# Server Boot

This chapter includes the following sections:

## Boot Policy

Boot policy overrides the boot order in the BIOS setup menu, and determines the following:

- Selection of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (vMedia), or you can select a SAN boot or a LAN (PXE) boot.

You can either create a named boot policy that can be associated with one or more service profiles, or create a boot policy for a specific service profile. A boot policy must be included in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the UCS domain applies the default boot policy.

**Note** Changes to a boot policy will be propagated to all service profiles created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is automatically triggered.

# Boot Order

Cisco UCS Central enables you to use standard or enhanced boot order for the global boot policies you create in Cisco UCS Central.

- Standard boot order is supported for all Cisco UCS servers, and allows a limited selection of boot order choices. You can add a local device, such as a local disk, CD-ROM, or floppy, or you can add SAN, LAN, or iSCSI boot.
- Enhanced boot order allows you greater control over the boot devices that you select for your boot policy. Enhanced boot order is supported for all Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers at release 2.2(1b) or greater.

The following boot order devices are supported for standard boot order, but can be used with both:

- **Local LUN/Local Disk**—Enables standard boot from a local hard disk. Do not enter a primary or secondary LUN name. Those are reserved for enhanced boot order only.
- **CD/DVD ROM Boot**—Enables standard boot from local CD/DVD ROM drive.
- **Floppy**—Enables standard boot from local floppy drive.
- **LAN Boot**—Enables standard boot from a specified vNIC.
- **SAN Boot**—Enables standard boot from a specified vHBA.
- **iSCSI Boot**—Enables standard boot from a specified iSCSI vNIC.

The following boot order devices are supported only for enhanced boot order:

- **Local LUN/Local Disk**—Enables boot from local hard disk, or local LUN.
- **Local CD/DVD**—Enables boot from local CD/DVD drive.
- **Local Floppy**—Enables boot from local floppy drive.
- **SD Card**—Enables boot from SD Card.
- **Internal USB**—Enables boot from Internal USB.
- **External USB**—Enables boot from External USB.
- **Embedded Local Disk**—Enables booting from the embedded local disk on the Cisco UCS C240 M4SX and C240 M4L servers.

  **Note** You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.

- **Embedded Local LUN**—Enables boot from the embedded local LUN on the Cisco UCS C240 M4SX and C240 M4L servers.

Note: You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.

- **Local JBOD**—Enables boot from a local disk.
- **KVM Mapped CD/DVD**—Enables boot from KVM mapped ISO images.
- **KVM Mapped Floppy**—Enables boot from KVM mapped image files.
- **CIMC Mapped HDD**—Enables boot from CIMC mapped vMedia drives.
- **CIMC MAPPED CD/DVD**—Enables boot from CIMC mapped vMedia CDs and DVDs.
- **LAN Boot**—Enables you to select a specific vNIC from which to boot.
- **SAN Boot**—Enables you to select a specific vHBA from which to boot.
- **iSCSI Boot**—Enables you to select a specific iSCSI vNIC from which to boot.
- **Remote Virtual Drive**—Enables boot from a remote virtual drive.

Note

- If a boot policy with enhanced boot order is applied to Cisco UCS M1 and M2 blade and rack servers, or to Cisco UCS M3 blade and rack servers with a release prior to Release 2.2(1b) installed, the association fails with configuration errors.
- You must enable USB for Virtual Media. If you modify the BIOS settings, that in turn affects the Virtual media. The following USB BIOS default settings are recommended for best performance:
  - **Make Device Non Bootable**—set to disabled
  - **USB Idle Power Optimizing Setting**—set to high-performance

# UEFI Boot Mode

Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. Cisco UCS uses UEFI to replace the BIOS firmware interfaces. This allows the BIOS to run in UEFI mode while still providing legacy support.

You can choose either legacy or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers, and allows you to enable UEFI secure boot mode.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is not supported on Cisco UCS B-Series M1 and M2 Blade Servers and Cisco UCS C-Series M1 and M2 Rack Servers.
- UEFI boot mode is not supported with the following combinations:

  - Gen-3 Emulex & QLogic adapters on Cisco UCS blade & rack servers integrated with Cisco UCS domain.
  - PXE boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS domain.
  - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS domain.

- You cannot mix UEFI and legacy boot mode on the same server.
- Make sure an UEFI-aware operating system is installed in the device. The server will boot correctly in UEFI mode only if the boot devices configured in the boot policy have UEFI-aware OS installed. If a compatible OS is not present, the boot device is not displayed on the **Boot Policies** page.
- In some corner cases, the UEFI boot may not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation could occur in the following situations:
  - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is manually powered on using the **Server** page or the front panel.
  - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.
  - If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

# UEFI Secure Boot

Cisco UCS Central supports UEFI secure boot on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and Rack Servers. When UEFI secure boot is enabled, all executables, such as boot loaders and adapter drivers, are authenticated by the BIOS before they can be loaded. To be authenticated, the images must be signed by either the Cisco Certificate Authority (CA) or a Microsoft CA.

The following limitations apply to UEFI secure boot:

- UEFI boot mode must be enabled in the boot policy.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.
- User-generated encryption keys are not supported.
- UEFI secure boot can only be controlled by Cisco UCS Manager or Cisco UCS Central.
- If you want to downgrade to an earlier version of Cisco UCS Manager, and you have a blade server in secure boot mode, you must disassociate and reassociate the blade server before downgrading. Otherwise, the blade will not be discovered successfully.

# Cautions and Guidelines for Downgrading a Boot Policy

You cannot downgrade to an earlier version of Cisco UCS Manager if:

- An associated server has a boot policy with UEFI boot mode enabled.

- An associated server has a boot policy with UEFI secure boot enabled.
- An associated server has a boot policy with enhanced boot order. For example, if an associated server has a boot policy which contains any of the following:
    - SD card
    - Internal USB
    - External USB
- An associated server has a boot policy that includes both SAN and local LUN.

# Creating or Editing a Boot Policy

### Procedure

**Step 1** In the **Actions** bar, type **Create Boot Policy** and press Enter.

**Step 2** Choose the organization from the drop-down list, and then enter a unique name and optional description for the policy.

**Step 3** Required: Click **Enabled** for **Reboot on Boot Order Change** to reboot all servers that use this boot policy after you make changes to the boot order.

For boot policies applied to a server with a non-Cisco VIC adapter, even if Reboot on Boot Order Change is disabled, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.

**Step 4** Required: Click **Enabled** for **Enforce Interface Name** to receive a configuration error if any of the vNICs, vHBAs or iSCSI vNICs in the Boot Order section match the server configuration in the service profile.

**Step 5** In **Boot Mode**, click **Legacy** or **Unified Extensible Firmware Interface (UEFI)**.

**Step 6** If you selected **Unified Extensible Firmware Interface (UEFI)**, choose if you want to enable UEFI secure boot.

**Step 7** Click **Boot Order** and perform the following:

a) Click the **Add** button to add boot options.

For information on each option, see Boot Order, on page 2.

b) Update the required properties for the boot option.

c) Use the up and down arrows to arrange the boot order.

**Note** If you create a boot policy for iSCSI boot in the HTML5 GUI, you can only update that boot policy in the HTML5 GUI.

**Step 8** Click **Save**.

# Configuring iSCSI Targets

**Note** This dialog box is read-only unless you configured the iSCSI targets directly under the service profile or service profile template using the Cisco UCS Central CLI or the Flash-based GUI.

### Procedure

**Step 1** From the **Service Profile** or **Service Profile Template** page, click the **Tools** icon and choose **Configure iSCSI Targets**.

**Step 2** In the **Configure iSCSI Targets** dialog box, click **Primary** or **Secondary** and enter the iSCSI vNIC.

**Step 3** Select the **iSCSI Target Definition Mode** and complete the necessary fields:

- **Static**—Specify a static target interface for the iSCSI vNIC.
- **Auto**—Allow the system to select an interface automatically using DHCP.
- **Decide Later**—Allows the system to ignore the iSCSI boot until you configure the iSCSI targets. You can also use this to delete a target you no longer want to use.

**Step 4** Click **Save**.