



## TECHNICAL WHITE PAPER

### CONTENTS & NAVIGATION

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices



# INTEL® OPTANE™ DC PERSISTENT MEMORY: CONFIGURATION AND SETUP ON HP Z6 G4 AND Z8 G4 WORKSTATIONS

## INTRODUCTION

### What is Intel® Optane™ DC Persistent Memory Module (DCPMM)?

Using 3D XPoint non-volatile memory, Intel®'s Optane™ DCPMM (Data Center Persistent Memory Module<sup>1</sup>)\* is the first NVDIMM offering performance and lifecycle characteristics for storage class memory and in some cases DRAM replacement. This paper discusses the different modes of operation and how to properly configure in a Z Workstation.

Intel® Optane™ DC Persistent Memory (DCPMM) is a revolutionary technology which blurs the traditional lines between memory and storage in computing. These new components are housed in the DIMM slots of the workstation and, depending on configuration, can act as memory or storage.

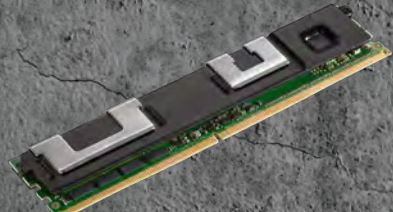
Intel® Optane™ DC Persistent Memory will be available on HP Z6 G4 and HP Z8 G4 Workstations using supported Intel® Xeon® 8200, 6200, 5200 and select 4200 series processors.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

DCPMM has been under development for several years. HP and Intel® together with Microsoft have been working on this new technology for HP Workstations since 2016. Like many new and disruptive computing technology innovations in the past, DCPMM first saw large scale deployment on servers in data center applications. Widespread adoption will gradually migrate down into workstation computing platforms for very high-performance applications.

## Modes of Operation

DCPMM can be configured in two modes of operation, Memory and Persistent Memory. Persistent Memory usage can be further broken down into Storage Mode and App Direct Mode.



**INTEL® OPTANE™ DC  
PERSISTENT MEMORY MODULE**

**Intel® Optane™ DCPMM works in three modes:**

- Memory mode (acts like standard DRAM and is volatile)
- Storage mode - storage over app direct
- App Direct Persistent Memory mode.

---

Memory Mode	Storage Mode	App Direct - Persistent Memory
<ul style="list-style-type: none"><li>• Fast Application Response</li><li>• Load entire complex models into memory</li><li>• Lower cost high cap memory configs</li></ul>	<ul style="list-style-type: none"><li>• Applications are ready today</li><li>• Free up PCIe slots for graphics+</li><li>• High storage performance for MMIO accesses</li></ul>	<ul style="list-style-type: none"><li>• App will need to be updated to support this feature</li><li>• Instant recovery from loss of power or app crashes</li><li>• Unlimited "undo" feature - no need to save</li></ul>

### Memory Mode

Memory Mode is the most straightforward use model for DCPMM. DCPMM modules are used as System Memory alongside DRAM modules which are used as cache memory. As memory, DCPMM has similar performance<sup>2</sup> to 2666 MHz DDR4 memory but at a lower cost for memory configurations greater than or equal to 128 GB. In this mode the DCPMM is volatile just like standard memory. If your workstation workflows require memory configurations of between 128 GB and 1 TB of memory, a DCPMM Memory Mode solution may be an option for you to consider.

### Persistent Memory Modes

Configured as Persistent Memory, DCPMM has the distinct advantage of being persistent like storage devices today. It can appear like any other disk or storage volume to the system. This means when your computer is turned off either because you intentionally shut down for the day or you experienced an unplanned power outage, your data will still be on the DCPMM modules just like it would for a traditional storage device. It can also be accessed like memory if configured for that type of access, by mapping the storage into application address space.

Persistent Memory supports two modes of operation called Storage Mode and App Direct Mode.

#### Storage Mode

Storage Mode (also called Storage over App Direct) deployment is very straight forward. In this case the DCPMM modules are configured as storage volumes and are available to your applications as storage using normal file systems and interfaces. The advantage of DCPMM in Storage Mode is much faster read performance because the modules are installed in a DIMM slot, so the data moves over the higher speed processor channels rather than through the slower PCIe or SATA busses typical of storage devices.

Applications do not need to be modified when using DCPMM in Storage Mode.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

A volume created in Storage Mode can be set up with a feature known as **Direct Access (DAX)**. When a volume is DAX-enabled, the storage can be modified by direct access to the persistent memory, bypassing the traditional form of block access. (Only some file systems in Windows and Linux support DAX).

An additional benefit of a DCPMM Storage solution is it allows the user to save their limited PCIe slots for other components like graphics cards. If your workflows involve models with very large data sets or require frequent data swaps between memory and storage, DCPMM is a technology you should investigate further.

## App Direct Mode

The real revolution for DCPMM will occur with the utilization, in applications, of App Direct Mode. In this mode the DCPMM technology offers the performance of memory with the persistence of storage. This provides Zero-copy where applications and user data do not have to be moved from storage devices to memory before execution. Applications that implement support for App Direct can deliver a near “Instant on” experience when launching the application, loading very large datasets, switching between many applications, or even resuming an application in the exact same state as it was in prior to shutting down the system.

New user experiences will also be possible. For instance, no more need for manual or automatic saves of your work, except for exporting files when needed. Undo / Redo functions that remember changes even between reboots. Virtually instant switching between data sets within an application. Transparently saving incremental (model versioning) or different versions of a user's work and models based only on the data actually modified, thus drastically limiting computing or space used, with virtually no responsiveness impact when switching between versions. Eventually, App Direct Mode will lead to a flat memory model where there will be no differentiation between storage and memory. The new and disruptive user experiences that will emerge can hardly be imagined today and will be a fascinating space to watch.

App Direct Mode is only compatible with new Persistent Memory (PMEM) aware file systems and applications. Most software applications are not written to take advantage of an App Direct Mode. If your business is development and sales of high-performance software applications, you will need to understand DCPMM and the promise of App Direct Mode early so your software can be modified to take advantage of this innovative technology.

This document does not thoroughly cover the procedures for setting up App Direct mode or modifying applications to use it. Some resources are named in Appendix H.

## HP Factory Configured Solutions

HP will initially offer several factory configurations of DCPMM for Memory and Storage Modes. See HP Z6 G4 and HP Z8 G4 QuickSpecs for list of supported configurations.

# Unique Attributes of Intel® Optane™ DCPMM

Intel® Optane™ DCPMM solutions are new and exciting. They are different than anything previously supported in Workstations. Because they are new and different, users and system administrators need a broader understanding on how to use DCPMM solutions:

- DRAM must be present in any configuration
  - Memory mode uses DRAM as cache for the DCPMM. The recommended ratio (DRAM:DCPMM) is 1:8.
  - Persistent Memory mode does not use DRAM as cache. DRAM serves as system memory as usual, so should be configured to meet system and application needs.
  - In both usages, there are some loading rules that must be followed, detailed later.
- Physical placement (load order) matters
  - Physical placement of DCPMM modules along with the DRAM DIMMs matters. If the load order of these DRAMs/DCPMMs are wrong, the system might not boot. See “How to Configure the System HW” section below for more info about load order.
- OS Revision matters
  - DCPMM configurations require a Persistent Memory (PMEM) Aware OS revision and updated OS patches. See the System Requirements section below for a list of supported OSes and minimum revision levels.
- DCPMM has embedded firmware
  - Unlike DRAM memory, DCPMM has firmware and might need to be updated over the life of the module. It is recommended that anytime the BIOS (UEFI Firmware) is updated, the BIOS release notes should be checked to see if the firmware on the DCPMM module(s) need to be updated as well. See below for instructions on how to update the firmware.
- Here we'll introduce some organizing terms relevant to Storage Mode and App Direct Modes that will be useful in the discussions that follow. These terms do not apply to Memory Mode.
  - The DCPMM modules located in the memory slots for a specific processor are called a **DCPMM set**.



1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

- The storage capacities in one or more DCPMMs in a set are grouped into a **region**.
  - Often, a region is created across the DCPMMs in the set, thus creating an **interleaved set**
- To be useful, a region is subdivided into one or more **namespaces**.
- Namespaces can have a capability identified as **BTT** (Block Translation Table).
  - BTT namespaces support ordinary file systems in the OS because the BTT allows the OS to see the DCPMM storage like a normal block-oriented device
  - Non-BTT namespaces (also called PM namespaces) are used in App Direct Mode
- In the OS, namespaces appear as raw storage devices that can be partitioned into volumes and formatted.
  - The DAX attribute can be attached to the volume. Details on doing this are covered in the procedural appendices for Windows and Linux

## Additional Notes about Storage Mode

- DCPMM are compatible with legacy/existing applications when using a PMEM-aware OS.
- When multiple DCPMMs are used on a processor, they should be configured to be interleaved for maximum performance.
- In Storage Mode, the DCPMMs are only interleaved on a single processor. If DCPMMs are distributed across two processors, there will be two independent storage devices.
- **When interleaved, it is important to know the exact loading of DCPMM. If the DIMMs need to be removed from the motherboard for any reason, (for example, motherboard replacements) make sure that the exact location of each DIMM is known.** Not placing the DCPMMs back in the exact Memory Slot will make the storage data unreadable and may make it difficult to recover the data.
- Adding DCPMMs or changing configurations requires additional steps not normally associated with adding or changing legacy storage devices.
- Storage Capacity available to the System will be slightly less than advertised capacity, for example:
  - 128 GB provides approximately 126 GB available capacity.
  - 256 GB provides approximately 252 GB available capacity.
  - 512 GB provides approximately 502 GB available capacity.
  - Note: Additional overhead capacity may be required for: Regions, Namespace, and File System.
- In Storage Mode, DRAM memory acts like regular system memory.
- See Appendix A through D for more details on how to configure.
- Further notes regarding DAX (Direct Access):
  - If your Windows system was ordered with DCPMM configured in Storage Mode, your DCPMM will be formatted with a DAX aware file system.
  - If your Linux-Ready system was ordered with DCPMM configured in Storage Mode, your DCPMM will be configured for Storage Mode, but will be unformatted. You will be required to format the DCPMM devices on your own. Instructions on configuring a Linux file system to be DAX-aware can be found in Appendix C.
  - For Windows:
    - PowerShell is required to enable DAX
    - DAX is only supported with NTFS on Windows systems
  - For Linux:
    - A terminal emulator and root permissions are required to enable DAX
    - DAX is only supported with DAX-enabled file systems such as EXT4 on Linux
      - > Check your file system documentation to find which file systems are DAX enabled and at what version.
  - A format operation is required to convert between DAX and non-DAX.
  - Software encryption is not available, for example BitLocker.
  - Software compression of the volume is not available.
  - Existing filter drivers will not function.

## Additional notes about Memory Mode

- As noted earlier, DRAM is required when configuring DCPMM in Memory Mode. The DRAM DIMMs are used as cache for the DCPMM. HP recommends a ratio of 1:8 for DRAM capacity to DCPMM capacity.
- Memory available to the System will be slightly less than advertised capacity, for example:
  - 128 GB provides approximately 126 GB available capacity.
  - 256 GB provides approximately 252 GB available capacity.
  - 512 GB provides approximately 502 GB available capacity.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

## Unsupported usages

- Legacy Boot Mode is not supported; only UEFI Boot Mode is supported.
- System Boot from the DCPMM modules is not supported.
- Dual Mode (configuring both Storages and Memory Modes at the same time on a single system) is not supported.

# DCPMM SECURITY OVERVIEW

This section provides an overview of DCPMM security features. Details are available in Appendix E.

- DCPMM uses full-time hardware encryption, even in Memory Mode. The encryption algorithm is XTS-AES256, a common choice for self-encrypting drives (SEDs). Encryption on each DCPMM uses an internal symmetric key that cannot be read by the workstation.
  - In Memory Mode, a new key is created at every reset, and deleted at every power off, so that contents cannot be retrieved across resets or power cycles, or by removing the memory modules. DCPMM passphrases are not used in this mode.
  - In App Direct Mode and Storage Mode, the key is non-volatile and can be tied to a passphrase, so that entering the passphrase instructs the DCPMM controller to unseal the key and unlock the DCPMM. The passphrase is also stored on the DCPMM and is unique to the module. As shipped, the DCPMMs do not have a passphrase set and on-device encryption is invisible to the rest of the computer (it applies to data at rest only).
  - This single-passphrase model of DCPMM differs from traditional disk security (e.g. HP DriveLock) where distinct user and admin passwords can be used. In order to make DCPMM security management consistent with other storage devices, HP has added a new feature, "Transparent Unlock", that lets both the user and admin unlock the DCPMMs, using their respective BIOS passwords, without having to know any of the passphrases. The actual DCPMM passphrases are generated by the workstation BIOS, set in the DCPMMs, and copies are stored on the motherboard using a separate layer of encryption, managed by the TPM. When an authorized user enters correct the BIOS power-on or admin password, the BIOS retrieves the passphrase copies, decrypts them using the TPM, and sends them to the individual DCPMMs to unlock them. This mechanism also avoids having to reuse identical passphrases across multiple DCPMMs.
  - Users can still enter per-DCPMM passphrases when Transparent Unlock is enabled, for instance when adding new DCPMMs to an existing set.
  - Transparent Unlock requires:
    - Secure Boot
    - TPM 2.0
    - The power-on BIOS password must be set (the administrator password may also be set)
- Migration
  - To simplify DCPMM migration between workstations, the BIOS includes a passphrase import/export feature, that can save the passphrases to a text file on a USB stick. The file itself can be independently encrypted using a user-supplied passphrase, so that theft or loss of the stick does not result in a security breach.
- Secure Erase
  - HP has also extended the BIOS Secure Erase feature to cover DCPMMs. Secure Erase first erases the internal encryption key on the DCPMM so that the contents cannot be decrypted, then erases the actual DCPMM media contents for reuse. Secure Erase follows NIST SP 800-88 rev.1 and ISO-IEC 27040.
- DCPMM security settings can be managed like other BIOS settings, through the F10 Setup Menu interface, and remotely using WMI tools including BiosConfigUtility.exe for Windows, and hp-repsetup for Linux. (Some NVDIMM management settings are only available through F10 Setup).

# SYSTEM REQUIREMENTS

- Processor Support
  - Not all processors support DCPMM. See **Z6 G4** and **Z8 G4** QuickSpecs for list of processors that support DCPMM.
  - Processor Memory Limits.
 

There are limits on the total amount of system memory capacity supported per processor.

    - Memory Mode:
      - > For purpose of meeting the processor limitations, the system memory capacity is defined

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

as the total of DCPMM capacity. The DRAM capacity does not count towards system memory (since it is serving only as cache).

- Storage Mode:
  - > For purpose of meeting the processor limitations, the system memory capacity is defined as the sum of the DCPMM capacity and DRAM capacity installed in the system
- “Base Memory” processors support up to 1TB of memory per processor, 2 TB per system for dual processor systems
- “Large Memory Optimized” processors supports up to 2TB of memory per processor, 4TB per system
  - > These processors are identified by having a “M” suffix added to the model number

- Recommended DCPMM vs memory ratios
  - In Memory Mode, HP recommended DRAM to DCPMM memory ratio is 1:8.
    - Example: 2x128 GB DCPMM should contain 32 GB of DRAM memory
    - Maximum performance is available by distributing the memory across as many memory channels as possible
    - HP factory-configured systems optimize the configuration for the customer
  - In Storage/App Direct Modes, there is no recommended ratio. Choose System Memory capacity as you would normally for any specific workloads.
- System requirements/limitations
  - HP Z6 G4 and Z8 G4 Workstations with DCPMM only support Registered Memory Configurations.
    - HP currently does not support DCPMM with LR DIMMs (Load Reduced Memory) configurations
  - Only a single DCPMM per memory channel is supported.
    - Z6 G4 Max DCPMM support: 4 modules per processor
    - Z8 G4 Max DCPMM support: 6 modules per processor
  - HP does not support mixing DCPMM capacities in a system.
  - Z6 G4 requires the Memory cooling duct in order to cool the DRAM and DCPMM modules appropriately.
  - With DCPMM in Memory Mode only NUMA memory mode is supported.
- Minimum BIOS/Firmware/OS support
  - BIOS: version 2.35 or later.
  - DCPMM Firmware version: 1.2.0.5417 or later.
  - Windows support:
    - Minimum: Windows 10 Pro for Workstations, 1903 or later, with all updates applied
  - Linux Support:
    - Linux has support for persistent memory devices as of kernel 4.0, but it is recommended that you use kernel 4.2 or above
    - You will need the community **ndctl** utility and the Intel **ipmctl** utility to update device firmware, configure goals and regions on your devices, and to configure your device's namespaces
    - Minimum OS versions:
      - > Ubuntu: 18.04 LTS
      - > Red Hat Enterprise Linux: 7.6, 8.0
      - > SUSE Linux Enterprise Desktop: 12 SP4, 15

# SYSTEM SETUP OVERVIEW

This section gives a high-level view of the steps needed to configure a system with DCPMMs. Most of the operations described here can be accomplished in various environments:

- BIOS F10 Setup
- Windows 10
- Linux
- UEFI Shell

Detailed procedures are covered in Appendices A through D for these environments.

## Basic steps for an initial setup

1. Choose the mode in which DCPMMs will be used:
  - Memory Mode
  - Storage Mode
  - App Direct Mode

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

2. Set up the hardware:
  - a) Check system setup as outlined in the above System Requirements Section.
  - b) Configure the hardware. See the “How to Configure System HW” subsection below.
  - c) HP Recommends BIOS and DCPMM FW be updated to latest version before SW configuration begins.
3. Put the modules into the desired mode (see appendices A through D as appropriate)
  - To set up the DCPMM into Memory Mode:
    - a) Configure NVDIMMs to Memory Mode following the procedure in the appropriate appendix (A through D).
    - b) Verify setup in BIOS and in the OS to make sure that the memory is reported as expected.
  - To set up the DCPMM into Storage Mode:
    - a) Create a Region (in F10 setup, automatically also creates namespace).
    - b) Create Namespace **with BTT** (only necessary if the region was created in UEFI or OS).
    - c) Enable BTT.
    - d) Enable Security if desired.
    - e) Go into the OS to partition and format the drive.
      - HP recommends that DAX be enabled in the file system
    - f) Review result and verify setup.
  - To set up the DCPMM into App Direct Mode:
    - a) Create a Region (in F10 Setup, automatically creates namespace).
    - b) Create Namespace **without BTT** (only necessary if the region was created in UEFI or OS).
    - c) Enable Security if desired.
    - d) Go into the OS to partition and format the drive.
    - e) Review result and verify setup.

## How to Configure System HW: DCPMM & Memory Load order/rules

- Load Rules:
  - At least one DRAM DIMM is required on the same side (memory controller) of a processor as a DCPMM.
  - Load the DRAM first and then load the DCPMM.
  - Load the memory modules in order of size, starting with the largest DRAM module.
  - After the DRAM memory is installed, continue to follow the loading order with the DCPMM.
  - See Service panel label on Chassis cover or the **Z6 G4** or **Z8 G4** Workstation Technical White paper for the complete memory loading rules.
  - See Appendix G for details on recommended module loading.
- Memory Mode:
  - To maximize bandwidth, install DRAM across as many channels as possible.
- Storage Mode
  - HP recommends loading the DCPMM in sets of two modules per CPU (to allow interleaving).
  - For a configuration of two DCPMMs on a dual processor system, HP recommends installing both DCPMMs on the first processor.

## Maintaining and upgrading modules

Here we outline some other common tasks associated with managing a system with DCPMMs. Detailed procedures are covered in Appendices A through D and in Appendix F.

- Update Firmware
  - There are occasions that will require the firmware on the DCPMM to be updated. When these occasions occur, HP will provide the firmware binary as a SoftPaq on the HP support website. The preferred method to update firmware is through F10 Setup. Firmware can also be updated from the OS or UEFI shell.
- Memory Mode:
  - Reconfigure (add, subtract, replace DCPMMs).
    - Install the DCPMM in the correct location based on the recommended loading rules
    - Verify setup in BIOS and in the OS
- Storage Mode:
  - Back up data
    - Data on DCPMM is to follow present day customer/company specific standards for ensuring there is a backup of important files crucial for day to day business. DCPMM backup should follow practices used on SATA, SAS, and NVMe® storage devices
  - Reset/reconfigure
    - There might be instances when you want to reset one or more DCPMM modules. This could be

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

to change the configuration or redeploy the hardware to a new user. Instructions for resetting DCPMM modules can be found in Appendix F

- Delete Namespace.
  - Deleting a namespace will remove all data from a DCPMM. Ensure that all data that needs to be retained is backed up prior to removing the namespace
  - Instructions for deleting a namespace can be found in the procedural appendices below
- Secure erase.
  - If all data needs to be removed from a DCPMM in a secure fashion, HP provides a Secure Erase mechanism in F10 Setup. More details about Secure Erase and instructions for performing a Secure Erase on a DCPMM can be found in Appendix E

# APPENDICES

## Configuring DCPMM – BIOS F10 Setup

### Update Firmware

1. Download and extract the SoftPak.
  - If there are system BIOS prerequisites for the firmware update, ensure that the system BIOS is updated prior to updating firmware on the DCPMM. BIOS prerequisites will be stated in the SoftPak notes.
2. Copy the contents of the SoftPak to a USB key.
3. Insert the USB key into an open USB port and turn on the workstation.
4. Press F10 during post to enter F10 Setup.
5. Navigate to the “Advanced” tab.
6. Click on “NVDIMM Management”.
7. Click on “Update Firmware on NVDIMMs”.
8. In the “Select File System” screen, select the USB key that contains the updated firmware.
9. Select the firmware file.
10. You will see a message confirming the firmware has been staged to the DCPMM, as well as the firmware version that has been loaded to each DCPMM.
  - For the firmware to be activated on the DCPMMs, a power cycle is required.
  - Click “Yes” to power cycle the system.
11. After the power cycle is complete, the new firmware will be active on the DCPMM.

### Memory Mode

1. Power on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Advanced” tab.
4. Click on “NVDIMM Management”.
5. Click on “NVDIMM Configuration”.
6. Select “Volatile Memory” in the drop-down menu.
7. Click on “Apply NVDIMM Configuration”.
8. You will be presented with the requested configuration.
  - Click “Yes” to continue.
    - If namespaces exist on the specified DCPMMs, the namespaces must be removed before you can configure the DCPMMs in Memory Mode – Instructions to remove namespaces are provided below.
9. A reboot is required to complete configuration. Click on the “OK” button to reboot the workstation.
10. After reboot, the workstation will return to the NVDIMM Management section in F10 Setup, where you can view that the configuration is complete.
11. Exit F10 Setup.

### Storage Mode

1. Power on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Advanced” tab.
4. Click on “NVDIMM Management”.
5. Click on “NVDIMM Configuration”.
6. Select “Persistent Memory with BTT” in the drop-down menu.



1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

- Click on “Apply NVDIMM Configuration”.
- You will be presented with the requested configuration.
  - Click “Yes” to continue.
    - If namespaces exist on the specified DCPMMs, the namespaces must be removed before you can configure the DCPMMs in Memory Mode – Instructions to remove namespaces are provided later in the document.
- A reboot is required to complete configuration. Click on the “OK” button to reboot the workstation.
- After reboot, the workstation will return to the NVDIMM Management section in F10 Setup, where you can view that the configuration is complete.

## Creating a Namespace

Namespaces are only required for Storage and App Direct Modes. This step is normally not required if the Region was created using F10 Setup as it will create the Namespace automatically.

- Power on the workstation.
- Press F10 to enter F10 Setup.
- Navigate to the “Advanced” tab.
- Click on “NVDIMM Management”.
- Click on “NVDIMM Namespace Management”.
- Select the Region ID(s) on which to create a namespace.
- By default, the entire capacity is used for the namespace.
  - If you would like to change this setting, click on “Namespace Capacity” and enter the desired capacity.
- By default, the namespace will be named “NewNameSpace”.
  - If you would like to change this setting, click on “Enter Namespace Name” and enter the desired string.
- For Storage Mode, ensure “Enable Storage Over AppDirect” is checked.
- Click on “Create Namespace”.
- Press F10 to save changes and exit F10 Setup.

## Deleting a Namespace

**Warning** - Deleting a Namespace will also delete all data contained on the namespace. Ensure any critical data is backed up prior to deleting a namespace.

- Power on the workstation.
- Press F10 to enter F10 Setup.
- Navigate to the “Advanced” tab.
- Click on “NVDIMM Management”.
- Click on “NVDIMM Namespace Management”.
- Select the namespace(s) you would like to delete.
- Click on “Delete Selected Namespace”.
- Confirm that you understand deleting the namespace will also delete all data from the namespace by clicking “Yes”.
- Press F10 to save changes and exit F10 Setup.

# Configuring DCPMM – Windows

## Software

- HP provides a SoftPaq that includes the Intel® Optane™ DC Persistent Memory Software utilities (DCPM\_Software.exe) – Download the SoftPaq and install this software.

## Update Firmware

- Open an Administrator Command Prompt.
- Change directory to c:\program files\Intel\DCPM Software, or wherever the DCPMM Software is installed.
- Verify the firmware image file fwname by using the following command:  
ipmctl.exe load -source “fwname” -examine -dimm  
If ipmctl.exe is in the same directory as the firmware, only the firmware file name is required. If ipmctl.exe and the firmware file are in different directories, the full path to the firmware file is required.
- Stage the firmware in the DCPMMs by using the following command:  
ipmctl.exe load -source “fwname” -dimm
- Verify the firmware was staged properly by using the following command:  
ipmctl.exe show -dimm -firmware
- Power cycle the workstation.
- After the power cycle is complete, the new firmware will be active on the DCPMMs.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

## Memory Mode

1. Power on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Security” tab.
4. Click on “NVDIMM Security Freeze”.
5. Select “5” from the drop-down menu for “Unfreeze NVDIMMs for this number of boot sequences”.
6. Press F10 to save changes and exit F10 Setup.
7. Boot into Windows.
8. Open an Administrator Command Prompt.
9. Change directory to c:\program files\Intel\DCPM Software, or wherever the DCPM Software is installed.
10. Configure the DCPMMs as volatile memory by using the following command:
  - ipmctl.exe create -goal MemoryMode=100
  - Press ‘y’ and then press ‘enter’
11. A reboot is required to complete the configuration.

## Storage Mode

1. Power on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Security” tab.
4. Click on “NVDIMM Security Freeze”.
5. Select “5” from the drop-down menu for “Unfreeze NVDIMMs for this number of boot sequences”.
6. Press F10 to save changes and exit F10 Setup.
7. Open an Administrator Command Prompt.
8. Change directory to c:\program files\Intel\DCPM Software, or wherever the DCPM Software is installed.
9. Configure the DCPMMs as persistent memory by using the following command:
  - ipmctl.exe create -goal persistentmemorytype=appdirect
  - Press ‘y’ and then press ‘enter’
10. A reboot is required to complete the configuration.

## Creating a Namespace

1. Open an Administrator Windows PowerShell prompt.
2. Interrogate the system to learn the available region ID(s) by running the following command:  
Get-PmemUnusedRegion  
The output will provide region ID(s) in a table format.
3. Create a namespace using a region ID RegionID as found in the previous step by running the following command:  
New-PmemDisk -RegionID “RegionID” -AtomicityType BlockTranslationTable

## Deleting a Namespace

**Warning** - Deleting a Namespace will also delete all data contained on the namespace. Ensure any critical data is backed up prior to deleting a namespace.

1. Open an Administrator Windows PowerShell prompt.
2. Interrogate the system to learn the available DiskNumber(s) by running the following command:  
Get-PmemDisk  
The output will provide DiskNumber(s) in a table format.
3. Delete the namespace by running the following command:  
Remove-PmemDisk -DiskNumber “DiskNumber”  
You will be asked to confirm the removal of the namespace, and all data associated with the namespace. Press “y” and then “enter”.

## Formatting DCPMM

1. Open an Administrator Windows PowerShell prompt.
2. Interrogate the system to learn the available DiskNumber(s) by running the following command:  
Get-PmemDisk  
The output will provide DiskNumber(s) in a table format.
3. To initialize the disk, use the following commands:
  - Initialize-Disk -number “DiskNumber” -PartitionStyle GPT
  - New-Partition -DiskNumber “DiskNumber” -AssignDriveLetter -UseMaximumSize

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

There will be a prompt to format the disk – Click on the “Cancel” button. The disk will be formatted in the next step.

- Format-Volume -DriveLetter "DriveLetter" -isDax 1
4. Dax Mode can be verified by using the following command:
- Fsutil fsinfo volumeinfo "DriveLetter:"

The drive letter must be followed by a colon.

(This same formatting procedure can be used in App Direct Mode if the Namespace does not have the BTT attribute).

## Configuring DCPMM – Linux

### Software

1. HP does not provide the Intel® Optane™ DC Persistent Memory Software or ndctl utilities for Linux.
2. To install ndctl:
  - On RHEL 8: “sudo yum install ndctl”.
  - On SLED 15: “sudo zypper install ndctl”.
  - On Ubuntu 18.04: “sudo apt install ndctl”.
  - It is recommended that you update your system before installing ndctl.
3. To install ipmctl, you must download and compile the source code from Intel’s Github repository at <https://github.com/intel/ipmctl>
  - Follow the instructions in the README.md document to compile and install.
  - You will need to manually install some dependencies before you are able to compile ipmctl.
  - Some distributions (such as fedora and SLED) may have ipmctl available in their package managers.
  - It is recommended that you update your system before compiling and installing ipmctl.

### Update Firmware

1. Run:
  - ipmctl load -source “firmware file” -examine -dimm  
This will check each DIMM for compatibility with the new firmware.
  - ipmctl load -source “firmware file” -dimm  
Without the “-examine” option, ipmctl will stage an update for the firmware on each DIMM.
  - ipmctl show -dimm -firmware  
Will show that the update has been properly staged.
  - poweroff  
Power down the system and turn it back on to activate the firmware on the DIMMs.

### Memory Mode

1. Power on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Security” tab.
4. Click on “NVDIMM Security Freeze”.
5. Select “5” from the drop-down menu for “Unfreeze NVDIMMs for this number of boot sequences”.
6. Press F10 to save changes and exit F10 Setup.
7. Log into a terminal window as the root user or use “sudo” for the following commands.
8. ipmctl create -dimm -goal MemoryMode=100  
“100” is the percent of capacity that will be dedicated to volatile memory.

### Storage Mode

1. Power on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Security” tab.
4. Click on “NVDIMM Security Freeze”.
5. Select “5” from the drop-down menu for “Unfreeze NVDIMMs for this number of boot sequences”.
6. Press F10 to save changes and exit F10 Setup.
7. Log into a terminal window as the root user or use “sudo” for the following commands.
8. ipmctl create -dimm -goal MemoryMode=0 PersistentMemoryType=[AppDirect/AppDirectNotInterleaved]
  - “0” is the percent of the goal dedicated to volatile memory.
  - You may choose between the AppDirectNotInterleaved memory type, which creates a separate storage pool on each DCPMM device, or an AppDirect memory type, which will interleave the DCPMM devices to create a single storage pool, similar to a RAID 0.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

## Creating a Namespace

To create and manage Namespaces, we use the `ndctl` utility

1. `ndctl list -NDR`  
This command will list all namespaces, devices, and regions on the system. Regions are the AppDirect/ AppDirectNotInterleaved pools we made in the previous step.
2. `ndctl create-namespace`  
This command will create an `fsdax` namespace with default parameters.
3. `ndctl create-namespace -m [raw/sector/fsdax/devdax]`  
using the `-m` (or `--mode=`) option will allow you to specify the mode of your namespace.

**There are four modes for namespaces in linux:**

1. `raw` mode will create a memory disk that does not support `dax`.
2. `sector` mode will enable BTT, which will ensure write atomicity at the cost of some performance.
3. `fsdax`, or `filesystem-dax`, is used to enable direct access on file systems and is the default mode when creating a namespace with `ndctl`. This mode will enable `dax`-aware file systems to take advantage of the features of `dax`.
4. `devdax`, or `device-dax`, enables memory mapping capabilities similar to `fsdax`, however instead of creating a block device capable of supporting a file system, `devdax` creates a character device. This character device can be used for assigning persistent memory to virtual machines, registering memory for RDMA, or for when gigantic memory mappings are required.

Please consult the `ndctl` documentation at <http://pmem.io/ndctl/> for more information on any of these modes.

- Use the `-r` (`--region=`) option to specify the region you want to create the namespace on if you've configured your system with multiple regions.

## Deleting a Namespace

**Warning** - Deleting a Namespace will also delete all data contained on the namespace. Ensure any critical data is backed up prior to deleting a namespace.

To delete a namespace, you must first disable and then delete using `ndctl`.

1. `ndctl list -N`
  - Will display all namespaces on the system. Note the namespace you wish to delete. Namespaces will usually have names like "namespace0.0" unless you set a custom one during namespace creation.
2. `ndctl disable-namespace namespace0.0`
  - this command will disable the namespace named "namespace0.0".
3. `ndctl destroy-namespace namespace0.0`
  - once the namespace is disabled, it can be deleted with the `destroy-namespace` command.

## Formatting DCPMM

1. Once you have the namespaces set up, the DCPMM device should show up as `/dev/pmem[N]` in your system (or something similar – different namespaces show up in the system differently). If it is a "sector" namespace, you can format this device or add it to a volume group or software RAID as you would with any normal block device. Consult your distribution's documentation on how to do this.
2. To enable `filesystem-dax` on a namespace created with the `fsdax` mode, the file system block size must be the same as the kernel page size. To determine the kernel page size, run this command:
  - `getconf PAGESIZE`  
This command should return your kernel page size.
  - You must then specify a block size for the file system the same size as the kernel page size during file system creation. An example for EXT4 file system:
    - `mkfs.ext4 -b <kernel page size> </path/to/device>`  
example: `mkfs.ext4 -b 4096 /dev/pmem1`
  - Once you have your file system set up, you need to mount it with the `dax` option to enable `dax`.
    - `mount -odax <other options> </path/to/device> </mount/point>`  
example: `mount -odax /dev/pmem1 /mnt/dcpmm`



1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

# Configuring DCPMM – UEFI Shell

## Software

- To create a bootable UEFI Shell USB key use the following steps:
  - Download the following file - <https://github.com/tianocore/edk2/blob/UDK2018/ShellBinPkg/UefiShell/X64/Shell.efi>
  - Rename the file to bootx64.EFI
  - Copy the file to a FAT32 formatted USB key in the following directory: \EFI\Boot\
- Included with the DCPMM firmware SoftPak is an UEFI executable (ipmctl.efi).
  - If there are system BIOS prerequisites for the firmware update, ensure that the system BIOS is updated prior to updating firmware on the DCPMM. BIOS prerequisites will be stated in the SoftPak notes.
- Copy the contents of the SoftPak to a bootable UEFI Shell USB key.

## Update Firmware

- Insert the USB key into an open USB port and turn on the workstation.
- Press F9 during post to enter the Boot Menu.
- You will be presented with a menu that includes all bootable sources.
  - Select the bootable UEFI Shell USB key.
- Select the file system of the USB key.
  - Often the file system of the USB Key is FS0, but it can vary.
- Navigate to where the firmware and utility were copied.
- Verify the firmware image in file fwname by using the following command:
  - ipmctl.efi load -source "fwname" -examine -dimm
    - If ipmctl.efi is in the same directory as the firmware, only the firmware file name is required. If ipmctl.efi and the firmware file are in different directories, the full path to the firmware file is required.
- Stage the firmware in the DCPMMs by using the following command:
  - ipmctl.efi load -source "fwname" -dimm
- Verify the firmware was staged properly by using the following command:
  - ipmctl.efi show -dimm -firmware
- Power cycle the workstation.
- After the power cycle is complete, the new firmware will be active on the DCPMMs.

## Unfreeze Security on NVDIMMs

Some configuration commands using the ipmctl.efi tool require security on the NVDIMMs to remain in an Unfrozen state. To Unfreeze Security for a limited number of boots:

- Power on the workstation.
- Press F10 to enter F10 Setup.
- Navigate to the "Security" tab.
- Click on "NVDIMM Security Freeze".
- Select "5" from the drop-down menu for "Unfreeze NVDIMMs for this number of boot sequences".
- Press F10 to save changes and exit F10 Setup.

## Memory Mode

- Insert the USB key into an open USB port and turn on the workstation.
- Press F10 to enter F10 Setup.
- Navigate to the "Security" tab.
- Click on "NVDIMM Security Freeze".
- Select "5" from the drop-down menu for "Unfreeze NVDIMMs for this number of boot sequences".
- Press F10 to save changes and exit F10 Setup.
- Press F9 during post to enter the Boot Menu.
- You will be presented with a menu that includes all bootable sources.
  - Select the bootable UEFI Shell USB key.
- Select the file system of the USB key.
  - Often the file system of the USB Key is FS0, but it can vary.
- Navigate to where the utility was copied.
- Configure the DCPMMs as volatile memory by using the following command:
  - ipmctl.efi create -goal MemoryMode=100
  - Press 'y' and then press 'enter'.
- A reboot is required to complete the configuration.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

## Storage Mode

1. Insert the USB key into an open USB port and turn on the workstation.
2. Press F10 to enter F10 Setup.
3. Navigate to the “Security” tab.
4. Click on “NVDIMM Security Freeze”.
5. Select “5” from the drop-down menu for “Unfreeze NVDIMMs for this number of boot sequences”
6. Press F10 to save changes and exit F10 Setup.
7. Press F9 during post to enter the Boot Menu.
8. You will be presented with a menu that includes all bootable sources.
  - Select the bootable UEFI Shell USB key.
9. Select the file system of the USB key.
  - Often the file system of the USB Key is FS0, but it can vary.
10. Navigate to where the utility was copied.
11. Configure the DCPMMs as volatile memory by using the following command:
  - `ipmctl.efi create -goal persistentmemorytype=appdirect`
  - Press ‘y’ and then press ‘enter’.
12. A reboot is required to complete the configuration.

## Creating a Namespace

1. Insert the USB key into an open USB port and turn on the workstation.
2. Press F9 during post to enter the Boot Menu.
3. You will be presented with a menu that includes all bootable sources.
  - Select the bootable UEFI Shell USB key.
4. Select the file system of the USB key.
  - Often the file system of the USB Key is FS0, but it can vary.
5. Navigate to where the utility was copied.
6. Interrogate the system to learn the available region ID(s) by running the following command:
 

```
ipmctl.efi show -region
```

  - The output will provide region ID(s) in a table format.
7. Create a namespace using a region ID regionID as found in the previous step by running the following command:
  - `ipmctl.efi create -namespace -region “regionID” Mode=Sector`

## Deleting a Namespace

**Warning** - Deleting a Namespace will also delete all data contained on the namespace. Ensure any critical data is backed up prior to deleting a namespace.

1. Interrogate the system to learn the available namespace ID(s) by running the following command:
 

```
ipmctl.efi show -namespace
```

  - The output will provide namespace ID(s) in a table format.
2. Delete a namespace by running the following command:
 

```
ipmctl.efi delete -namespace “namespace ID”
```

  - Confirm that you would like to delete the namespace by pressing “y” and then “enter”.

## Security Procedures

DCPMM uses full-time hardware encryption, even in Memory Mode. The encryption algorithm is XTS-AES256, a common choice for self-encrypting drives (SEDs). Encryption on each DCPMM uses an internal symmetric key that cannot be read by the workstation.

In Memory Mode, a new key is created at every reset, and deleted at every power off, so that contents cannot be retrieved across resets or power cycles, or by removing the memory modules. DCPMM passphrases are not used in this mode.

In App Direct Mode and Storage Mode, the internal key is non-volatile and can be tied to a user passphrase, so that entering the passphrase unlocks the DCPMM. The passphrase is stored on the DCPMM and is unique to the module. As shipped, the DCPMMs do not have a passphrase set and on-device encryption is invisible to the rest of the computer (it applies to data at rest only).

This single-passphrase model differs from traditional disk security (e.g. HP DriveLock) where distinct user and admin passwords can be used. In order to make DCPMM security management consistent with other storage devices, HP has added a new feature, “Transparent Unlock”, that lets both the user and admin unlock the DCPMMs,

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

using their respective BIOS passwords, without having to know any of the passphrases. The actual DCPMM passphrases are generated by the workstation BIOS and copies are stored on the motherboard using a separate layer of encryption, managed by the TPM. This also avoids having to reuse passphrases across multiple DCPMMs.

## Enabling Transparent Unlock (recommended)

1. Set power-on password and reboot.
2. In F10 Setup go to Security > NVDIMM Transparent Unlock and check ☒ Enable NVDIMM Transparent Unlock by selecting the setting and pressing Enter.
3. Save changes.
4. This sets up a different machine-created random passphrase on each DCPMM.
5. To be able to recover DCPMM data if you forget or reset your BIOS passwords, you are prompted to insert a USB key (FAT32) to export DCPMM passphrases.
6. You are then prompted to select between “Encrypted or plain text?”
7. Encrypted: prompts for encryption password (used only for encrypting this file, it is separate from the BIOS power-on and administrator passwords). saves to .der file (binary) using PKCS7 (Cryptographic Message Syntax Standard), a common method to encrypt messages, including email.
8. Plain text: saves to UTF16 text file. Keep the USB key in a safe location!
9. File is saved to root folder. Name is NVDIMMPassphrases\_GUID\_date.txt, e.g. NvdimmPassphrases\_ACF42627-1FCF-9B8F-FA9C-1C549637D132\_2019-05-08T212307Z.txt, or NVDIMMPassphrases\_GUID\_date.der if encrypted.
10. Workstation power cycles.
11. BIOS asks for power-on password on reboot; when entered, this automatically unlocks all the NVDIMMs.

## Viewing DCPMM passphrases

1. Enter F10 Setup.
2. Go to Security > NVDIMM Transparent Unlock > Show NVDIMM passphrases.
3. Enter BIOS password again.
4. Passphrases are displayed.

## Exporting DCPMM passphrases

See above under the procedure “Enable Transparent Unlock”.

## Viewing the Transparent Unlock log

The Workstation BIOS maintains a log of Transparent Unlock operations, including failures to unlock. The log contains 32 entries and is circular. You can view the log using BCU (BiosConfigUtility) in Windows and Linux. The following is a sample log output:

### NVDIMM Transparent Unlock Log Entries

```
[INFO] 2019-05-07 11:30 Successfully exported passphrases to plain text file.
[INFO] 2019-05-07 11:30 Transparent unlock enabled.
[ERROR MINOR] 2019-05-08 09:58 Failed exporting passphrases to file.
[INFO] 2019-05-08 09:59 Successfully exported passphrases to encrypted file.
[INFO] 2019-05-08 10:03 Transparent unlock disabled.
[INFO] 2019-05-08 10:07 Successfully exported passphrases to plain text file.
[INFO] 2019-05-08 10:07 Transparent unlock enabled.
[INFO] 2019-05-08 10:11 Transparent unlock disabled.
```

## Disabling Transparent Unlock

1. Enter F10 Setup.
2. Go to Security > NVDIMM Transparent Unlock and uncheck ☐ Enable NVDIMM Transparent Unlock by selecting the setting and pressing Enter.
3. Save changes.
4. Notification screen: “Transparent Unlock has been disabled”, “All NVDIMMs’ security passphrases have been disabled.”
5. Workstation power cycles.
6. This removes passphrases from each DCPMM. It does not erase any data.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

## Recovering NVDIMMs with lost passphrases

1. If you are unable to unlock an NVDIMM because you do not know its passphrase, you can still clear the passphrase and reuse the NVDIMM. This destroys all data on the NVDIMM. To recover:
2. Enter F10-Setup.
3. Go to Security > NVDIMM lost passphrase recovery.
4. Select the NVDIMMs that you want to recover.
5. Select "Continue" to confirm that you want the contents erased.

## Power-on password and Transparent Unlock

If you clear the power-on password, Transparent Unlock is temporarily inaccessible until a new power-on password is created, but the NVDIMMs are still locked. The Transparent Unlock key and DCPMM passphrases are not cleared during this process. To disable Transparent Unlock, see above.

## Using DriveLock to set passphrases manually

1. HP DriveLock is the existing mechanism to manage disk drive passwords; it has been extended to accommodate DCPMMs.
2. With DriveLock, you need to enter each DCPMM passphrase separately on every boot. BIOS passwords (administrator or power-on) are not needed.
3. Note that each Optane DCPMM only has a single passphrase, which is handled as the DriveLock user password. There is no DriveLock master password.
4. Security > Hard Drive Utilities > DriveLock/Automatic DriveLock.
5. Select a drive.
6. The user interface shows the list of NVDIMMs and their locations.
7. Select the first DCPMM and press Enter.
8. Opens DriveLock Security Options menu.
9. At the "Enable DriveLock" prompt, press Enter.
10. Set DriveLock User Password, enter it again to confirm.
11. Changes are applied immediately.
12. Repeat for each DCPMM.
13. Exit F10-Setup.
14. Workstation power cycles.
15. On reboot:
16. POST Power-On Password prompt if present.
17. DriveLock User Password prompt for each DCPMM.
18. "Correct password entered" appears briefly.

## About Automatic DriveLock

Automatic DriveLock is a Workstation BIOS feature that lets you reuse the BIOS power-on and administrator passwords as the drive user and master passwords, respectively, so that you do not have to enter the drive passwords from the keyboard on every boot. Because Optane DCPMM does not have separate user and master passwords, Automatic DriveLock cannot be used with DCPMM.

## About ndctl

ndctl is a Linux-based tool to manage DCPMMs. When Transparent Unlock is enabled, you cannot use ndctl to manage passphrases. The BIOS also freezes the DCPMMs before booting, which locks out ndctl from other operations.

## About Bitlocker and other drive encryption tools

Existing drive encryption tools do not know how to handle DCPMM encryption and cannot be used with DCPMM.

## Unfreezing

The BIOS normally freezes the NVDIMMs before booting. This makes it impossible for OS-based software to modify or set passphrases, which prevents ransomware-type attacks where malware installs its own passphrases, locking you out of the NVDIMM data. You can temporarily unfreeze the NVDIMMs for a set number of boot cycles from F10-Setup. To unfreeze:

1. Enter F10-Setup.
2. Go to Security > NVDIMM security freeze.



1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

3. Select for how many reboots (1-5) you want to keep the NVDIMMs unfrozen.
4. Save and Exit.

## Secure Erase

1. Secure Erase works by deleting the internal encryption key and generating a new one, which instantly crypto-scrambles/randomizes all existing user data in the DCPMM and marking the contents as erased. The contents are then sampled for validation.
2. Secure Erase follows NIST SP 800-88 rev.1 and ISO-IEC 27040.
3. If Transparent Unlock is enabled, you must disable it first (see above).
4. If Namespaces are enabled, you must delete them first (see above).
5. Security > Hard Drive Utilities > Secure Erase.
6. In the "Select a Drive" list, select the first DCPMM to erase.
7. Select "Continue".
8. If there is no passphrase on the DCPMM at this point, you must create one so that the contents stay protected in case the secure erase operation aborts. "Please enter a DriveLock password to allow the drive to be erased." Re-enter the passphrase to confirm.
9. The actual erase process takes under a second.
10. Repeat for all DCPMMs to erase.

## Statement of Volatility

Like other memory and storage devices, the DCPMM will retain information after the system is shut down. When clearing the info from a module, it is important to clear both types of Non-Volatile memory on the module:

1. Like DRAM memory, the DCPMM contains an SPD. The SPD memory will not be modified during standard operation of the workstation system. It will not hold any user data or settings. This NVM memory could potentially be vulnerable due to the fact that it can be modified freely using third party tools. If there is a possibility that the SPD region has been tampered with, HP recommends either re-writing the SPD with third party tools.
2. DCPMM also contains storage media that can be cleared using the Secure Erase process outline above.

If there are concerns around retaining information on the module, destroy the DCPMM.

# DCPMM System Management Tasks

## Migrating DCPMMs

### Migrating DCPMMs without data retention

When moving a set of DCPMMs to another system, the recommended procedure is to back up all data, reconfigure the DCPMM, then restore the data to the DCPMM. In Memory Mode it is not necessary to back up and restore as there is no persistent data on the DCPMMs.

1. Back up all data from the DCPMM if they are in a Persistent Memory mode.
2. Install the DRAM in the new system in same configuration as the previous system (or following the configuration rules in Appendix G).
3. Power on the system. Update BIOS to the latest version.
4. Move the DCPMMs from the previous system to the new system in exactly the same configuration noting which DCPMMs are in which DIMM slots (following the configuration rules in Appendix G).
5. Go into F10 Setup and reconfigure the DCPMMs in Advanced -> NVDIMM Configuration.
6. Complete the configuration following the steps in the section "Configuring DCPMM – BIOS F10 Setup".
7. Restore all data back to the storage volume(s) on the DCPMMs.

### Migrating DCPMMs with data retention

If it is necessary to move DCPMMs in a Persistent Memory mode and retain the data on the DCPMM follow these steps. This is the procedure to use when replacing the motherboard.

1. The DRAM in the new system must be in the same configuration and DIMM slots as the old system.
2. If Transparent Unlock is enabled (see Appendix E), export the current passphrases to a USB stick.
3. Turn AC power off. Remove the DCPMMs from the source workstation, and for each one note down the DIMM slot it came from and the last digits of the serial number.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

4. With the AC power off, install each DCPMM into the target workstation, using the same DIMM slots as on the source workstation.
5. Reboot the system and check for any POST errors. If the DCPMMs are not installed in the correct DIMM slots you may see a POST message indicating the correct DIMM slot(s). Note down the correct slots, power off the workstation, and move the DCPMMs to these DIMM slots.
6. If DCPMM passphrases were set on the source workstation, you will be prompted for the passphrases for the these DCPMMs on the target workstation. If Transparent Unlock was enabled on the source workstation, import the passphrase file from the USB stick.
7. The storage volume(s) on the DCPMMs should be seen by the target workstation with all data still present. It is not necessary to configure the DCPMMs in F10 Setup. The previous configuration will be retained.

## DCPMM Status Checks

1. All the following commands can be run from the UEFI Shell command prompt. Those noted cannot be run from Windows.
2. To create a bootable UEFI Shell USB key use the following steps:
  - Download the following file – <https://github.com/tianocore/edk2/blob/master/ShellBinPkg/UefiShell/X64/Shell.efi>
  - Rename the file to bootx64.EFI
  - Copy the file to a FAT32 formatted USB key in the following directory: \EFI\Boot\
3. Download the SoftPaq that includes the Intel® Optane™ DC Persistent Memory EFI utility (ipmctl.efi)
  - Extract and copy the contents of the SoftPaq to the bootable UEFI Shell USB key.
4. For Windows, HP provides a SoftPaq that includes the Intel® Optane™ DC Persistent Memory Software utilities (DCPM\_Software.exe) – Download the SoftPaq and install this software.
5. Commands to view configuration:
  - ipmctl.efi show -memoryresources
    - This shows the configuration when in Memory Mode.
  - ipmctl.efi show -a -region
    - This shows the AppDirect regions present on the modules.
  - ipmctl.efi show -a namespace
    - This shows the AppDirect namespaces present on the modules.
    - This command does not work in Windows, instead use Get-PmemDisk from an Administrator PowerShell prompt.
  - ipmctl.efi show -a -socket
    - This shows the memory limit of the processor.
6. Commands to check the status of the modules.
  - ipmctl.efi show -dimm
    - This shows information about all installed DCPMMs – DimmID, Capacity, HealthState, LockState, FW Revision.
  - ipmctl.efi show -sensor
    - This shows basic health information about all installed DCPMMs.
  - ipmctl.efi show -topology
    - This shows the topology of installed DCPMMs and DRAM.
  - ipmctl.efi show -socket
    - This shows the memory limit of the installed processor(s).
  - ipmctl.efi show -memoryresources
    - This shows information about how the installed DCPMMs are configured.
  - ipmctl.efi show -sensor ControllerTemperature
    - This shows the controller temperature of the installed DCPMM.
  - ipmctl.efi show -sensor MediaTemperature
    - This shows the media temperature of the installed DCPMM.

## Resetting a DCPMM to Factory State

- Ensure DCPMM is in an unfrozen state.
- To reset the DCPMMs to a known/factory state as they came from Intel use the following UEFI command sequence. This should work regardless of the configuration of the DCPMM. These commands must be run from an UEFI Shell.
- Commands are as follows:
  - ipmctl.efi delete -force -dimm -pcd LSA
  - ipmctl.efi delete -force -dimm
  - ipmctl.efi create -force -goal MemoryMode=100

1

Introduction

5

DCPMM Security Overview  
System Requirements

6

System Setup Overview

8

Appendices

# BIOS Post Errors Decoded

The following table shows some of most likely DCPMM-related messages you might see from system BIOS during a reboot.

BIOS Error Message	Implication	Suggested Resolution
NVDIMMs are present with inaccessible capacity. They may need to be reconfigured.	Not all capacity of the hardware is available to be used.	Reconfigure the NVDIMMs in the system to take all NVDIMM capacity.
Interleave set is in the wrong order. Swap the DIMMs as follows:	The storage volume is not accessible because the interleave set is not configured correctly.	Turn the system off and arrange the NVDIMMs as noted on the screen.
Interleave is missing the DIMM with serial number: XXXX.	The storage volume is not accessible because the interleave set is missing a member NVDIMM.	Turn the system off and insert the missing NVDIMM.
System memory configuration does not support volatile memory on the NVDIMMs. You need at least 1 DDR4 and 1 NVDIMM per populated memory controller.	The system can utilize NVDIMMs in Memory Mode, however Storage mode is not available.	Reconfigure the NVDIMMs and DDR4 DIMMs as outlined in this document.
The firmware version on the installed NVDIMMs is not consistent. Please update all NVDIMMs to the same firmware version.	There may be performance or functionality issues with configured NVDIMMs.	Update the firmware on the NVDIMMs to the latest revision.
S3 support has been disable because the firmware version on one or more installed NVDIMMs does not support S3. Please update all NVDIMMs to the latest firmware version.	The ability for the operating system to go into Standby (S3) has been disabled.	Update the firmware on the NVDIMMs to the latest revision.
The addressing capability of the installed graphics card has caused the system memory map to be truncated. As a result, the NVDIMMs could not be properly configured. You will need to remove some memory or update to a newer graphics card. The system is now halted.	The configuration of the NVDIMMs is not valid or incorrect.	Reduce the memory in the system or remove the incompatible graphics card(s).

## Known Issues

These are some known issues you might experience.

1. When you boot up, you might see high CPU utilization on 25% to 75% of the cores in memory mode. This will persist for about two to ten minutes. The fix is expected in 20H1 version of Windows 10.
2. Some AMD Graphics cards have a 1TB system memory limit. See HP QuickSpecs for graphics card details. System limit includes the total memory capacity of DCPMM and DRAM memory.
3. If more total system memory is installed than the CPU supports, the system might not operate as expected. Remove memory until below the CPU memory limit then configure the system.
4. Limited Linux support.
  - Red Hat Enterprise Linux
    - The Filesystem Dax mode (fsdax) is in Feature Preview mode in RHEL 7.6+ and RHEL 8.0.
    - Full Support will likely come with RHEL 8.1.
    - At the time of this writing, fsdax will remain in Feature Preview mode in the RHEL 7.x stream.
  - SUSE Linux Enterprise
    - The Filesystem Dax mode (fsdax) is only supported with the zfs filesystem.

1

Introduction

5

DCPMM Security Overview  
System Requirements

6

System Setup Overview

8

Appendices

# DCPMM Loading Tables

Z6 G4 Single Processor System with Intel® Optane™ DCPMMs								
MEM Qty	DRAM Qty	DCPMM Qty	CPU 0					
			IMC 0			IMC 1		
			Ch 2	Ch 1	Ch 0	Ch 0	Ch 1	Ch 2
			CPU0-DIMM1	CPU0-DIMM2	CPU0-DIMM3	CPU0-DIMM4	CPU0-DIMM5	CPU0-DIMM6
2	1	1	DRAM		PMM			
3	2	1	DRAM	PMM	DRAM			
4	2	2	DRAM		PMM	PMM		DRAM
5 S	4	1	DRAM	PMM	DRAM	DRAM		DRAM
6	2	4	DRAM	PMM	PMM	PMM	PMM	DRAM
6	4	2	DRAM	PMM	DRAM	DRAM	PMM	DRAM

IMC = Integrated Memory Controller

PMM = Intel® Optane™ DCPMM

DRAM = Standard DDR4 module

Memory Quantity Legend for HP Recommended DCPMM Memory Configurations:

- #: Number of Memory Modules – Can be configured in Memory Mode or Storage Mode.
- M: Configurations can only be used in Memory Mode.
- S: Configurations can only be used in Storage Mode.

HP factory configurations are balanced and can be configured as either Memory or Storage Mode.

Z6 G4 Dual Processor System with Intel® Optane™ DCPMMs														
MEM Qty	DRAM Qty	DCPMM Qty	CPU 0						CPU 1					
			IMC 0			IMC 1			IMC 1			IMC 0		
			Ch 2	Ch 1	Ch 0	Ch 0	Ch 1	Ch 2	Ch 2	Ch 1	Ch 0	Ch 0	Ch 1	Ch 2
			CPU0-DIMM1	CPU0-DIMM2	CPU0-DIMM3	CPU0-DIMM4	CPU0-DIMM5	CPU0-DIMM6	CPU1-DIMM1	CPU1-DIMM2	CPU1-DIMM3	CPU1-DIMM4	CPU1-DIMM5	CPU1-DIMM6
5 S	4	1	DRAM		PMM			DRAM	DRAM				DRAM	
6 M	4	2	DRAM	PMM	DRAM				DRAM	PMM	DRAM			
6 S	4	2	DRAM		PMM	PMM		DRAM	DRAM				DRAM	
7 S	6	1	DRAM		DRAM	PMM		DRAM	DRAM		DRAM		DRAM	
8	4	4	DRAM		PMM	PMM		DRAM	DRAM		PMM	PMM	DRAM	
9 S	8	1	DRAM	PMM	DRAM	DRAM		DRAM	DRAM		DRAM	DRAM	DRAM	
10 S	8	2	DRAM	PMM	DRAM	DRAM	PMM	DRAM	DRAM		DRAM	DRAM	DRAM	
12	4	8	DRAM	PMM	PMM	PMM	PMM	DRAM	DRAM	PMM	PMM	PMM	DRAM	
12	8	4	DRAM	PMM	DRAM	DRAM	PMM	DRAM	DRAM	PMM	DRAM	DRAM	PMM	

IMC = Integrated Memory Controller

PMM = Intel® Optane™ DCPMM

DRAM = Standard DDR4 module

Memory Quantity Legend for HP Recommended DCPMM Memory Configurations:

- #: Number of Memory Modules – Can be configured in Memory Mode or Storage Mode.
- M: Configurations can only be used in Memory Mode.
- S: Configurations can only be used in Storage Mode.

HP factory configurations are balanced and can be configured as either Memory or Storage Mode.



CONTENTS & NAVIGATION

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

Z8 G4 Single Processor System with Intel® Optane™ DCPMMs														
MEM Qty	DRAM Qty	DCPMM Qty	CPU 0											
			IMC 0						IMC 1					
			Channel 2		Channel 1		Channel 0		Channel 0		Channel 1		Channel 2	
			CPU0-DIMM1	CPU0-DIMM2	CPU0-DIMM3	CPU0-DIMM4	CPU0-DIMM5	CPU0-DIMM6	CPU0-DIMM7	CPU0-DIMM8	CPU0-DIMM9	CPU0-DIMM10	CPU0-DIMM11	CPU0-DIMM12
2	1	1	DRAM		PMM									
3	2	1	DRAM		DRAM		PMM							
4	2	2	DRAM		PMM							PMM		DRAM
5 S	4	1	DRAM		DRAM		PMM					DRAM		DRAM
6	4	2	DRAM		DRAM		PMM			PMM		DRAM		DRAM
6	2	4	DRAM		PMM		PMM			PMM		PMM		DRAM
8 S	6	2	DRAM	PMM	DRAM		DRAM			DRAM		DRAM	PMM	DRAM
8	4	4	DRAM	PMM	DRAM		PMM			PMM		DRAM	PMM	DRAM
10 S	6	4	DRAM	PMM	DRAM	PMM	DRAM			DRAM	PMM	DRAM	PMM	DRAM
12	8	4	DRAM	DRAM	DRAM	PMM	DRAM	PMM	PMM	DRAM	PMM	DRAM	DRAM	DRAM
12	6	6	DRAM	PMM	DRAM	PMM	DRAM	PMM	PMM	DRAM	PMM	DRAM	PMM	DRAM

IMC = Integrated Memory Controller

PMM = Intel® Optane™ DCPMM

DRAM = Standard DDR4 module

Memory Quantity Legend for HP Recommended DCPMM Memory Configurations:

- #: Number of Memory Modules – Can be configured in Memory Mode or Storage Mode.
- M: Configurations can only be used in Memory Mode.
- S: Configurations can only be used in Storage Mode.

HP factory configurations are balanced and can be configured as either Memory or Storage Mode.

CONTENTS & NAVIGATION

1

Introduction

5

DCPMM Security Overview  
System Requirements

6

System Setup Overview

8

Appendices

Z8 G4 Dual Processors with Intel® Optane™ DC PMMs														
MEM Qty	DRAM Qty	DCPMM Qty	CPU 0											
			IMC 0						IMC 1					
			Channel 2		Channel 1		Channel 0		Channel 0		Channel 1		Channel 2	
			CPU0-DIMM1	CPU0-DIMM2	CPU0-DIMM3	CPU0-DIMM4	CPU0-DIMM5	CPU0-DIMM6	CPU0-DIMM7	CPU0-DIMM8	CPU0-DIMM9	CPU0-DIMM10	CPU0-DIMM11	CPU0-DIMM12
6 M	4	2	DRAM		DRAM		PMM							
6 S	4	2	DRAM		PMM							PMM		DRAM
8	4	4	DRAM		PMM							PMM		DRAM
12	4	8	DRAM		PMM		PMM			PMM		PMM		DRAM
12	8	4	DRAM		DRAM		PMM			PMM		DRAM		DRAM
16	8	8	DRAM	PMM	DRAM		PMM			PMM		DRAM	PMM	DRAM
16 S	12	4	DRAM	PMM	DRAM		DRAM			DRAM		DRAM	PMM	DRAM
20 S	12	8	DRAM	PMM	DRAM	PMM	DRAM			DRAM	PMM	DRAM	PMM	DRAM
24	12	12	DRAM	PMM	DRAM	PMM	DRAM	PMM	PMM	DRAM	PMM	DRAM	PMM	DRAM

Z8 G4 Dual Processors with Intel® Optane™ DC PMMs														
MEM Qty	DRAM Qty	DCPMM Qty	CPU 1											
			IMC 1						IMC 0					
			Channel 2		Channel 1		Channel 0		Channel 0		Channel 1		Channel 2	
			CPU1-DIMM1	CPU1-DIMM2	CPU1-DIMM3	CPU1-DIMM4	CPU1-DIMM5	CPU1-DIMM6	CPU1-DIMM7	CPU1-DIMM8	CPU1-DIMM9	CPU1-DIMM10	CPU1-DIMM11	CPU1-DIMM12
6 M	4	2	DRAM		DRAM		PMM							
6 S	4	2	DRAM											DRAM
8	4	4	DRAM		PMM							PMM		DRAM
12	4	8	DRAM		PMM		PMM			PMM		PMM		DRAM
12	8	4	DRAM		DRAM		PMM			PMM		DRAM		DRAM
16	8	8	DRAM	PMM	DRAM		PMM			PMM		DRAM	PMM	DRAM
16 S	12	4	DRAM	PMM	DRAM		DRAM			DRAM		DRAM	PMM	DRAM
20 S	12	8	DRAM	PMM	DRAM	PMM	DRAM			DRAM	PMM	DRAM	PMM	DRAM
24	12	12	DRAM	PMM	DRAM	PMM	DRAM	PMM	PMM	DRAM	PMM	DRAM	PMM	DRAM

IMC = Integrated Memory Controller

PMM = Intel® Optane™ DCPMM

DRAM = Standard DDR4 module

Memory Quantity Legend for HP Recommended DCPMM Memory Configurations:

- #: Number of Memory Modules – Can be configured in Memory Mode or Storage Mode.
- M: Configurations can only be used in Memory Mode.
- S: Configurations can only be used in Storage Mode.

HP factory configurations are balanced and can be configured as either Memory or Storage Mode.

1	Introduction
5	DCPMM Security Overview System Requirements
6	System Setup Overview
8	Appendices

## RESOURCE LINKS

1. Intel® Optane™ DC Persistent Memory Module References  
<https://www.intel.com/content/www/us/en/architecture-and-technology/optane-dc-persistent-memory.html>
2. Configuring and Using NVDIMM  
Intro to Overall Architecture <http://pmem.io/2014/08/27/crawl-walk-run.html>
3. Configuration Tools  
Ipmctl Documentation and Source: <https://github.com/intel/ipmctl>  
NDCTL: <https://pmem.io/ndctl>
4. Developing Applications and SW for Persistent Memory  
**Intel® Developer Zone**  
**SNIA – Persistent Memory** and the **SNIA NVM Programming Model**  
**Persistent Memory Development Kit (PMDK)** and **PMDK Programmers Guide** are available on <https://pmem.io/>

## Glossary

- DCPMM: Data Center Persistent Memory Module.
- DRAM Memory/DIMM: Dynamic Random-Access Memory - Standard memory module.
- NVDIMM: Non-Volatile memory.
- DIMM: Dual In-Line Memory Module.
- Namespace: Similar to an NVMe® Namespace or a Logical Unit (LUN) on a SCSI disk, this is a software mechanism for managing ranges of persistence on DCPMMs.
- Region: A region is a grouping of one or more NVDIMMs, or an interleaved set, that can be divided up into one or more Namespaces.
- DAX: Direct Access - File system extensions to bypass the page cache and block layer to memory map persistent memory, from a PMEM block device, directly into a process address space.
- Interleaved Memory – A technique for spreading address across multiple memory devices to increase the bandwidth.
- NUMA Memory Mode – Non-Uniform Memory Access – shared memory architecture that describes the placement of main memory modules with respect to processors in a multiprocessor system.
- BTT: Block Translation Table
  - BTT is utilized to provide atomic sector updates. When DCPMM is used in Storage Mode, the operating system and storage subsystem expect to be writing to a standard block size, which is 4 kilobytes. BTT emulates a standard block size and ensures that writes are committed in 4K chunks. This ensures that all data that is expected to be written will be committed to media.
- IMC: Integrated Memory Controller.
  - On the Intel® Xeon® SP processors, there are two memory controllers per processor. Each memory controller contains 3 channels. A single IMC is represented by the group of 3 (Z6) or 6 (Z8) DIMM sockets on one side of the processor.
- Zero Copy: Computer operations in which the CPU does not perform the task of copying data from one memory area to another. This is frequently used to save CPU cycles and memory bandwidth.

<sup>1</sup> Intel® Optane™ DC Persistent Memory can be used as main memory on select HP Z6 G4 and Z8 G4 workstations with Intel® Xeon® 8200, 6200, 5200 and select 4200 series processors, Windows 10 64bit for Workstations version 1903 or higher and select Linux releases. Latency differences between DCPMM and DRAM are inherent. For data that is not in DRAM cache, DCPMM could experience latencies that are 10x versus data directly from DRAM.

<sup>2</sup> Intel® Optane™ DC Persistent Memory can be used as main memory. Latency differences between DCPMM and DRAM are inherent. For reads that are not in DRAM cache, accesses from DCPMM could experience latencies that are 10x versus reads directly from DRAM.





CONTACT US