.

     ```
     power reset npar pnum=0 [bootopt=BOOTOPT] [force]
     ```

     ```
     reboot npar pnum=0 [bootopt=BOOTOPT] [force]
     ```

     - If power is on, the `power reset` or `reboot` commands perform a graceful OS shutdown then restart the server.
     - If `force` is specified, the commands perform an OS immediate (non-graceful) shutdown instead.

Setting up boot order with UEFI

Procedure

1. Interrupt the boot process and access UEFI.

   Press **F2** to access the UEFI Boot Manager.

2. Select the **Boot Maintenance Manager** menu.
3. Select the **Change Boot Order** menu.
4. To select the boot options, press **Enter**.
5. Change the boot order.

   a. Use the up and down arrow keys to select a boot option.

   b. To move the boot option up, press **+**. To move the boot option down, press **-**.

   c. To finish setting the boot order, press **Esc**.

   d. To commit the changes and exit, press the down arrow and select **Commit Changes and Exit**. The changes take effect immediately and are applied on the next system boot.

Secure boot

HPE Superdome Flex 280 Server systems support features that secure the boot process. When enabled, Secure Boot prevents execution of OS loaders, drivers, and UEFI applications that are not signed with an acceptable digital signature.

Secure boot features

When secure boot is enabled on Superdome Flex 280 Server, system firmware verifies OS loader, driver, and UEFI application signatures before executing them.

By default, secure boot is disabled. This default applies to systems shipped from the factory.

Many secure boot configuration changes require resetting the system before booting an OS or accessing the UEFI Shell.

Secure boot protection applies both at the Boot Manager menu and at the UEFI Shell. In secure boot mode, the UEFI Shell disables the `mm`, `hexedit`, and `setvar` commands, and restricts the `dmpstore` command.

System logs record changes to the secure boot mode. Secure boot checks performed during firmware verification also are logged.

Default secure boot keys

The default keys include signatures for supported operating systems.

The Superdome Flex 280 Server default secure keys permit execution of images signed by the following certificates.

- HPE KEK 2016
- Microsoft Corporation KEK CA 2011
- SUSE Linux Enterprise Secure Boot CA
- HPE DB 2016
- HP DB 2013
- Microsoft Corporation UEFI CA 2011
- Microsoft Windows Production PCA 2011
- SUSE Linux Enterprise Secure Boot Signkey
- VMware certificate 2017

Configuring Secure Boot on HPE Superdome Flex 280 Server

Secure Boot can be configured on Superdome Flex 280 Server through the RMC web GUI, the RMC CLI, or through UEFI.

Procedure

- **Configure Secure Boot with the RMC web GUI**
- **Configure Secure Boot with the RMC CLI**
- **Configure Secure Boot with UEFI Boot Manager**

Configuring Secure Boot with the RMC web GUI

Procedure

1. Log in to the RMC web GUI.
2. Click **nPartition** from the main screen or the menu bar on the left.
3. Click the **Boot Options** tab.
4. To verify the status of Secure Boot, check the **Next Boot** entry under the **Secure Boot** heading.
5. Under the **Secure Boot** heading, toggle the **Next Boot** control to either enable or disable Secure Boot on the next system boot.
6. To apply the changes, reboot the system.

Configuring Secure Boot with the RMC CLI

Secure Boot can be enabled and disabled with RMC CLI commands.

Prerequisites

System must be powered off.

Procedure

To enable Secure Boot:

1. Log in to the RMC CLI.
2. Verify if the system is powered off. If not, enter the `power off npar` command.
3. Enter the `modify npar` command.
   - To enable Secure boot, enter the following command.

     ```
     modify npar secure_boot=on
     ```

   - To disable Secure boot, enter the following command.

     ```
     modify npar secure_boot=off
     ```

4. Verify the Secure Boot state using the `show` command.

   ```
   show npar verbose
   ```

5. Power on the system.

   ```
   power on npar
   ```

Configuring Secure Boot with UEFI Boot Manager

Procedure

1. Access UEFI Boot Manager from the nPartition console.
2. Access the **Secure Boot Configuration** menu.
   At Boot Manager, select the **Device Manager** menu, then select the **Secure Boot Configuration** menu.

3. Enable or disable secure boot.

   To enable secure boot:

   You can either enable with default keys, or install a custom set of keys.

   a. Enable Secure Boot with the default keys.

      Select the **Attempt Secure Boot** option.

   b. Install custom keys.

      Enable the **Custom Secure Boot Options** menu by changing the **Secure Boot Mode** setting to **Custom Mode**. After installing custom keys, verify that the **Attempt Secure Boot** option is selected to enable secure boot.

   To disable secure boot, clear the **Attempt Secure Boot** option.

4. To apply the changes, reset the system.

   The system must be reset before you can load an OS or access the UEFI Shell. If you select "Continue" at the Boot Manager or attempt to use the Boot Manager to boot any option, a pop-up window will display:

   ```
   Configuration changed. Reset to apply it now. Press ENTER to reset.
   ```

   Press **Enter** to reset the system.

More information

Default secure boot keys

Installing or reinstalling default Secure Boot keys

When installing default keys, all secure boot data is written with a default set for supported operating systems.

Prerequisites

The system automatically installs default keys if all Secure Boot keys have been deleted.

Procedure

1. Access UEFI Boot Manager from the nPartition console.
2. Access the **Secure Boot Configuration** menu.
   At Boot Manager select the **Device Manager** menu, then select the **Secure Boot Configuration** menu.
3. Select the **Custom Secure Boot Options** menu.

   Change the **Secure Boot Mode** option to **Custom Mode**, then select the **Custom Secure Boot Options** menu.
4. Delete all KEK keys.

   Select the **KEK Options** menu, then select the **Delete KEK** menu. For each key displayed, toggle the corresponding checkbox to delete the key.
5. Delete all DB keys.

   Select the **DB Options** menu, then select the **Delete Signature** menu. For each key displayed, toggle the corresponding checkbox to delete the key.
6. Delete all DBX keys.

   Select the **DBX Options** menu, then select the **Delete Signature** menu. Select the **Delete All Signature List** option and press **Y** to confirm.

7. Delete the PK key.

   Select the **PK Options** menu, then select the **Delete Pk** checkbox. Press **Y** to confirm.

8. Reset the system to apply the changes.

   You must reset the system before you can load an OS or access the UEFI Shell.

More information

Default secure boot keys

Setting up remote media files with the RMC web GUI

HPE Superdome Flex 280 Server can access up to two ISO or image files on a remote file server.

Prerequisites

- A file server configured on the local network using CIFS or NFS.
- Network address details for the file server.
- Credentials to access the file server.

Procedure

1. Log in to the RMC web GUI.
2. Click **nPartition** from the main screen or the menu bar on the left.
3. Click the **Remote Console & Media** tab.
4. Enable Remote Media by clicking **Remote Media**.
5. Under the **File Server** heading, click the configure icon ().

   This enables you to configure the file server options, IP address, media path, and login credentials.
6. Connect to the file server by clicking **Connect**.
7. Select the image files.

   Two image files can be selected and inserted.

   To remove an image file, click **Eject**.

   a. Click the **Select Media Files** drop-down list under the **Media Files** heading.
   b. Select an image file in the specified file path.
   c. Click **Insert**. The selected image file is inserted.

Websites

HPE Superdome Flex 280 Server websites

- Product page

  www.hpe.com/support/superdomeflex280-product
- Customer documentation

  www.hpe.com/support/superdomeflex280-docs
- Software

  www.hpe.com/support/superdomeflex280-software
- Hewlett Packard Enterprise server operating systems and virtualization software

  www.hpe.com/us/en/servers/server-operating-systems.html
- HPE Superdome Flex 280 Server QuickSpecs

  www.hpe.com/support/superdomeflex280-quickspecs
- Customer advisories

  www.hpe.com/support/superdomeflex280-customer-advisories
- Spare parts list

  www.hpe.com/support/superdomeflex280-spareparts
- Release sets (support matrix)

  www.hpe.com/support/superdomeflex280-release-sets
- Safety and regulatory information

  www.hpe.com/support/Safety-Compliance-EnterpriseProducts
- Recycling information

  www.hpe.com/recycle
- Visio templates

  www.visiocafe.com/hpe.htm

  The `HPE-Integrity-MC` stencil includes HPE Superdome Flex 280 Server front and rear physical shapes.
- Supported browsers

  Google Chrome, Mozilla Firefox, and Microsoft Edge (based on chromimum)

HPE Superdome Flex 280 Server support documentation

HPE Superdome Flex 280 Server documentation for support specialists is available at **www.hpe.com/support/superdomeflex280-docs-restricted** by signing in to **Hewlett Packard Enterprise Support Center** with an entitled account.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  https://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  https://www.hpe.com/support/downloads

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  https://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Pointnext Tech Care

https://www.hpe.com/services/techcare

HPE Datacenter Care

https://www.hpe.com/services/datacentercare

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the **Feedback** button and icons (located at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. All document information is captured by the process.