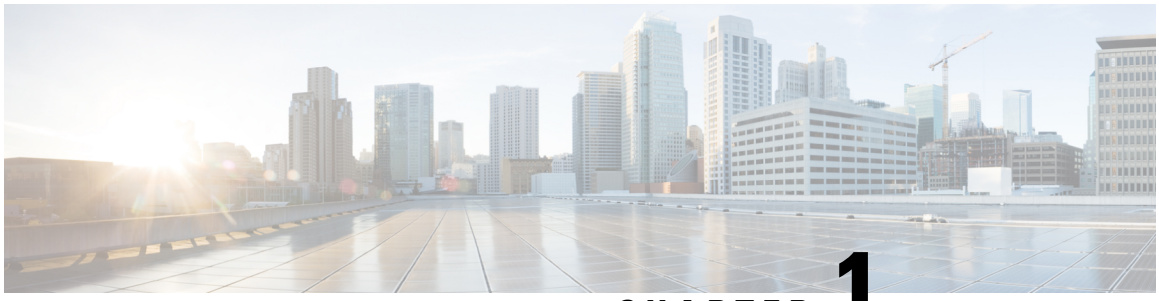
Cisco UCS: Configuring and Managing Intel® Optane™ Data Center Persistent Memory Modules

First Published: 2019-05-27

Last Modified: 2021-06-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Introduction to Persistent Memory

Persistent Memory Modules

Cisco IMC and Cisco UCS Manager Release 4.0(4) introduce support for the Intel® Optane™ Data Center persistent memory modules on the UCS M5 servers that are based on the Second Generation Intel® Xeon® Scalable processors. Starting with Cisco UCS Manager Release 4.2, the support for the Intel® Optane™ Data Center persistent memory modules on the UCS M6 servers that are based on the Second Generation Intel® Xeon® Scalable are also provided. Intel® Optane™ DC persistent memory modules can be used only with the Second Generation Intel® Xeon® Scalable processors.

This release provides the ability to configure Intel® Optane™ DC persistent memory modules through Cisco IMC and Cisco UCS Manager. Persistent memory modules are non-volatile memory modules that bring together the low latency of memory and the persistence of storage. Persistent memory modules provide faster access to data and retain data across power cycles, based on the mode.

Persistent Memory Module Population Guidelines

To ensure the best server performance, it is important that you are familiar with memory performance guidelines and population rules before you install or replace persistent memory modules.

The population guidelines can be divided into the following, based on the number of CPU sockets:

- Dual CPU for UCS X210c M6 and UCS X210c M7
- Dual CPU for UCS C220 M7 and UCS C240 M7 servers.

- Dual CPU for UCS C220 M6, UCS C240 M6, and UCS B200 M6 servers
- Dual CPU for UCS C220 M5, C240 M5, and B200 M5 servers
- Quad CPU for UCS C480 M5 and B480 M5 servers
- Dual CPU for UCS S3260 M5 servers

Note For UCS M5 and M6 B-Series and C-Series servers, the Near Memory (NM): Far Memory ratio (FM) ratio (DRAM + PMEM) is supported between 1:4 and 1:16 in 100% memory mode.

Example, 8 + 4 DRAM (16G) in 8 slots [populated in slot-1 of each-channel] + PMEM (128G) in 4 slots [A2, C2, E2, G2] =128G [8*16G] : 512G [4*128G] that is 1:4.

Cisco UCS-Managed and Host-Managed Modes

You can manage persistent memory module configuration using **UCS-managed** mode (Cisco IMC or UCS Manager) or the **host-managed** mode. In the **UCS-managed** mode, you can use Cisco UCS Manager or Cisco IMC to configure and manage persistent memory modules. In the **host-managed** mode, you can use the host tools to configure and manage persistent memory modules. When using the **UCS-managed**, you can perform configuration tasks using the Cisco UCS management interfaces or the host tools.

Cisco recommends that you use Cisco UCS management interfaces for all security operations and region management, and use the host tools only for namespace configurations if required.

Goal

A goal is used to configure how persistent memory modules connected to a CPU socket are used. You can configure a persistent memory module to be used in **Memory Mode**, **App Direct Mode**, or **Mixed Mode**. When a persistent memory module is configured as 100% Memory Mode, it can be used completely as volatile memory. Conversely, when it is configured as 0% Memory Mode, it becomes **App Direct Mode** and can be used completely as persistent memory. When you configure a persistent memory module as *x*% Memory Mode, *x*% is used as memory and the remaining is used as persistent memory. For example, when you configure 20% Memory Mode, 20 percent of the persistent memory module is used as memory and the remaining 80 percent is used as persistent memory. This mode is called **Mixed Mode**.

In mixed mode, the percentage may not linearly translate into the actual memory available. The actual memory size obtained may not accurately correspond to the specified percentage. Also, if the percentage is changed, the resultant memory obtained may not change in the same proportion.

Note In memory mode, DDR4 memory is used as a cache layer to the persistent memory module, and, is therefore not visible to the OS. For example, if you have 1.5 Tb of persistent memory in memory mode and 256 Gb DDR4, the OS/Hypervisor would still only see 1.5 Tb of total memory.

For completely persistent memory or mixed mode, you can configure the persistent memory type as **App Direct** or **App Direct Non Interleaved**. The **App Direct** type configures all the memory modules connected

to a socket into one interleaved set, and creates one region for it. The **App Direct Non Interleaved** type configures one region for each memory module.

You can create a goal only at the server level for all sockets together, and not for each socket separately. After a goal is created and applied on a server, the regions that are created are visible in the server inventory. A region is a grouping of one or more persistent memory modules that can be divided up into one or more namespaces. When a host application uses namespaces, it stores application data in them.

Note For UCS M5 S-Series servers:

- The only supported goal configuration is 0% **Memory Mode** and **App Direct Non Interleaved** persistent memory type.

  The persistent memory modules for S-Series servers are shipped with 100% **Memory Mode**. To use the persistent memory modules for S-Series servers do one of the following:

  - Perform a persistent memory scrub (Cisco UCS Manager) or reset persistent memory module to factory defaults (Cisco IMC).
  - Create a goal with 0% **Memory Mode**.

- The system does not restrict you from configuring any other combination of Memory Mode % and persistent memory type. However, unsupported goal configurations cannot be used.
- After a persistent memory scrub (Cisco UCS Manager) or reset persistent memory module to factory defaults (Cisco IMC), the default goal is 0% **Memory Mode** and **App Direct Non Interleaved** persistent memory type.

Goal modification is a destructive operation. When a goal is modified, new regions are created based on the modified goal configuration. This results in the deletion of all existing regions and namespaces on the associated servers, which leads to the loss of data currently stored in the namespaces.

Before modifying the **Persistent Memory Type** in a goal, delete the existing namespaces. This is because, in the **App Direct** persistent memory type you do not specify a DIMM number for each namespace. In the **App Direct Non Interleaved** persistent memory type, each namespace has a DIMM number specified.

For UCS M5 and M6 B-Series and C-Series servers, deleting a goal deletes all related regions and namespaces on the associated servers, and disables security. For UCS M5 S-Series servers, deleting a goal deletes all namespaces on the associated servers, and disables security. Goal deletion also returns the persistent memory module to its default state. The default state of a persistent memory module is:

- UCS M5 and M6 B-Series and C-Series servers—100% **Memory Mode**
- UCS M5 S-Series servers—0% **Memory Mode** and **App Direct Non Interleaved** persistent memory type

Region

A region is a grouping of one or more persistent memory modules that can be divided up into one or more namespaces. A region is created based on the persistent memory type selected during goal creation.

When you create a goal with the **App Direct** persistent memory type, it creates one region for all the memory modules connected to a socket. When you create a goal with the **App Direct Non Interleaved** persistent memory type, it creates one region for each memory module.

Namespace

A namespace is a partition of a region. When using the **App Direct** persistent memory type, you can create namespaces on the region mapped to the socket. When using the **App Direct Non Interleaved** persistent memory type, you can create namespaces on the region mapped to a specific memory module on the socket.

A namespace can be created in **Raw** or **Block** mode. A namespace created in **Raw** mode is seen as a raw mode namespace in the host OS. A namespace created in **Block** mode is seen as a sector mode namespace in the host OS.

Deleting a namespace is a destructive operation, and results in the loss of data stored in the namespace.

Security

You can enable security on a persistent memory module and lock it by using a secure passphrase. In Release 4.0(4), the secure passphrase for persistent memory modules is stored and managed locally.

Local Security

You can configure local security for a persistent memory module. This contains the secure passphrase to be applied on the servers. All the persistent memory modules on a server are secured with a single secure passphrase. Until you configure a secure passphrase, the persistent memory modules are not locked or secured.

Configuring a secure passphrase has the following constraints:

- The minimum length of the secure passphrase must be 8 characters, and the maximum length must be 32 characters.
- The allowed characters are letters (A-Z, a-z), numbers (0-9), special characters (!, @, #, $, %, ^, &, *, -, _, +, =), or a combination of all of them.

A deployed secure passphrase is the passphrase that is currently deployed on a server. You can modify a configured secure passphrase after you correctly enter the currently deployed secure passphrase for verification, and the new secure passphrase to be set. Before disabling security, ensure that all persistent memory modules are unlocked.

Security States

The following table describes each possible security state of a persistent memory module:

Security State	Description
Disabled	This means that the security of persistent memory modules is disabled.
Enabled	This means that the security of persistent memory modules is enabled.

Security State	Description
Locked	This means that security is enabled for persistent memory modules, and they are locked with a secure passphrase. The secure passphrase is required to unlock them.
Unlocked	This means that the security of persistent memory modules is enabled, and they are currently unlocked.
Frozen	This means that the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules.
Not Frozen	This means that the host OS can configure the persistent memory modules, use them, and configure the security of these persistent memory modules. This state is typically seen in the host-managed mode.
Count Expired	This means that the **Max Retry Count**, which is maximum number of unlock attempts allowed, has expired. It is no longer possible to unlock the persistent memory modules until the next reset or reboot. The maximum number of incorrect unlock attempts allowed: • Host-managed mode—3 incorrect unlock attempts • UCS-managed mode with security disabled—3 incorrect unlock attempts • UCS-managed mode with security enabled—2 incorrect unlock attempts
Count Not Expired	This means that the **Max Retry Count**, which is maximum number of unlock attempts allowed, has not yet expired. It is still possible to unlock the persistent memory modules with the secure passphrase. The maximum number of incorrect unlock attempts allowed: • Host-managed mode—3 incorrect unlock attempts • UCS-managed mode with security disabled—3 incorrect unlock attempts • UCS-managed mode with security enabled—2 incorrect unlock attempts

These are the possible security statuses that are displayed for each persistent memory module :

Status	Description
Disabled, Unlocked, Frozen, Count Not Expired	Security is disabled, secure passphrase is not configured, the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules, retry count has not expired
Disabled, Unlocked, Not Frozen, Count Not Expired	Security is disabled, secure passphrase is not configured, the host OS can configure security of persistent memory modules, retry count has not expired

Status	Description
Enabled, Unlocked, Frozen, Count Not Expired	Security is enabled, persistent memory modules are unlocked, the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules, retry count has not expired
Enabled, Locked, Not Frozen, Count Not Expired	Security is enabled, persistent memory modules are locked by using the secure passphrase, the host OS can configure security of persistent memory modules, retry count has not expired
Enabled, Locked, Not Frozen, Count Expired	Security is enabled, persistent memory modules are locked by using the secure passphrase, the host OS can configure security of persistent memory modules, retry count has expired
Unknown	The host is powered down.

These are the overall security states that are displayed for each server.

Overall Security State	Description
Disabled-Frozen	Persistent memory modules are in UCS Managed mode and security is disabled on all persistent memory modules.
Disabled	Persistent memory modules are in Host Managed mode and security is disabled on all persistent memory modules.
Unlocked-Frozen	Persistent memory modules are in UCS Managed mode and security is enabled on all persistent memory modules.
Enabled, Locked	Persistent memory modules are in Host Managed mode and security is enabled on all persistent memory modules.
Mixed-State	Some persistent memory modules have security enabled and the rest have security disabled.

BIOS Support for Persistent Memory Module Security

The following outline the BIOS support for persistent memory module security:

- The BIOS supports one secure passphrase for all persistent memory modules in a server.
- When the BIOS is provided with a secure passphrase to lock all the persistent memory modules, it does the following for each persistent memory module:
  - Enable security for the persistent memory module
  - Lock the persistent memory module with the secure passphrase provided

  After all the persistent memory modules are locked, the server is rebooted.
- For the host OS to use the persistent memory modules, after the server reboots, the BIOS unlocks the persistent memory module and puts it in a **Frozen** state. In this state, the host OS can configure the persistent memory modules and use them, but cannot change the security passphrase of the persistent memory modules. The state of each persistent memory module, then, appears as **Unlocked and Frozen**.

- The BIOS does not support goal modification and secure passphrase modification operations at the same time. These operations, however, can be performed one after the other. Performing these operations simultaneously will result in failure.

  Cisco UCS Manager prevents you from trying to perform goal modification and secure passphrase modification operations at the same time.

Persistent Memory Server Operations

Secure Erase

The secure erase functionality allows you to erase data in a region, namespaces and disable security in a specific persistent memory module. You can perform secure erase on a specific set of persistent memory modules, or all the persistent memory modules on a server. The secure erase functionality is also supported when security is disabled, in which case, no passphrase is required.

- A set of persistent memory modules—You can use this option to perform secure erase on a specific set of one or more persistent memory modules. If the server is configured with a secure passphrase, you must provide the secure passphrase for verification. When this operation is complete, data in the regions for the selected persistent memory modules is erased, all namespaces on these persistent memory modules are deleted, and security is disabled on these persistent memory modules.
- All the persistent memory modules on a server—You can use this option to perform secure erase on the persistent memory configuration of the server. If the server is configured with a secure passphrase, you must provide the secure passphrase for verification. When this operation is complete, data in all the regions on the server is erased, all namespaces on the server are deleted, and security is disabled on all persistent memory modules on the server.

Unlock Foreign Persistent Memory Modules

When a persistent memory module that is locked with a secure passphrase is moved to a different server that has security enabled with a different secure passphrase, it remains locked on the new server. You must unlock this persistent memory module to be able to use it on the new server. After you unlock this persistent memory module by using its deployed secure passphrase, it is secured with the single secure passphrase of the new server. For example, if persistent memory module DIMM_A2 from server 1 is locked with secure passphrase "A", and is then moved to server 2, it is identified as a locked persistent memory module on server 2. The secure passphrase of the persistent memory modules on server 2 is "B". To manage persistent memory module DIMM_A2 on server 2, you must unlock the module by using secure passphrase "A". After persistent memory module DIMM_A2 is successfully unlocked, it is secured with the secure passphrase of server 2, which is "B".

Persistent Memory Scrub

Persistent memory scrub allows you to remove the persistent memory configuration and data from the persistent memory modules on a server.

In Cisco IMC, you can scrub persistent memory by resetting the persistent memory modules to factory defaults.

In Cisco UCS Manager, you can scrub persistent memory by using one of the following methods:

- Disassociating the service profile and the scrub policy, which has the persistent memory scrub option set to yes
- Performing a **Reset to Factory Default** operation on the server with the persistent memory scrub option set to yes
- Deleting a goal

After persistent memory scrub is complete, the following happen:

- All persistent memory data is erased
- Persistent memory configuration is reset to factory default settings.

  For B-Series and C-Series servers, 100% Memory Mode is applied. For S-Series servers, 0% Memory Mode and App Direct Non Interleaved type are applied.
- Persistent memory module security is disabled

Persistent Memory Firmware Update

Persistent memory modules have firmware running on it. This firmware is packaged in the blade and rack server (B and C) bundles. Ensure that the blade and rack package versions are set to Release 4.0(4) or later releases.

In Cisco UCS Manager, you can use these firmware packages in service profiles to upgrade persistent memory firmware by defining a host firmware policy and including it in the service profile associated with a server. For instructions about defining a host firmware policy in Cisco UCS Manager, see the Cisco UCS Manager Firmware Management Guide.

You can upgrade or downgrade persistent memory firmware on the standalone Cisco UCS C-Series and Cisco UCS S-Series servers using the Cisco UCS Host Update Utility (HUU). For instructions to update the firmware, see Cisco Host Upgrade Utility User Guide

Cisco recommends that all the persistent memory modules on a server run the same and the latest firmware version.

Persistent Memory Policy and Its Components in Cisco UCS Manager

This section describes the persistent memory policy, its components, and guidelines for configuring them in Cisco UCS Manager.

Persistent Memory Policy for Cisco UCS Manager

In Cisco UCS Manager, a persistent memory policy allows you to configure how persistent memory modules are used. It contains goals and namespaces.

You must include this policy in a service profile and that service profile must be associated with a server for this policy to take effect. While each service profile can have one persistent memory policy, one persistent memory policy can be mapped to several service profiles.

The behavior of the persistent memory policy and its components will be based on whether the policy is referred to by a server or not. If the policy is not referred by any server, you can perform all operations—create, modify, delete—without any restrictions. If the policy is referred to by a server, specific restrictions apply. For example, when a persistent memory policy is referred to by a server, namespaces configured by it cannot be modified.

Some of the operations that you can perform on a persistent memory policy and its components are destructive. Such an operation results in the loss of created structures and data. The operations that you can perform on a persistent memory policy and its components, which could lead to loss of data are:

- Modification of a goal
- Deletion of a goal
- Deletion of a namespace
- Replacement of a persistent memory policy in a service profile associated with a server

To perform a destructive operation, you must explicitly apply the new configuration on the server. You can do this by using the **Force Configuration** option in the persistent memory policy. You must select this option everytime you perform a destructive operation.

Guidelines for Configuring Persistent Memory Policy Components

Here are the guidelines for configuring the persistent memory policy components:

Goal

Goal creation, modification, and deletion can all be done without any endpoint restriction when the service profile that it is included in is not associated to a server. Data loss is not applicable in these cases because the policy is not applied to a server.

Goal creation on a server with a pre-existing persistent memory configuration is a destructive operation. However, goal creation without any preexisting config is not destructive.

Goal modification is a destructive operation. When a goal is modified, new regions and namespaces are created based on the modified goal configuration. This results in the deletion of all existing regions and namespaces on the associated servers, which leads to the loss of data currently stored in the namespaces.

When you delete a goal, it deletes all related regions and namespaces on the associated servers. It also returns the persistent memory module to its default state. The default state of a persistent memory module is:

- UCS M5 and M6 B-Series and C-Series servers—100% **Memory Mode**.
- UCS M5 S-Series servers—0% **Memory Mode** and **App Direct Non Interleaved** persistent memory type.

Namespace

Namespace creation, modification, and deletion can all be done without any endpoint restriction when the persistent memory policy that contains the namespace is not referred to by a server. Data loss is not applicable in these cases because the policy is not applied to a server.

You can modify a namespace only if the persistent memory policy that contains the namespace is not referred to by a server. Modifying a namespace is not an allowed operation if the persistent memory policy that contains the namespace is referred to by a server.

Deleting a namespace is a destructive operation, and results in the loss of the namespace, and the data stored in it.

Local Security

In Cisco UCS Manager, a local security policy for persistent memory modules allows you to configure the secure passphrase for the server. It contains the secure passphrase for the persistent memory policy, which is then applied on servers. Initially, the security state for all the persistent memory modules on a server is set to **Disabled**. When a persistent memory policy with a secure passphrase is applied on the server, the security state for all the persistent memory modules on the server is set to **Enabled**, and the modules are locked with the specified, single secure passphrase.

You can modify local security configuration after you correctly enter the currently deployed secure passphrase for verification, and the new secure passphrase to be set.

Local security configuration can be deleted. Deleting the local security configuration unlocks the persistent memory module and disables security for the persistent memory policy.

Unlock Foreign Persistent Memory Modules

To unlock the foreign persistent memory modules in Cisco UCS Manager, you can use the following workflow:

1. Decommission the server.
2. Change the persistent memory modules.
3. Recommission the server.
4. Associate the server to a service-profile without a persistent memory policy.
5. Ensure that the server is in the powered-on state, and BIOS POST is completed.
6. In the persistent memory inventory, select the persistent memory modules to be unlocked, and perform the unlock foreign DIMMs operation by providing the secure passphrase of the persistent memory modules.
7. Check whether the persistent memory modules get unlocked after the ExecuteActions FSM completes. Now, the persistent memory modules are ready to be used.
8. Attach a persistent memory policy.
9. Check whether the associate FSM completes.

Unlocking Foreign Persistent Memory Modules Based on Security

The following workflows apply to unlocking foreign persistent memory modules based on server security configuration:

When security is disabled:

- Unassigning the persistent memory policy will change management to host-managed mode.
- After the unlock operation, assigning a new persistent policy will override the existing configuration in the system. If the server has any existing regions or namespace, they will be deleted.

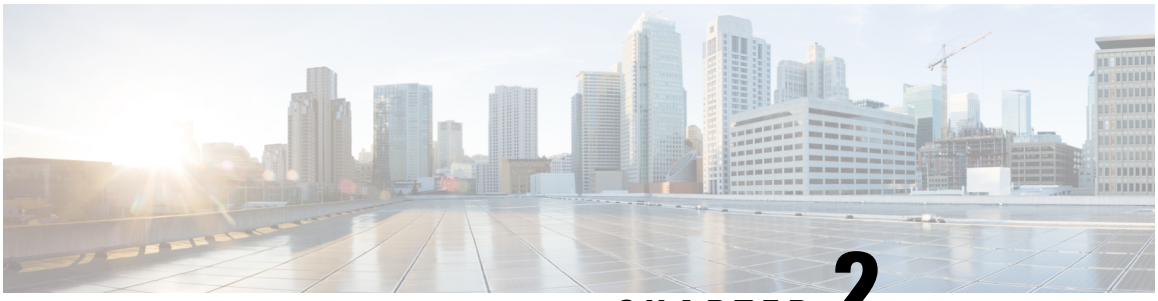
When security is enabled:

- Server-level security is enabled.

- Unassigning the security-enabled persistent memory policy will change management to host-managed mode.
- You can unlock foreign persistent memory modules, after which you must apply server-level security to the unlocked persistent memory modules.
- After the unlock operation, assigning a new persistent policy will override the existing configuration in the system. If the server has any existing regions or namespace, they will be deleted.

PART I

Configuring Persistent Memory Modules Using Cisco IMC



CHAPTER 2

Configuring Persistent Memory Modules Using Cisco IMC GUI

Viewing Persistent Memory Details

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the persistent memory **General** area, review the following information:

Name	Description
Total Capacity field	The total capacity of non-volatile DIMM(s) in GiB.
Persistent Memory field	The persistent memory capacity of all the persistent memory modules on the server in GiB.
Memory Capacity field	The volatile memory capacity of all the persistent memory modules on the server in GiB.
Reserved Capacity field	The reserved capacity of all the persistent memory modules on the server in GiB.

Name	Description
Namespace Status field	It provides the status of the namespace creation. When the user configures the namespaces and reboot the host, **Namespace Status** will give the status of the namespace creation that are configured. When you click on the information icon following detail appears: • **Name** —The name of the namespace. • **Status** — Indicates whether the namespace was successfully created or failed. **Note** The status appears after the host reboot.
Memory Regions field	The number of regions configured in persistent memory.
Configuration Result field	Provides the last configuration result. Possible values are: • **Success** • **Error_AlreadyConfigured** • **NotApplicable** • **Error_BadConfig** • **Error_NameSpaceConfig** • **Error_GoalCreate** • **Error_NameSpaceCreate** • **Error_BadSeqNo** • **Error_BadEraseConfig** • **Error_SecureErase-NamespaceExists** • **Error_SecureErase** • **Error_Unlock** • **Error_SecurityConfig** **Note** When you click on the information icon, the configuration result description appears in detail.
Configuration State field	Provides the last configuration state of persistent memory.
Cisco IMC Managed field	It indicates if persistent memory is manageable from Cisco IMC or not. **Note** **Cisco IMC Managed** field provides the state of the **Enable/Disable Cisco IMC Management**. Default value: **True**.

Name	Description
Security State field	Provides the security state on all the persistent DIMMs. This can be one of the following: • **Disabled-Frozen**: While Persistent Memory modules in Cisco IMC Managed mode and security disabled on all DIMMs. • **Disabled**: While Persistent Memory modules in Host Managed mode and security disabled on all DIMMs. • **Unlocked-Frozen**: While Persistent Memory modules in Cisco IMC Managed mode and security enabled on all DIMMs. • **Enabled,Locked**: While Persistent Memory modules in Host Managed mode and security enabled on all DIMMs. • **Mixed-State**: Few DIMMs have security enabled and few have security disabled.
Import/Export Status field	Provides import/export status of persistent memory configuration. When you click on the information icon, following detail appears: • **Operation** — Indicates whether import or export operation is in progress. • **Operation Status** — Indicates the import or export status. This can be: **For Export:** **ERROR_REMOTE_CONNECTION** **For Import :** • **ERROR_REMOTE_CONNECTION** • **ERROR_INVALID_JSON_FILE** • **ERROR_DUPLICATE_NAMESPACE_EXIST** • **ERROR_SECURITY_ENABLED**

Step 4 In the persistent memory **DIMM Details** area, review the following information:

Name	Description
ID column	The unique ID of the persistent memory DIMM.

Name	Description
Health column	Provides the health status of the persistent memory DIMM. Following are the heath status options: • **Healthy** • **NonCriticalFailure** • **CriticalFailure** • **Unmanagable** • **NonFunctional** • **FatalFailure**
Status column	Provides the status of the DIMMs. The column indicates one of the following DIMM security conditions: • **Disabled, Unlocked, Frozen, Count Not Expired** • **Disabled, Unlocked, Not-Frozen, Count Not Expired** • **Enabled, Unlocked, Frozen, Count Not Expired** • **Enabled, Unlocked, Not-Frozen, Count Not Expired** • **Enabled, Locked, Not-Frozen, Count Not Expired** • **Enabled, Locked, Not-Frozen, Count Expired** **Note** First element provides the security state of DIMM, second element provides the locked status of DIMM, third elements provides frozen state of DIMM and fourth element provides password retry status. The maximum number of retries allowed is two.
Local DIMM Number column	The physical DIMM number local to CPU.
Firmware Version column	Provides the firmware version of the persistent memory DIMM.
Memory (GiB) column	Provides the memory capacity in GiB. • **Total** - The total capacity of the persistent memory DIMM. • **Persistent** - The persistent memory capacity of the DIMM. • **Volatile** - The volatile memory capacity of the persistent memory DIMM.

Name	Description
Capacity (GiB) column	**Reserved** - The reserved capacity of the persistent memory DIMM. **App Direct** - The App Direct capacity of the persistent memory DIMM.
Last Security Operation Status column	Provides the last security operation status of the persistent DIMM.
Serial Number column	Serial number associated with the DIMM.
Socket ID column	The CPU socket ID to which the DIMM belongs.
DIMM UID column	The unique ID of the persistent memory DIMM.

On selection of the DIMM(s), following actions can be performed:

Action	Description
Secure Erase button	Securely erases the persistent memory DIMM(s). Erases the regions and namespaces of the selected DIMMs. If the DIMMs are locked with a secure passphrase, enter the secure passphrase to continue with the operation.
Unlock DIMM(s) button	Unlocks the locked persistent memory DIMM(s). If the DIMMs are locked with a secure passphrase, enter their deployed secure passphrase to continue with the operation. **Note** If the DIMM security status is enabled, locked, not-frozen, and count not expired, only then the unlock DIMM(s) button is enabled.

Step 5 In the persistent memory **Region** area, review the following information:

Table 1: Charts

Name	Description
Chart View	Displays the volatile and non-volatile memory share across regions in a chart view.
Table View	Displays the region details in the table view.

Name	Description
ID column	The unique ID of the region.
Local DIMM Number column	Local DIMM number out of which a region is created in non-interleaved mode. Local DIMM number is zero in interleaved mode.

Name	Description
Socket column	The CPU socket ID to which the region belongs.
Type column	The type of persistent memory configuration. This can be one of the following: • **AppDirect**: Configures one region for all the persistent memory modules connected to a socket. • **AppDirectNonInterleaved**: Configures one region for each persistent memory module. **Note** The default persistent memory type for UCS M5 S-Series servers is **AppDirectNonInterleaved**.
DIMM ID column	The collection of silk screen IDs of DIMMs participating in the region.
State column	The health state of the configured region.
Total Capacity (GiB) column	The total capacity of the region in GiB.
Free Capacity (GiB) column	The capacity of the region available for the new namespace creation.

Step 6 In the persistent memory **Namespace** area, review the following information:

Table 2: Charts

Name	Description
Chart View	Displays the Namespace memory size in the chart view.
Table View	Displays the Namespace details in the table view.

Name	Description
Name column	The unique name of the namespace.
Capacity column	Provides the memory capacity of the namespace in GiB.
State column	Provides the health state of the namespace.
Version column	Provides the version number of the applied namespace.
Region column	The region ID to which the namespace belongs.
Socket ID column	The CPU socket to which the namespace belongs.
Local DIMM Number column	Local DIMM number out of which a namespace is created in non-interleaved mode. Local DIMM number is zero in interleaved mode.

Name	Description
Block Size column	The block size of the namespace.
Mode column	The mode in which the namespace is created. This can be one of the following: • **Raw**: A namespace created in **Raw** mode is seen as a raw mode namespace in the host OS. This mode is for character devices. Data access and control is at a character level. • **Block**: A namespace created in **Block** mode is seen as a sector mode namespace in the host OS. This mode is for block devices. Data access and control is per block.
UUID column	The UUID of the namespace.

On selection of the namespace, following actions can be performed:

Actions	Description
Create Namespace button	This option allows you to create a namespace.
Delete Namespace button	This option allows you to delete the applied namespace.

Configuring Memory Usage for Persistent Memory

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click on **Configure Memory Usage** action.

Step 4 In the **Configure Memory Usage** action area, configure goal or namespace or review the pending goal or namespace configuration:

Name	Description
Goal field	This option allows you to create memory goals to direct the controller as to how the memory will be used. **Note** Only one goal can be created at a time. Select the **Goal** in the left navigation tree and configure the following parameters: • **Socket**: ALL **Note** As the **Goal** is applied across the server, all the sockets participate in the goal creation. • **Memory Mode**: The percentage of volatile memory required for goal creation. **Note** The actual volatile and persistent size allocated to the region may differ with the % given. • **Persistent Memory Type**: Type of persistent memory configuration. This can be one of the following: **AppDirect** — Configures one region for all the persistent memory modules connected to a socket. or **AppDirectNonInterleaved** — Configures one region for each persistent memory module. Click **Create Goal** button to create a new goal and then click **Save**. **Note** You can click **Save** to create and apply goal OR You can save later after creating namespaces and then apply both goal and namespace together.

Name	Description
Namespace field	The following properties are to be defined when creating namespaces: • **Name:** The unique name of the namespace. • **Socket ID:** The CPU socket ID on which the namespace has to be created. • **Local DIMM Number:** The local DIMM number on which the namespace is to be created. **Note** Local DIMM number is not available if selected persistent memory type is **AppDirect**. • **Capacity:** Memory capacity in GiB. • **Mode:** The mode of the Namespace. This can be one of the following: • **Raw** — A namespace created in **Raw** mode is seen as a raw mode namespace in the host OS. This mode is for character devices. Data access and control is at a character level. • **Block** — A namespace created in **Block** mode is seen as a sector mode namespace in the host OS. This mode is for block devices. Data access and control is per block. Click **Create** button to create a namespace and then click **Save**. **Note** You can create multiple namespaces and save all of them together.

Creating a Namespace

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Namespace** tab, click on + icon and provide the following information for creating a namespace:

Name	Description
Name field	The name of the namespace.
Socket ID drop-down list	The CPU socket ID on which the namespace has to be created. **Note** The number of sockets is based on the CPU population.
Local DIMM Number drop-down list	The local DIMM number on which the namespace is to be created. **Note** This option is available only when the persistent memory type is App Direct Non Interleaved. The number of local DIMMs per socket is based on the population of the DIMMs.
Capacity field	The memory capacity of the namespace in GiBs.
Mode drop-down list	The mode in which the namespace is created. This can be: • **Raw** — A namespace created in **Raw** mode is seen as a raw mode namespace in the host OS. This mode is for character devices. Data access and control is at a character level. • **Block** — A namespace created in **Block** mode is seen as a sector mode namespace in the host OS. This mode is for block devices. Data access and control is per block.

Note New namespace in pending state can be modified or deleted before applying it.

Deleting a Namespace

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Namespace** area, click the **X** icon for deleting an applied namespace.

Step 4 Click **Yes** at the confirmation prompt to delete the namespace.

A warning message appears as follows:

Host power-cycle is required to apply the configuration. Do you want to power-cycle the server now?

Step 5 Click **OK** if you want to power-cycle the server. Otherwise, click **Cancel**.

Note After the namespace deletion, if you do not opt for host power-cycle, and the namespace is in pending state, you can delete or revert the namespace.

Exporting Persistent Memory Configuration

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click **Export Configuration** link and provide the following information:

Name	Description
Export Configuration To Remote Server drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server to which the persistent memory configuration file will be exported. Depending on the setting in the **Export Configuration To Remote Server** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename Cisco IMCCIMC should use when exporting the file to the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 4 Click **Export**.

Importing Persistent Memory Configuration

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click **Import Configuration** link and provide the following information:

Name	Description
Import Configuration From Remote Server drop-down list	The remote server type. This can be one of the following: • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Server IP/Hostname field	The IPv4 or IPv6 address, or hostname of the server on which the persisten memory configuration file resides. Depending on the setting in the **Import Configuration From Remote Server** drop-down list, the name of the field may vary.
Path and Filename field	The path and filename of the configuration file on the remote server.
Username	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Password	The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Step 4 Click **Import**.

Resetting Persistent Memory DIMMs to Factory Defaults

Reset factory defaults feature is used to scrub the persistent memory module. When you perform a reset all the DIMMs will be securely erased (all the configuration and data will be lost) and the DIMMs are restored to 100% memory mode. Security will be disabled.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click **Reset to factory Default** link and provide the following information:

Name	Description
Secure Passphrase field	Enter the passphrase to reset the persistent memory DIMMs to factory defaults. **Note** This dialog box appears only when security is in enabled state.

Note Host will reboot on confirming this action.

Persistent memory will be configured in 100% memory mode after the reboot on C240 M5, C220 M5, and C480 M5 servers.

In S3260, persistent memory will be configured in 0% memory with **AppDirectNonInterleaved** persistent memory type.

Enabling Security for Persistent Memory Configuration

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click **Enable Security** link and provide the following information:

Name	Description
Secure Passphrase field	Enter the passphrase to enable security on all persistent memory DIMMs.
Confirm Secure Passphrase field	Re-enter the secure passphrase to confirm.

Step 4 Click **OK** to enable security.

On confirming to enable security, host will reboot.

Disabling Security for Persistent Memory Configuration

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click **Disable Security** link and provide the following information:

Name	Description
Secure Passphrase field	Enter the passphrase to disable security on all persistent memory DIMMs. **Note** This option is available only when security is in enabled state.

Step 4 Click **OK** to disable security.

Note On confirming to disable security, host will reboot.

Modifying Passphrase

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click **Modify Passphrase** action and provide the following information in the **Modify Security Passphrase** dialog box.

Note This option is available only when security is in enabled state.

Name	Description
Current Secure Passphrase field	Enter the current passphrase of the persistent memory DIMMs.
New Secure Passphrase field	Enter the new secure passphrase to be set for the persistent memory DIMMs.
Confirm New Secure Passphrase field	Re-enter the new secure passphrase to confirm.

Step 4 Click **Save**.

Securely Erasing Persistent Memory Module Data

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **DIMM Details** table, select DIMM(s), and click on **Secure Erase** button.

Name	Description
Secure Passphrase field	Enter the passphrase to securely erase data on the selected persistent memory DIMMs. **Note** This dialog box appears only when security is in enabled state.

Note On confirming **Secure Erase** the host reboots.

Unlocking Persistent Memory DIMMs

Scenarios while populating DIMMs:

- When system security is disabled, after populating a security enabled DIMM the overall security status will be in mixed state. You must unlock the newly populated DIMM with its deployed security key to unlock and disable security of the DIMM.
- When system security is enabled, after populating a security enabled DIMM the overall security status will be in mixed state. You must unlock the newly populated DIMM with its deployed security key. When you unlock it, the security key of the DIMM changes to the system deployed key.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **DIMM Details** area, select DIMM(s), and click **Unlock DIMM(s)** button.

Name	Description
Secure Passphrase field	Enter the passphrase to unlock the persistent memory DIMMs.

Disabling Cisco IMC Management

You can manage persistent memory module configuration using Cisco IMC or by the host tools. In the Cisco IMC management mode, you can perform configuration tasks using the Cisco IMC interfaces or by the host tools. When the Cisco IMC management mode is disabled you cannot perform any configuration using Cisco IMC interfaces.

Cisco recommends you to use Cisco IMC interfaces for all security operations and regions management and use the host tools only for namespace configurations if required.

Before you begin

You must log in with admin privileges to perform this task.

Step 1 In the **Navigation** pane, click the **Compute** menu.

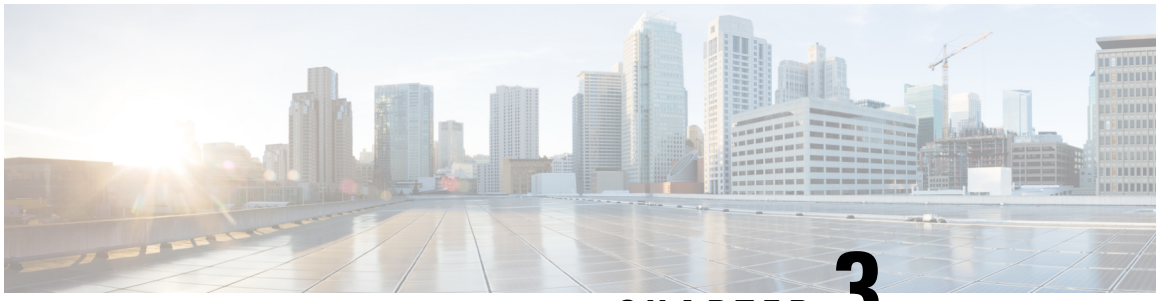
Step 2 In the **Compute** menu, click the **Persistent Memory** tab.

Step 3 In the **Persistent Memory** tab, click the **Disable Cisco IMC Management** button.

Note A warning message appears as follows:

Disabling Cisco IMC Management will block any further configurations changes. Do you want to Continue?

Step 4 Click **Yes** to disable Cisco IMC management.



CHAPTER 3

Configuring Persistent Memory Modules Using Cisco IMC CLI

Viewing Persistent Memory Module Properties

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **show detail**	Displays the persistent memory module details.

Example

This example shows how to view persistent memory module details:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # show detail
Persistent Memory Settings:
Persistent Memory Mgmt Mode: imc-managed
Configured State : Configured
Configured Result : Error_NameSpaceCreate
Total Capacity (GiB): 2020
Persistent Memory Capacity (GiB): 2016
Memory Capacity (GiB): 0
Reserved Capacity (GiB): 0
Total Regions : 8
Total DIMMs: 8
Security State: Unlocked-Frozen
Secure Firmware Downgrade: disabled
Server /chassis/persistent-memory #
```

Viewing Persistent Memory DIMMs Properties

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **show persistent-memory-dimm detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show persistent-memory-dimm detail**	Displays the persistent memory DIMM details.

Example

This example shows how to view persistent memory DIMM details:

```
Server # scope chassis
Server /chassis # show persistent-memory-dimm detail
Persistent Memory DIMMs:
```

```
    DIMM Locator Id: DIMM_A2
    DIMM UID: 8089-A2-1834-000007BA
    Socket Id: 1
    Total Capacity (GiB): 126
    Persistent Memory Capacity (GiB): 64
    Memory Capacity (GiB): 62
    App Direct Capacity (GiB): 64
    Reserved Capacity (GiB): 0
    Firmware Version: 1.2.0.5360
    Health State: Healthy
    Socket Local DIMM Number: 2
    Serial Number: 000007BA
    Status: Enabled, UnLocked, Frozen, Count not expired
Persistent Memory DIMMs:
    DIMM Locator Id: DIMM_B2
    DIMM UID: 8089-A2-1834-0000057E
    Socket Id: 1
    Total Capacity (GiB): 126
    Persistent Memory Capacity (GiB): 64
    Memory Capacity (GiB): 62
    App Direct Capacity (GiB): 64
    Reserved Capacity (GiB): 0
    Firmware Version: 1.2.0.5360
    Health State: Healthy
    Socket Local DIMM Number: 4
    Serial Number: 0000057E
    Status: Enabled, UnLocked, Frozen, Count not expired
    .
    .
    .
Displays the details of all the available DIMMs
Server /chassis/persistent-memory #
```

Viewing Namespace Properties

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **show namespace detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **show namespace detail**	Displays the persistent memory namespace details.

Example

This example shows how to view persistent memory namespace details:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # show namespace detail
Namespace:
    Name: ns 1
    Socket Id: 2
    Socket Local DIMM Number: Not applicable
    Region Id:
    Capacity (GiB): 1
    Mode: block
    Block Size:
    Label Version:
    UUID :
    Health State :
    Config State: Pending
Namespace:
    Name: 1
    Socket Id: 1
    Socket Local DIMM Number: Not applicable
    Region Id:
    Capacity (GiB): 2
    Mode: raw
    Block Size:
    Label Version:
    UUID :
    Health State :
    Config State: Pending
Namespace:
    Name: _
    Socket Id: 1
    Socket Local DIMM Number: Not applicable
    Region Id:
    Capacity (GiB): 2
    Mode: raw
    Block Size:
    Label Version:
    UUID :
    Health State :
    Config State: Pending
    .
    .
    .
Displays the details of all the available namespaces
Server /chassis/persistent-memory #
```

Viewing Goal Properties

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **show goal detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **show goal detail**	Displays the goal details.

Example

This example shows how to view goal details:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # show goal detail
Goal Settings:
    Soket Id: ALL
    Memory Mode: 14
    Persistent Memory Type: app-direct
Server /chassis/persistent-memory #
```

Viewing Region Properties

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **show region detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **show region detail**	Displays the persistent memory region details.

Example

This example shows how to view persistent memory region details:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # show region detail
Region:
    Id: 1
    Socket Local Dimm Number: Not applicable
    Socket Id: 1
    Interleaved Set Id: 5559c3d06c7e8888
    Persistent Memory Type: AppDirect
    Health State : Healthy
    Total Capacity (GiB): 256
```

```
    Free Capacity (GiB): 192
    DIMM Locator Ids: DIMM_A2,DIMM_B2,DIMM_D2,DIMM_E2
Region:
    Id: 2
    Socket Local Dimm Number: Not applicable
    Socket Id: 2
    Interleaved Set Id: 49e9c3d0f47e8888
    Persistent Memory Type: AppDirect
    Health State : Healthy
    Total Capacity (GiB): 256
    Free Capacity (GiB): 256
    DIMM Locator Ids: DIMM_G2,DIMM_H2,DIMM_K2,DIMM_L2
Server /chassis/persistent-memory #
```

Creating a Goal

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **create-goal** *{all-sockets |volatile-memory-percentage |{app-direct | app-direct-non-interleaved}*
4. Enter **y** at the two confirmation prompts.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.

Step 3	Server /chassis/persistent-memory # **create-goal** *{all-sockets |volatile-memory-percentage |{app-direct	app-direct-non-interleaved}*	• Enter **ALL** to create goal for all sockets.
			• Enter the percentage of memory on the persistent memory module that is configured as volatile memory.
			• Choose the type of persistent memory. This can be one of the following:
			  • **app-direct**—Configures one region for all the persistent memory modules connected to a socket.
			  • **app-direct-non-interleaved**—Configures one region for each persistent memory module.

	Command or Action	Purpose
		Note • The default persistent memory type for UCS C-Series servers is App Direct. • The default persistent memory type for UCS M5 S-Series servers is App Direct Non Interleaved. Initiates goal creation.
Step 4	Enter **y** at the two confirmation prompts.	A goal on all sockets is created.

Example

This example shows how to create a goal on persistent memory module:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # create-goal ALL 14 app-direct
Configuration of goal will clear the existing regions and namespaces.
Do you want to forcefully apply the goal configuration?[y|N]y
Goal is configured
Configuration of Goal will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.
Server /chassis/persistent-memory #
```

Creating a Namespace

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **create namespace** *namespace name*
4. Server /chassis/persistent-memory/namespace *# **set capacity** *value*
5. Server /chassis/persistent-memory/namespace *# **set mode** *{block \ raw}*
6. Server /chassis/persistent-memory/namespace *# **set socket-id** *{1 \ 2 \ 3 \ 4}*
7. Server /chassis/persistent-memory *# **set socket-local-dimm-number** *{2 | 4 | 6 | 8 | 10 | 12}*
8. Server /chassis/persistent-memory/namespace * # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **create namespace** *namespace name*	Enter the name of the namespace. Initiates the creation of a namespace.
Step 4	Server /chassis/persistent-memory/namespace *# **set capacity** *value*	Enter the memory capacity of the namespace in GiBs.
Step 5	Server /chassis/persistent-memory/namespace *# **set mode** *{block \ raw}*	Enter mode in which the namespace is created.
Step 6	Server /chassis/persistent-memory/namespace *# **set socket-id** *{1 \ 2 \ 3 \ 4}*	The CPU socket ID on which the namespace is created.
Step 7	Server /chassis/persistent-memory *# **set socket-local-dimm-number** *{2 | 4 | 6 | 8 | 10 | 12}*	The local DIMM number for the region to which this namespace belongs. **Note** This option is available only when the persistent memory type is App Direct Non Interleaved.
Step 8	Server /chassis/persistent-memory/namespace * # **commit**	Enter **y** at the confirmation prompt. Commits the transaction to the system configuration.

Example

This example shows how to create a persistent memory namespace:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # create namespace test1
Server /chassis/persistent-memory/namespace *# set capacity 12
Server/chassis/persistent-memory/namespace *# set mode block
Server /chassis/persistent-memory/namespace *# set socket-id 2
Server /chassis/persistent-memory/namespace *# set socket-local-dimm-number 4
Server /chassis/persistent-memory/namespace * # commit
Server /chassis/persistent-memory/namespace #
```

Modifying a Goal

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **scope goal ALL**

4. Server /chassis/persistent-memory/goal # **set persistent-memory-type** *{app-direct | app-direct-non-interleaved}*
5. Server /chassis/persistent-memory/goal* # **set volatile-memory-percentage** *percentage*
6. Server /chassis/persistent-memory/goal* # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **scope goal ALL**	Enters the goal command mode. • Enter **ALL** to create goal for all sockets. • Enter the percentage of memory on the persistent memory module that is configured as volatile memory. Initiates goal creation.
Step 4	Server /chassis/persistent-memory/goal # **set persistent-memory-type** *{app-direct | app-direct-non-interleaved}*	• Choose the type of persistent memory. This can be one of the following: • **App Direct**—Configures one region for all the persistent memory modules connected to a socket. • **App Direct Non Interleaved**—Configures one region for each persistent memory module. **Note** • The default persistent memory type for UCS C-Series servers is App Direct. • The default persistent memory type for UCS M5 S-Series servers is App Direct Non Interleaved.
Step 5	Server /chassis/persistent-memory/goal* # **set volatile-memory-percentage** *percentage*	Enter the percentage of memory on the persistent memory module that is configured as volatile memory.
Step 6	Server /chassis/persistent-memory/goal* # **commit**	Enter **y** at the confirmation prompt. Commits the transaction to the system configuration.

Example

This example shows how to modify a goal properties on persistent memory module:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # scope goal ALL
Server /chassis/persistent-memory/goal # set persistent-memory-type app-direct
Server /chassis/persistent-memory/goal * # set volatile-memory-percentage 10
```

```
Server /chassis/persistent-memory/goal * # commit
Server /chassis/persistent-memory/goal #
```

Deleting a Goal

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **delete-goal ALL**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **delete-goal ALL**	Enter **y** at the confirmation prompt to delete the goal.

Example

This example shows how to delete persistent memory goal:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # delete-goal ALL
Do you want to delete the pending goal configuration?[y|N]y
Pending goal configuration is deleted
Server /chassis/persistent-memory #
```

Deleting a Namespace

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **delete namespace** *Namespace Name*
4. Server /chassis/persistent-memory * # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **delete namespace** *Namespace Name*	Enter the name of the namespace to be deleted.
Step 4	Server /chassis/persistent-memory * # **commit**	Enter **y** at the confirmation prompt. Commits the transaction to the system configuration. Deletes the chosen namespace.

Example

This example shows how to delete a namespace:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # delete namespace test1
Server /chassis/persistent-memory * # commit
Namespace test1 is deleted
Deletion of namespace will require a reboot.
Do you want to reboot the system?[y|N]y
Server /chassis/persistent-memory #
```

Exporting Persistent Memory Configuration

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **scope import-export-config**
4. Server /chassis/persistent-memory/import-export-config # **export-config** *{remote-protocol | IP Adderss |Persistent Memory Config file}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **scope import-export-config**	Enters the command mode that enables the import or export of persistent memory configuration.

	Command or Action	Purpose
Step 4	Server /chassis/persistent-memory/import-export-config # **export-config** *{remote-protocol | IP Adderss |Persistent Memory Config file}*	• Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP • **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • The IPv4 or IPv6 address, or hostname of the server to which the configuration file will be exported. • The path and filename Cisco IMC should use when exporting the file to the remote server. • The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. Initiates the export of the persistent memory configuration.

Example

This example exports the persistent memory configuration:

```
Server # scope chassis
Server /chassis # scope persistent-memory
```

```
Server /chassis/persistent-memory # scope import-export-config
Server /chassis/persistent-memory/import-export-config # export-config scp 10.10.10.10
/home/jygSJGkj/
Server (RSA) key fingerprint is xxxxxxxx
Do you wish to continue? [y/N]y
Username: xxxxxx
Password: *******
Persistent Memory Configuration exported successfully
Server /chassis/persistent-memory #
```

Importing Persistent Memory Configuration

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **scope import-export-config**
4. Server /chassis/persistent-memory/import-export-config # **import-config** {*remote-protocol* |*IP Adderss* |*Persistent Memory Config file* }

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **scope import-export-config**	Enters the command mode that enables the import or export of persistent memory configuration.

Step 4	Server /chassis/persistent-memory/import-export-config # **import-config** {*remote-protocol* |*IP Adderss* |*Persistent Memory Config file* }	• Specifies the protocol to connect to the remote server. It can be of the following types:
		  • TFTP
		  • FTP
		  • SFTP
		  • SCP
		  • HTTP

	Command or Action	Purpose
		• **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. • The IPv4 or IPv6 address, or hostname of the server to which the configuration file will be imported. • The path and filename Cisco IMC should use when importing the file to the remote server. • The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP. Initiates the import of the persistent memory configuration.

Example

This example imports the persistent memory configuration:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # scope import-export-config
Server /chassis/persistent-memory/import-export-config # import-config scp 10.10.10.10
/home/jygSJGkj/AEP_UCSM2BIOS_EXPORT
Server (RSA) key fingerprint is xxxxxxxx
Do you wish to continue? [y/N]y
Username: xxxxxx
Password: *******Persistent Memory Configuration imported successfully
Import of Persistent Memory Configuration will require a reboot.
Do you want to reboot the system?[y|N]N
Configuration will be applied on next reboot.
Server /chassis/persistent-memory #
```

Resetting Persistent Memory Module to Factory Defaults

Reset factory defaults feature is used to scrub the persistent memory module. When you perform a reset all the DIMMs will be securely erased (all the configuration and data will be lost) and the DIMMs are restored to 100% memory mode. Security will be disabled.

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **factory-default**
4. Enter the passphrase at the prompt.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **factory-default**	Enter **y** at the confirmation prompt to reboot the host. Resets the persistent memory module to factory defaults. **Note** • Persistent memory will be configured in 100% memory mode after the reboot on C240 M5, C220 M5, and C480 M5 servers. • In S3260, Persistent memory will be configured in 0% memory with **AppDirectNonInterleaved** persistent memory type.
Step 4	Enter the passphrase at the prompt.	**Note** You will be prompted to enter passphrase only when security is in enabled state. Enter **y** at the confirmation prompt.

	Command or Action	Purpose
		Note • Persistent memory will be configured in 100% memory mode after the reboot on C240 M5, C220 M5, and C480 M5 servers. • In S3260, persistent memory will be configured in 0% memory with **AppDirectNonInterleaved** persistent memory type.

Example

This example resets the persistent memory module to factory defaults:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # factory-default
This operation will reset the persistent memory configuration to factory default and reboot
 the system.
All your configuration will be lost.
Continue?[y|N]y
A system reboot has been initiated.
Server /chassis/persistent-memory #
```

Enabling Security on Persistent Memory Module

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **enable-security**
4. Enter the passphrase and confirm the passphrase at the respective prompts.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **enable-security**	Enables security on the persistent memory module.
Step 4	Enter the passphrase and confirm the passphrase at the respective prompts.	Enter **y** at the confirmation prompt to reboot the host.

Example

This example enables security on persistent memory module:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # disable-security
Enter passphrase:********
Confirm passphrase:********
Enabling security will reboot the host. Do you want to continue?[y|N]y
A system reboot has been initiated.
Server /chassis/persistent-memory #
```

Disabling Security on Persistent Memory DIMMs

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **disable-security**
4. Enter the passphrase at the prompts.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **disable-security**	Disables security on the persistent memory DIMMs.
Step 4	Enter the passphrase at the prompts.	Enter **y** at the confirmation prompt to reboot the host.

Example

This example disables security on persistent memory module:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # disable-security
Enter passphrase:********
Disabling security will reboot the host. Do you want to continue?[y|N]y
A system reboot has been initiated.
Server /chassis/persistent-memory #
```

Modifying Passphrase

Before you begin

- You must log in with admin privileges to perform this task.
- Security must be in enabled state.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **modify-passphrase**
4. Enter the **Existing Passphrase**, **New Passphrase**, and **Confirm New Passphrase** at the respective prompts.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **modify-passphrase**	Modifies the passphrase.
Step 4	Enter the **Existing Passphrase**, **New Passphrase**, and **Confirm New Passphrase** at the respective prompts.	Enter **y** at the confirmation prompt to reboot the host.

Example

This example how to modify the passphrase on persistent memory module:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # modify-passphrase
Enter Existing Passphrase:********
Enter New Passphrase: ********
Confirm New Passphrase:********
Modifying the passphrase will reboot the host. Do you want to continue?[y|N]y
A system reboot has been initiated.
Server /chassis/persistent-memory #
```

Performing Secure Erase on Persistent Memory Modules

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **secure-erase** {*Socket ID* |*Persistent Memory DIMM Number*}
4. Securely erases data on the persistent memory modules. Enter the passphrase at the prompt.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **secure-erase** {*Socket ID* |*Persistent Memory DIMM Number*}	You can use the following socket ID and IMMs combinations to erase data on the DIMMs: • Socket ID as ALL and DIMM IDs as ALL will erase data on all the DIMMs on all sockets. • Socket ID and ALL to unlock the all the DIMMs on the chosen socket. • Socket ID and DIMM ID to unlock particular DIMMs on the chosen socket.
Step 4	Securely erases data on the persistent memory modules. Enter the passphrase at the prompt.	**Note** The passphrase prompt appears only when security is in enabled state. Enter **y** at the confirmation prompt to reboot the host.

Example

This example securely erases data on the persistent memory DIMMs 2 and 6 on socket 1:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # secure-erase 1 2,6
Enter passphrase:********
All the pending configurations will be discarded and host will be rebooted.
Do you want to continue with secure erase?[y|N]y
Secure Erase sucessfully completed.
A system reboot has been initiated.
Server /chassis/persistent-memory #
```

Unlocking Persistent Memory DIMMs

Scenarios while populating DIMMs:

- When system security is disabled, after populating a security enabled DIMM the overall security status will be in mixed state. You must unlock the newly populated DIMM with its deployed security key to unlock and disable security of the DIMM.

- When system security is enabled, after populating a security enabled DIMM the overall security status will be in mixed state. You must unlock the newly populated DIMM with its deployed security key. When you unlock it, the security key of the DIMM changes to the system deployed key.

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **unlock-dimm** {*socket ID* |*DIMM IDs*}
4. Enter the passphrase at the prompt.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **unlock-dimm** {*socket ID* |*DIMM IDs*}	You can use the following socket ID and DIMMs combinations to unlock the DIMMs: • Socket ID and ALL to unlock the all the DIMMs on the chosen socket. • Socket ID and DIMM ID to unlock particular DIMMs on the chosen socket.
Step 4	Enter the passphrase at the prompt.	Enter **y** at the confirmation prompt. Unlocks the selected persistent memory DIMMs.

Example

This example unlocks the persistent memory DIMMs 2 and 4 on socket 1:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # unlock-dimm 1 2,4
Enter passphrase:********
Do you want to unlock the DIMM?[y|N]y
Unlock DIMM successful.
Server /chassis/persistent-memory #
```

Setting Persistent Memory Module Management Mode

You can manage persistent memory module configuration using the Cisco IMC interfaces or by the host tools. In the Cisco IMC management mode, you can perform configuration tasks using the Cisco IMC interfaces or

by the host tools. When the Cisco IMC management mode is disabled, you cannot perform any configuration using Cisco IMC interfaces.

Cisco recommends you to use Cisco IMC interfaces for all security operations and regions management and use the host tools only for namespace configurations if required.

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope persistent-memory**
3. Server /chassis/persistent-memory # **set mgmt-mode** *{host-managed \ imc-managed}*
4. Server /chassis/persistent-memory * # **commit**

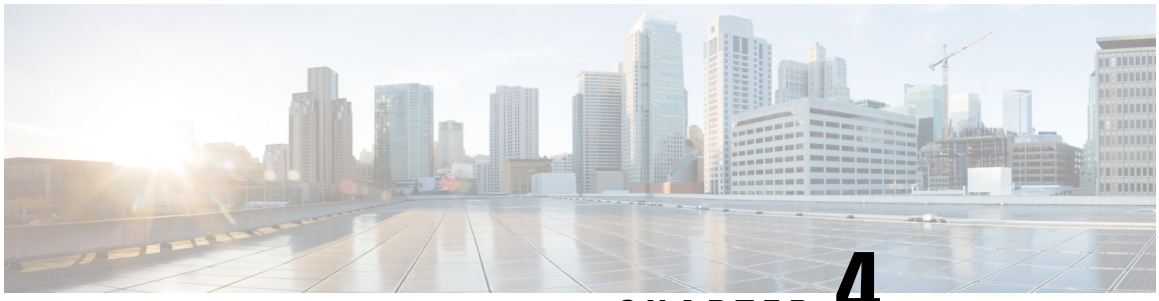
DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope persistent-memory**	Enters the persistent memory command mode.
Step 3	Server /chassis/persistent-memory # **set mgmt-mode** *{host-managed \ imc-managed}*	Enables you to set the persistent memory management mode. This can be one of the following: • **host-managed** —When you choose this option persistent memory is managed by the host. • **imc-managed**—When you choose this option persistent memory is managed using Cisco IMC.
Step 4	Server /chassis/persistent-memory * # **commit**	Commits the transaction to the system configuration.

Example

This example shows how to set persistent memory module management to Cisco IMC mode:

```
Server # scope chassis
Server /chassis # scope persistent-memory
Server /chassis/persistent-memory # set mgmt-mode imc-managed
Server /chassis/persistent-memory * commit#
Server /chassis/persistent-memory #
```



CHAPTER 4

Configuring Persistent Memory Modules Using Cisco IMC XML API

Persistent Memory Module XML API Examples

The examples in this section show how to use the Cisco IMC XML API to perform Persistent Memory Module tasks. Each example shows the XML API request followed by the response from Cisco IMC.

This section includes the following examples:

Viewing Persistent Memory Unit Inventory Details

Request:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryUnit"/>
```

Response:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970" response="yes"

classId="memoryPersistentMemoryUnit">
  <outConfigs>
    <memoryPersistentMemoryUnit array="1" location="DIMM_A2" capacity="128704" clock="2666"
 formFactor="DIMM"
id="2" model="8089A2174700000C66 " operState="operable" operability="operable"
presence="equipped"
serial="00000C66" type="Logical non-volatile device" vendor="0x8900" visibility="yes"
width="64"
memoryTypeDetail="Synchronous Non-volatile " bankLocator="NODE 0 CHANNEL 0 DIMM 1"
socketId="1"
uid="8089-A2-1747-00000C66" totalCapacity="126" persistentMemoryCapacity="96"
memoryCapacity="29"
appDirectCapacity="96" reservedCapacity="0" firmwareVersion="1.0.0.4351" healthState="Healthy"

socketLocalDimmNumber="2" securityStatus=" Enabled, UnLocked, Frozen, Count not expired "
lastSecurityOperStatus="No Error" dn="sys/rack-unit-1/board/memarray-1/pmem-2"/>
    <memoryPersistentMemoryUnit array="1" location="DIMM_D2" capacity="128704" clock="2666"
 formFactor="DIMM"
id="8" model="8089A2174700000A63 " operState="operable" operability="operable"
presence="equipped"
serial="00000A63" type="Logical non-volatile device" vendor="0x8900" visibility="yes"
width="64"
memoryTypeDetail="Synchronous Non-volatile " bankLocator="NODE 0 CHANNEL 3 DIMM 1"
socketId="1"
uid="8089-A2-1747-00000A63" totalCapacity="126" persistentMemoryCapacity="96"
memoryCapacity="29" appDirectCapacity="96" reservedCapacity="0" firmwareVersion="1.0.0.4351"

healthState="Healthy" socketLocalDimmNumber="8"
securityStatus=" Enabled, UnLocked, Frozen, Count not expired " lastSecurityOperStatus="No
 Error"
dn="sys/rack-unit-1/board/memarray-1/pmem-8"/>
```

```
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Configuration Details

Request:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryConfiguration"/>
```

Response:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
response="yes" classId="memoryPersistentMemoryConfiguration">
  <outConfigs>
    <memoryPersistentMemoryConfiguration dn="sys/rack-unit-1/board/pmemory-config"
configState="Configured"
totalCapacity="503" persistentMemoryCapacity="384" memoryCapacity="116" reservedCapacity="0"
 numOfRegions="4"
numOfDimms="4" securityState="Unlocked-Frozen"/>
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Region Details

Request:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryRegion"/>
```

Response:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970" response="yes"

classId="memoryPersistentMemoryRegion">
  <outConfigs>
    <memoryPersistentMemoryRegion id="1" socketLocalDimmNumber="2" socketId="1"
interleavedSetId="7c4bda90ad238a22"
persistentMemoryType="AppDirectNonInterleaved" healthState="Healthy" totalCapacity="96"
freeCapacity="86"
dimmLocatorIds="DIMM_A2" dn="sys/rack-unit-1/board/pmemory-config/region-1"/>
    <memoryPersistentMemoryRegion id="2" socketLocalDimmNumber="8" socketId="1"
interleavedSetId="5e37da90aa218a22" persistentMemoryType="AppDirectNonInterleaved"
healthState="Healthy"
totalCapacity="96" freeCapacity="96" dimmLocatorIds="DIMM_D2"
dn="sys/rack-unit-1/board/pmemory-config/region-2"/>
    <memoryPersistentMemoryRegion id="3" socketLocalDimmNumber="2" socketId="2"
interleavedSetId="8105da90941c8a22" persistentMemoryType="AppDirectNonInterleaved"
healthState="Healthy" totalCapacity="96" freeCapacity="96" dimmLocatorIds="DIMM_G2"
dn="sys/rack-unit-1/board/pmemory-config/region-3"/>
    <memoryPersistentMemoryRegion id="4" socketLocalDimmNumber="8"
socketId="2" interleavedSetId="d641da9036228a22"
persistentMemoryType="AppDirectNonInterleaved"
healthState="Healthy" totalCapacity="96" freeCapacity="96" dimmLocatorIds="DIMM_K2"
dn="sys/rack-unit-1/board/pmemory-config/region-4"/>
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Namespace Details

Request:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryNamespace"/>
```

Response:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
response="yes" classId="memoryPersistentMemoryNamespace">
  <outConfigs>
    <memoryPersistentMemoryNamespace name="TEST-91" operMode="raw"
capacity="10" labelVersion="1.2" uuid="894806e0-ecab-468d-8da4-5f74e6d2a7cb"
healthState="Healthy"
dn="sys/rack-unit-1/board/pmemory-config/region-1/ns-894806e0-ecab-468d-8da4-5f74e6d2a7cb"/>

  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory ConfigResult

Request:

```
<configResolveClass cookie="1551864178/d8c72c79-8369-1369-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryConfigResult"/>
```

Response:

```
<configResolveClass cookie="1551864178/d8c72c79-8369-1369-8002-943e485a6970"
response="yes" classId="memoryPersistentMemoryConfigResult">
  <outConfigs>
    <memoryPersistentMemoryConfigResult dn="sys/rack-unit-1/board/pmemory-config/cfg-result"

configState="Configured" configResult="NotApplicable" configError="Success"/>
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Namespace ConfigResult

Request:

```
<configResolveClass cookie="1551335940/65142995-82ef-12ef-8002-d8e6ed6a0f70"
inHierarchical="false" classId="memoryPersistentMemoryNamespaceConfigResult"/>
```

Response:

```
<configResolveClass cookie="1551335940/65142995-82ef-12ef-8002-d8e6ed6a0f70"
response="yes" classId="memoryPersistentMemoryNamespaceConfigResult">
  <outConfigs>
    <memoryPersistentMemoryNamespaceConfigResult name=" TEST-91" socketId="1"
socketLocalDimmNumber="4" configStatus="Success"
dn="sys/rack-unit-1/board/pmemory-config/cfg-result/nscr-NSS-1"/>
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Logical Configuration

Request:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryLogicalConfiguration"/>
```

Response:

```
<configResolveClass cookie="1553603882/d1f622a3-84fe-14fe-8002-943e485a6970" response="yes"

classId="memoryPersistentMemoryLogicalConfiguration">
  <outConfigs>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"/>
```

```
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Goal

Request:

```
<configResolveClass cookie="1551867321/750375cb-836a-136a-8002-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryGoal"/>
```

Response:

```
<configResolveClass cookie="1551867321/750375cb-836a-136a-8002-943e485a6970"
response="yes" classId="memoryPersistentMemoryGoal">
  <outConfigs>
    <memoryPersistentMemoryGoal socketId="ALL" memoryModePercentage="70"
persistentMemoryType="app-direct-non-interleaved"
dn="sys/rack-unit-1/board/pmemory-lconfig/goal-ALL"/>
  </outConfigs>
</configResolveClass>
```

Viewing Persistent Memory Logical Namespace

Request:

```
<configResolveClass cookie="1553667047/a46f89ac-850d-150d-8004-943e485a6970"
inHierarchical="false" classId="memoryPersistentMemoryLogicalNamespace"/>
```

Response:

```
<configResolveClass cookie="1553667047/a46f89ac-850d-150d-8004-943e485a6970" response="yes"

classId="memoryPersistentMemoryLogicalNamespace">
  <outConfigs>
    <memoryPersistentMemoryLogicalNamespace socketId="1" socketLocalDimmNumber="2" name="ns2"
 capacity="5"
mode="raw" dn="sys/rack-unit-1/board/pmemory-lconfig/lns-ns2"/>
    <memoryPersistentMemoryLogicalNamespace socketId="1" socketLocalDimmNumber="2" name="ns1"
 capacity="5"
mode="raw" dn="sys/rack-unit-1/board/pmemory-lconfig/lns-ns1"/>
  </outConfigs>
</configResolveClass>
```

Configuring Persistent Memory Goal

Request:

```
<configConfMo cookie="1553659537/970809a2-850b-150b-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"
 rebootOnUpdate="no" forceConfig="yes">
      <memoryPersistentMemoryGoal dn="sys/rack-unit-1/board/pmemory-lconfig/goal-ALL"
rn="goal-ALL" socketId="ALL" memoryModePercentage="50"
persistentMemoryType="app-direct"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553659537/970809a2-850b-150b-8002-943e485a6970" response="yes">
  <outConfig>
```

```
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"
 rebootOnUpdate="no" forceConfig="no"
adminAction="no-op" mgmtMode="imc-managed" status="modified"/>
  </outConfig>
</configConfMo>
```

Modifying Pending Goal

Request:

```
<configConfMo cookie="1553664656/92a5bb89-850d-150d-8003-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="yes" mgmtMode="imc-managed">
      <memoryPersistentMemoryGoal dn="sys/rack-unit-1/board/pmemory-lconfig/goal-ALL"
memoryModePercentage="70" persistentMemoryType="app-direct" status="modified"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Deleting a Goal

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="yes">
      <memoryPersistentMemoryGoal dn="sys/rack-unit-1/board/pmemory-lconfig/goal-ALL"
socketId="ALL"
status="deleted"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring a Namespace

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"
 rebootOnUpdate="no" forceConfig="yes">
      <memoryPersistentMemoryLogicalNamespace
dn="sys/rack-unit-1/board/pmemory-lconfig/lns-ns1" rn="lns-ns1" name="ns1" socketId="1"
socketLocalDimmNumber="2" mode="raw" capacity="25"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"
 rebootOnUpdate="no" forceConfig="no"
adminAction="no-op" mgmtMode="imc-managed" status="modified"/>
  </outConfig>
</configConfMo>
```

Modifying Pending Namespace

Request:

```
<configConfMo cookie="1553664656/92a5bb89-850d-150d-8003-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="yes" mgmtMode="imc-managed">
      <memoryPersistentMemoryLogicalNamespace
dn="sys/rack-unit-1/board/pmemory-lconfig/lns-ns1" rn="lns-ns1"
socketId="1" socketLocalDimmNumber="2" mode="raw" capacity="5" status="modified"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Deleting a Namespace

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"
```

```
rebootOnUpdate="no" forceConfig="yes">
      <memoryPersistentMemoryLogicalNamespace name="ns1" status="deleted"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring Goal and Namespace

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="yes" mgmtMode="imc-managed">
      <memoryPersistentMemoryGoal dn="sys/rack-unit-1/board/pmemory-lconfig/goal-ALL"
memoryModePercentage="70"
persistentMemoryType="app-direct-non-interleaved"/>
      <memoryPersistentMemoryLogicalNamespace
dn="sys/rack-unit-1/board/pmemory-lconfig/lns-ns2" rn="lns-ns2"
socketId="1" socketLocalDimmNumber="2" mode="raw" capacity="5"/>
      <memoryPersistentMemoryLogicalNamespace
dn="sys/rack-unit-1/board/pmemory-lconfig/lns-ns1" rn="lns-ns1"
socketId="1" socketLocalDimmNumber="2" mode="raw" capacity="5"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring Enable Security

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

adminAction="enable-security" forceConfig="yes" rebootOnUpdate="yes">
      <memoryPersistentMemorySecurity
```

```
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security"
rn="pmemory-security">
        <memoryPersistentMemoryLocalSecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security/local"
rn="local" securePassphrase="password"/>
      </memoryPersistentMemorySecurity>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring Disable Security

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

adminAction="disable-security" forceConfig="yes" rebootOnUpdate="yes">
      <memoryPersistentMemorySecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security"
rn="pmemory-security">
        <memoryPersistentMemoryLocalSecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security/local"
rn="local" deployedSecurePassphrase=”password"/>
      </memoryPersistentMemorySecurity>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Modifying Secure Passphrase

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" inHierarchical="false"

dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"
```

```
adminAction="modify-passphrase" forceConfig="yes" rebootOnUpdate="yes">
      <memoryPersistentMemorySecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security"
rn="pmemory-security">
        <memoryPersistentMemoryLocalSecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security/local"
rn="local" securePassphrase="newpassword" deployedSecurePassphrase="password"/>
      </memoryPersistentMemorySecurity>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Unlocking DIMM(s)

Request:

```
<configConfMo cookie="1553519711/f92b8b8f-84eb-14eb-8002-d8e6ed6a0f70"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

adminAction="unlock-dimms" rebootOnUpdate="yes">
      <memoryPersistentMemorySecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security"
rn="pmemory-security">
        <memoryPersistentMemoryLocalSecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security/local"
rn="local" deployedSecurePassphrase="password"/>
      </memoryPersistentMemorySecurity>
      <memoryPersistentMemoryDimms rn="pmemory-dimms-1" socketId="1"
socketLocalDimmNumbers="2"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring Secure Erase

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

adminAction="secure-erase" forceConfig="yes" rebootOnUpdate="yes">
      <memoryPersistentMemorySecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security"
rn="pmemory-security">
        <memoryPersistentMemoryLocalSecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security/local"
rn="local" deployedSecurePassphrase="password"/>
      </memoryPersistentMemorySecurity>
      <memoryPersistentMemoryDimms rn="pmemory-dimms-1" socketId="1"
socketLocalDimmNumbers="2"/>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Resetting Persistent Memory to Factory Default Settings

Request:

```
<configConfMo cookie="1553669878/b263ca00-850e-150e-8002-943e485a6970"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

adminAction="reset-factory-default" forceConfig="yes" rebootOnUpdate="yes">
      <memoryPersistentMemorySecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security"
rn="pmemory-security">
        <memoryPersistentMemoryLocalSecurity
dn="sys/rack-unit-1/board/pmemory-lconfig/pmemory-security/local"
rn="local" deployedSecurePassphrase="password"/>
      </memoryPersistentMemorySecurity>
    </memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Exporting of Persistent Memory Configuration

Request:

```
<configConfMo cookie="1553668752/ca5726fe-850d-150d-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-config/export-config">
  <inConfig>
    <memoryPersistentMemoryBackup dn="sys/rack-unit-1/board/pmemory-config/export-config"
proto="sftp" hostname="10.10.10.10" remoteFile="FilePath" user="xxx"
pwd="password"> </memoryPersistentMemoryBackup>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-config/export-config"
cookie="1553668752/ca5726fe-850d-150d-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryBackup dn="sys/rack-unit-1/board/pmemory-config/export-config"
fsmDescr="export-config" proto="none" hostname="" remoteFile="" user="" pwd=""
fsmStatus="success"
status="modified"/>
  </outConfig>
</configConfMo>
```

Importing of Persistent Memory Configuration

Request:

```
<configConfMo cookie="1553668752/ca5726fe-850d-150d-8002-943e485a6970"
dn="sys/rack-unit-1/board/pmemory-config/import-config">
  <inConfig>
    <memoryPersistentMemoryImporter dn="sys/rack-unit-1/board/pmemory-config/import-config"

rebootOnUpdate="no" proto="sftp" hostname="10.10.10.10" remoteFile="FilePath"
user="xxx" pwd="password"> </memoryPersistentMemoryImporter>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-config/import-config"
cookie="1553668752/ca5726fe-850d-150d-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryImporter dn="sys/rack-unit-1/board/pmemory-config/import-config"

fsmDescr="import-config" proto="none" hostname="" remoteFile="" user="" pwd=""
fsmStatus="success"
rebootOnUpdate="yes" status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring Host Managed Mode

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

mgmtMode="host-managed" forceConfig="no" rebootOnUpdate="no">
</memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="host-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

Configuring Cisco IMC Managed Mode

Request:

```
<configConfMo cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970"
inHierarchical="false" dn="sys/rack-unit-1/board/pmemory-lconfig">
  <inConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

mgmtMode="imc-managed" forceConfig="no" rebootOnUpdate="no">
</memoryPersistentMemoryLogicalConfiguration>
  </inConfig>
</configConfMo>
```

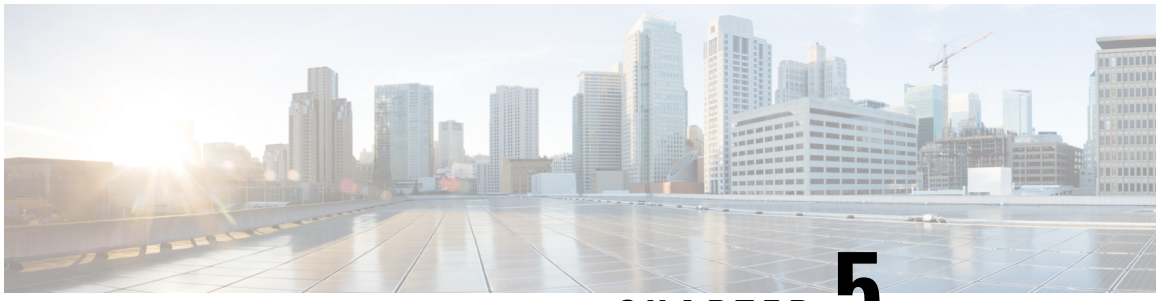
Response:

```
<configConfMo dn="sys/rack-unit-1/board/pmemory-lconfig"
cookie="1553660570/86d0435c-850c-150c-8002-943e485a6970" response="yes">
  <outConfig>
    <memoryPersistentMemoryLogicalConfiguration dn="sys/rack-unit-1/board/pmemory-lconfig"

rebootOnUpdate="no" forceConfig="no" adminAction="no-op" mgmtMode="imc-managed"
status="modified"/>
  </outConfig>
</configConfMo>
```

PART II

Configuring Persistent Memory Using Cisco UCS Manager



CHAPTER 5

Configuring Persistent Memory Using Cisco UCS Manager GUI

Creating a Persistent Memory Policy

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Persistent Memory Policy** and select **Create Persistent Memory Policy**.

Step 5 In the **Properties** area of the **Create Persistent Memory Policy** dialog box, enter the following information:

Name	Description
Name field	The name of the persistent memory policy. This is a mandatory field.
Description field	A short description of the policy.

Step 6 To create a goal, click the **Add** button in the **Goals** area of the **Create Persistent Memory Policy** dialog box and complete the fields.

Creating a Goal, on page 71 has detailed information.

Step 7 Click **OK**.

Step 8 To create a namespace, click the **Add** button in the **Configure Namespace** area of the **Create Persistent Memory Policy** dialog box and complete the fields.

Creating a Namespace, on page 72 has detailed information.

Step 9 Click **OK**.

Including a Persistent Memory Policy in a Service Profile

Before you can use a persistent memory policy to manage persistent memory in Cisco UCS Manager, you must include the persistent memory policy in a service profile. After a persistent memory policy is included in a service profile, you can associate the service profile with a Cisco UCS server.

If you include a persistent memory policy in a service profile associated to a server, the persistent memory configuration on the server is **UCS-managed**. In the **UCS-managed** mode, you can use Cisco UCS Manager and host tools to configure and manage persistent memory modules.

If a persistent memory policy is not included in the service profile associated to a server, the persistent memory configuration on the server is **host-managed**. In the **host-managed** mode, you can use the host tools to configure and manage persistent memory modules.

The following procedure describes how to include a persistent memory policy in a service profile.

Before you begin

Create the persistent memory policy that you want to include in a service profile.

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Server** > **Service Profiles**
Step 3 Select the service profile in which you want to include the persistent memory policy.
Step 4 In the **Work** pane, click the **Policies** tab.
Step 5 In the **Policies** area, expand **Persistent Memory Policy**.
Step 6 From the **Persistent Memory Policy** drop-down list, select the persistent memory policy that you want to include in this service profile.
Step 7 Click **Save Changes**.

The persistent memory policy is applied on the server to which the service profile is associated.

Removing a Persistent Memory Policy from a Service Profile

Removing a persistent memory policy from a service profile does not change any region or namespace configuration. It changes persistent memory from UCS-managed to host-managed. The following procedure describes how to remove a persistent memory policy from a service profile.

After you remove the persistent memory policy from the service profile that is associated to a server, the server is considered host-managed with respect to persistent memory configuration.

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Server** > **Service Profiles**
Step 3 Select the service profile from which you want to remove the persistent memory policy.
Step 4 In the **Work** pane, click the **Policies** tab.
Step 5 In the **Policies** area, expand **Persistent Memory Policy**.
Step 6 From the **Persistent Memory Policy** drop-down list, select **<not set>**.
Step 7 Click **Save Changes**.

The persistent memory policy is removed from the service profile and its associated server.

Creating a Goal

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Servers** > **Policies**.
Step 3 Expand the node for the organization where you want to create the goal.
Step 4 Select the persistent memory policy in which you want to create the goal.
Step 5 In the **Goals** area of the **General** tab, click the **Add** button.
Step 6 In the **Create Goal** dialog box, enter the following information:

Name	Description
Socket ID radio button	The CPU sockets on which the configured goal is applied. The default option is **All-Sockets**.
Memory Mode (%) field	The percentage of memory on the persistent memory module that is configured as volatile memory. • When **Memory Mode** is set to 100%, it can be used completely as volatile memory. • When **Memory Mode** is set to 0%, it becomes **App Direct Mode** and can be used completely as persistent memory. • When **Memory Mode** is set to *x*%, *x*% is used as memory and the remaining is used as persistent memory. This is called **Mixed Mode**. **Note** • The default memory mode percentage for: • UCS M5 B-Series and C-Series servers is 100%. • UCS M5 S-Series servers is 0%. • For UCS M6 B-Series and C-Series servers: • The **Mixed Mode** is not supported. For 8+1 POR, the **App Direct Non Interleaved Mode** is the only supported configuration. • The default memory mode percentage is 0%. • For UCS M5 and M6 servers, the Near Memory (NM) : Far Memory ratio (FM) (DRAM + PMEM) is supported between 1:4 - 1:16 in 100% memory mode.
Persistent Memory Type radio button	The type of persistent memory. This can be one of the following: • **App Direct**—Configures one region for all the persistent memory modules connected to a socket. • **App Direct Non Interleaved**—Configures one region for each persistent memory module.

Step 7 Click **OK**.

Creating a Namespace

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the namespace.

Step 4 Select the persistent memory policy in which you want to create the namespace.

Step 5 In the **Configure Namespace** area of the **General** tab, click the **Add** button.

Step 6 In the **Create Namespace** dialog box, enter the following information:

Name	Description
Name field	The name of the namespace. The namespace name has the following constraints: • Must be between 1 and 63 characters in length. • The first character must be a letter (A-Z or a-z), a number(0-9), or a special character(#, -, or _) • The remaining characters can be a combination of letters (A-Z or a-z), numbers (0-9), and special characters (#, -, _, space)
Socket ID drop-down list	The CPU socket ID for the region to which this namespace belongs. This can be: • **Socket 1** • **Socket 2** • **Socket 3** • **Socket 4** **Note** For UCS M6 B-Series and C-Series servers, only **Socket 1**and **Socket 2** are supported.

Name	Description
Socket Local DIMM Number drop-down list	The local DIMM number for the region to which this namespace belongs. This can be: • The only option avilable for **App Direct** persistent memory type—**Not Applicable** • The options available for the **App Direct Non Interleaved** persistent memory type include: • **Socket Local DIMM No 2** • **Socket Local DIMM No 3** • **Socket Local DIMM No 4** • **Socket Local DIMM No 6** • **Socket Local DIMM No 7** • **Socket Local DIMM No 8** • **Socket Local DIMM No 10** • **Socket Local DIMM No 11** • **Socket Local DIMM No 12** • **Socket Local DIMM No 14** • **Socket Local DIMM No 15** • **Socket Local DIMM No 16** **Note** The **Socket Local DIMM No 3, 7, 11, 14, 15, and 16** are applicable only for UCS M6 B-Series and C-series servers.
Mode radio button	The mode in which the namespace is created. This can be: • **Raw** • **Block**
Capacity field	The memory capacity of the namespace in GiBs.

Step 7 Click **OK**.

Creating Local Security Configuration

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to configure the persistent memory security.

Step 4 Select the persistent memory policy for which you want to configure the security.

Step 5 In the **Actions** area of the **Security** tab, click **Create Local Security**.

Step 6 In the **Create Local Security** dialog box, enter the following information:

Name	Description
Secure Passphrase field	The secure passphrase to be set for the persistent memory policy. The secure passphrase has the following constraints: • Must be between 8 and 32 characters in length. • These characters can be a combination of letters (A-Z or a-z), numbers (0-9), and special characters (!, @, #, $, %, ^, &, *, -, _, +, =).
Deployed Secure Passphrase field	Currently deployed secure passphrase for the persistent memory policy. The **Deployed Secure Passphrase** is required when the server that you are configuring has a secure passphrase from a previous deployment. This is required only for secure passphrase modification.

Step 7 Click **OK**.

Modifying a Persistent Memory Policy

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand **Persistent Memory Policy** and select the persistent memory policy that you want to modify.

Step 4 In the **Properties** area of the **General** tab, modify the following:

a) **Description** field—Enter a short description of the policy.

b) **Force Configuration** checkbox—Check this checkbox to force the configuration on all associated servers. Clear this checkbox to return this to the default state.

Step 5 Click **Save Changes**.

Modifying a Goal

Modifying a goal will result in the loss of data currently stored in the persistent memory.

Because goal modification is a destructive operation, you must check the **Force Configuration** checkbox before modifying the goal.

Before modifying the **Persistent Memory Type**, delete the existing namespaces. This is because, in the **App Direct** persistent memory type you do not specify a DIMM number for each namespace. In the **App Direct Non Interleaved** persistent memory type, each namespace has a DIMM number specified.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand **Persistent Memory Policy** and select the persistent memory policy within which you want to modify a goal.

Step 4 In the **Properties** area of the **General** tab, check the **Force Configuration** checkbox.

Step 5 In the **Goals** area of the **General** tab, select the goal to be modified and click **Modify**.

Step 6 In the dialog box that appears, modify the following:

a) In the **Memory Mode (%)** field, enter the percentage of memory on the persistent memory module to be configured as volatile memory.

Note
- The default memory mode percentage for UCS M5 and M6 B-Series and C-Series servers is 100%.
- The default memory mode percentage for UCS M5 S-Series servers is 0%.

b) Select the **Persistent Memory Type**.

- **App Direct**—Configures one region for all the persistent memory modules connected to a socket.
- **App Direct Non Interleaved**—Configures one region for each persistent memory module.

To modify the **Persistent Memory Type**, you must first delete the existing namespaces.

Step 7 Click **OK**.

Step 8 In the **General** tab, click **Save Changes**.

Modifying a Namespace

You can modify a namespace only if the persistent memory policy that contains the namespace is not referred to by a server. Modifying a namespace is not an allowed operation if the persistent memory policy that contains the namespace is referred to by a server.

The following steps are applicable only when the persistent memory policy that contains the namespace is not referred to by a server.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand **Persistent Memory Policy** and select the persistent memory policy within which you want to modify a namespace.

Step 4 In the **Namespaces** area of the **General** tab, select the namespace to be modified and click **Modify**.

Step 5 In the dialog box that appears, modify the following:

a) Select the persistent memory **Mode** for the namespace.

- **Raw**

- **Block**

b) In the **Capacity** field, modify the capacity of the namespace.

Step 6 Click **OK**.

Step 7 In the **General** tab, click **Save Changes**.

Modifying Local Security Configuration

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to modify the persistent memory security.

Step 4 Select the persistent memory policy for which you want to modify the security.

Step 5 In the **Local Security** area of the **Security** tab, enter the following information:

Name	Description
Secure Passphrase field	The new secure passphrase to be set for the persistent memory policy.
Deployed Secure Passphrase field	The currently deployed secure passphrase for the persistent memory policy. The secure passphrase entered in this field must match the currently deployed secure passphrase.

Step 6 Click **Save Changes**.

Deleting a Persistent Memory Policy

You cannot delete a persistent memory policy when the policy is referred to by a server. To delete a persistent memory policy when it is not referred to by a server, follow these steps:

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Click **Persistent Memory Policy** and in the **Work** pane, select the persistent memory policy that you want to delete.

Step 4 Click **Delete**.

Step 5 Click **Yes** to confirm deletion.

Deleting a Goal

For UCS M5 and M6 B-Series and C-Series servers, deleting a goal deletes all related regions and namespaces on the associated servers, and disables security. For UCS M5 S-Series servers, deleting a goal deletes all namespaces on the associated servers, and disables security. Goal deletion also returns the persistent memory module to its default state. The default state of a persistent memory module is:

- UCS M5 and M6 B-Series and C-Series servers—100% **Memory Mode** and **App Direct** persistent memory type
- UCS M5 S-Series servers—0% **Memory Mode** and **App Direct Non Interleaved** persistent memory type

Because goal deletion is a destructive operation, you must check the **Force Configuration** checkbox before deleting the goal.

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Servers** > **Policies**.
Step 3 Expand **Persistent Memory Policy** and select the persistent memory policy within which you want to delete a goal.
Step 4 In the **Properties** area of the **General** tab, check the **Force Configuration** checkbox.
Step 5 In the **Goals** area of the **General** tab, select the goal to be deleted and click **Delete**.
Step 6 Click **OK**.
Step 7 In the **General** tab, click **Save Changes**.

Deleting a Namespace

Deleting a namespace will result in the loss of data currently stored in the namespace.

Because namespace deletion is a destructive operation, you must check the **Force Configuration** checkbox before deleting the namespace.

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Servers** > **Policies**.
Step 3 Expand **Persistent Memory Policy** and select the persistent memory policy within which you want to delete a namespace.
Step 4 In the **Properties** area of the **General** tab, check the **Force Configuration** checkbox.
Step 5 In the **Namespaces** area of the **General** tab, select the namespace to be deleted and click **Delete**.
Step 6 Click **OK**.
Step 7 In the **General** tab, click **Save Changes**.

Deleting Local Security Configuration

Deleting the security configuration will disable security.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to delete the persistent memory security.

Step 4 Select the persistent memory policy for which you want to delete local security.

Step 5 In the **Actions** area of the **Security** tab, click **Delete Local Security**.

Step 6 In the **Delete** confirmation dialog box that appears, click **Yes**.

Physical Configuration and Inventory for Persistent Memory

You can view the physical inventory and configuration of all the persistent memory modules on a B-Series, C-Series, or S-Series server. The following parameters are detailed:

- DIMMs—Properties of persistent memory modules.

  Persistent memory modules on the same server are locked by using a single secure passphrase. If locked persistent memory modules are brought over from a different server, they need to be unlocked before they can be managed from the new server.

- Configuration—Overall server-level persistent memory configuration.

- Region—Properties of all the regions on the server.

  A region is a grouping of one or more persistent memory modules that can be divided up into one or more namespaces. A region is created based on the persistent memory type selected during goal creation.

  The **App Direct** persistent memory type configures one region for all the memory modules connected to a socket. The **App Direct Non Interleaved** persistent memory type configures one region for each memory module.

- Namespace—Properties of all the logical namespaces available on the server.

  These namespaces are seen by the host OS as block devices or raw devices.

Secure Erase

You can perform secure erase on a specific persistent memory module or all the persistent memory modules on a server. This operation deletes the region data and namespaces.

For the secure erase operation, you must provide a secure passphrase when security is enabled. When security is disabled, a secure passphrase in not required for the secure erase operation.

Viewing the Persistent Memory Modules on a Server

You can view the inventory of all the persistent memory modules on a B-Series, C-Series, or S-Series server.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view the persistent memory module inventory.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **DIMMS** subtab. The following information appears:

Name	Description
Selectcolumn	Checkbox that allows selection of one or more persistent memory modules. Use this for **Secure Erase** and **Unlock Foreign DIMMs** actions only.
Namecolumn	A navigation tree that allows you to view a particular component and its subcomponents. You can right-click a component to view any actions available for that component.
Clock (MHZ)column	The speed at which the memory bus is running in Megahertz.
Location column	The location in which the persistent memory module is installed.
Socket ID drop-down list	The CPU socket ID for the region to which this namespace belongs. This can be: • **Socket 1** • **Socket 2** • **Socket 3** • **Socket 4** **Note** For UCS M6 B-Series and C-Series servers, only **Socket 1** and **Socket 2** are supported.

Name	Description
Socket Local DIMM Number drop-down list	The local DIMM number for the region to which this namespace belongs. This can be: • The only option avilable for **App Direct** persistent memory type—**Not Applicable** • The options available for the **App Direct Non Interleaved** persistent memory type include: • **Socket Local DIMM No 2** • **Socket Local DIMM No 3** • **Socket Local DIMM No 4** • **Socket Local DIMM No 6** • **Socket Local DIMM No 7** • **Socket Local DIMM No 8** • **Socket Local DIMM No 10** • **Socket Local DIMM No 11** • **Socket Local DIMM No 12** • **Socket Local DIMM No 14** • **Socket Local DIMM No 15** • **Socket Local DIMM No 16** **Note** The **Socket Local DIMM No 3, 7, 11, 14, 15, and 16** are applicable only for UCS M6 B-Series and C-series servers.
Health column	The health status of the persistent memory module.

Name	Description
Status column	Security status of the persistent memory module. The security states can be: • **Disabled, Unlocked, Frozen, Count Not Expired**—Security is disabled, secure passphrase is not configured, the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules, retry count has not expired • **Disabled, Unlocked, Not Frozen, Count Not Expired**—Security is disabled, secure passphrase is not configured, the persistent memory module can be configured, retry count has not expired • **Enabled, Unlocked, Frozen, Count Not Expired**—Security is enabled, persistent memory modules are unlocked, the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules, retry count has not expired • **Enabled, Locked, Not Frozen, Count Not Expired**—Security is enabled, persistent memory modules are locked by using the secure passphrase, the persistent memory module can be configured, retry count has not expired • **Enabled, Locked, Not Frozen, Count Expired**—Security is enabled, persistent memory modules are locked by using the secure passphrase, the persistent memory module can be configured, retry count has expired
Firmware Version column	The firmware version of the persistent memory module.
Total Capacity (GiB) column	The total capacity of the persistent memory module in GiB.

Viewing Persistent Memory Module Properties

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view persistent memory module properties.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **DIMMS** subtab.

Step 6 Select a persistent memory module.

Click on the persistent memory module name. Do not click the **Select** checkbox for the persistent memory module.

Step 7 Click **Info**. The **Properties** dialog box appears with the following information:

Properties area

Name	Description
ID field	The identifier for the persistent memory module.
Location field	The slot in which the persistent memory module is installed.
Product Name field	The persistent memory module name.
Socket ID field	The CPU socket ID for the persistent memory module. This can be: • **Socket 1** • **Socket 2** • **Socket 3** • **Socket 4** **Note** For UCS M6 B-Series and C-Series servers, only **Socket 1** and **Socket 2** are supported.

Socket Local DIMM Number field	The local DIMM number for the persistent memory module. This can be:
	• The only option avilable for **App Direct** persistent memory type—**Not Applicable**
	• The options available for the **App Direct Non Interleaved** persistent memory type include:
	  • **Socket Local DIMM No 2**
	  • **Socket Local DIMM No 3**
	  • **Socket Local DIMM No 4**
	  • **Socket Local DIMM No 6**
	  • **Socket Local DIMM No 7**
	  • **Socket Local DIMM No 8**
	  • **Socket Local DIMM No 10**
	  • **Socket Local DIMM No 11**
	  • **Socket Local DIMM No 12**
	  • **Socket Local DIMM No 14**
	  • **Socket Local DIMM No 15**
	  • **Socket Local DIMM No 16**
	Note The **Socket Local DIMM No 3, 7, 11, 14, 15, and 16** are applicable only for UCS M6 B-Series and C-series servers.

Vendor field	The name of the manufacturer.

Name	Description
PID field	The server model PID.
Revision field	The revision number.
Vendor Serial (SN) field	The serial number assigned by the manufacturer.
Array field	The array containing the persistent memory module.
Bank field	The bank within the array.
Clock (MHz) field	The persistent memory module speed.
Form Factor field	The persistent memory module form factor.
Health State field	The health status of the persistent memory module.
Latency (ns) field	The delay incurred when the server accesses this persistent memory module.
Set field	If this persistent memory module is part of set, this field displays the identifier for the set.
Type field	The persistent memory module type.
Width field	The persistent memory module width.
Capacity (MB) field	The size of the persistent memory module.
Persistent Memory Capacity (GiB) field	The persistent memory capacity of the persistent memory module in GiB.
Total Capacity (GiB) field	The total capacity of the persistent memory module in GiB.
Reserved Capacity field	The reserved capacity of the persistent memory module in GiB.
App Direct Capacity (GiB) field	The App Direct memory capacity of the persistent memory module.
Memory Capacity (GiB) field	The volatile memory capacity of the persistent memory module in GiB.

Name	Description
Security Status field	Security status of the persistent memory module. The security states can be: • **Disabled, Unlocked, Frozen, Count Not Expired**—Security is disabled, secure passphrase is not configured, the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules, retry count has not expired • **Disabled, Unlocked, Not Frozen, Count Not Expired**—Security is disabled, secure passphrase is not configured, the persistent memory module can be configured, retry count has not expired • **Enabled, Unlocked, Frozen, Count Not Expired**—Security is enabled, persistent memory modules are unlocked, the host OS can configure the persistent memory modules and use them, but cannot configure the security of these persistent memory modules, retry count has not expired • **Enabled, Locked, Not Frozen, Count Not Expired**—Security is enabled, persistent memory modules are locked by using the secure passphrase, the persistent memory module can be configured, retry count has not expired • **Enabled, Locked, Not Frozen, Count Expired**—Security is enabled, persistent memory modules are locked by using the secure passphrase, the persistent memory module can be configured, retry count has expired
UID field	The unique hardware ID for the persistent memory module.

Firmware area

Name	Description
Running Version field	The firmware version used by the persistent memory module.
Package Version field	The version of the firmware included in the package.
Startup Version field	The version of the firmware that takes effect the next time that the component reboots.
Activate Status field	This can be one of the following: • **Ready**—Activation succeeded and the component is running the new version. • **Activating**—The system is activating the new firmware version. • **Failed**—The firmware activation failed. For more information, double-click the failed component to view its status properties.

Performing Secure Erase on a Persistent Memory Module

For the secure erase operation, you must provide a secure passphrase when security is enabled. When security is disabled, a secure passphrase is not required for the secure erase operation.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to securely erase the persistent memory modules.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **DIMMS** subtab.

Step 6 Click the **Select** checkbox for the persistent memory modules that you want to securely erase.

Step 7 Click **Secure Erase** and then click **Yes**.

Securely erasing persistent memory modules is a destructive operation, and will result in deletion of region data and namespaces.

Step 8 In the **Secure Erase** dialog box:

- If security is enabled, enter the secure passphrase and click **OK**.
- If security is not enabled, click **OK** (empty passphrase).

Unlocking Foreign Persistent Memory Modules

Before you begin

Before you use the following procedure to select the persistent memory modules to be unlocked, and perform the unlock foreign DIMMs operation, ensure that you do the following:

1. Decommission the server.
2. Change the persistent memory modules.
3. Recommission the server.
4. Associate the server to a service-profile without a persistent memory policy.
5. Ensure that the server is in the powered-on state, and BIOS POST is completed.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**

- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server on which you want to unlock foreign persistent memory modules.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **DIMMS** subtab.

Step 6 Click the **Select** checkbox for the foreign persistent memory modules that you want to unlock.

Step 7 Click **Unlock Foreign DIMMs**.

Step 8 In the dialog box that appears, enter the currently deployed secure passphrase for the foreign persistent memory modules, and click **OK**.

You must provide the same passphrase that is already deployed on the foreign persistent memory module taken from a different server.

What to do next

1. Check whether the persistent memory modules get unlocked after the ExecuteActions FSM completes. Now, the persistent memory modules are ready to be used.
2. Attach a persistent memory policy.
3. Check whether the associate FSM completes.

Viewing the Persistent Memory Configuration of a Server

You can view the configuration of persistent memory modules on a B-Series, C-Series, or S-Series server.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view the persistent memory configuration.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **Configuration** subtab. The following information appears:

Table 3: Properties Area

Name	Description
Memory Capacity (GiB) field	The volatile memory capacity of all the persistent memory modules on the server in GiB.
Persistent Memory Capacity (GiB) field	The persistent memory capacity of all the persistent memory modules on the server in GiB.

Name	Description
Reserved Capacity field	The reserved capacity of all the persistent memory modules on the server in GiB.
Total Capacity (GiB) field	The total capacity of all the persistent memory modules on the server in GiB.
Configured Result Error Description field	The errors in the persistent memory configuration of the server.
Config Result field	The result of the persistent memory configuration.
Config State field	The state of the persistent memory configuration.
Security State field	Security status of the persistent memory configuration. The security states can be: • **Disabled-Frozen**—When persistent memory modules are in UCS Managed mode and security is disabled on all persistent memory modules. • **Disabled**—When persistent memory modules are in Host Managed mode and security is disabled on all persistent memory modules. • **Unlocked-Frozen**—When persistent memory modules are in UCS Managed mode and security is enabled on all persistent memory modules. • **Enabled,Locked**—When persistent memory modules are in Host Managed mode and security is enabled on all persistent memory modules. • **Mixed-State**—When some persistent memory modules have security enabled and the rest have security disabled.

Performing Secure Erase on All Persistent Memory Modules on a Server

For the secure erase operation, you must provide a secure passphrase when security is enabled. When security is disabled, a secure passphrase in not required for the secure erase operation.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to securely erase the persistent memory modules.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **Configuration** subtab.

Step 6 Click **Secure Erase**.

Securely erasing persistent memory modules is a destructive operation, and will result in deletion of all the region data and namespaces on the server.

Viewing the Regions on a Server

You can view the inventory of the regions on a B-Series, C-Series, or S-Series server.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view the region inventory.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **Regions** subtab. The following information appears:

Name	Description
Id column	The ID of the region.
Socket ID column	The CPU socket ID for the region. This can be: • **Socket 1** • **Socket 2** • **Socket 3** • **Socket 4** **Note** For UCS M6 B-Series and C-Series servers, only **Socket 1** and **Socket 2** are supported.

Name	Description
Socket Local DIMM Number column	The local DIMM number for the region. This can be: • The only option avilable for **App Direct** persistent memory type—**Not Applicable** • The options available for the **App Direct Non Interleaved** persistent memory type include: • **Socket Local DIMM No 2** • **Socket Local DIMM No 3** • **Socket Local DIMM No 4** • **Socket Local DIMM No 6** • **Socket Local DIMM No 7** • **Socket Local DIMM No 8** • **Socket Local DIMM No 10** • **Socket Local DIMM No 11** • **Socket Local DIMM No 12** • **Socket Local DIMM No 14** • **Socket Local DIMM No 15** • **Socket Local DIMM No 16** **Note** The **Socket Local DIMM No 3, 7, 11, 14, 15, and 16** are applicable only for UCS M6 B-Series and C-series servers.
DIMM Locator IDs	The locator IDs of the DIMMs in the region.
Persistent Memory Type	The type of persistent memory. This can be one of the following: • **App Direct**—Configures one region for all the persistent memory modules connected to a socket. • **App Direct Non Interleaved**—Configures one region for each persistent memory module.
Total Capacity column	The total capacity of the region in GiB.
Free Capacity column	The available capacity of the region in GiB.
Health Status column	The health status of the region.

Viewing Region Properties

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view persistent memory module properties.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **Regions** subtab.

Step 6 Select a region.

Step 7 Click **Info**. The **Properties** dialog box appears with the following information:

Name	Description
ID field	The identifier for the region.
Socket ID field	The CPU socket ID for the region.
Local DIMM Slot ID field	The local DIMM slot ID for the region.
DIMM Locator IDs field	The locator IDs of the DIMMs in the region.
Operational Mode field	The persistent memory type of the region.
Total Capacity (GiB) field	The total capacity of the region in GiB.
Free Capacity (GiB) field	The available capacity of the region in GiB.
Health State field	The health status of the region.
Interleaved Set ID field	The ID of the interleaved set for the region.

Viewing the Namespaces on a Server

You can view the inventory of the namespaces on a B-Series, C-Series, or S-Series server.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view the namespace inventory.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **Namespace** subtab. The following information appears:

Name	Description
Name column	The name of the namespace.
Mode column	The mode in which the namespace is created. This can be: • **Raw** • **Block**
Capacity(GiB) column	The memory capacity of the namespace in GiBs.
Health Status column	The health status of the namespace.

Viewing Namespace Properties

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand to a server using one of the following paths:

- For a blade server, expand **Equipment** > **Chassis** > ***Chassis-Number*** > **Servers**
- For a rack-mount server, expand **Equipment** > **Rack Mounts** > **Servers**

Step 3 Select the server for which you want to view namespace properties.

Step 4 In the **Work** pane, click the **Inventory** tab and then the **Persistent Memory** subtab.

Step 5 Click the **Namespace** subtab.

Step 6 Select a namespace within a region.

Step 7 Click **Info**. The **Properties** dialog box appears with the following information:

Name	Description
Name field	The name of the namespace.
Capacity (GiB) field	The total capacity of the namespace in GiB.
Health Status field	The health status of the namespace.
Label Version field	The label version of the namespace.
Operational Mode field	The persistent memory type of the namespace.
UUID field	The unique hardware ID of the persistent memory module on which the namespace is created.

Performing Persistent Memory Scrub

In Cisco UCS Manager, you can scrub persistent memory by using one of the following methods:

- Disassociating the Service Profile and the Scrub Policy with Persistent Memory Scrub Selected
- Resetting a Server to Factory Defaults With Persistent Memory Scrub Selected
- Deleting a Goal

Disassociating the Service Profile and the Scrub Policy with Persistent Memory Scrub Selected

Disassociating the service profile and the scrub policy, which has the persistent memory scrub option selected will result in deletion of all regions and namespaces and its data in all the persistent memory modules. Security will be disabled, if it is already enabled. The following procedure describes how to disassociate a service profile and a scrub policy.

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Server** > **Service Profiles**

Step 3 Select the service profile.

Step 4 In the **Work** pane, click the **Policies** tab.

Step 5 In the **Policies** area, expand **Scrub Policy**.

Step 6 From the **Scrub Policy** drop-down list, select a scrub policy with the persistent memory scrub option enabled.

Step 7 Click **Save Changes**.

The scrub policy now gets associated with the service profile.

Step 8 Right-click the service profile and select **Disassociate Service Profile**.

Step 9 In the **Disassociate Service Profile** dialog box, click **Yes** to confirm that you want to disassociate the service profile.

On UCS M5, M6 B-Series and C-Series servers: Regions and namespaces will be deleted after successful disassociation.

On UCS M5 S-Series servers: Namespaces will be deleted after successful disassociation.

Resetting a Server to Factory Defaults With Persistent Memory Scrub Selected

You can reset a server to its factory settings. By default, the factory reset operation does not affect storage drives, persistent memory modules, and flexflash drives. This is to prevent any loss of data. However, you can choose to reset these devices to a known state as well.

Important Resetting storage devices will result in loss of data.

Perform the following procedure to reset the server to factory default settings, and delete persistent memory configuration and data.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Choose the server that you want to reset.

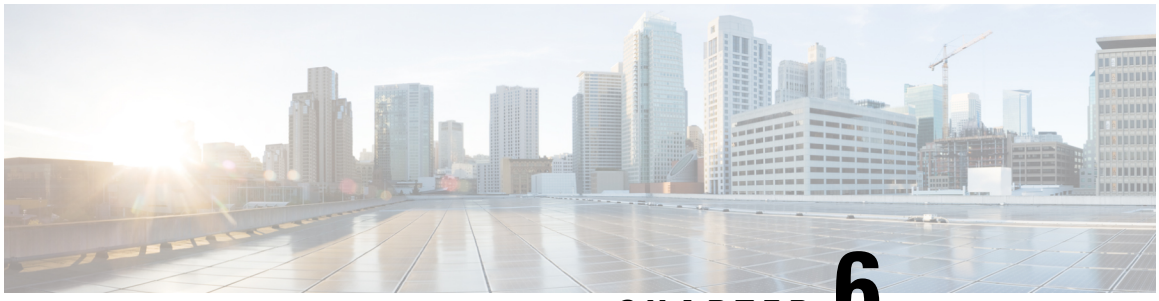
Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Server Maintenance**.

Step 6 Select the **Reset to Factory Default** checkbox, and click **OK**.

Step 7 In the **Maintenance Server** dialog box, select the **Persistent Memory Scrub** checkbox, and click **OK**.

The server settings are set to factory default, persistent memory configuration and data are deleted.



CHAPTER 6

Configuring Persistent Memory Using Cisco UCS Manager CLI

- Performing Persistent Memory Scrub, on page 130
- Disassociating the Service Profile and the Scrub Policy with Persistent Memory Scrub Selected, on page 130
- Resetting a Server to Factory Defaults With Persistent Memory Scrub Selected, on page 131

Creating a Persistent Memory Policy

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **create persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy* # **set descr** *policy-description*
4. UCS-A /org/persistent-memory-policy* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **create persistent-memory-policy** *policy-name*	Creates a persistent memory policy with the specified policy name, and enters the persistent memory policy mode.
Step 3	UCS-A /org/persistent-memory-policy* # **set descr** *policy-description*	Adds a short description of the policy.
Step 4	UCS-A /org/persistent-memory-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a persistent memory policy:

```
UCS-A# scope org
UCS-A /org # create persistent-memory-policy sample
UCS-A /org/persistent-memory-policy* # set descr "This is a persistent memory policy"
UCS-A /org/persistent-memory-policy* # commit-buffer
UCS-A /org/persistent-memory-policy
```

What to do next

- Create a goal
- Create a namespace

Including a Persistent Memory Policy in a Service Profile

Before you can use a persistent memory policy to manage persistent memory in Cisco UCS Manager, you must include the persistent memory policy in a service profile. After a persistent memory policy is included in a service profile, you can associate the service profile with a Cisco UCS server.

If you include a persistent memory policy in a service profile associated to a server, the persistent memory configuration on the server is **UCS-managed**. In the **UCS-managed** mode, you can use Cisco UCS Manager and host tools to configure and manage persistent memory modules.

If a persistent memory policy is not included in the service profile associated to a server, the persistent memory configuration on the server is **host-managed**. In the **host-managed** mode, you can use the host tools to configure and manage persistent memory modules.

The following procedure describes how to include a persistent memory policy in a service profile.

Before you begin

Create the persistent memory policy that you want to include in a service profile.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *service-profile-name*
3. UCS-A /org/service-profile # **set persistent-memory-policy** *persistent-memory-policy-name*
4. UCS-A /org/service-profile* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name .
Step 2	UCS-A /org # **scope service-profile** *service-profile-name*	Enters organization service profile mode for the specified service profile.
Step 3	UCS-A /org/service-profile # **set persistent-memory-policy** *persistent-memory-policy-name*	Sets the persistent memory policy that you want to include in this service profile.
Step 4	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The persistent memory policy is applied on the server to which the service profile is associated.

Example

This example shows how to include a persistent memory policy in a service profile:

```
UCS-A# scope org
UCS-A /org # scope service-profile sample
UCS-A /org/service-profile # set persistent-memory-policy policy1
UCS-A /org/service-profile* # commit-buffer
```

```
UCS-A /org/service-profile #
```

Removing a Persistent Memory Policy from a Service Profile

Removing a persistent memory policy from a service profile does not change any region or namespace configuration. It changes persistent memory from UCS-managed to host-managed. The following procedure describes how to remove a persistent memory policy from a service profile.

After you remove the persistent memory policy from the service profile that is associated to a server, the server is considered host-managed with respect to persistent memory configuration.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *service-profile-name*
3. UCS-A /org/service-profile # **set persistent-memory-policy noset**
4. UCS-A /org/service-profile* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name .
Step 2	UCS-A /org # **scope service-profile** *service-profile-name*	Enters organization service profile mode for the specified service profile.
Step 3	UCS-A /org/service-profile # **set persistent-memory-policy noset**	Removes the persistent memory policy that was included in this service profile.
Step 4	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The persistent memory policy is removed from the service profile and its associated server.

Example

This example shows how to remove a persistent memory policy from a service profile:

```
UCS-A# scope org
UCS-A /org # scope service-profile sample
UCS-A /org/service-profile # set persistent-memory-policy noset
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Creating a Goal

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **create goal all-sockets**
4. UCS-A /org/persistent-memory-policy/goal* # **set persistent-memory-type** {app-direct | app-direct-non-interleaved}
5. UCS-A /org/persistent-memory-policy/goal* # **set memory-mode-percentage** *percentage*
6. UCS-A /org/persistent-memory-policy/goal* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the specified persistent memory policy, and the persistent memory policy mode.
Step 3	UCS-A /org/persistent-memory-policy # **create goal all-sockets**	Creates a goal for all sockets. The default option is **all-sockets**.
Step 4	UCS-A /org/persistent-memory-policy/goal* # **set persistent-memory-type** {app-direct | app-direct-non-interleaved}	Configures the type of persistent memory. This can be one of the following: • **app-direct**—Configures one region for all the persistent memory modules connected to a socket. • **app-direct-non-interleaved**—Configures one region for each persistent memory module.
Step 5	UCS-A /org/persistent-memory-policy/goal* # **set memory-mode-percentage** *percentage*	Sets percentage of memory on the persistent memory module that is configured as volatile memory.

	Command or Action	Purpose

		Note
		• The default memory mode percentage for:
		  • UCS M5 B-Series and C-Series servers is 100%.
		  • UCS M5 S-Series servers is 0%.
		• For UCS M6 B-Series and C-Series servers:
		  • The **Mixed Mode** is not supported. For 8+1 POR, the **App Direct Non Interleaved Mode** is the only supported configuration.
		  • The default memory mode percentage is 0%.
		• For UCS M5 and M6 servers, the Near Memory (NM) : Far Memory ratio (FM) (DRAM + PMEM) is supported between 1:4 - 1:16 in 100% memory mode.

Step 6	UCS-A /org/persistent-memory-policy/goal* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a goal:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # create goal all-sockets
UCS-A /org/persistent-memory-policy/goal* # set persistent-memory-type app-direct
UCS-A /org/persistent-memory-policy/goal* # set memory-mode-percentage 10
UCS-A /org/persistent-memory-policy/goal* # commit-buffer
UCS-A /org/persistent-memory-policy/goal #
```

Creating a Namespace

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **create logical-namespace** *namespace-name*
4. UCS-A /org/persistent-memory-policy/logical-namespace* # **set capacity** *memory-capacity*

5. UCS-A /org/persistent-memory-policy/logical-namespace* # **set mode** {block | raw}
6. UCS-A /org/persistent-memory-policy/logical-namespace* # **set socket-id** {socket-1 | socket-2 | socket-3 | socket-4
7. UCS-A /org/persistent-memory-policy/logical-namespace* # **set socket-local-dimm-number** {not-applicable | socket-local-dimm-no-2 | socket-local-dimm-no-3 | socket-local-dimm-no-4 | socket-local-dimm-no-6 | socket-local-dimm-no-7 | socket-local-dimm-no-8 | socket-local-dimm-no-10 | socket-local-dimm-no-11 | socket-local-dimm-no-12 | socket-local-dimm-no-14 | socket-local-dimm-no-15 | socket-local-dimm-no-16
8. UCS-A /org/persistent-memory-policy/logical-namespace* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the specified persistent memory policy, and the persistent memory policy mode.
Step 3	UCS-A /org/persistent-memory-policy # **create logical-namespace** *namespace-name*	Creates a namespace with the specified name. The namespace name has the following constraints: • Must be between 1 and 63 characters in length. • The first character must be a letter (A-Z or a-z), a number(0-9), or a special character(#, -, or _) • The remaining characters can be a combination of letters (A-Z or a-z), numbers (0-9), and special characters (#, -, _, space)
Step 4	UCS-A /org/persistent-memory-policy/logical-namespace* # **set capacity** *memory-capacity*	Sets the memory capacity of the namespace in GiBs.
Step 5	UCS-A /org/persistent-memory-policy/logical-namespace* # **set mode** {block | raw}	Sets the mode in which the namespace is created. This can be: • **raw** • **block**
Step 6	UCS-A /org/persistent-memory-policy/logical-namespace* # **set socket-id** {socket-1 | socket-2 | socket-3 | socket-4	Sets the socket ID for the region to which this namespace belongs. This can be: • **socket-1** • **socket-2** • **socket-3** • **socket-4** **Note** For UCS M6 B-Series and C-Series servers, only **socket-1**and **socket-2** are supported.

	Command or Action	Purpose
Step 7	UCS-A /org/persistent-memory-policy/logical-namespace* # **set socket-local-dimm-number** {not-applicable | socket-local-dimm-no-2 | socket-local-dimm-no-3 | socket-local-dimm-no-4 | socket-local-dimm-no-6 | socket-local-dimm-no-7 | socket-local-dimm-no-8 | socket-local-dimm-no-10 | socket-local-dimm-no-11 | socket-local-dimm-no-12 | socket-local-dimm-no-14 | socket-local-dimm-no-15 | socket-local-dimm-no-16	Sets the local DIMM number for the region to which this namespace belongs. This can be: • The only option avilable for **app-direct** persistent memory type—**not-applicable** • The options available for the **app-direct-non-interleaved** persistent memory type include: • **socket-local-dimm-no-2** • **socket-local-dimm-no-3** • **socket-local-dimm-no-4** • **socket-local-dimm-no-6** • **socket-local-dimm-no-7** • **socket-local-dimm-no-8** • **socket-local-dimm-no-10** • **socket-local-dimm-no-11** • **socket-local-dimm-no-12** • **socket-local-dimm-no-14** • **socket-local-dimm-no-15** • **socket-local-dimm-no-16** **Note** The socket-local-dimm-no-3, 7, 11, 14, 15, and 16 are applicable only for UCS B-Series and C-Series M6 servers.
Step 8	UCS-A /org/persistent-memory-policy/logical-namespace* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a namespace:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # create logical-namespace space1
UCS-A /org/persistent-memory-policy/logical-namespace* # set capacity 10
UCS-A /org/persistent-memory-policy/logical-namespace* # set mode block
UCS-A /org/persistent-memory-policy/logical-namespace* # set socket-id socket-1
UCS-A /org/persistent-memory-policy/logical-namespace* # set socket-local-dimm-number
socket-local-dimm-no-2
UCS-A /org/persistent-memory-policy/logical-namespace* # commit-buffer
UCS-A /org/persistent-memory-policy/logical-namespace #
```

Creating Local Security Configuration

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **create security**
4. UCS-A /org/persistent-memory-policy/security* # **create local-security**
5. UCS-A /org/persistent-memory-policy/security/local-security* # **set secure-passphrase** *secure-passphrase*
6. (Optional) UCS-A /org/persistent-memory-policy/security/local-security* # **set deployed-secure-passphrase** *deployed-secure-passphrase*
7. UCS-A /org/persistent-memory-policy/security/local-security* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the specified persistent memory policy, and the persistent memory policy mode.
Step 3	UCS-A /org/persistent-memory-policy # **create security**	Creates a security policy policy and enters the persistent memory security mode.
Step 4	UCS-A /org/persistent-memory-policy/security* # **create local-security**	Creates a local security policy and enters persistent memory local security mode.
Step 5	UCS-A /org/persistent-memory-policy/security/local-security* # **set secure-passphrase** *secure-passphrase*	Configures the secure passphrase to be set for the persistent memory policy. The secure passphrase has the following constraints: • Must be between 8 and 32 characters in length. • These characters can be a combination of letters (A-Z or a-z), numbers (0-9), and special characters (!, @, #, $, %, ^, &, *, -, _, +, =).
Step 6	(Optional) UCS-A /org/persistent-memory-policy/security/local-security* # **set deployed-secure-passphrase** *deployed-secure-passphrase*	Configures the currently deployed secure passphrase for the persistent memory policy. The deployed secure passphrase is required when the server that you are configuring has a secure passphrase from a previous deployment. This is required only for secure passphrase modification.

	Command or Action	Purpose
Step 7	UCS-A /org/persistent-memory-policy/security/local-security* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a local security policy for a persistent memory policy:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # create security
UCS-A /org/persistent-memory-policy/security* # create local-security
UCS-A /org/persistent-memory-policy/security/local-security* # set secure-passphrase
a1b2c3d4e5f6
UCS-A /org/persistent-memory-policy/security/local-security* # set deployed-secure-passphrase
 a1b2c3d4e5f6
UCS-A /org/persistent-memory-policy/security/local-security* # commit-buffer
UCS-A /org/persistent-memory-policy/security/local-security #
```

Modifying a Persistent Memory Policy

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **set descr** *policy-description*
4. UCS-A /org/persistent-memory-policy* # **set force-configuration** {no | yes}
5. UCS-A /org/persistent-memory-policy* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **set descr** *policy-description*	Modifies the short description of the policy.
Step 4	UCS-A /org/persistent-memory-policy* # **set force-configuration** {no | yes}	Configures whether **Force Configuration** has been selected or not. This can be one of the following: • **no**—**Force Configuration** is not selected. This is the default value.

	Command or Action	Purpose
		When **Force Configuration** is not selected, the persistent memory policy is not forcibly applied on associated servers. • **yes**—**Force Configuration** is selected. When this is done, the persistent memory policy is forcibly applied on all the associated servers. This will not have any effect if the existing configuration on the server matches the policy configuration. This will also apply the policy on recommissioned servers. Certain operations can lead to data loss due to goal or namespace modification, and hence result in errors. To successfully perform these operations, you must forcefully apply the new configuration on the server. You can do this by setting the **Force Configuration** option to **yes** in the persistent memory policy. **Force Configuration** autiomatically gets set to **no** after each operation. You must select this option everytime you perform one of these operations.
Step 5	UCS-A /org/persistent-memory-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to modify a persistent memory policy:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # set descr "This is a modified memory policy description"
UCS-A /org/persistent-memory-policy* # set force-configuration yes
UCS-A /org/persistent-memory-policy* # commit-buffer
UCS-A /org/persistent-memory-policy
```

Modifying a Goal

Modifying a goal will result in the loss of data currently stored in the persistent memory.

Because goal modification is a destructive operation, you must set **Force Configuration** to **yes** before modifying the goal.

Before modifying the **Persistent Memory Type**, delete the existing namespaces. This is because, in the **App Direct** persistent memory type you do not specify a DIMM number for each namespace. In the **App Direct Non Interleaved** persistent memory type, each namespace has a DIMM number specified.

SUMMARY STEPS

1. UCS-A# **scope org**

2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **set force-configuration** {no | yes}
4. UCS-A /org/persistent-memory-policy* # **commit-buffer**
5. UCS-A /org/persistent-memory-policy # **scope goal all-sockets**
6. UCS-A /org/persistent-memory-policy/goal # **set persistent-memory-type** {app-direct | app-direct-non-interleaved}
7. UCS-A /org/persistent-memory-policy/goal* # **set memory-mode-percentage** *percentage*
8. UCS-A /org/persistent-memory-policy/goal* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **set force-configuration** {no | yes}	Configures whether **force-configuration** has been selected or not. This can be one of the following: • **no**—**Force Configuration** is not selected. This is the default value. When **Force Configuration** is not selected, the persistent memory policy is not forcibly applied on associated servers. • **yes**—**Force Configuration** is selected. When this is done, the persistent memory policy is forcibly applied on all the associated servers. This will not have any effect if the existing configuration on the server matches the policy configuration. This will also apply the policy on recommissioned servers. Goal modification is a destructive operation.To successfully modify a goal, you must set **force-configuration** to **yes**.
Step 4	UCS-A /org/persistent-memory-policy* # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /org/persistent-memory-policy # **scope goal all-sockets**	Enters the goal.
Step 6	UCS-A /org/persistent-memory-policy/goal # **set persistent-memory-type** {app-direct | app-direct-non-interleaved}	Configures the type of persistent memory. This can be one of the following: • **app-direct**—Configures one region for all the persistent memory modules connected to a socket. • **app-direct-non-interleaved**—Configures one region for each persistent memory module. Ensure that you delete the namespaces before changing the persistent memory type.

	Command or Action	Purpose

Step 7	UCS-A /org/persistent-memory-policy/goal* # **set memory-mode-percentage** *percentage*	Sets the percentage of memory on the persistent memory module that is configured as volatile memory.
		Note
		• The default memory mode percentage for:
		  • UCS M5 B-Series and C-Series servers is 100%.
		  • UCS M5 S-Series servers is 0%.
		• For UCS M6 B-Series and C-Series servers:
		  • The **Mixed Mode** is not supported. For 8+1 POR, the **App Direct Non Interleaved Mode** is the only supported configuration.
		  • The default memory mode percentage is 0%.
		• For UCS M5 and M6 servers, the Near Memory (NM) : Far Memory ratio (FM) (DRAM + PMEM) is supported between 1:4 - 1:16 in 100% memory mode.

Step 8	UCS-A /org/persistent-memory-policy/goal* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to modify a goal:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # set force-configuration yes
UCS-A /org/persistent-memory-policy* # commit-buffer
UCS-A /org/persistent-memory-policy # scope goal all-sockets
UCS-A /org/persistent-memory-policy/goal # set persistent-memory-type app-direct
UCS-A /org/persistent-memory-policy/goal* # set memory-mode-percentage 10
UCS-A /org/persistent-memory-policy/goal* # commit-buffer
UCS-A /org/persistent-memory-policy/goal
```

Modifying a Namespace

You can modify a namespace only if the persistent memory policy that contains the namespace is not referred to by a server. Modifying a namespace is not an allowed operation if the persistent memory policy that contains the namespace is referred to by a server.

The following steps are applicable only when the persistent memory policy that contains the namespace is not referred to by a server.

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **scope logical-namespace** *namespace-name*
4. UCS-A /org/persistent-memory-policy/logical-namespace # **set capacity** *memory-capacity*
5. UCS-A /org/persistent-memory-policy/logical-namespace* # **set mode** {block | raw}
6. UCS-A /org/persistent-memory-policy/logical-namespace* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **scope logical-namespace** *namespace-name*	Enters the namespace mode for the specified namespace.
Step 4	UCS-A /org/persistent-memory-policy/logical-namespace # **set capacity** *memory-capacity*	Sets the memory capacity of the namespace in GiBs.
Step 5	UCS-A /org/persistent-memory-policy/logical-namespace* # **set mode** {block | raw}	Sets the mode in which the namespace is created. This can be: • **raw** • **block**
Step 6	UCS-A /org/persistent-memory-policy/logical-namespace* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to modify a namespace:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # scope logical-namespace NS1
UCS-A /org/persistent-memory-policy/logical-namespace # set capacity 10
UCS-A /org/persistent-memory-policy/logical-namespace* # set mode block
UCS-A /org/persistent-memory-policy/logical-namespace* # commit-buffer
```

```
UCS-A /org/persistent-memory-policy/logical-namespace #
```

Modifying Local Security Configuration

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **scope security**
4. UCS-A /org/persistent-memory-policy/security # **scope local-security**
5. UCS-A /org/persistent-memory-policy/security/local-security* # **set deployed-secure-passphrase** *deployed-secure-passphrase*
6. UCS-A /org/persistent-memory-policy/security/local-security* # **set secure-passphrase** *secure-passphrase*
7. UCS-A /org/persistent-memory-policy/security/local-security* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the specified persistent memory policy, and the persistent memory policy mode.
Step 3	UCS-A /org/persistent-memory-policy # **scope security**	Enters the persistent memory security mode.
Step 4	UCS-A /org/persistent-memory-policy/security # **scope local-security**	Enters persistent memory local security mode.
Step 5	UCS-A /org/persistent-memory-policy/security/local-security* # **set deployed-secure-passphrase** *deployed-secure-passphrase*	Configures the deployed secure passphrase for the persistent memory policy. The secure passphrase entered here must match the currently deployed secure passphrase.
Step 6	UCS-A /org/persistent-memory-policy/security/local-security* # **set secure-passphrase** *secure-passphrase*	Sets the new secure passphrase for the persistent memory policy. The new secure passphrase can be set only if the deployed secure passphrase is authenticated.
Step 7	UCS-A /org/persistent-memory-policy/security/local-security* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to modify the secure passphrase of a local security policy for a persistent memory policy:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # scope security
UCS-A /org/persistent-memory-policy/security # scope local-security
UCS-A /org/persistent-memory-policy/security/local-security # set deployed-secure-passphrase
 a1b2c3d4e5f6
UCS-A /org/persistent-memory-policy/security/local-security* # set secure-passphrase
g7h8i9j0k1l2
UCS-A /org/persistent-memory-policy/security/local-security* # commit-buffer
UCS-A /org/persistent-memory-policy/security/local-security #
```

Viewing Properties of a Persistent Memory Policy

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **show persistent-memory-policy** *policy-name* [detail]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **show persistent-memory-policy** *policy-name* [detail]	Displays the properties of the policy.

Example

This example shows how to view the properties of a persistent memory policy:

```
UCS-A# scope org
UCS-A /org # show persistent-memory-policy sample detail

Persistent Memory Policy:
    Name: sample
    Description:
    Policy Owner: Local
    Force Configuration: No
UCS-A /org #
```

Viewing Properties of a Goal

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **show goal** [detail]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **show goal** [detail]	Displays the properties of the goal.

Example

This example shows how to view the properties of a goal:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # show goal detail

Persistent Memory Goal:
    Socket ID: All Sockets
    Memory Mode Percentage: 0
    Persistent Memory Type: App Direct
UCS-A /org/persistent-memory-policy/goal #
```

Viewing Properties of a Namespace

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **enter persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **show logical-namespace** *namespace-name* [detail]
4. (Optional) UCS-A /org/persistent-memory-policy # **show logical-namespace** [detail]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **enter persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **show logical-namespace** *namespace-name* [detail]	Displays the properties of the specified namespace.
Step 4	(Optional) UCS-A /org/persistent-memory-policy # **show logical-namespace** [detail]	Displays the properties of all namespaces in the persistent memory policy.

Example

This example shows how to view the properties of a specific namespace:

```
UCS-A# scope org
UCS-A /org # enter persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # show logical-namespace NS1 detail

Persistent Memory Logical Namespace:
    Name: NS1
    Capacity (GiB): 10
    Socket ID: Socket 1
    Socket Local Dimm Number: Not Applicable
    Mode: Raw
UCS-A /org/persistent-memory-policy #
```

This example shows how to display the properties of all namespaces in the persistent memory policy:

```
UCS-A# scope org
UCS-A /org # enter persistent-memory-policy sample
UCS-A /org/persistent-memory-policy # show logical-namespace detail

Persistent Memory Logical Namespace:
    Name: NS1
    Capacity (GiB): 10
    Socket ID: Socket 1
    Socket Local Dimm Number: Not Applicable
    Mode: Raw

    Name: NS2
    Capacity (GiB): 20
    Socket ID: Socket 2
    Socket Local Dimm Number: Not Applicable
    Mode: Raw

    Name: NS3
    Capacity (GiB): 15
    Socket ID: Socket 2
    Socket Local Dimm Number: Not Applicable
    Mode: Raw

UCS-A /org/persistent-memory-policy #
```

Viewing Local Security Configuration Properties

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **scope security**
4. UCS-A /org/persistent-memory-policy/security # **scope local-security**
5. UCS-A /org/persistent-memory-policy/security/local-security # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **scope security**	Enters the persistent memory security mode.
Step 4	UCS-A /org/persistent-memory-policy/security # **scope local-security**	Enters the local security mode.
Step 5	UCS-A /org/persistent-memory-policy/security/local-security # **show detail**	Displays details of the local security configuration.

Example

This example shows how to view details of a local security policy:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy PMemP_1
UCS-A /org/persistent-memory-policy # scope security
UCS-A /org/persistent-memory-policy/security # scope local-security
UCS-A /org/persistent-memory-policy/security/local-security # show detail

Persistent Memory Local Security:
Secure Passphrase: ****
Deployed Secure Passphrase: ****
UCS-A /org/persistent-memory-policy/security/local-security #
```

Deleting a Persistent Memory Policy

You cannot delete a persistent memory policy when the policy is referred to by a server. To delete a persistent memory policy when it is not referred to by a server, follow these steps:

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **delete persistent-memory-policy** *policy-name*
3. UCS-A /org* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **delete persistent-memory-policy** *policy-name*	Deletes the specified persistent memory policy.

	Command or Action	Purpose
Step 3	UCS-A /org* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to delete a persistent memory policy when it is not referred to by a server:

```
UCS-A# scope org
UCS-A /org # show persistent-memory-policy

Persistent Memory Policy:
    Name                 Force Configuration
    -------------------- -------------------
    PMemP_1              No
    PMemP_2              No
    PMemP_3              No
    PMemP_4              No
    PMemP_5              No
    PMemP_6              No

UCS-A /org # delete persistent-memory-policy PMemP_4
UCS-A /org* # commit-buffer
UCS-A /org # show persistent-memory-policy

Persistent Memory Policy:
    Name                 Force Configuration
    -------------------- -------------------
    PMemP_1              No
    PMemP_2              No
    PMemP_3              No
    PMemP_5              No
    PMemP_6              No


UCS-A /org #
```

Deleting a Goal

For UCS M5 , M6 B-Series and C-Series servers, deleting a goal deletes all related regions and namespaces on the associated servers, and disables security. For UCS M5 S-Series servers, deleting a goal deletes all namespaces on the associated servers, and disables security. Goal deletion also returns the persistent memory module to its default state. The default state of a persistent memory module is:

- UCS M5 ,M6 B-Series and C-Series servers—100% **Memory Mode** and **App Direct** persistent memory type
- UCS M5 S-Series servers—0% **Memory Mode** and **App Direct Non Interleaved** persistent memory type

Because goal deletion is a destructive operation, you must set **Force Configuration** to **yes** before deleting the goal.

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **set force-configuration** {no | yes}
4. UCS-A /org/persistent-memory-policy* # **delete goal all-sockets**
5. UCS-A /org/persistent-memory-policy* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **set force-configuration** {no | yes}	Configures whether **force-configuration** has been selected or not. This can be one of the following: • **no**—**Force Configuration** is not selected. This is the default value. When **Force Configuration** is not selected, the persistent memory policy is not forcibly applied on associated servers. • **yes**—**Force Configuration** is selected. When this is done, the persistent memory policy is forcibly applied on all the associated servers. This will not have any effect if the existing configuration on the server matches the policy configuration. This will also apply the policy on recommissioned servers. Goal deletion is a destructive operation.To successfully delete a goal, you must set **force-configuration** to **Yes**.
Step 4	UCS-A /org/persistent-memory-policy* # **delete goal all-sockets**	Deletes the goal.
Step 5	UCS-A /org/persistent-memory-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to delete a goal:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy PMemP_1
UCS-A /org/persistent-memory-policy # set force-configuration yes
UCS-A /org/persistent-memory-policy* # delete goal all-sockets
UCS-A /org/persistent-memory-policy* # commit-buffer
UCS-A /org/persistent-memory-policy #
```

Deleting a Namespace

Deleting a namespace will result in the loss of data currently stored in the namespace.

Because namespace deletion is a destructive operation, you must set **Force Configuration** to **yes** before deleting the namespace.

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **set force-configuration** {no | yes}
4. UCS-A /org/persistent-memory-policy* # **delete logical-namespace** *namespace-name*
5. UCS-A /org/persistent-memory-policy* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **set force-configuration** {no | yes}	Configures whether **Force Configurationforce-configuration** has been selected or not. This can be one of the following: • **Nono**—**Force Configuration** is not selected. This is the default value. When **Force Configuration** is not selected, the persistent memory policy is not forcibly applied on associated servers. • **Yesyes**—**Force Configuration** is selected. When this is done, the persistent memory policy is forcibly applied on all the associated servers. This will not have any effect if the existing configuration on the server matches the policy configuration. This will also apply the policy on recommissioned servers. Namespace modification is a destructive operation.To successfully modify a namespace, you must set **Force Configurationforce-configuration** to **Yes**.
Step 4	UCS-A /org/persistent-memory-policy* # **delete logical-namespace** *namespace-name*	Deletes the specified namespace.
Step 5	UCS-A /org/persistent-memory-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to delete a namespace:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy PMemP_2
UCS-A /org/persistent-memory-policy # set force-configuration yes
UCS-A /org/persistent-memory-policy* # delete logical-namespace NSP1
UCS-A /org/persistent-memory-policy* # commit-buffer
UCS-A /org/persistent-memory-policy #
```

Deleting Local Security Configuration

Deleting the security configuration will disable security.

SUMMARY STEPS

1. UCS-A# **scope org**
2. UCS-A /org # **scope persistent-memory-policy** *policy-name*
3. UCS-A /org/persistent-memory-policy # **scope security**
4. UCS-A /org/persistent-memory-policy/security # **delete local-security**
5. UCS-A /org/persistent-memory-policy/security* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org**	Enters the root organization mode
Step 2	UCS-A /org # **scope persistent-memory-policy** *policy-name*	Enters the persistent memory policy mode for the specified policy.
Step 3	UCS-A /org/persistent-memory-policy # **scope security**	Enters the persistent memory security mode.
Step 4	UCS-A /org/persistent-memory-policy/security # **delete local-security**	Deletes the local security policy.
Step 5	UCS-A /org/persistent-memory-policy/security* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to delete a local security policy:

```
UCS-A# scope org
UCS-A /org # scope persistent-memory-policy PMemP_1
UCS-A /org/persistent-memory-policy # scope security
UCS-A /org/persistent-memory-policy/security # delete local-security
UCS-A /org/persistent-memory-policy/security* # commit-buffer
UCS-A /org/persistent-memory-policy/security #
```

Physical Configuration and Inventory for Persistent Memory

You can view the physical inventory and configuration of all the persistent memory modules on a B-Series, C-Series, or S-Series server. The following parameters are detailed:

- DIMMs—Properties of persistent memory modules.

  Persistent memory modules on the same server are locked by using a single secure passphrase. If locked persistent memory modules are brought over from a different server, they need to be unlocked before they can be managed from the new server.

- Configuration—Overall server-level persistent memory configuration.
- Region—Properties of all the regions on the server.

  A region is a grouping of one or more persistent memory modules that can be divided up into one or more namespaces. A region is created based on the persistent memory type selected during goal creation.

  The **App Direct** persistent memory type configures one region for all the memory modules connected to a socket. The **App Direct Non Interleaved** persistent memory type configures one region for each memory module.

- Namespace—Properties of all the logical namespaces available on the server.

  These namespaces are seen by the host OS as block devices or raw devices.

Secure Erase

You can perform secure erase on a specific persistent memory module or all the persistent memory modules on a server. This operation deletes the region data and namespaces.

For the secure erase operation, you must provide a secure passphrase when security is enabled. When security is disabled, a secure passphrase in not required for the secure erase operation.

Viewing the Persistent Memory Modules on a Server

You can view the inventory of all the persistent memory modules on a B-Series, C-Series, or S-Series server.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **show persistent-memory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **show persistent-memory**	Displays the list of all persistent memory modules on the specified server.

Example

This example shows how to view all the persistent memory modules on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # show persistent-memory
DIMM Location   Presence         Overall Status           Type
Capacity (MB) Clock
---- ---------- ---------------- ------------------------ --------------------------
------------- -----
   2 DIMM_A2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
   8 DIMM_D2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
  14 DIMM_G2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
  20 DIMM_K2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
  26 DIMM_N2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
  32 DIMM_R2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
  38 DIMM_U2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
  44 DIMM_X2    Equipped         Operable                 Logical Non Volatile Device 129408
         2666
```

Viewing Persistent Memory Module Properties

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope memory-array** *ID*
3. UCS-A /chassis/server/memory-array # **scope persistent-memory-dimm** *dimm-ID*
4. UCS-A /chassis/server/memory-array/persistent-memory-dimm # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope memory-array** *ID*	Enters memory-array configuration mode for the selected memory array.
Step 3	UCS-A /chassis/server/memory-array # **scope persistent-memory-dimm** *dimm-ID*	Enters persistent-memory-dimm mode within the memory array for the selected persistent memory module.
Step 4	UCS-A /chassis/server/memory-array/persistent-memory-dimm # **show detail**	Displays properties of the selected persistent memory module.

Example

This example shows how to view the properties of a specific persistent memory module on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope memory-array 1
UCS-A /chassis/server/memory-array # scope persistent-memory-dimm 2
UCS-A /chassis/server/memory-array/persistent-memory-dimm # show detail

Persistent Memory Unit:
    ID: 2
    Location: DIMM_A2
    Presence: Equipped
    Operability: Operable
    Visibility: Yes
    Overall Status: Operable
    Admin State: Policy
    Oper Qualifier: N/A
    Product Name: Intel Optane DC Persistent Memory, 128GB, 2666MHz
    PID: UCS-MP-128GS-A0
    VID: V01
    Vendor: 0x8900
    Vendor Description: Intel
    Vendor Part Number: NMA1XBD128GQS
    Vendor Serial (SN): 000003B8
    HW Revision: 0
    Form Factor: DIMM
    Type: Logical Non Volatile Device
    Capacity (MB): 129408
    Clock: 2666
    Latency: 0.400000
    Width: 64
    Threshold Status: N/A
    Power State: N/A
    Thermal Status: OK
    Voltage Status: N/A
    Socket Id: Socket 1
    Socket Local Dimm Number: Socket Local Dimm No 2
    Total Capacity (GiB): 126
    Persistent Memory Capacity (GiB): 126
    Memory Capacity (GiB): 0
    App Direct Capacity (GiB): 126
    Reserved Capacity (GiB): 0
    Firmware Version: 1.2.0.5355
    Health State: Healthy
    Security Status: Disabled, UnLocked, Frozen, Count not expired
    Uid: 8089-A2-1847-000003B8
    Selected: No
```

Performing Secure Erase on a Persistent Memory Module

For the secure erase operation, you must provide a secure passphrase when security is enabled. When security is disabled, a secure passphrase in not required for the secure erase operation. Press the **Enter** key (empty passphrase) at the **Enter Secure Passphrase** prompt.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope memory-array** *ID*
3. UCS-A /chassis/server/memory-array # **scope persistent-memory-dimm** *dimm-ID*
4. UCS-A /chassis/server/memory-array/persistent-memory-dimm # **set selected** {yes | no}
5. UCS-A /chassis/server/memory-array/persistent-memory-dimm* # **exit**
6. UCS-A /chassis/server/memory-array* # **secure-erase persistent-memory-dimms**
7. UCS-A /chassis/server/memory-array* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope memory-array** *ID*	Enters memory-array configuration mode for the selected memory array.
Step 3	UCS-A /chassis/server/memory-array # **scope persistent-memory-dimm** *dimm-ID*	Enters persistent-memory-dimm mode within the memory array.
Step 4	UCS-A /chassis/server/memory-array/persistent-memory-dimm # **set selected** {yes | no}	Configures whether the persistent memory module is selected or not.
Step 5	UCS-A /chassis/server/memory-array/persistent-memory-dimm* # **exit**	Exits to the memory-array configuration mode.
Step 6	UCS-A /chassis/server/memory-array* # **secure-erase persistent-memory-dimms**	Performs secure erase on the selected persistent memory modules. If security is enabled, enter the secure passphrase in the prompt. If security is not enabled, press the **Enter** key (empty passphrase) at the prompt. Securely erasing persistent memory modules is a destructive operation, and will result in deletion of region data and namespaces.
Step 7	UCS-A /chassis/server/memory-array* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to perform secure erase on a persistent memory module on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope memory-array 1
UCS-A /chassis/server/memory-array # scope persistent-memory-dimm 2
UCS-A /chassis/server/memory-array/persistent-memory-dimm # set selected yes
UCS-A /chassis/server/memory-array/persistent-memory-dimm* # exit
UCS-A /chassis/server/memory-array* # secure-erase persistent-memory-dimms
Enter Secure Passphrase:************
UCS-A /chassis/server/memory-array* # commit-buffer
```

```
UCS-A /chassis/server/memory-array #
```

Unlocking Foreign Persistent Memory Modules

Before you begin

Before you use the following procedure to select the persistent memory modules to be unlocked, and perform the unlock foreign DIMMs operation, ensure that you do the following:

1. Decommission the server.
2. Change the persistent memory modules.
3. Recommission the server.
4. Associate the server to a service-profile without a persistent memory policy.
5. Ensure that the server is in the powered-on state, and BIOS POST is completed.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope memory-array** *ID*
3. UCS-A /chassis/server/memory-array # **scope persistent-memory-dimm** *foreign-dimm-ID*
4. UCS-A /chassis/server/memory-array/persistent-memory-dimm # **set selected** {yes | no}
5. UCS-A /chassis/server/memory-array/persistent-memory-dimm* # **exit**
6. UCS-A /chassis/server/memory-array* # **unlock foreign persistent-memory-dimms**
7. UCS-A /chassis/server/memory-array* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope memory-array** *ID*	Enters memory-array configuration mode for the selected memory array.
Step 3	UCS-A /chassis/server/memory-array # **scope persistent-memory-dimm** *foreign-dimm-ID*	Enters persistent-memory-dimm mode for the selected foreign persistent memory module within the memory array.
Step 4	UCS-A /chassis/server/memory-array/persistent-memory-dimm # **set selected** {yes | no}	Configures whether the specified foreign persistent memory module is selected or not.
Step 5	UCS-A /chassis/server/memory-array/persistent-memory-dimm* # **exit**	Exits to the memory-array configuration mode.
Step 6	UCS-A /chassis/server/memory-array* # **unlock foreign persistent-memory-dimms**	Unlocks the selected foreign persistent memory modules. Enter the secure passphrase in the prompt.

	Command or Action	Purpose
		You must provide the same passphrase that is already deployed on the foreign persistent memory module taken from a different server.
Step 7	UCS-A /chassis/server/memory-array* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to unlock a foreign persistent memory module on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope memory-array 1
UCS-A /chassis/server/memory-array # scope persistent-memory-dimm 4
UCS-A /chassis/server/memory-array/persistent-memory-dimm # set selected yes
UCS-A /chassis/server/memory-array/persistent-memory-dimm* # exit
UCS-A /chassis/server/memory-array* # unlock foreign persistent-memory-dimms
Enter Secure Passphrase:************
UCS-A /chassis/server/memory-array* # commit-buffer
UCS-A /chassis/server/memory-array #
```

What to do next

1. Check whether the persistent memory modules get unlocked after the ExecuteActions FSM completes. Now, the persistent memory modules are ready to be used.
2. Attach a persistent memory policy.
3. Check whether the associate FSM completes.

Cancelling the ExecuteActions FSM for Secure Erase and Unlock Foreign DIMM Operations

If the Secure Erase or Unlock Foreign DIMM operation fails, you can cancel the ExecuteActions FSM to proceed with other operations. For example, if you try to unlock a foreign persistent memory module with an incorrect secure passphrase, the FSM will fail. You can use the following commands to cancel the ExecuteActions FSM.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **cancel execute-actions-fsm**
4. UCS-A /chassis/server/persistent-memory-config* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters persistent-memory configuration mode for the server.
Step 3	UCS-A /chassis/server/persistent-memory-config # **cancel execute-actions-fsm**	Cancels the ExecuteActions FSM.
Step 4	UCS-A /chassis/server/persistent-memory-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to cancel the ExecuteActions FSM after performing secure erase or unlock foreign DIMM operations:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
UCS-A /chassis/server/persistent-memory-config # cancel execute-actions-fsm
UCS-A /chassis/server/persistent-memory-config* # commit-buffer
```

Viewing the Persistent Memory Configuration of a Server

You can view the configuration of persistent memory modules on a B-Series, C-Series, or S-Series server.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters persistent-memory configuration mode for the server.
Step 3	UCS-A /chassis/server/persistent-memory-config # **show detail**	Displays the overall configuration of all persistent memory modules on the specified server.

Example

This example shows how to view all the persistent memory modules on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
```

```
UCS-A /chassis/server/persistent-memory-config # show detail

Persistent Memory Configuration:
    Total Capacity (GiB): 1011
    Persistent Memory Capacity (GiB): 1008
    Memory Capacity (GiB): 0
    Reserved Capacity (GiB): 0
    Number Of Regions: 4
    Number Of Dimms: 8
    Security State: Disabled-Frozen
```

Performing Secure Erase on All Persistent Memory Modules on a Server

For the secure erase operation, you must provide a secure passphrase when security is enabled. When security is disabled, a secure passphrase in not required for the secure erase operation. Press the **Enter** key (empty passphrase) at the **Enter Secure Passphrase** prompt.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **secure-erase persistent memory configuration**
4. UCS-A /chassis/server/persistent-memory-config* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters persistent-memory configuration mode for the server.
Step 3	UCS-A /chassis/server/persistent-memory-config # **secure-erase persistent memory configuration**	Securely erases all the persistent memory module configuration on the server. If security is enabled, enter the secure passphrase in the prompt. If security is not enabled, press the **Enter** key (empty passphrase) at the prompt. Securely erasing persistent memory modules is a destructive operation, and will result in deletion of all the region data and namespaces on the server.
Step 4	UCS-A /chassis/server/persistent-memory-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to securely erase all persistent memory module configuration on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
UCS-A /chassis/server/persistent-memory-config # secure-erase persistent memory configuration

Enter Secure Passphrase:************
UCS-A /chassis/server/persistent-memory-config* # commit-buffer
UCS-A /chassis/server/persistent-memory-config #
```

Viewing the Regions on a Server

You can view the inventory of the regions on a B-Series, C-Series, or S-Series server.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **show region**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters the persistent memory configuration mode.
Step 3	UCS-A /chassis/server/persistent-memory-config # **show region**	Displays details of all regions across persistent memory modules on the specified server.

Example

This example shows how to view all the regions on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
UCS-A /chassis/server/persistent-memory-config # show region

Pmemory Region:
    Id         Socket Id Socket Local Dimm Number Interleaved Set Id
    ---------- --------- ----------------------- ------------------
             1 Socket 1  Not Applicable           5d54eeb8b2392444
             2 Socket 2  Not Applicable           d380eeb8af3b2444
             3 Socket 3  Not Applicable           9bb4eeb8573f2444
             4 Socket 4  Not Applicable           8d78eeb8e6392444
```

Note For UCS M6 B-Series and C-Series servers, only **socket-1**and **socket-2** are supported.

Viewing Region Properties

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **scope region** *region-ID*
4. UCS-A /chassis/server/persistent-memory-config/region #**show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters the persistent memory configuration mode.
Step 3	UCS-A /chassis/server/persistent-memory-config # **scope region** *region-ID*	Enters the configuration mode for the selected region.
Step 4	UCS-A /chassis/server/persistent-memory-config/region #**show detail**	Displays properties of the selected region.

Example

This example shows how to view the properties of a specific region on a server:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
UCS-A /chassis/server/persistent-memory-config # scope region 2
UCS-A /chassis/server/persistent-memory-config/region # show detail

Persistent Memory Region:
    Id: 2
    Socket Id: Socket 2
    Socket Local Dimm Number: Not Applicable
    Interleaved Set Id: 1796eeb8553c2444
    Persistent Memory Type: AppDirect
    Dimm Locater Ids: DIMM_G2,DIMM_K2
    Health State: Healthy
    Total Capacity (GiB): 252
    Free Capacity (GiB): 252
```

Viewing Namespaces in a Region

You can view the inventory of the namespaces on a B-Series, C-Series, or S-Series server.

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **scope region** *region-id*
4. UCS-A /chassis/server/persistent-memory-config/region # **show namespace** [detail]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters the persistent memory configuration mode.
Step 3	UCS-A /chassis/server/persistent-memory-config # **scope region** *region-id*	Enters the region configuration mode.
Step 4	UCS-A /chassis/server/persistent-memory-config/region # **show namespace** [detail]	Displays details of all namespaces in the specified region.

Example

This example shows how to view all the namespaces in a region:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
UCS-A /chassis/server/persistent-memory-config # scope region 1
UCS-A /chassis/server/persistent-memory-config/region # show namespace detail

Pmemory Namespace:
    Name: NS1
    Capacity (GiB): 100
    Uuid: 7286246-48cf-4750-b066-647f6684ac28
    Oper Mode: Raw
    Health State: Healthy
    Label Version: 1.2

    Name: NS2
    Capacity (GiB): 10
    Uuid: 7312f895-7f70-4646-b08d-8d5ef5b98577
    Oper Mode: Raw
    Health State: Healthy
    Label Version: 1.2
```

Viewing Namespace Properties

SUMMARY STEPS

1. UCS-A# **scope server** *chassis-num* / *server-num*
2. UCS-A /chassis/server # **scope persistent-memory-config**
3. UCS-A /chassis/server/persistent-memory-config # **scope region** *region-ID*
4. UCS-A /chassis/server/persistent-memory-config/region # scope namespace *namespace-Uuid*
5. UCS-A /chassis/server/persistent-memory-config/region/namespace #**show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-num* / *server-num*	Enters server mode for the specified chassis and server.
Step 2	UCS-A /chassis/server # **scope persistent-memory-config**	Enters the persistent memory configuration mode.
Step 3	UCS-A /chassis/server/persistent-memory-config # **scope region** *region-ID*	Enters the configuration mode for the selected region.
Step 4	UCS-A /chassis/server/persistent-memory-config/region # scope namespace *namespace-Uuid*	Enters the configuration mode for the selected namespace.
Step 5	UCS-A /chassis/server/persistent-memory-config/region/namespace #**show detail**	Displays properties of the selected namespace.

Example

This example shows how to view the properties of a specific namespace in a specific region:

```
UCS-A# scope server 1/5
UCS-A /chassis/server # scope persistent-memory-config
UCS-A /chassis/server/persistent-memory-config # scope region 2
UCS-A /chassis/server/persistent-memory-config/region # scope namespace
e09a549d-3ed7-44cb-b086-c54321c12345
UCS-A /chassis/server/persistent-memory-config/region/namespace # show detail

Persistent Memory Namespace:
    Name: NS1
    Uuid: e09a549d-3ed7-44cb-b086-c54321c12345
    Capacity (GiB) (MB): 30
    Mode: Raw
    Health State: Healthy
    Label Version: 1.2
```

Performing Persistent Memory Scrub

In Cisco UCS Manager, you can scrub persistent memory by using one of the following methods:

- Disassociating the Service Profile and the Scrub Policy with Persistent Memory Scrub Selected
- Resetting a Server to Factory Defaults With Persistent Memory Scrub Selected
- Deleting a Goal

Disassociating the Service Profile and the Scrub Policy with Persistent Memory Scrub Selected

Disassociating the service profile and the scrub policy, which has the persistent memory scrub option selected will result in deletion of all regions and namespaces and its data in all the persistent memory modules. Security will be disabled, if it is already enabled. The following procedure describes how to disassociate a service profile and a scrub policy.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **scope service-profile** *service-profile-name*
3. UCS-A /org/service-profile # **set scrub-policy scrub-policy-name**
4. UCS-A /org/service-profile* # **commit-buffer**
5. UCS-A /org/service-profile # **disassociate**
6. UCS-A /org/service-profile* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name .
Step 2	UCS-A /org # **scope service-profile** *service-profile-name*	Enters organization service profile mode for the specified service profile.
Step 3	UCS-A /org/service-profile # **set scrub-policy scrub-policy-name**	Assigns scrub policy to this service profile. Select a scrub policy with the persistent memory scrub option set to **yes**.
Step 4	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration. Association of the scrub policy to the service profile is completed.
Step 5	UCS-A /org/service-profile # **disassociate**	Disassociates the service profile from the server.
Step 6	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.

On UCS M5, M6 B-Series and C-Series servers: Regions and namespaces will be deleted after successful disassociation.

On UCS M5 S-Series servers: Namespaces will be deleted after successful disassociation.

Example

This example shows how to disassociate the service profile and the scrub policy with persistent memory scrub selected:

```
UCS-A# scope org
UCS-A /org # scope service-profile sample
UCS-A /org/service-profile # set scrub-policy pmemscrub
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile disassociate
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Resetting a Server to Factory Defaults With Persistent Memory Scrub Selected

You can reset a server to its factory settings. By default, the factory reset operation does not affect storage drives, persistent memory modules, and flexflash drives. This is to prevent any loss of data. However, you can choose to reset these devices to a known state as well.

Important Resetting storage devices will result in loss of data.

Perform the following procedure to reset the server to factory default settings, and delete persistent memory configuration and data.

SUMMARY STEPS

1. UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]
2. UCS-A /chassis/server # **reset factory-default** [**delete-persistent-memory** | **delete-flexflash-storage** | **delete-storage** [**create-initial-storage-volumes**]]
3. UCS-A /chassis/server* # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	Enters server mode for the specified server.
Step 2	UCS-A /chassis/server # **reset factory-default** [**delete-persistent-memory** | **delete-flexflash-storage** | **delete-storage** [**create-initial-storage-volumes**]]	Resets server settings to factory default using the following command options:

	Command or Action	Purpose
		• **factory-default**—Resets the server to factory defaults without deleting storage • **delete-persistent-memory**—Resets the server to factory defaults and deletes persistent memory configuration and data • **delete-flexflash-storage**—Resets the server to factory defaults and deletes flexflash storage • **delete-storage**—Resets the server to factory defaults and deletes all storage • **create-initial-storage-volumes**—Resets the server to factory defaults, deletes all storage, sets all disks to their initial state **Important** Do not use the **create-initial-storage-volumes** command option if you want to use storage profiles. Creating initial volumes when you are using storage profiles may result in configuration errors.
Step 3	UCS-A /chassis/server* # **commit-buffer**	Commits any pending transactions.

Example

The following example resets the server settings to factory default, deletes persistent memory configuration and data, and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # reset factory-default delete-persistent-memory

UCS-A /chassis/server* # commit-buffer
```