Firmware Management

- Firmware Management, page 1
- Firmware Management for Cisco UCS Domains, page 1
- Recommendations for Firmware Management, page 2
- Firmware Upgrade Process, page 3
- Host Firmware Packages and Maintenance Policies, page 3

Firmware Management

Configuring global firmware management enforces a policy in which all domains within a domain group (v1.4 and below) or maintenance group (v1.5 and above) run a consistent version of the firmware and hardware capability catalog. Enable a global policy resolution when you want to enforce consistent versions of infrastructure firmware among all domains in a domain group or maintenance group.

When a domain group or maintenance group consists of multiple Cisco UCS domains, and you have switched to a global firmware management control policy, be careful of any operational (global) firmware policy changes to that group. Cisco UCS Central tries to upgrade all domains that are members of that domain group or maintenance group, along with any subdomain groups, as defined in the maintenance policy. The default maintenance policy behavior requires user acknowledgment before any updates occur. You can override this behavior by scheduling an acknowledgment or performing an immediate acknowledgment.

Firmware Management for Cisco UCS Domains

Upgrading Cisco UCS domains used to be a manual process, unless you used a Cisco UCS Firmware Upgrade script.

The current release of Cisco UCS Manager includes a firmware automatic-install feature to help automate tasks that were previously manual. Cisco UCS Central builds upon this new feature to help in automating firmware upgrades across multiple Cisco UCS domains.

There are several types of firmware:

- **Infrastructure firmware (A package)**: Refers to the images that run in the I/O modules, the fabric interconnects, and Cisco UCS Manager.

- **Server Blade firmware (B Package)**: Refers to the images that run on a physical Cisco UCS blade server BIOS, CIMC, adaptors, and controllers.

Note Currently, Cisco UCS Central does not support direct endpoint upgrades of blades servers. Use a Host Firmware policy and global service profile association to upgrade the blade or server firmware.

- **Rack-Mounted Server firmware (C Package)**: Refers to the images that run on a physical Cisco UCS-managed rack-mounted server BIOS, CIMC, adaptors, and controllers.
- **Cisco UCS Mini firmware (E Package)**: Refers to the images that run on a physical blade server BIOS, CIMC, adaptors, and controllers that are a part of Cisco UCS Mini.

The best practice for server firmware is to leverage host firmware packages as part of the service profile definition, to guarantee configuration consistency at the application level.

Recommendations for Firmware Management

There are no implicit maintenance policies for server firmware updates. Therefore, a best practice is to explicitly define a maintenance policy that governs server firmware bundle updates.

Infrastructure firmware updates are disruptive to the server. Therefore, when you create your global service profiles, always enable the user-acknowledgment settings. Using user-acknowledgments in your maintenance policy prevents untimely service disruptions.

You must understand the following firmware management issues.

Service Degradation and Disruption

Any Cisco UCS infrastructure firmware update causes service degradation, because each fabric interconnect must sequentially go through a reboot cycle. To avoid service disruption, ensure that appropriate application-level availability schemes are in place, such as Cisco UCS fabric failover, high-availability (HA), NIC bonding, and host-based storage multipathing.

Pending Acknowledgment

Rebooting fabric interconnects requires explicit acknowledgment from the Cisco UCS Central administrator. For domain/maintenance groups of more than one UCS domain, you can switch the Policy Resolution Control to local for each domain you do not wish to upgrade. This prevents simultaneous requests to upgrade UCS domains. Thereafter, changing the Policy Resolution Control to global would cause the upgrade process to proceed.

The default behavior is that you must acknowledge all firmware upgrades (infra-fw) and reboots (fi-reboot) before they proceed. View progress in Cisco UCS Central in the infrastructure firmware upgrade page.

For an individual Cisco UCS domain within Cisco UCS Manager, follow **Operations** > **Firmware** > **FW Operations**.

Firmware Upgrade Process

The upgrade process requires several acknowledgments.

In Cisco UCS Central, multiple upgrades can proceed in parallel. If you are connected to Cisco UCS Manager, those connections to Cisco UCS Manager are reset during an upgrade. As with standalone Cisco UCS Manager upgrades, the infrastructure firmware upgrade takes roughly one hour to complete, but can run in parallel across multiple domains. Blade server upgrades can take longer, depending on the scope of servers involved and whether virtual workloads require migration (vMotion/Life Migration) prior to upgrading the host.

Firmware management can complement host firmware policies. When loading a new Cisco UCS domain for the first time, use both infrastructure and host firmware automatic installation processes. Ensure that a new domain is current with all low-level host firmware, before releasing it to production.

Host Firmware Packages and Maintenance Policies

Host firmware packages and maintenance policies are both visible and configurable from domain groups and organizations.

The expected behavior for Cisco UCS Central is:

- Global service profiles refer to the host firmware policy that is defined under organization and not the domain group.
- After you acknowledge the maintenance policy, Cisco UCS Central pulls the host firmware package, maintenance policy, and any other referenced policies, from Cisco UCS Manager to Cisco UCS Central.
- A local service profile can either reference a local host firmware policy and a local maintenance policy, a global host firmware policy, or global maintenance policy.

The best practice is to configure and use host firmware packages, maintenance policies, and schedules exclusively from the organization.