
cisco Live!
Let's go

The bridge to possible

Intersight Managed Mode (IMM) for UCS Manager admins

A technical overview of IMM

Vincent Esposito, Technical Solutions Architect
@vesposit

Session objectives

- Get familiar with Intersight Managed Mode
- Understand what are its main differences & benefits from UCS Manager/Central
- Know how to perform common configuration & deployment tasks of both fabric and server components
- Discuss when and how to transition from UCS Manager/Central to IMM

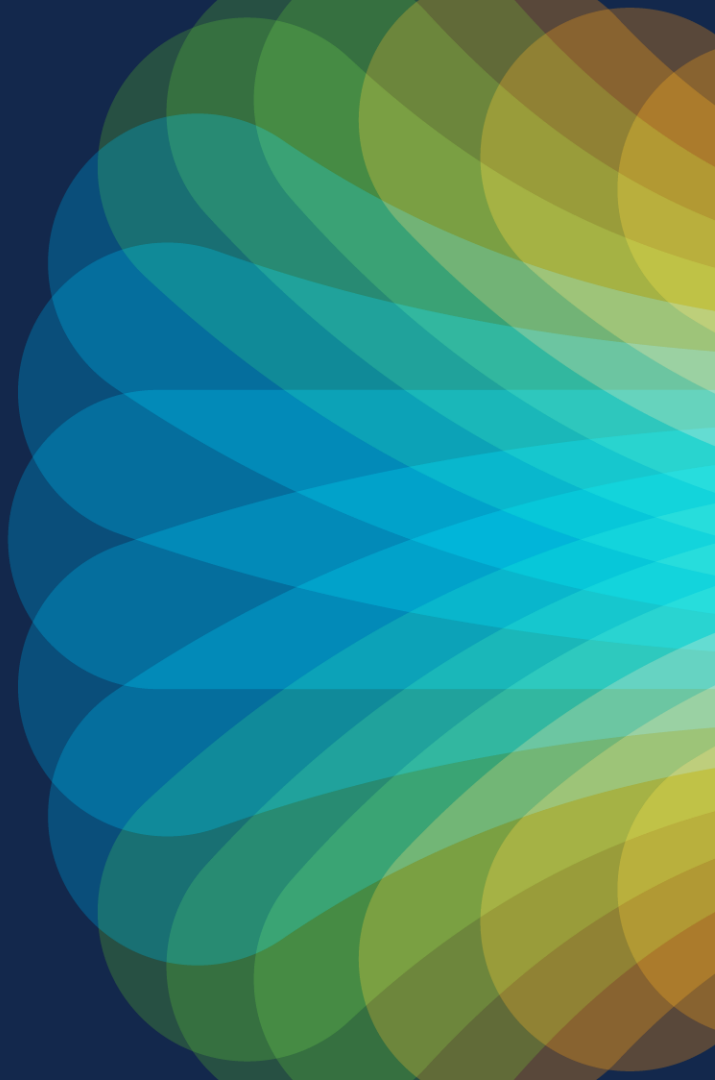
Session non-objectives

- This session **does not include**:
  - A technical overview of the UCS architecture and its components
  - A detailed presentation of Intersight
  - An in-depth comparison of each individual policy between UCSM & IMM
  - An exhaustive list of all possible operations in IMM
  - An explanation of the Intersight licensing model
  - A step-by-step guide on how to transition a domain to IMM

Agenda

- Introduction
- What is Intersight Managed Mode?
- Why Intersight Managed Mode?
- How to use Intersight Managed Mode?
- Transitioning to Intersight Managed Mode
- Key Takeaways

Introduction



Intersight

IT Operations. Simplified.

Visualize

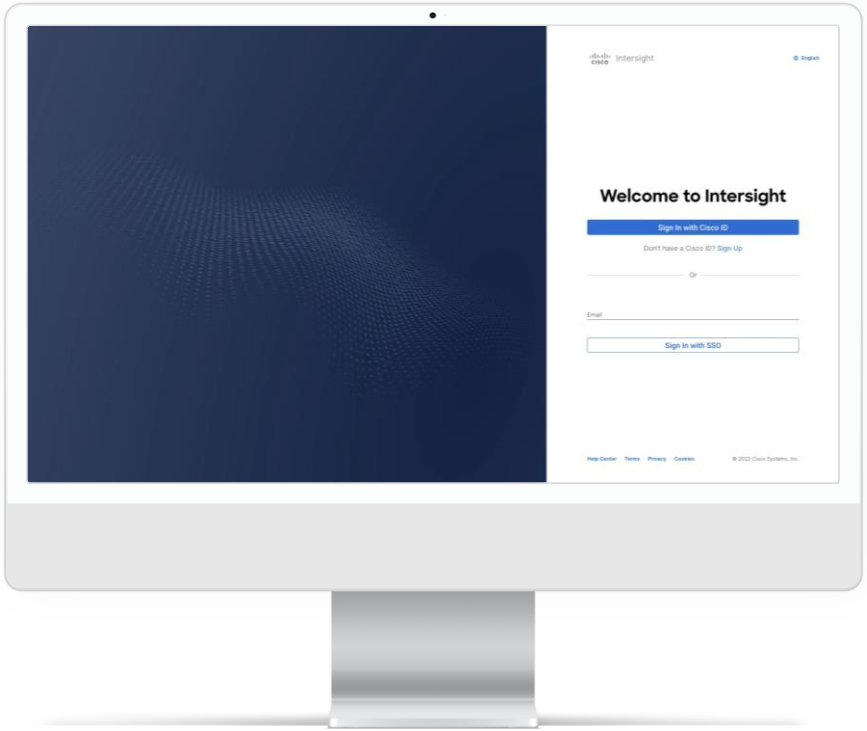
Your global on-premises, cloud, and edge environments

Automate

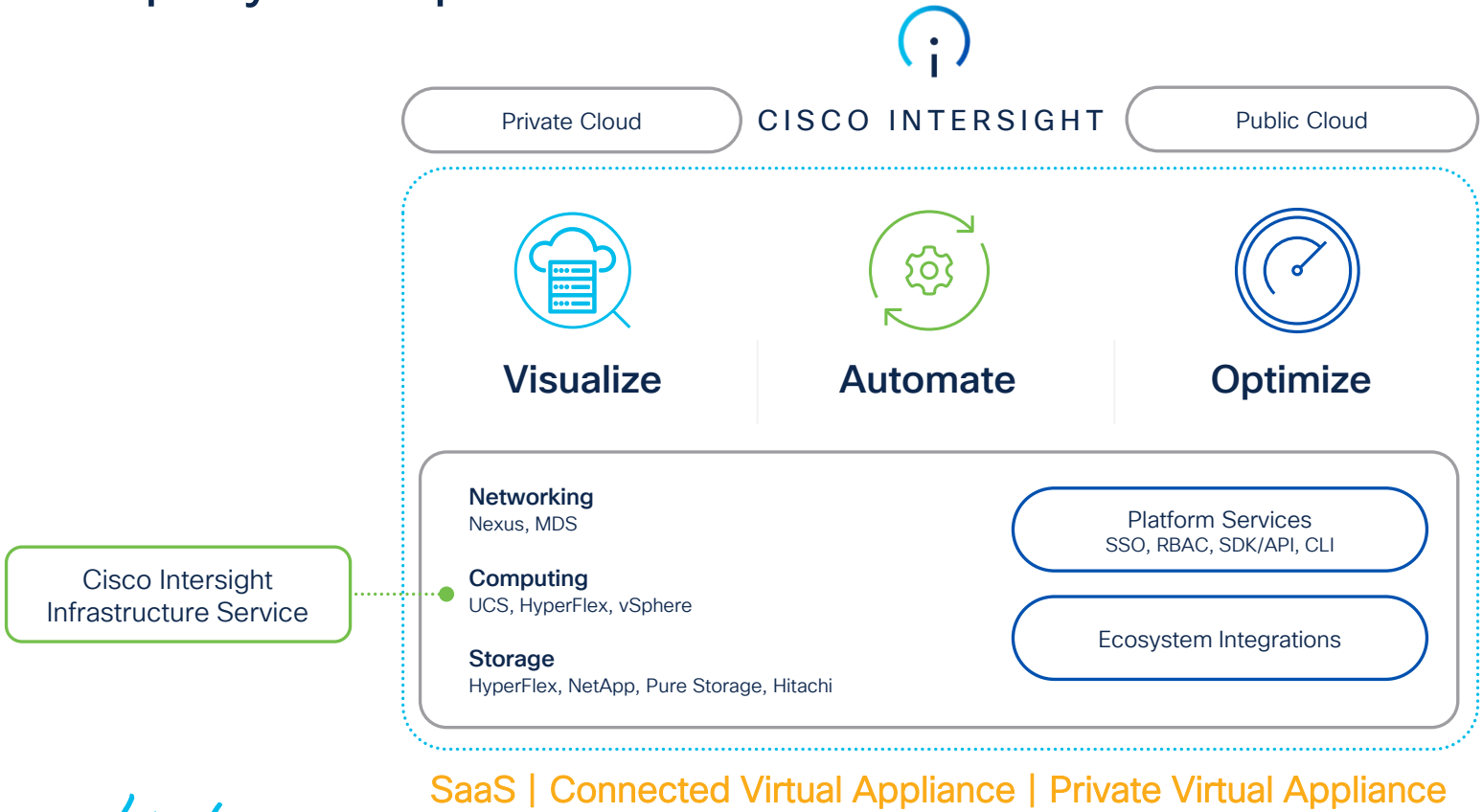
Networking and computing deployments and configuration

Optimize

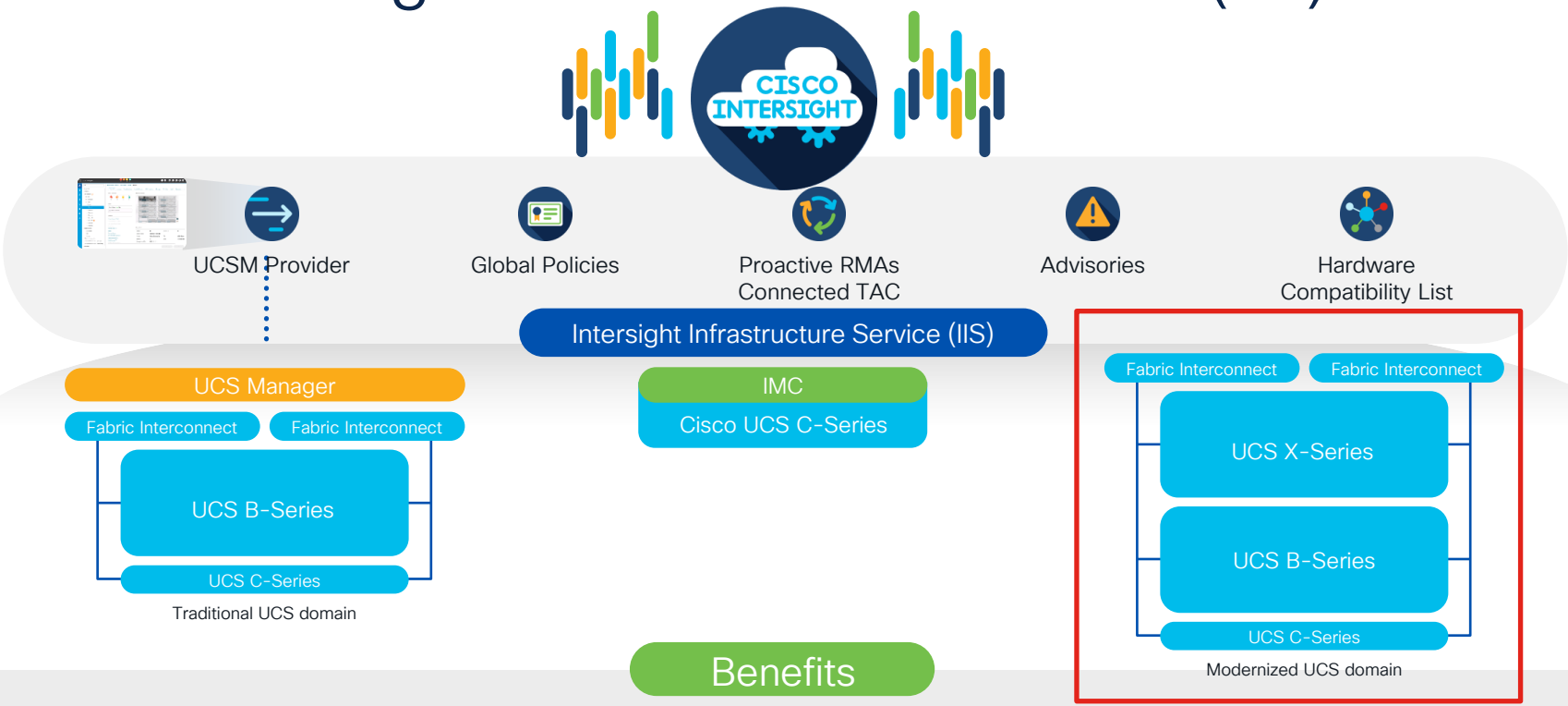
Performance, cost, and user experience



Simplify IT Operations



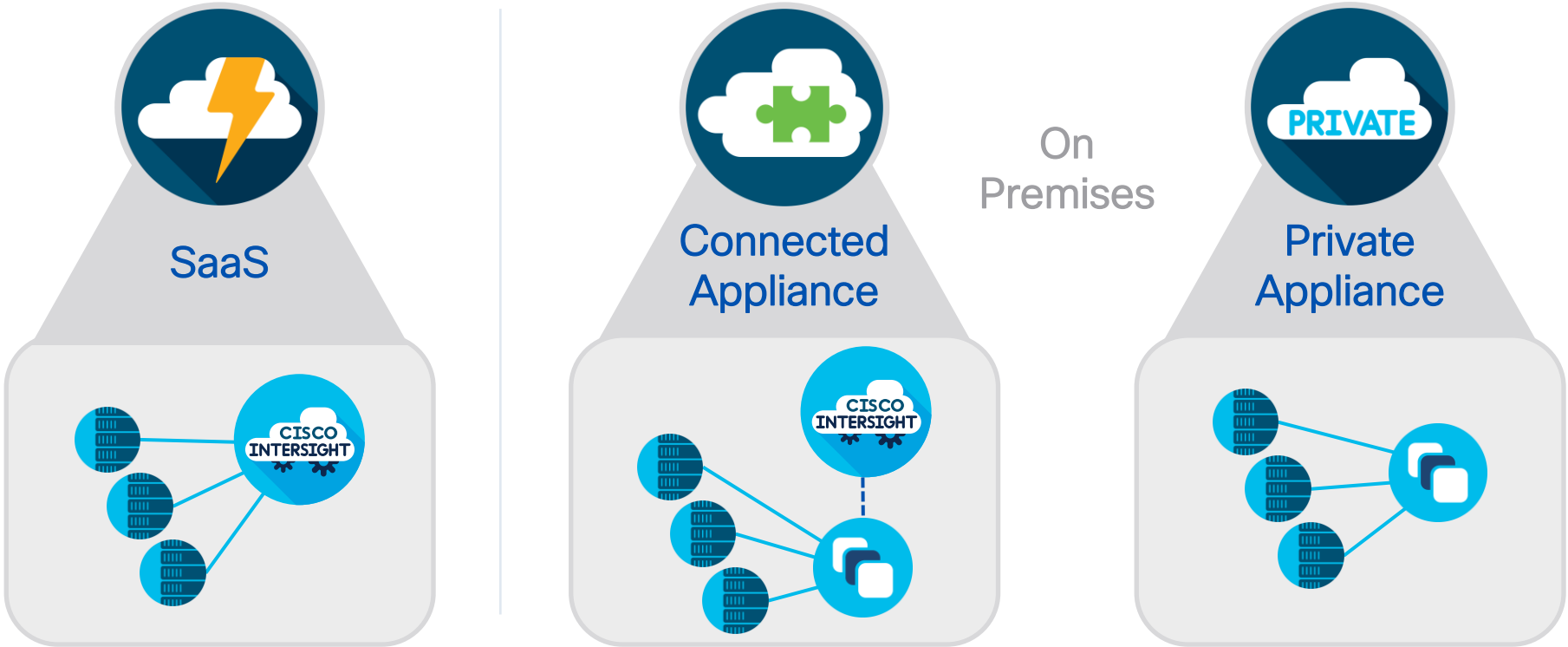
Cisco Intersight Infrastructure Service (IIS)



Benefits

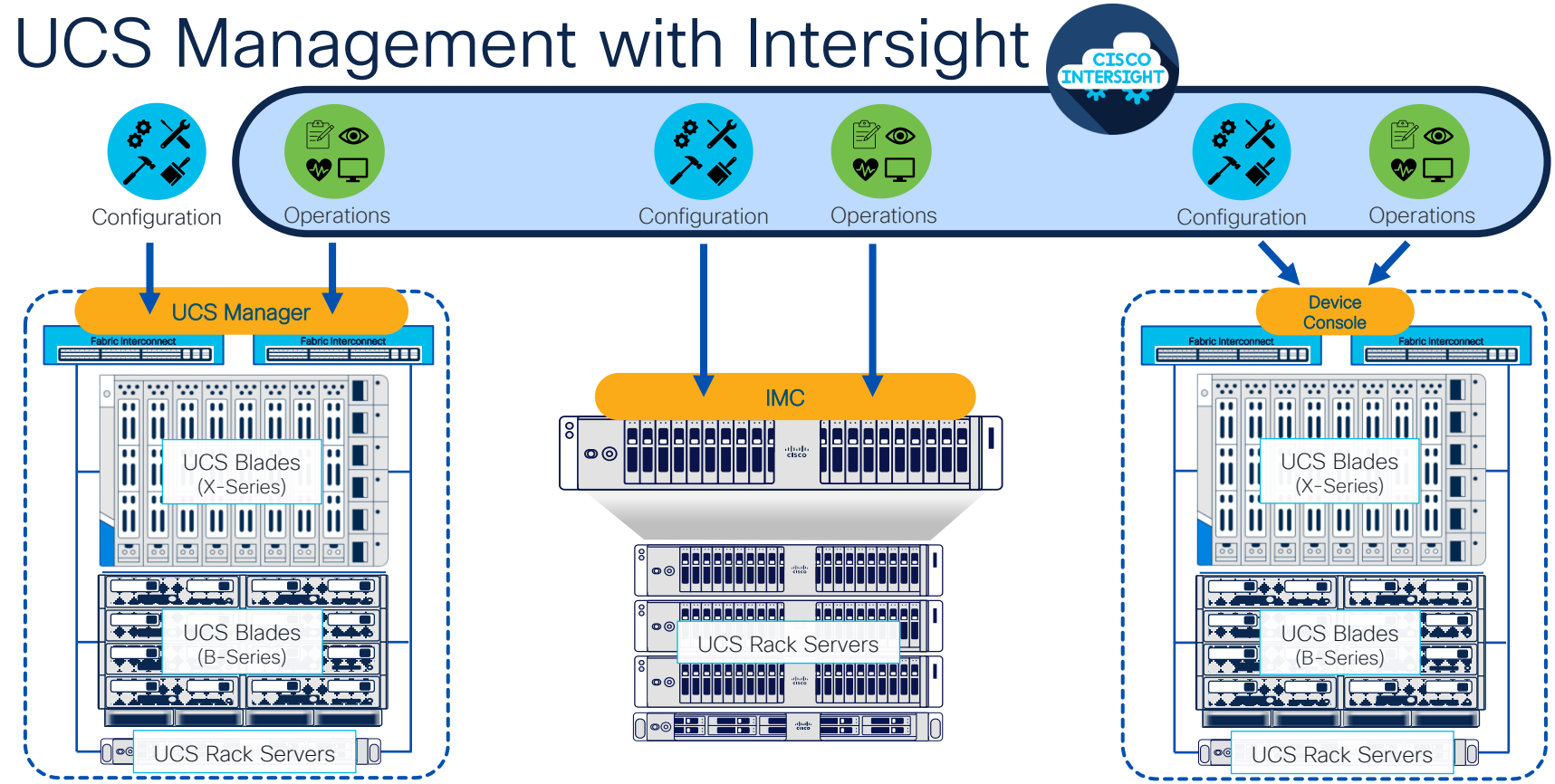
Single Pane of Glass for the entire infrastructure | Common operational model | Proactive services

Intersight Deployment Modes



What is Intersight Managed Mode?

UCS Management with Intersight

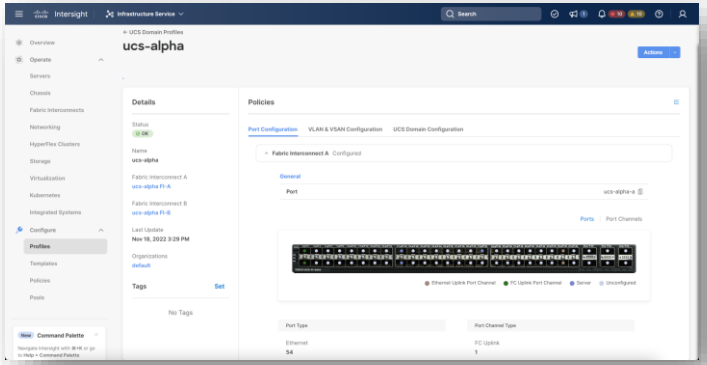


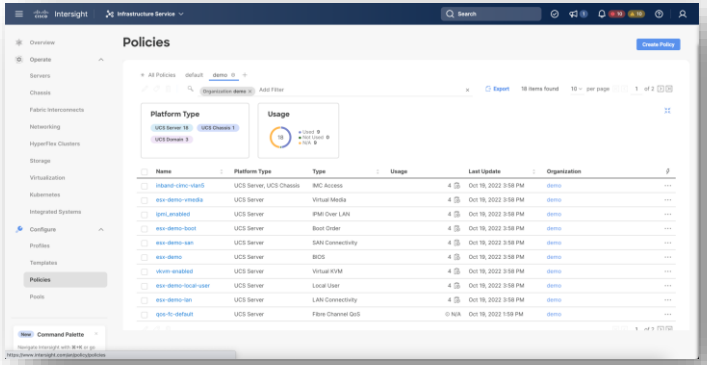
UCSM Managed Mode (UMM)

C-Series Standalone Mode (SARS)

Intersight Managed Mode (IMM)

Intersight Managed Mode (IMM)





UCS policy-based management for servers & fabric in Intersight

Intersight Managed Mode

Hardware & Software Requirements

Hardware

- Fabric Interconnects: 6454/64108/6536 (x2)
- IO Modules: 2204/2208/2304/2408
- IFM: 9108-25G/9108-100G
- Servers: B-, C- & X-Series M5, M6 & M7
- VIC: 1300/1400/15000

Firmware

- Infrastructure (A-bundle): 4.1(3) or higher
- Servers (B/C-bundles): 4.1(3) or higher
- 4.2(3)+ for most comprehensive support

Licensing

Intersight: Essentials or higher (all servers in domain)

Scope

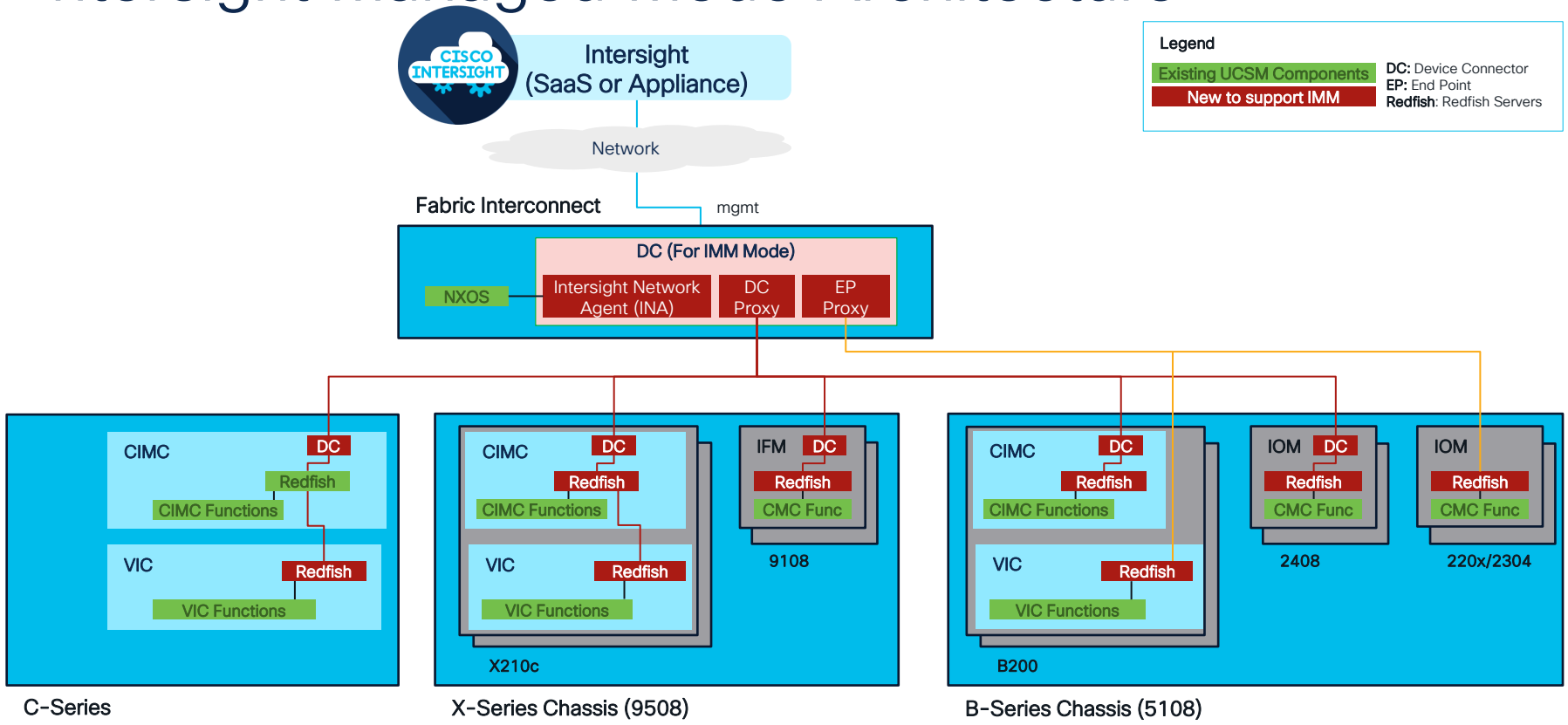
Entire UCS domain will be configured in Intersight Managed Mode (exclusive of UCS Manager)

Scale

20 chassis / 160 servers (same as UCSM)

https://intersight.com/help/saas/supported_systems#supported_hardware_for_intersight_managed_mode

Intersight Managed Mode Architecture



Why Redfish?

- Standard, Scalable, Secure replacement for IPMI
- RESTful API with **JSON-formatted** data
  - Modern replacement for the UCS XML API
- Supports OEM/vendor extensions
  - VIC management
  - Firmware management
  - Custom actions (Reset CMOS, Clear TPM, ...)
- Available on many server platforms
  - Support for third-party servers (C890 M5, Dell, HPE)

GET /redfish/v1/Chassis/{ChassisId}/Thermal


```
{
  "@odata.context": "/redfish/v1/$metadata#Thermal.Thermal",
  "@odata.id": "/redfish/v1/Chassis/FCH22347N7W/Thermal",
  "@odata.type": "#Thermal.v1_6_2.Thermal",
  "Description": "Represents the properties for Temperature",
  "Id": "Thermal",
  "Name": "Thermal",
  "Status": {
    "Health": "OK",
    "State": "Enabled"
  },
  "Temperatures": [
    {
      "@odata.id": "/redfish/v1/Chassis/FCH22347N7W/Thermal#/Temperatures/0",
      "MemberId": "0",
      "Name": "TEMP_SENS_FRONT",
      "PhysicalContext": "Front",
      "ReadingCelsius": 22,
      "Status": {
        "Health": "OK",
        "State": "Enabled"
      },
      "UpperThresholdCritical": 75,
      "UpperThresholdFatal": 85
    },
    {
      "@odata.id": "/redfish/v1/Chassis/FCH22347N7W/Thermal#/Temperatures/1",
      "MemberId": "1",
      "Name": "TEMP_SENS_REAR",
      "PhysicalContext": "Back",
      "ReadingCelsius": 33,
      "Status": {
        "Health": "OK",
        "State": "Enabled"
      },
      "UpperThresholdCritical": 75,
      "UpperThresholdFatal": 85
    },
```

Why Intersight Managed Mode?

Benefits of the IMM model

Modernize

- Feature velocity with CI/CD
- Modern RESTful API with OpenAPI
- **Redfish** standard

Simplify

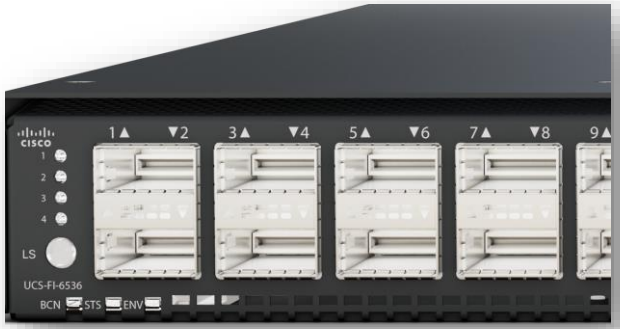
- Common management framework for all Cisco Compute
- Merging of Local & Global Service Profile/Template (Multi domain)
- Policy Model simplification

Safer operations

- Configuration consistency for domains
- Decoupling of firmware / software features
- Improved Change Control with Assign/Deploy steps
- Better policy scale – not limited by FI resources

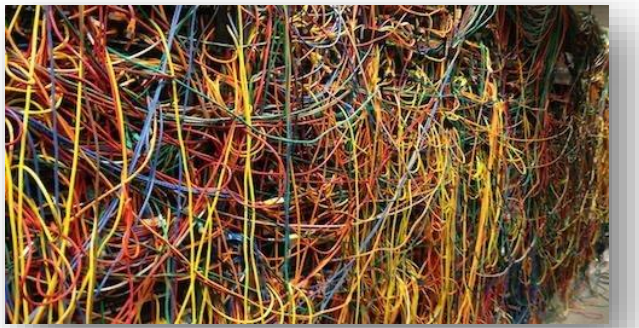
When should you start using IMM?

Hardware refresh



New domain deployment / Greenfield

X-Series adoption



Lab / Tests

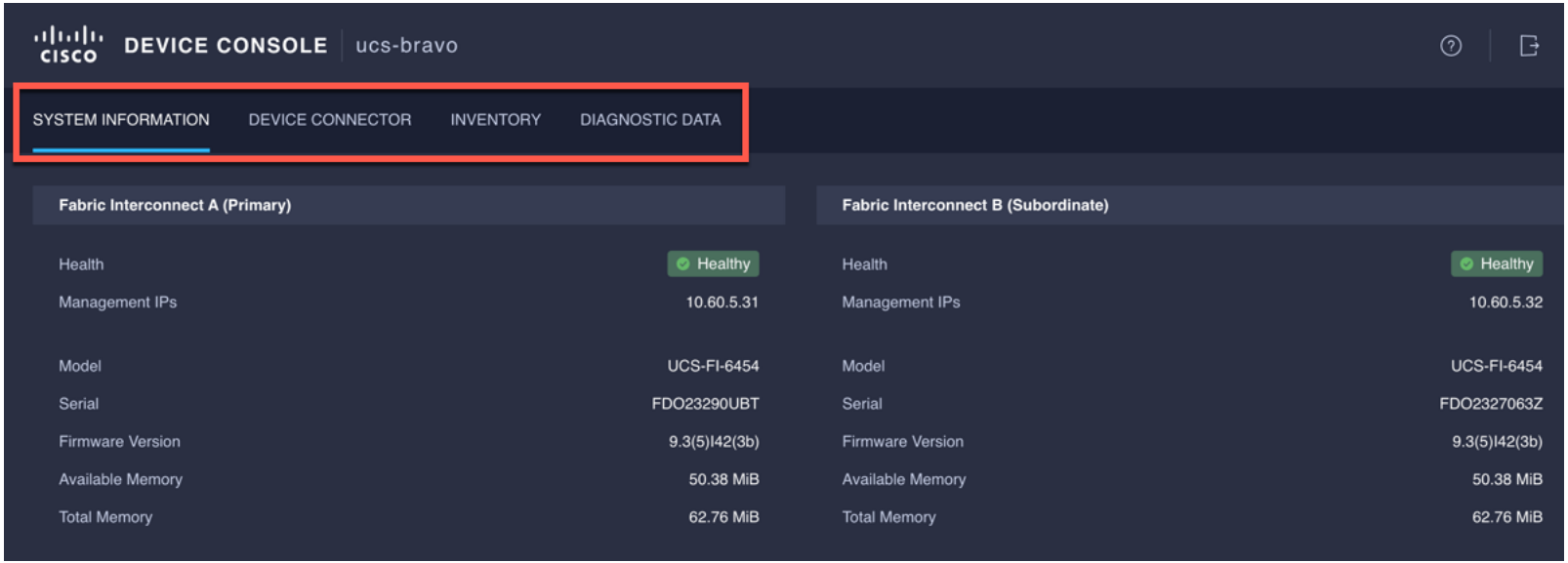
How to use Intersight Managed Mode?

Setting up a domain in Intersight Managed Mode

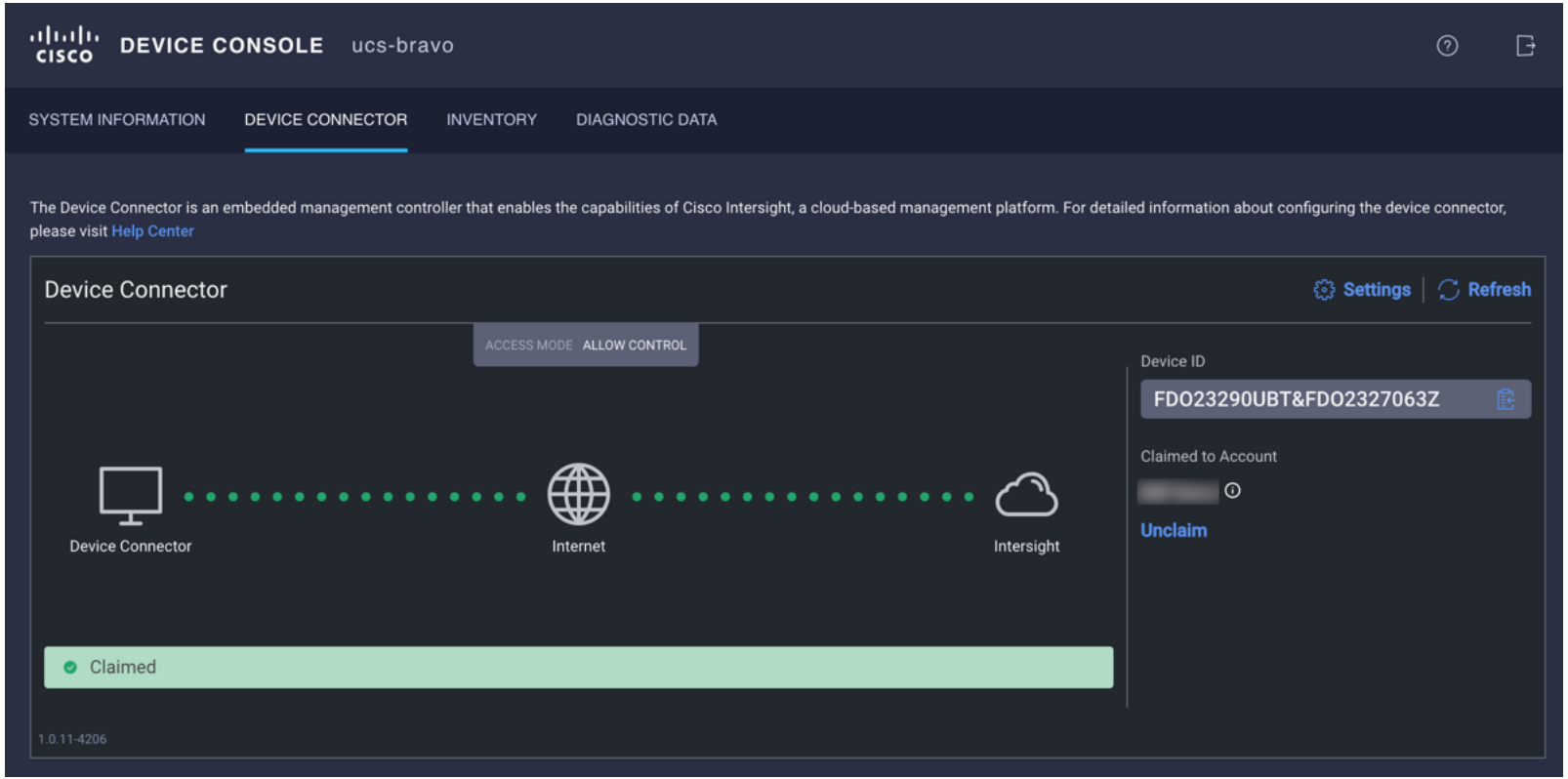
Management mode

```
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.

first-setup:    Warning:  is EMPTY. using switch as name

   Starting GUI for initial setup.

   Switch can now be configured from GUI. Use https://172.16.105.242 and click
   on 'Express Setup' link. If you want to cancel the configuration from GUI and go back,
   press the 'ctrl+c' key and choose 'X'. Press any other key to see the installation progress from
GUI
   Note: Intersight management mode setup available through console based configuration method alone
.



^C
  Type 'reboot' to abort configuration and reboot system
  or Type 'X' to cancel GUI configuratuion and go back to console  or Press any other key to see the
 installation progress from GUI (reboot/X) ? X

  Enter the configuration method. (console/gui) ? console

  Enter the management mode. (ucsm/intersight)? intersight

  You have chosen to setup a new Fabric interconnect in "intersight" managed mode. Continue? (y/n):
y
```

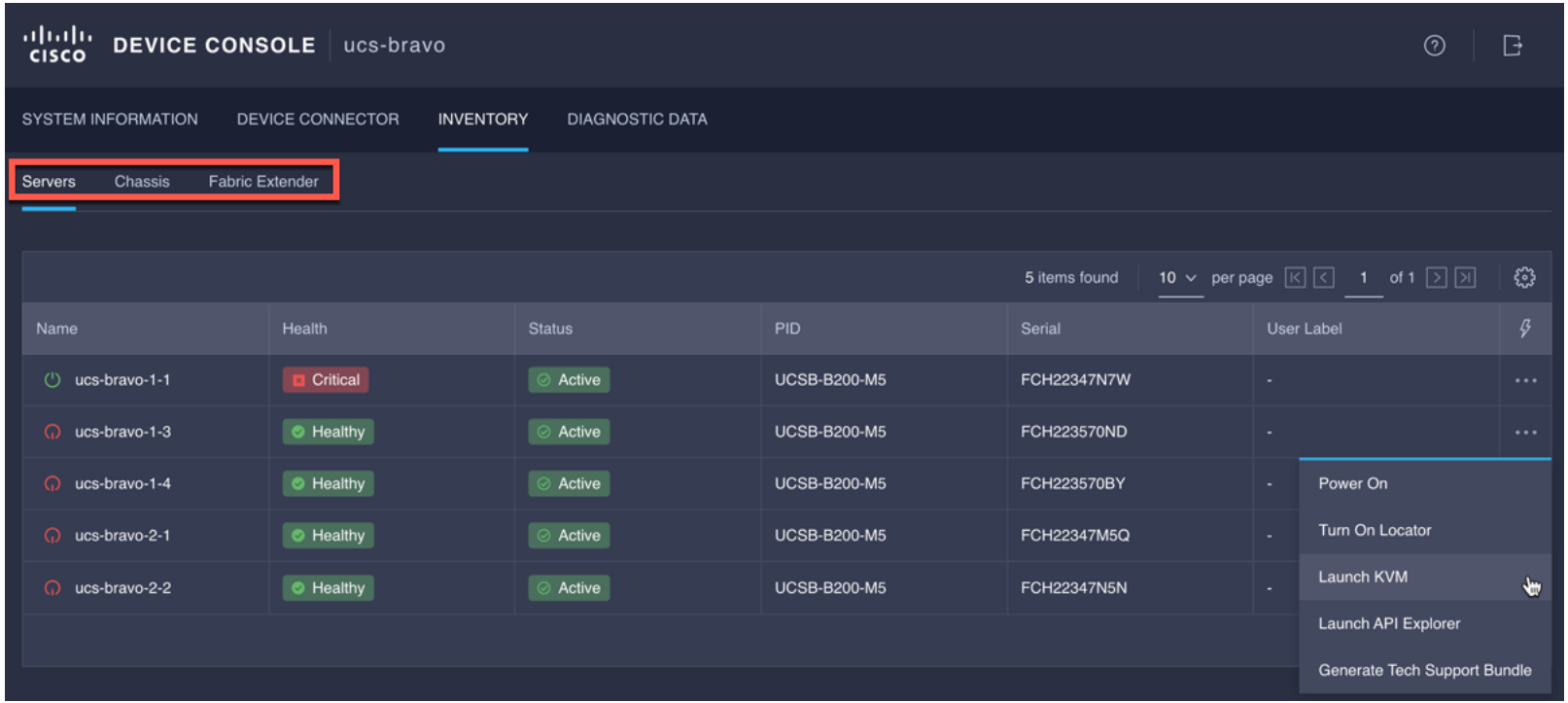
Device Console – System Information



Device Console – Device Connector



Device Console - Inventory

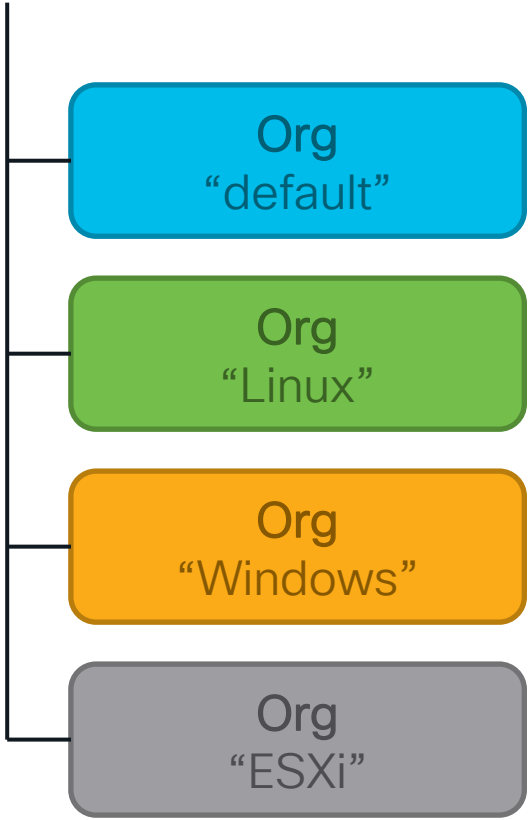


And... that’s it!

Everything else is done on

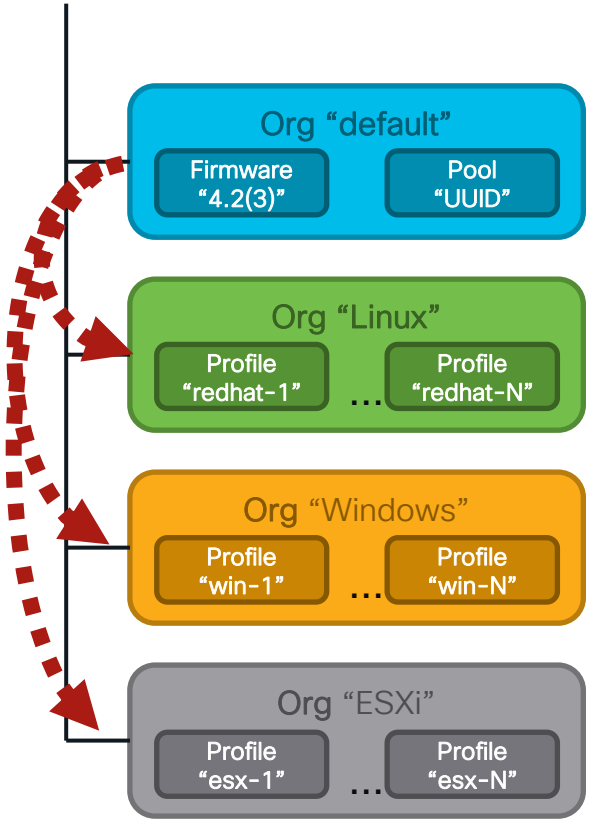
Organizations in Intersight

- Flat structure (no hierarchy like in UCSM/Central)
- Logical container to hold:
  - Logical resources (policies / pools / profiles / ...)
  - Physical resources (servers, storage, ...)
    - Grouped into Resource Groups
    - A physical resource can belong to multiple organizations
- Used to perform Role-Based Access Control
  - Users are assigned Roles (set of Privileges)
  - Roles are assigned a Scope (”all” or a list of organizations)
- Sharing between orgs
- Support of up to 50 orgs



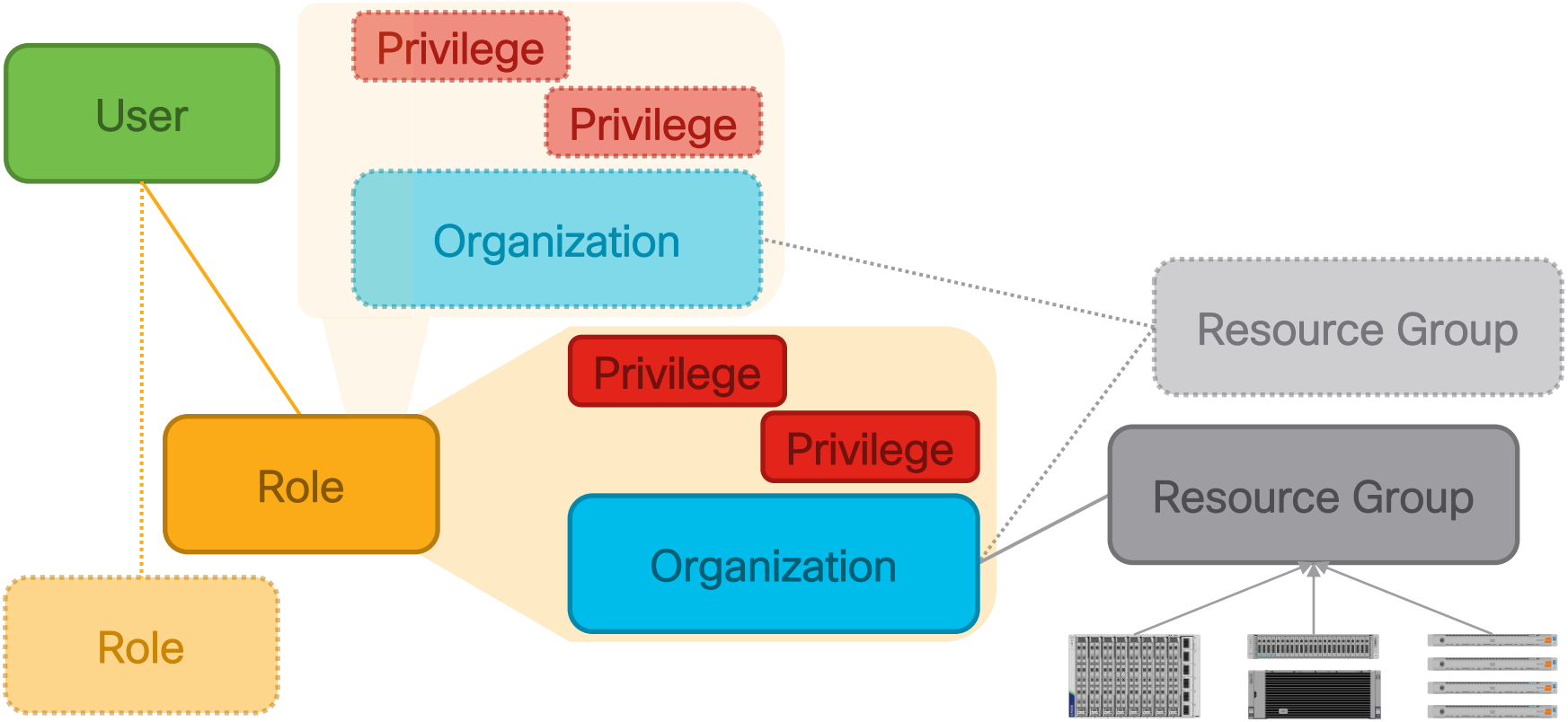
Organization Sharing

- Per organization setting
- Control sharing scope
  - List of organizations to share with
- Limitations
  - Support of up to 200 sharing rules
  - No support for sharing if org is associated with Resource Groups (hardware)
  - No support for transitive sharing (no multilevel sharing)
  - No support for org sharing with Port Policy & sub-policies



https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/imm-con-sharing-across-organization-cloning-wp.html

Role-Based Access Control with Intersight



Policy-based Model

- Similar to UCS Manager / Central

Pools	Policies
Profiles	Templates

- Everything is configured via policies
  - Servers, Chassis, **Fabric**
- Provides configuration consistency
- Ensures compliance
- Policy resolution via MOID, not name-based

Intersight Managed Mode

Pools, Policies, Profiles & Templates

Pools

- IP Pools
- MAC Pools
- WWNN Pools
- WWPN Pools
- IQN Pools
- UUID Pools
- Resource Pools

Policies

Domain Policies
- VLAN/VSAN
- Port
- NTP/DNS/QoS/Switch
- SNMP/Syslog

Server Policies
- BIOS
- Boot
- Storage/SD Card
- LAN/SAN Connectivity
- IMC Access
- KVM/IPMI/Serial/vMedia
- SNMP/Syslog
- Power/Thermal
- Firmware

Chassis Policies
- SNMP
- IMC Access (for SNMP)
- Power/Thermal

Profiles

- Domain Profiles
- Server Profiles
- Chassis Profiles

Templates

- Domain Profile Templates*
- Server Profile Templates
- Chassis Profile Templates*
- vNIC/vHBA Templates*

** Other Templates in roadmap*

IMM Pools

Key differences with UCS Manager/Central

For your reference

Missing/Removed

- No **WWxN** pools
- No **Qualification policies*** for Resource (Server) Pools

Added/Simplified

- **Rename** pools
- Blocks with **up to 1024 entries** for all pool types
- **Sequential** allocation only
- Preliminary support for **VRF** to allow **overlapping** addresses

Changed

- **Netmask/Prefix, Gateway, DNS** on a per-IP Pool basis (per-block* in roadmap)
- No **default** pools

** In roadmap*

IMM Policies

Key differences with UCS Manager/Central

For your reference

Missing/Removed

- No **Scrub*** policies

Added/Simplified

- **Rename** policies
- **Domain policies** for consistent configuration across domains
- **Single** policy type per function
- **Shared policies** between Standalone & FI-Attached

Changed

- No **default** policies
- **Sourcing of catalog values** when creating Adapter policies

** In roadmap*

IMM Profiles & Templates

Key differences with UCS Manager/Central

For your reference

Missing/Removed

- No **Initial** Templates (use cloning instead)
- No support for **assigning IP at the physical server** level (only at the profile)*
- No support for static IP assignment*

Added/Simplified

- *Did I mention* **Rename** profiles & templates
- No need for **Maintenance Policy**
- **Merging of Local & Global** Service Profile/Template

Changed

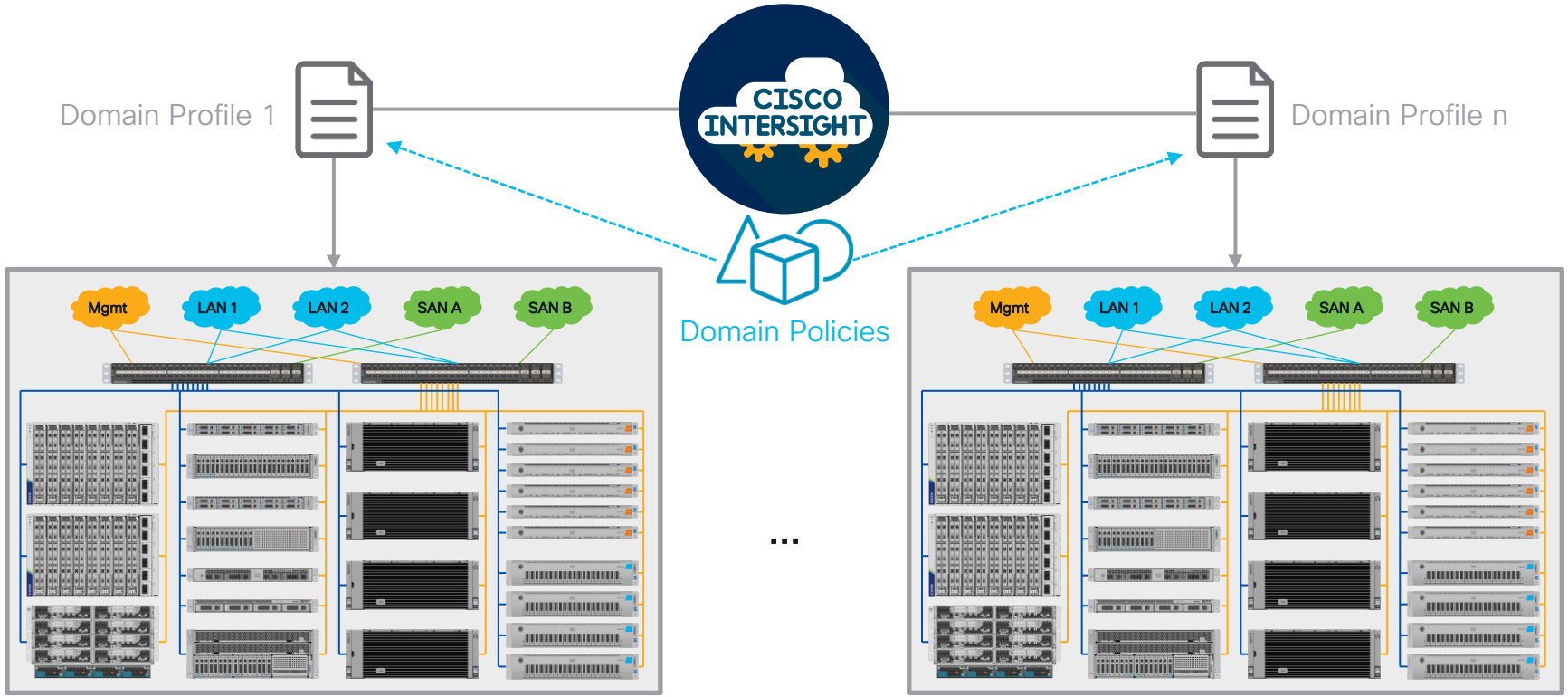
- **Improved change control** (separate assign, deploy & activate steps)

** In roadmap*

Managing UCS Domains

UCS Domain Profiles

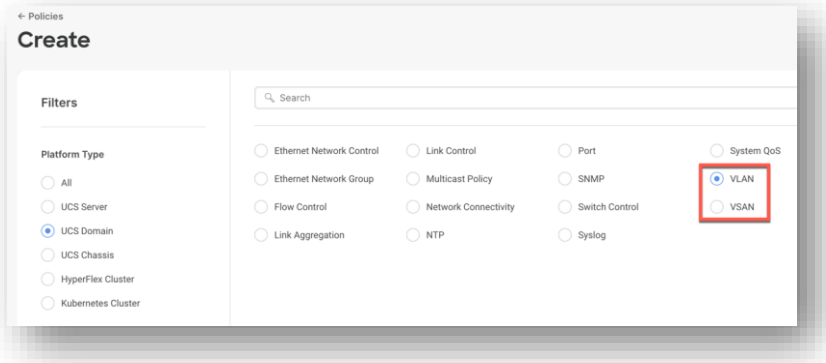
Policy-based configuration of the UCS fabric

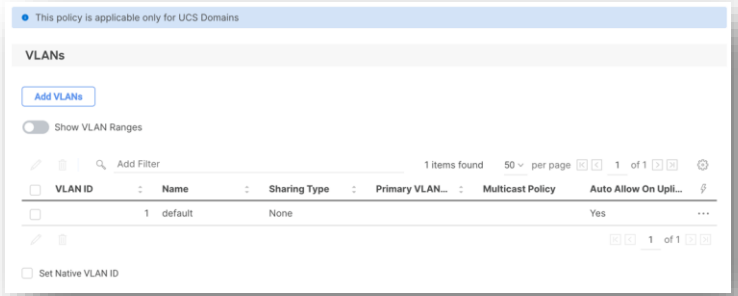


UCS Domain Profiles

VLAN / VSAN Policy

- Defines the list of VLANs / VSANs that need to be deployed at the Fabric Interconnect level
- Domain Profile can use:
  - a common policy for both Fabrics (common scenario for VLANs) or
  - separate policies (VSANs are often different on each Fabric Interconnect)
- VLANs can be defined using a range to simplify configuration
- Private VLANs supported
- Multicast Policy required for all VLANs

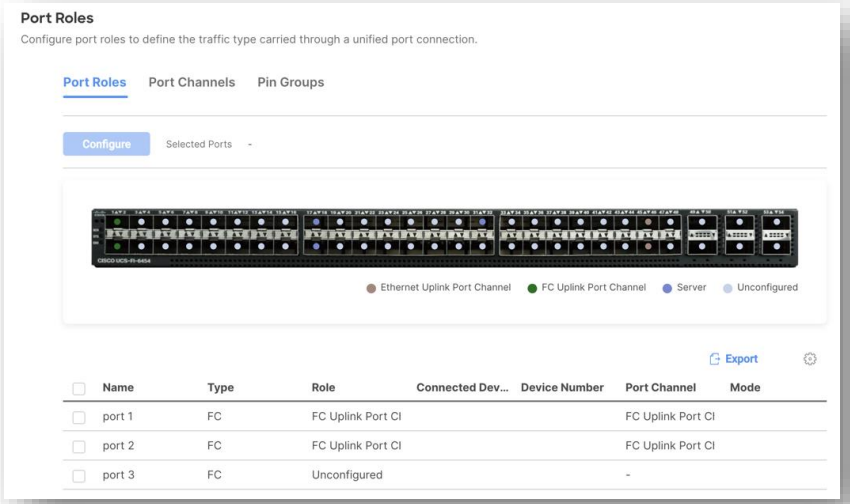




UCS Domain Profiles

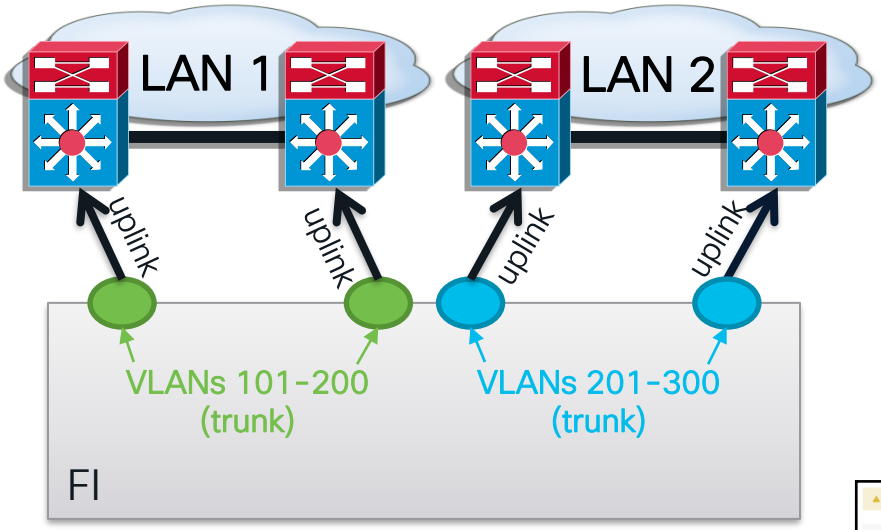
Port Policy

- Defines the port configuration of the Fabric Interconnects
  - Unified Port configuration (range) (requires a reboot during deployment)
  - Breakout Port configuration
  - Port Roles configuration (Server, LAN/SAN/FCoE Uplink, Appliance, FC Storage, Port-Channels)
- Domain Profile can use either:
  - a common policy for both Fabrics (for symmetric deployments)
  - separate policies for each Fabric (for better granularity) Recommended
- Ability to pre-define device ID for chassis/racks discovery

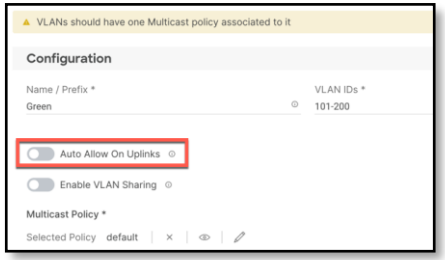


Disjoint Layer 2 configuration in IMM

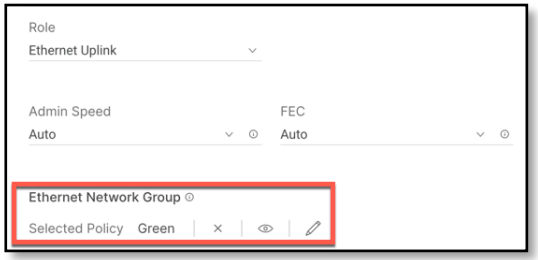
For your reference



- To connect to disjoint L2 networks, VLANs can be filtered on uplink ports (or port-channels)
  - A single uplink port is designated as broadcast/multicast receiver for each VLAN
- VLANs must be grouped as part of Ethernet Network Group Policies (Green and Blue)
  - **All VLANs used for Disjoint L2 must have "Auto Allow On Uplinks" set to Disabled**
  - Native VLAN can be defined per Eth. Network Group Policy
- Ports with role "Ethernet Uplink" part of Port Policy can be assigned an Ethernet Network Group Policy



VLAN Policy

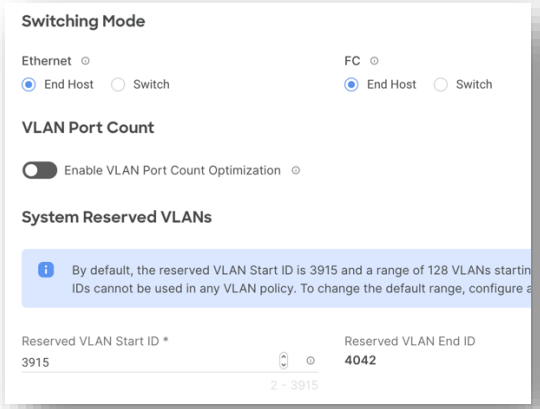


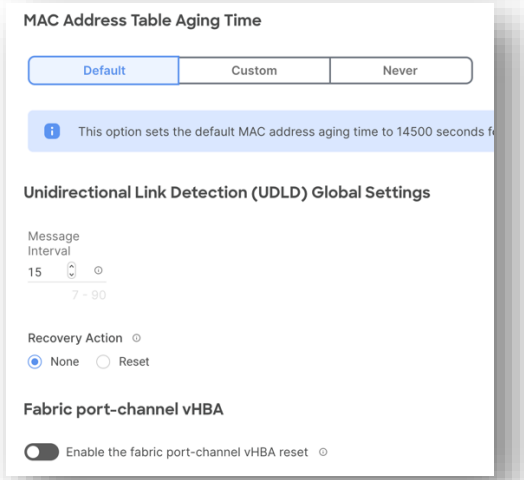
Port Policy

UCS Domain Profiles

Switch Control Policy

- Defines the network settings of the Fabric Interconnects
- Ethernet & FC End-Host / Switch Mode
  - End-Host mode recommended
  - FC Switch mode for direct-attached SAN Storage
  - Reboot required to change mode
- Advanced settings
  - VLAN Port Count Optimization (16K → 108K)
  - Reserved VLAN Range (128 internal VLANs)
  - MAC Address Aging settings
  - UDLD Settings
  - Fabric Port-Channel vHBA Reset





UCS Domain Profiles

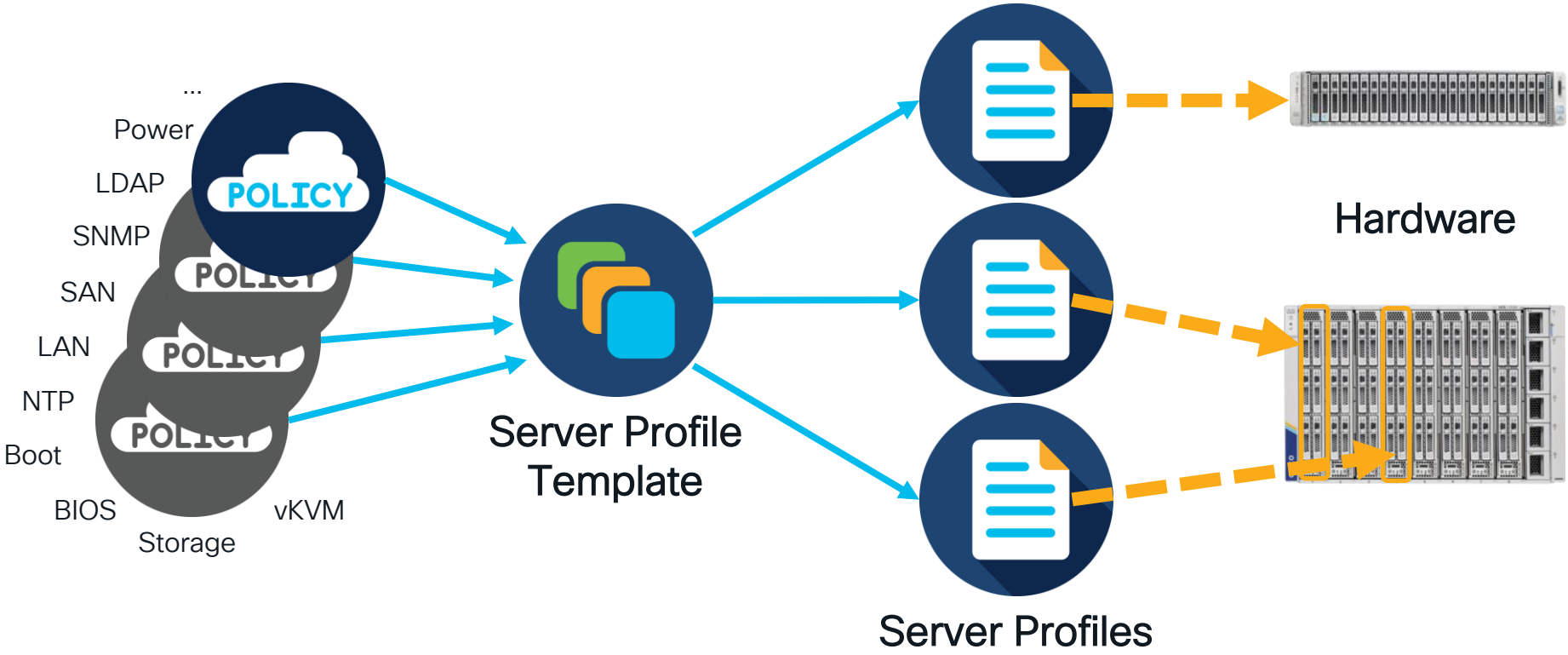
System Settings Policies

- These policies define the Fabric Interconnects configuration
  Similar to Domain Group settings in UCS Central.
  - Network Connectivity Policy: Defines DNS settings
  - NTP Policy: NTP & Timezone settings
  - System QoS Policy: QoS classes settings
  - Switch Control Policy: VLAN compression, MAC Address aging, Link Control, Switch modes for Ethernet & FC
  - SNMP Policy: SNMP settings
  - Syslog Policy: Syslog settings
- Multiple policies are generic and can be shared with other platform types (Standalone server, FI-Attached server, Chassis)

Managing UCS Servers

UCS Server Profiles & Templates

Policy-based configuration of the UCS servers



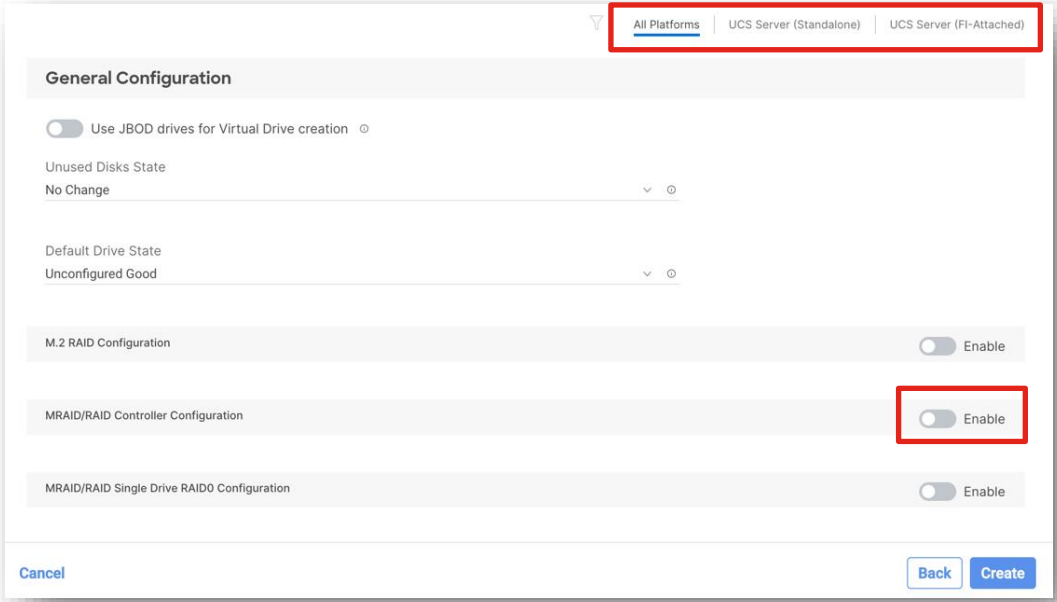
UCS Server Profiles & Templates

Server Configuration Policies

- Server configuration policies – similar to UCS Manager/Central policies
  - BIOS Policy: Defines BIOS settings
  - Boot Order Policy: Defines server boot order
  - LAN Connectivity Policy: Defines vNICs
  - Power Policy: Configures power management (profiling & restore)
  - SAN Connectivity Policy: Defines vHBAs
  - SD Card Policy: Defines SD Card settings (M5 servers only)
  - Storage Policy: Defines local storage settings (M.2 and RAID controllers)
  - Thermal Policy: Configures fan speed control (rack servers only)
- Multiple policies are generic and can be shared with other platform types (Standalone server, FI-Attached server, Chassis)

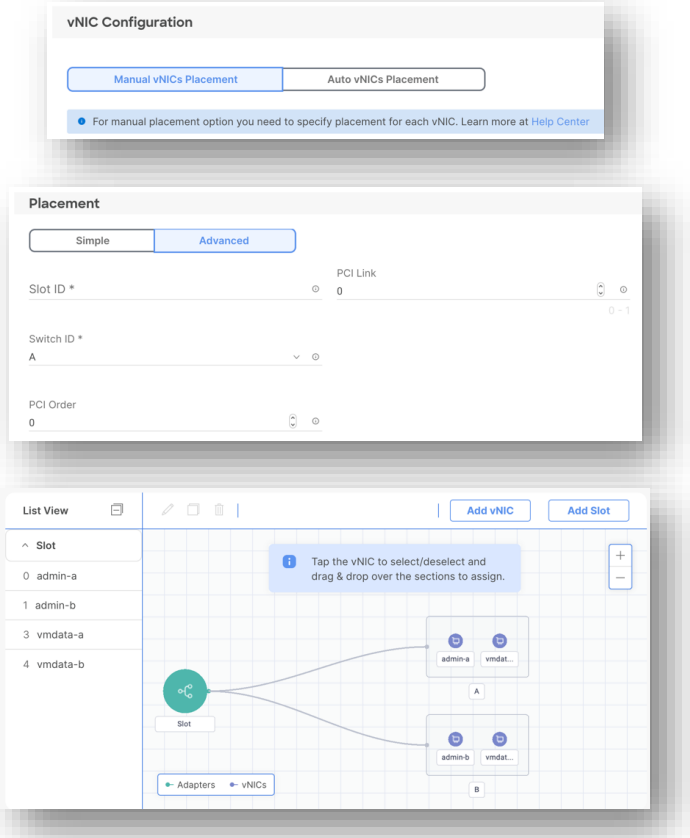
Storage Policy: All in One!

- Single policy for everything Storage
  - Replaces *Local Disk Config Policy*, *Disk Group Policy* & *Storage Profile*
  - Applies to Standalone & IMM servers
- Simple toggle button for M.2 RAID configuration
- Supports setting default & unused drives state
- Support for automatic disk assignment in roadmap

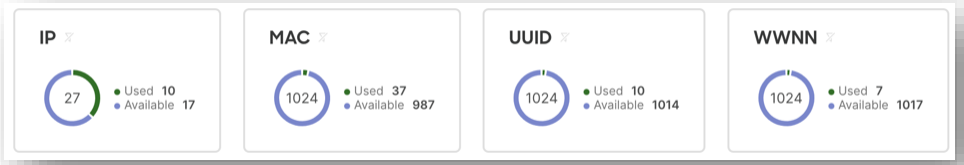


LAN/SAN Connectivity Policy changes

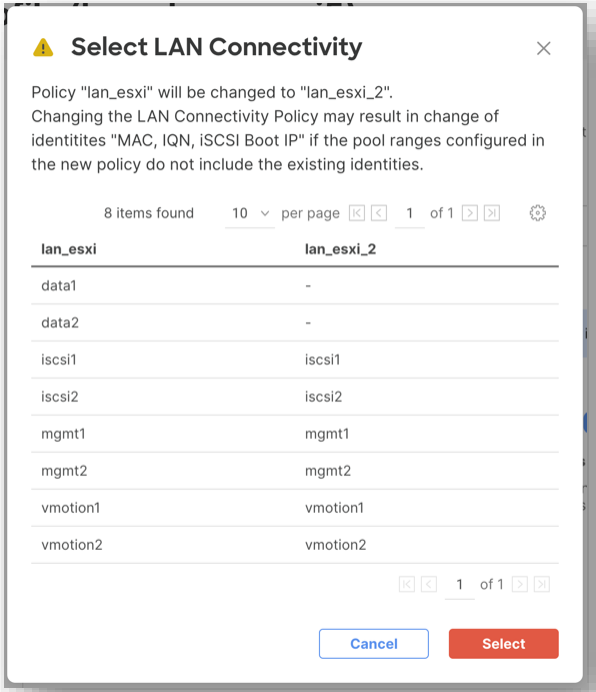
- Merging of “inline” vNICs/vHBAs and LAN/SAN Connectivity Policies
- No concept of “desired” and “actual” order
  - “*Auto*” placement automatically distributes vNICs/vHBAs
  - “*Manual*” placement lets you specify PCI order at the vNIC/vHBA level – Recommended
    Order needs to start at 0 and be contiguous for all vNICs/vHBAs
- vCon placement simplified
  - Use “Simple” placement for single-VIC deployments (automatically sets “Slot ID” and “PCI Link”)
  - Use “Advanced” placement to define the “Slot ID” for each vNIC/vHBA (and “PCI Link” for VIC 1300)
- vNIC/vHBA Templates in roadmap
- Graphical vNIC Editor for visual representation



Identities allocation



- Identities are allocated using an “Always Lowest ID” scheme
  - Across all blocks within the pool
  - Predictible allocation scheme – identical to UCSM/Central
- MAC, WWNN, WWPN, UUID are allocated at Server Profile creation
- IP and IQN are allocated at Server Profile deployment
- No support for ID Range Access Control Policy*
- Maintains identifers when swapping LAN/SAN Connectivity Policy or Detaching/Attaching to Template
  - Only works when swapping policies (single operation) – No detach & attach
  - Identifier is kept only if vNIC/vHBA has the same name



** In roadmap*

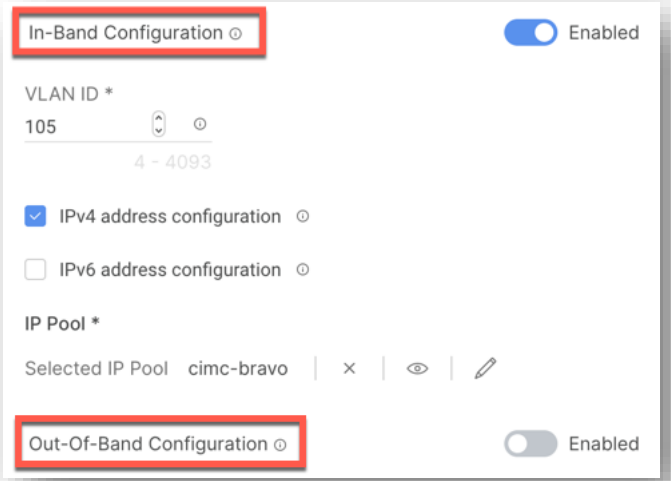
UCS Server Profiles & Templates

Server Management Policies

- Server management policies – similar to UCS Manager/Central policies
  - Firmware Policy: Configures firmware package versions for all server models
  - IMC Access Policy: Defines VLAN/IP address for server CIMC
  - IPMI over LAN Policy: Defines IPMI settings
  - Local User Policy: Configures local users for KVM/IPMI/SNMP access
  - Serial over LAN Policy: Defines SoL settings
  - SNMP Policy: Configures SNMP for server CIMC
  - Virtual KVM Policy: Defines vKVM settings
  - Virtual Media Policy: Configures vMedia settings
- Multiple policies are generic and can be shared with other platform types (Standalone server, FI-Attached server, Chassis)

IMC Access Policy – Required!

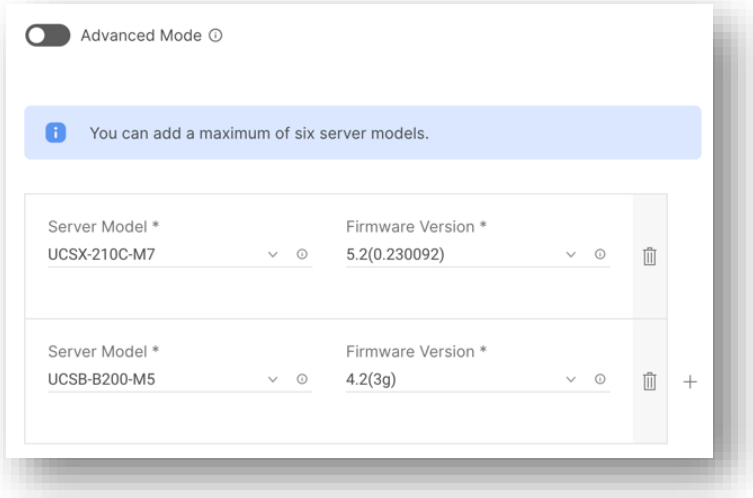
- Provides connectivity to the server's CIMC
  - IP assigned to Server Profile, not physical server*
  - Also used for accessing the chassis' CMC (SNMP)
  - No static IP assignment support*
- Inband configuration
  - VLANs 1-3 not supported (same as UCSM)
  - IPv4 & IPv6
- Out-Of-Band configuration
  - IPv4 only
  - No support for OS Install*
- Corresponds to "*Management IP Address*" + "*Inband Profile*" in UCS Manager



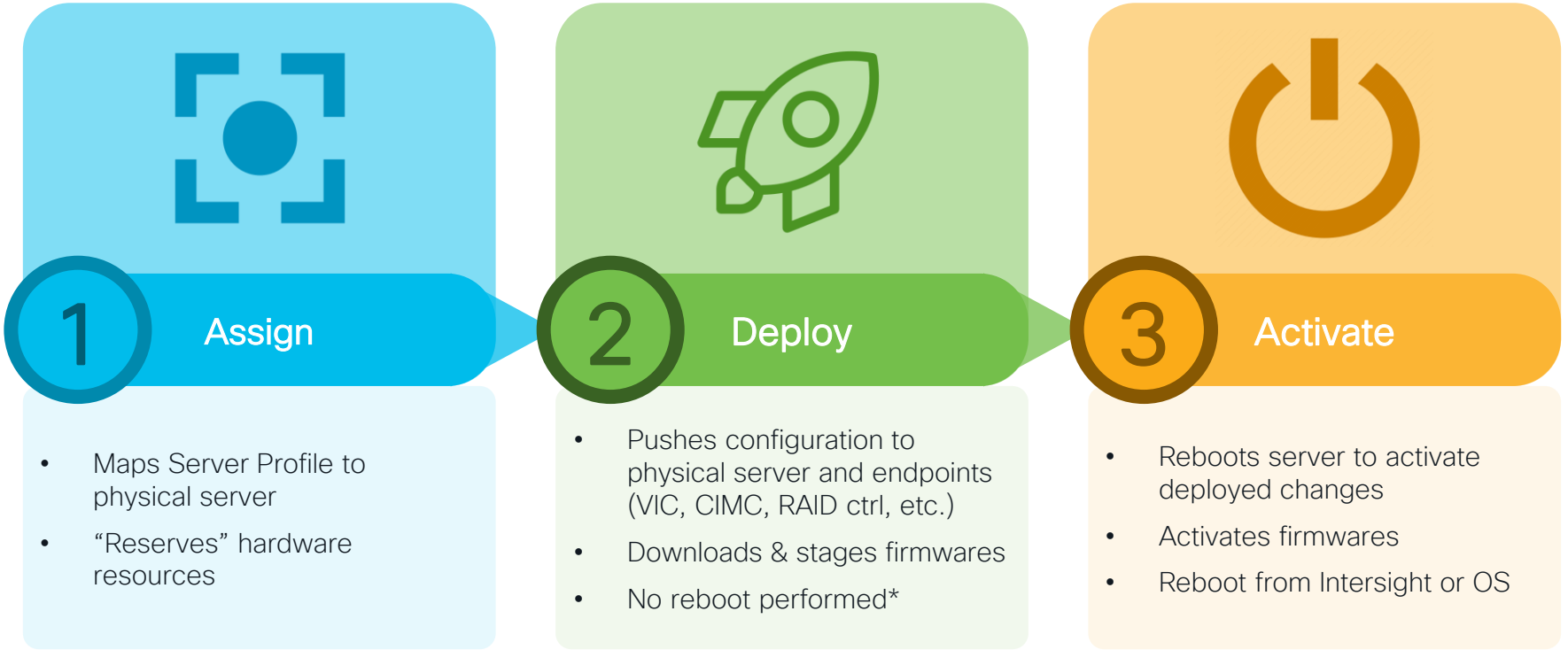
* *In roadmap*

Firmware Policy

- Automates firmware management within the Server Profile/Template
  - Replaces the *Host Firmware Package Policy* in UCS Manager/Central
  - Supports firmware upgrade & downgrade
- Downloads & stages firmware during Profile deployment phase
- Activates new firmware during Profile activation phase
- Per-model firmware version support (up to 6)
- Ability to exclude Storage Controllers & Drives (Advanced Mode)
- Supported with Standalone & IMM servers



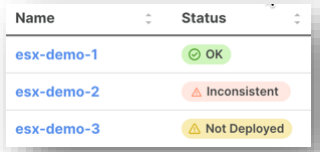
Improved change control

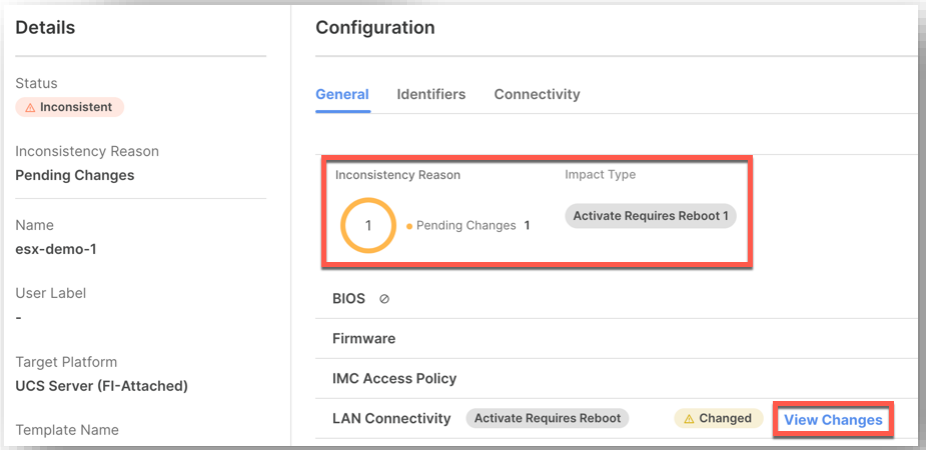


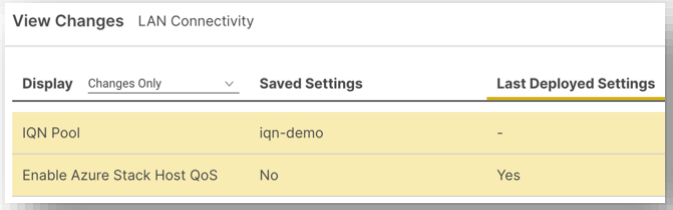
** Except for Persistent Memory Policy*

Improved change control

- No need for a “Maintenance Policy”
- Profile status: OK, Not Deployed, Inconsistent (with reason)
- Estimates impact of deploying & activating changes for each policy
  - “Activate Requires Reboot” indicates a reboot requirement
  - “Management Network Outage” indicates a CIMC connectivity loss
- Ability to view the pending changes before deploying, with a side-by-side comparison view
- Same change control for Domain & Chassis Profiles



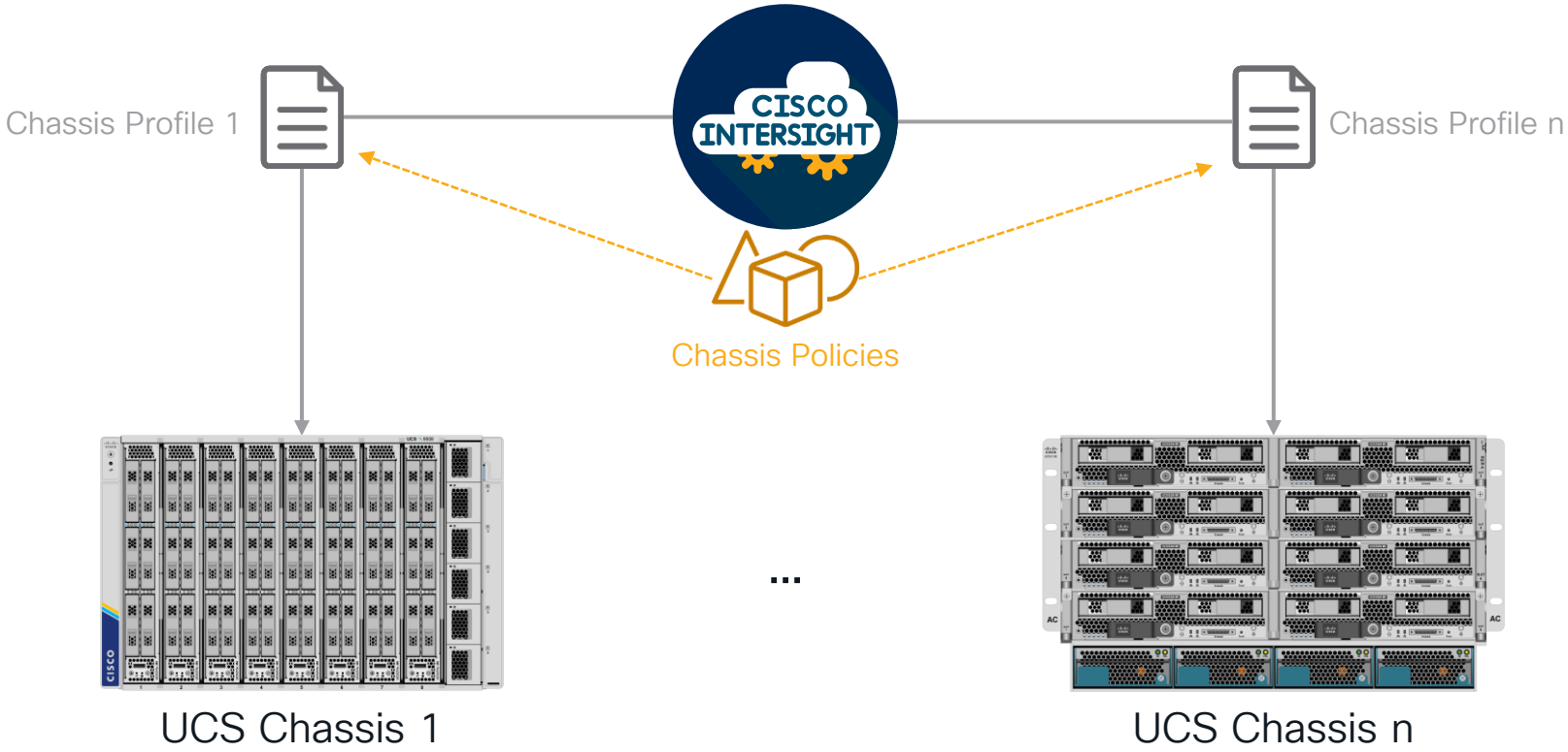




Managing UCS Chassis

UCS Chassis Profiles

Policy-based configuration of the UCS chassis



UCS Chassis Profiles

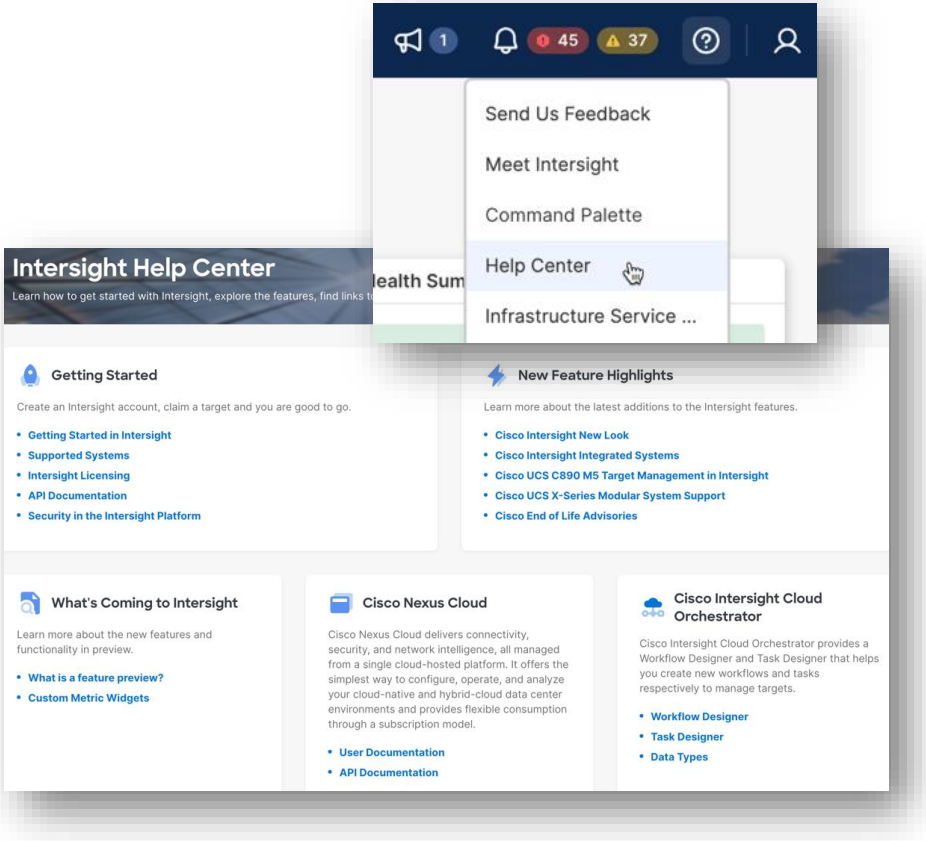
Chassis Policies

- Chassis policies – to support per-chassis settings (different from UCSM)
  - IMC Access Policy: Defines VLAN/IP address for chassis CMC (used by SNMP)
  - Power Policy: Configures power management (redundancy & power budget)
  - SNMP Policy: SNMP settings
  - Thermal Policy: Fan control settings
- Multiple policies are generic and can be shared with other platform types (Standalone server, FI-Attached server, Chassis)
- Not required to have a fully functioning chassis (defaults to Grid power)

Performing (some) Operations

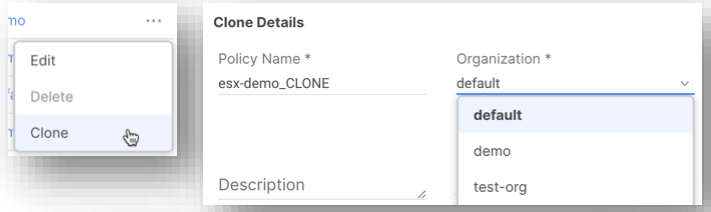
Intersight Help Center & documentation

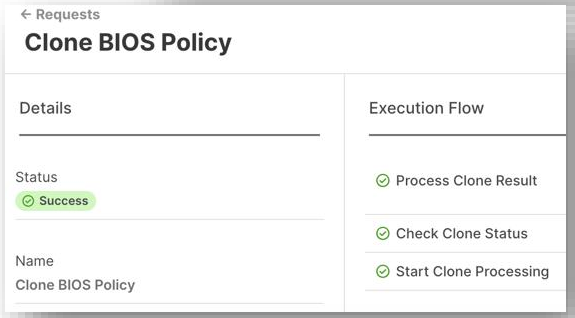
- All documentation is available via the Help Center
  - SaaS: https://intersight.com/help/saas
  - Appliance: https://intersight.com/help/appliance or on the Appliance
- Release Notes & Release Bundle Contents
  - https://www.cisco.com/c/en/us/support/servers-unified-computing/intersight/products-release-notes-list.html

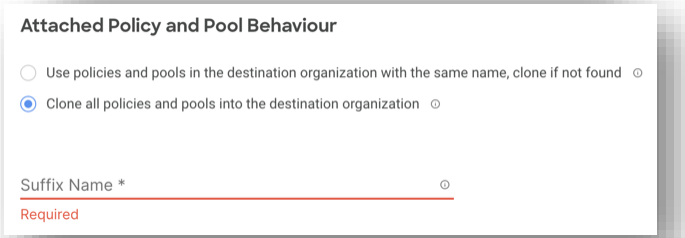


Cloning Objects

- Cloning Policies
  - Supports cloning across orgs
  - Triggers clone workflow for tracking
- Cloning Complex Policies (referencing other policies/pools) behavior:
  - Reuse existing policies/pools (default)
  - Force clone all policies/pools (provide unique suffix)
- Cloning Profiles/Templates
  - Not applicable to Profiles derived from Template
  - Supports up to 25 clones per clone operation
  - Support for cloning across orgs in roadmap
- No support for cloning Pools

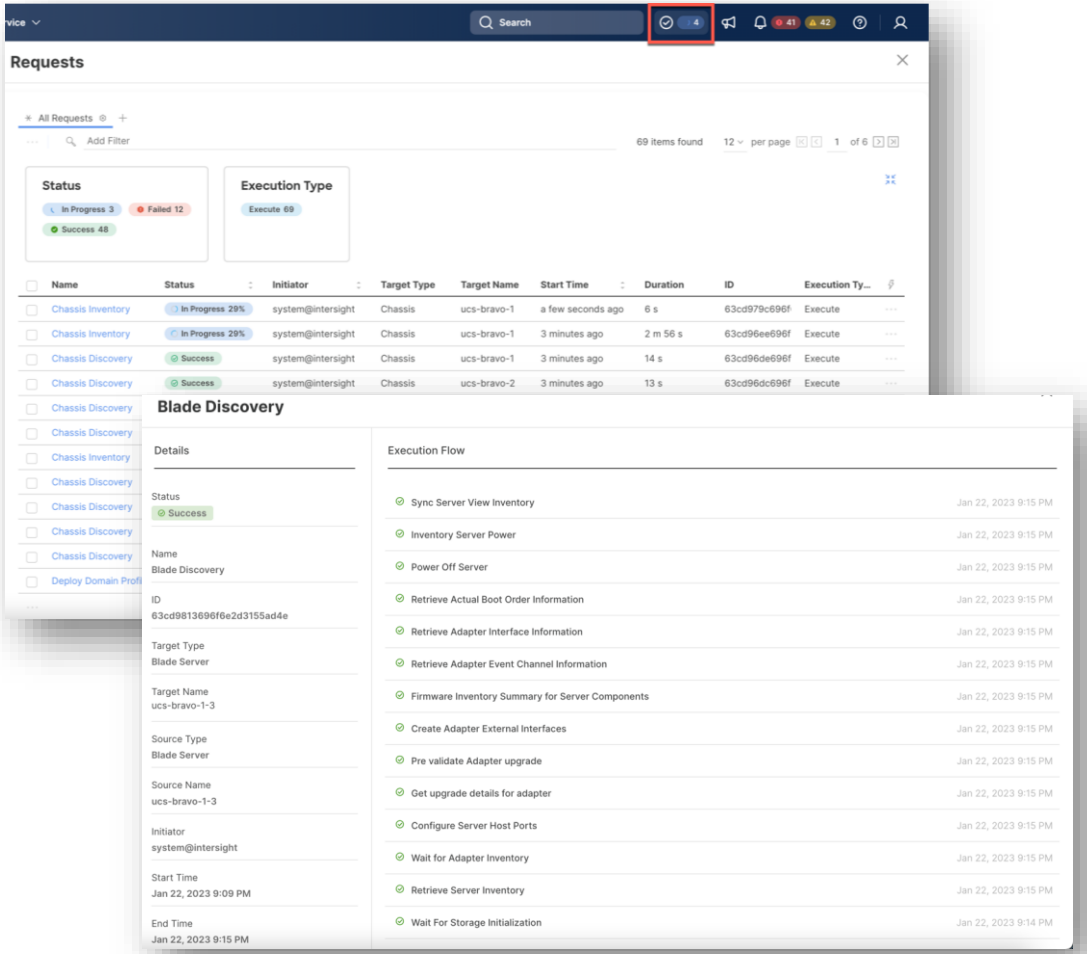






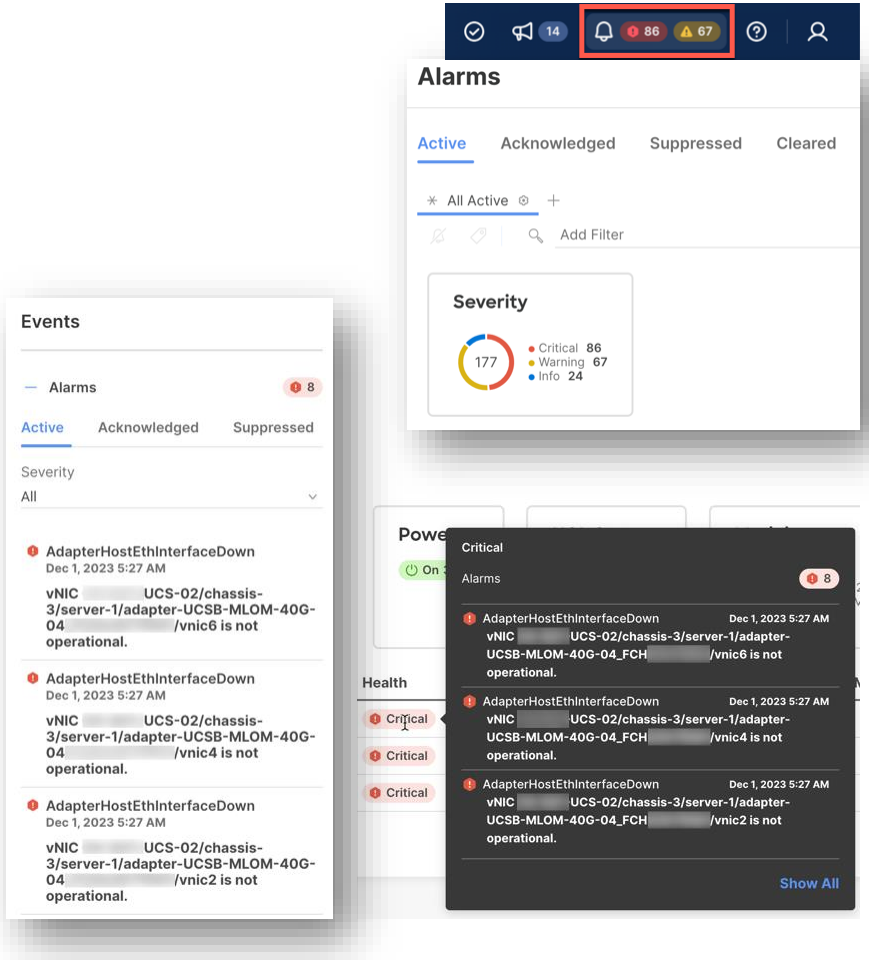
Where is my FSM?

- Common place for all requests and workflows (orchestrator)
  - In progress, successful or failed
- View request details with individual steps



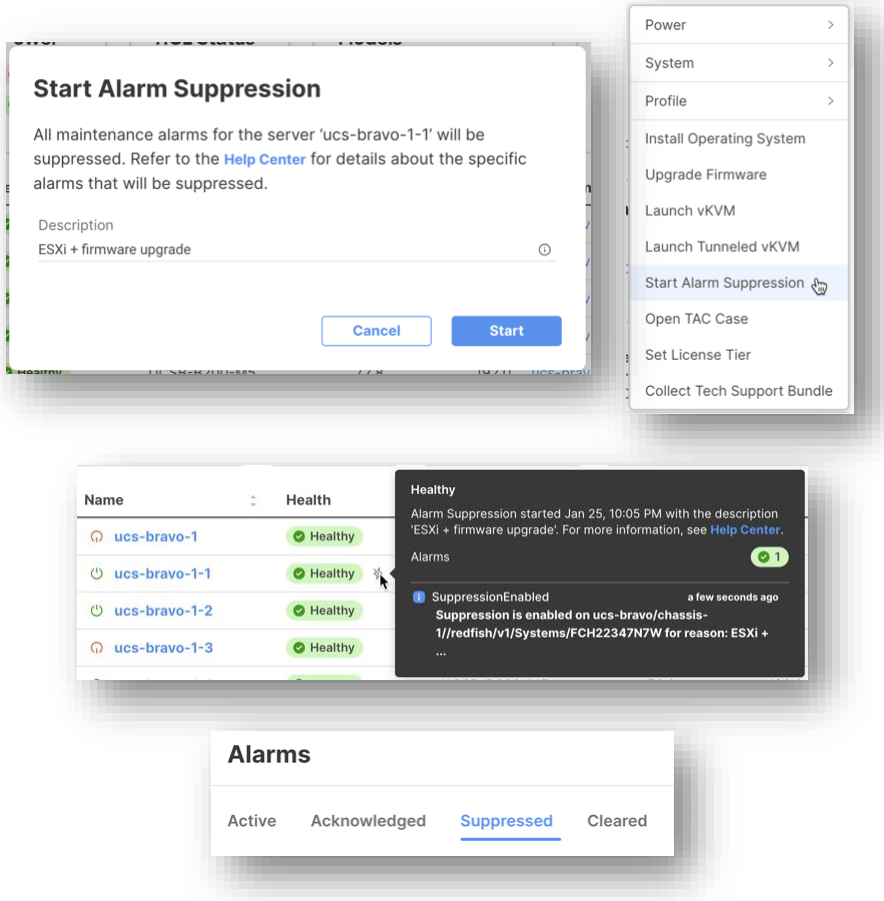
Alarms & Notifications

- Drawer containing all alarms
  - Critical, Warning & Info levels
- Acknowledging an alarm removes it from the Active section
- Cleared alarms are available for troubleshooting & post mortem analysis
- Contextual alarms list in table views and detailed views (click to see details)
- New alarm codes with readable name (e.g. **AdapterHostEthInterfaceDown**)
  - Alarms Reference Guide: https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM_Alarms_Guide/b_cisco_intersight_alarms_reference_guide.html



Alarm Suppression

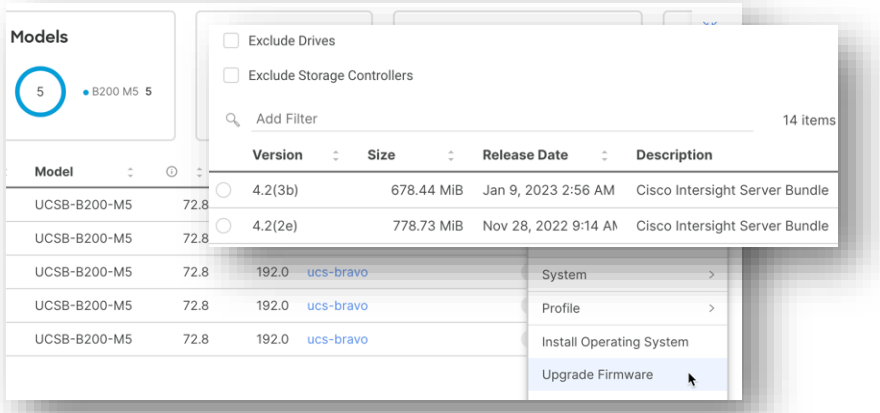
- Temporarily mutes alarms notifications
- Useful during maintenance window or other planned activities (upgrades, etc.)
- Suppressed alarms can still be seen under the “Suppressed” tab in the Alarms drawer
- Applicable at physical server level



Managing Firmwares

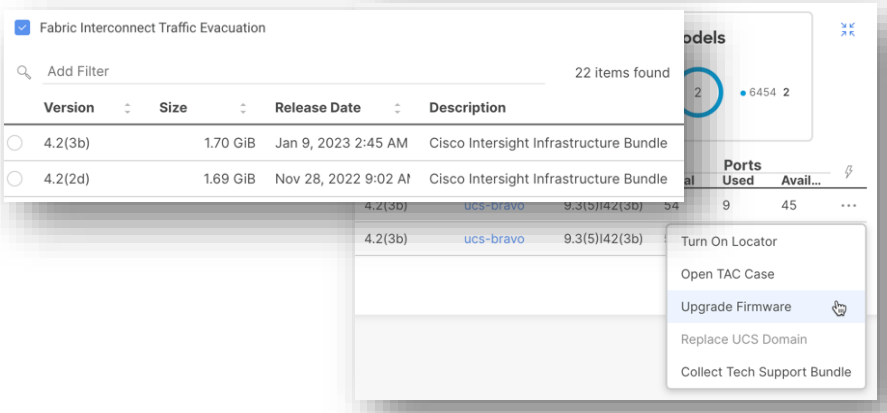
UCS Servers

- Single/Multi-server parallel upgrade
  - Firmwares installed on next boot or immediately
- Similar for IMM and standalone servers
- Firmware Policy for automated management



UCS Infrastructure

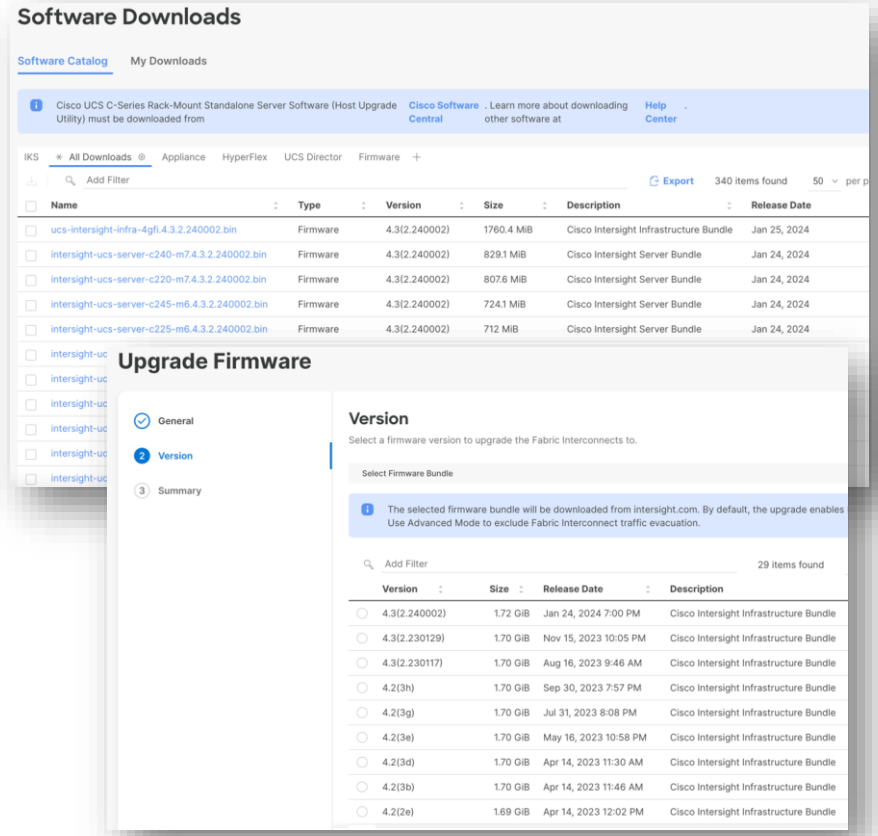
- Similar to UCS Manager Auto-Install
- User acknowledgement for each FI reboot
- Integration of fabric Traffic Evacuation



Automatic download of firmware from Intersight.com (for SaaS & CVA) to the FIs cache

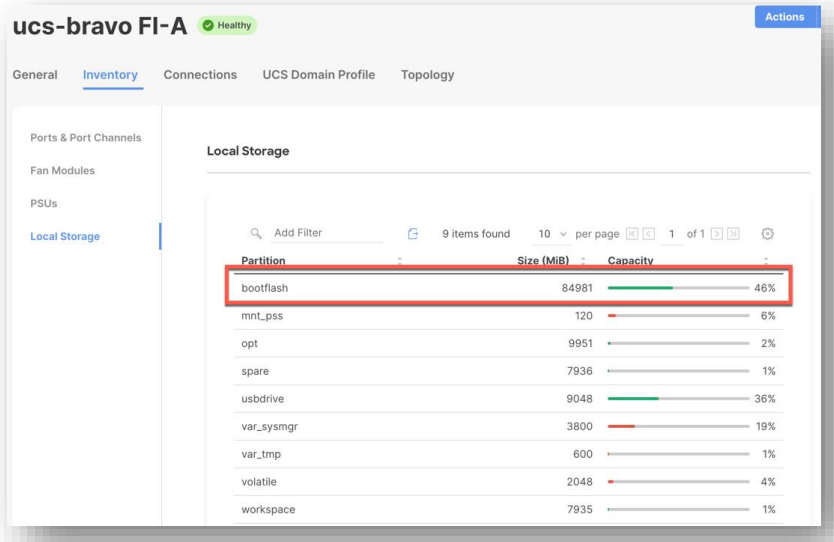
Where to download firmware bundles?

- For SaaS & CVA, download is automatically performed from intersight.com
  - When performing firmware upgrade operation on server(s)
  - When deploying Server Profile(s) with a Firmware Policy
- For PVA, firmwares need to be manually uploaded to the Software Repository first
  - Create an Intersight Appliance Account: https://www.intersight.com/pvapp
  - Download firmwares for:
    - Infrastructure (4GFI = 6400 series, 5GFI = 6500 series)
    - Servers (one file per server model)
    - Intersight Appliance & Appliance Intelligence bundle
  - Upload firmwares to Software Repository → Software section
  - Help: https://intersight.com/help/appliance/getting_started/downloading_software_packages_for_appliance



Managing FI firmware cache

- All firmwares (infrastructure & server bundles) used to perform a firmware upgrade are automatically stored on FI cache
  - Downloaded from intersight.com for SaaS & CVA
  - Downloaded from Software Repository for PVA
  - Synchronized between both FIs
- If cache becomes full, it will prevent firmware to be downloaded
- Monitor cache space utilization under the FI inventory
- To clear cache space, use the `clear-firmware-cache` CLI command, specifying a firmware bundle ID to remove (use `list-firmware-cache` to list bundle IDs)
  - Perform clear on both Fabric Interconnects
- Automatic cache space management in roadmap

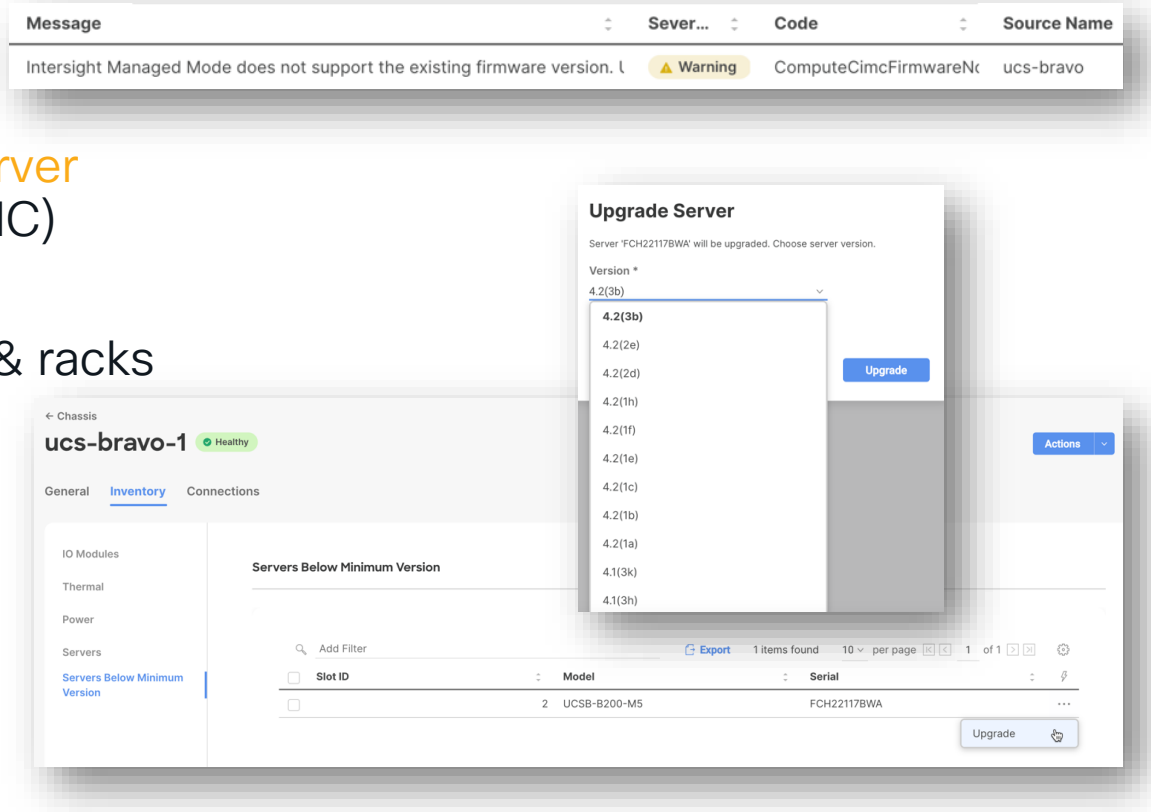



```
ucs-bravo-A# list-firmware-cache
DOWNLOADED DATE     IDENTIFIER                        IMAGE NAME
2023-09-13          650216eb65676131019d57ad          ucs-intersight-infra-4gfi.4.3.2.230117.bin
2023-10-30          653fbea3656761310100d082          intersight-ucs-server-b200-m5.4.2.3f.bin
2023-11-02          6543c63e656761310112aeba          intersight-ucs-server-b200-m5.5.1.0.230054.bin
2023-11-19          655a7771656761310121512d          intersight-ucs-server-210c-m6.5.2.0.230092.bin
2023-11-19          655a77f56567613101215368          intersight-ucs-server-b200-m5.5.2.0.230100.bin
2023-11-19          655a8bd9656761310121a9aa          intersight-ucs-server-c220m5.4.3.2.230270.bin
2023-11-20          655bd6bd6567613101276637          ucs-intersight-infra-4gfi.4.3.2.230129.bin
2023-11-22          655e0f9265676130057f6761          intersight-ucs-server-b200-m5.5.1.0.230073.bin
2023-12-11          6576dd556567613101d09d47          intersight-ucs-server-b200-m5.4.2.3b.bin
2024-01-24          65b1355d65676130059f01b7          intersight-ucs-server-b200-m5.5.1.0.230073.bin
```

```
ucs-bravo-A# clear-firmware-cache 6543c63e656761310112aeba
6543c63e656761310112aeba
The Intersight cache will be cleared.
Are you sure? Enter 'y' to continue:y
Cache cleared
```

Handling Servers below minimum version

- Alarm generated
- Mechanism to upgrade server firmware (CIMC, BIOS & VIC) running older versions
- Supports both M5 blades & racks
- Found under chassis/FI inventory
- Typical use case: RMA

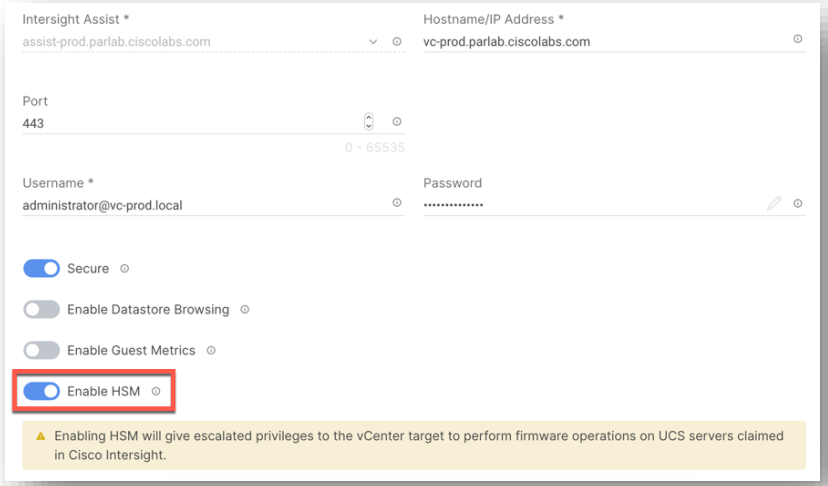


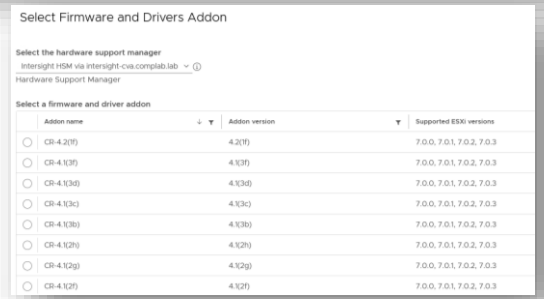
VMware vLCM/HSM Integration

- Automate UCS servers firmware updates via vLCM
- Claim vCenter in Intersight
  - **Enable HSM** when claiming
- No additional setup/plugin required

- Select "**Firmware and Driver Addon**" bundle directly from vLCM (auto-populated)
- Run Pre-Check & Remediate Hosts

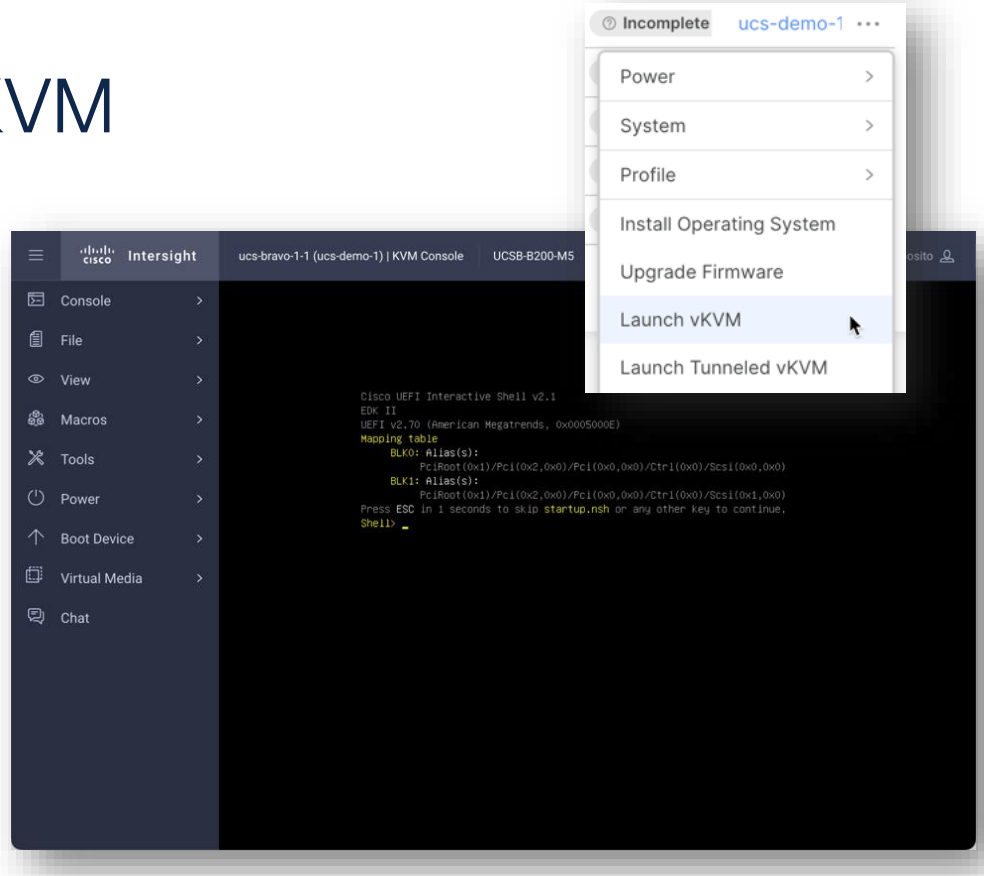
- Supported on SaaS & Appliance
- Supported with Standalone & IMM servers





Connecting to Virtual KVM

- Virtual KVM Policy
  - Enable/Disable vKVM
  - Tunneled vKVM support (via Intersight)
- Virtual Media Policy
  - Disabled by default
  - Virtual Media mounts
- IMC Access Policy required
  - Inband or Out of Band support
- Authentication
  - SSO from Intersight by default
  - Local User Policy required for KVM Direct
- One Time Boot device support
- Session Management: under System → Sessions



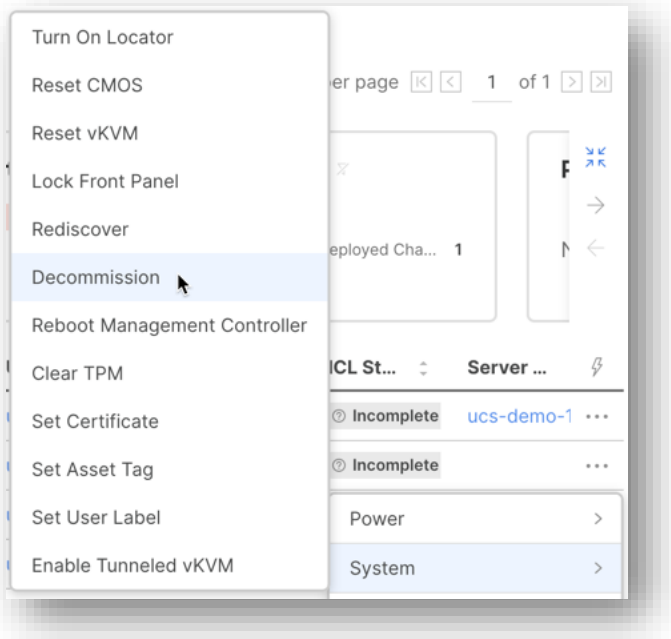
New Cisco vKVM with M5*/M6/M7 servers

** blades only*

Decommission / Recommission / Remove

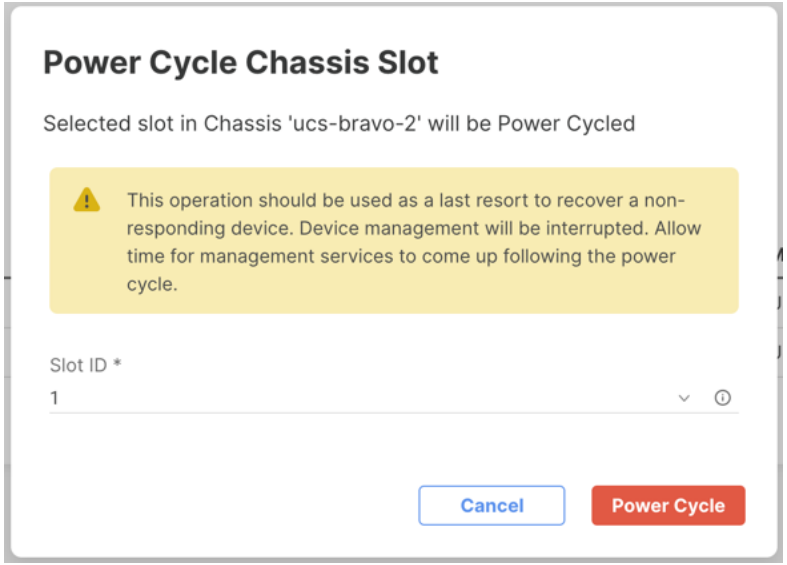
- Similar to UCS Manager

- To recommission:
  - Fabric Interconnect → Connections → Decommissioned
  - Can also be removed
- Ability to change ID of chassis / rack server / FEX when recommissioning
- Remove operation available when server is physically unplugged from the chassis



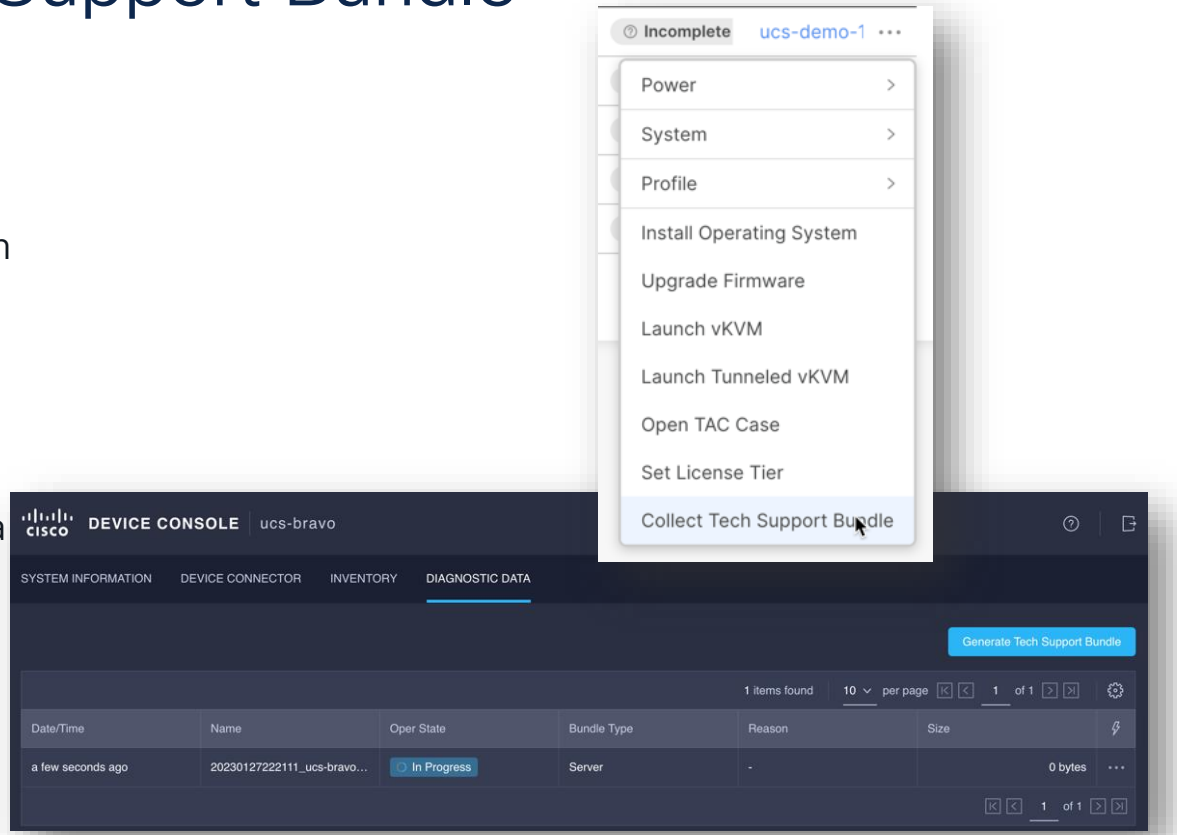
Power Cycle Chassis Slot (Slot Reset)

- For troubleshooting purposes only!
  - Power cycles both CIMC and server simultaneously
  - Highly disruptive to server operation
- Useful if CIMC is not reachable, or if server is stuck due to hardware/software issue and requires a reseat (hot plug) operation
- Action performed from Chassis view
- Resetting secondary slot for X410c M7 is not necessary

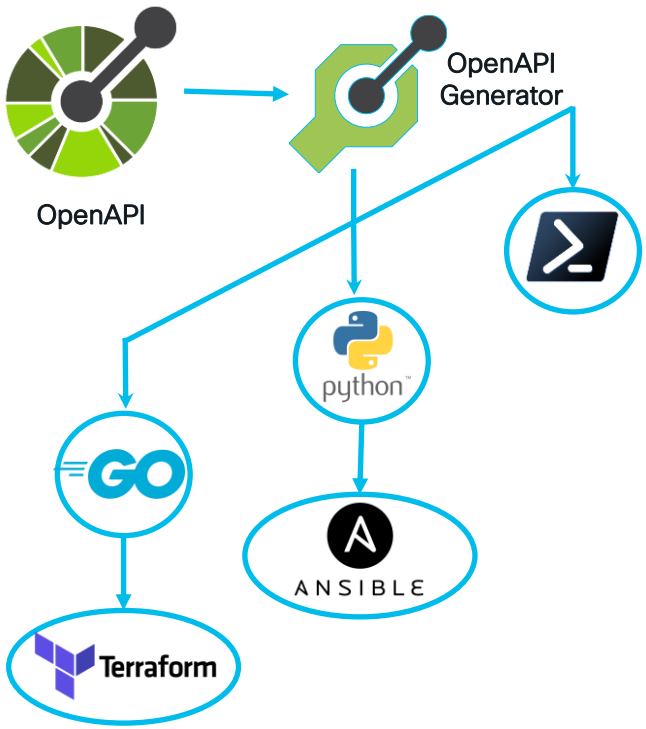


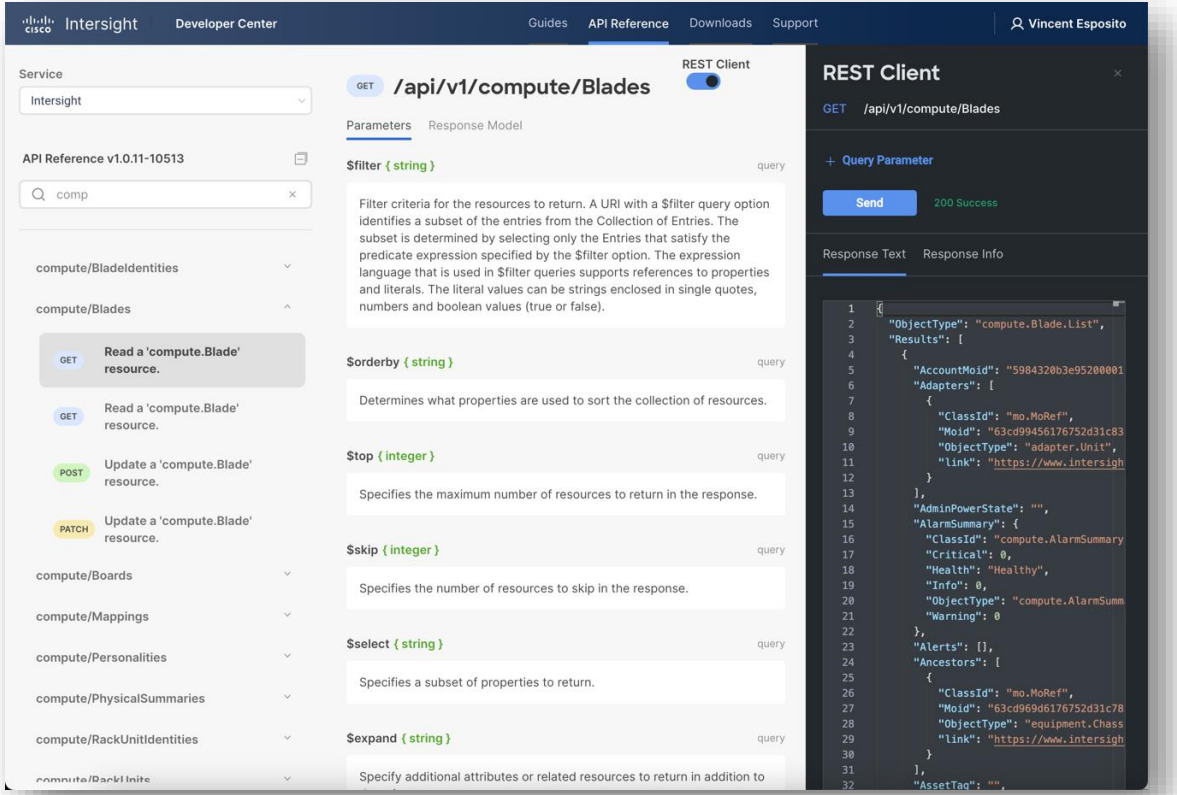
Collecting a Tech Support Bundle

- From Intersight
  - Action menu of the equipment
  - Download under System → Tech Support Bundles
- From Device Console
  - Action menu of the equipment under Inventory
  - Download under Diagnostic Data
- Connected TAC
  - Automated with SaaS and Connected Appliance



API is the new UI

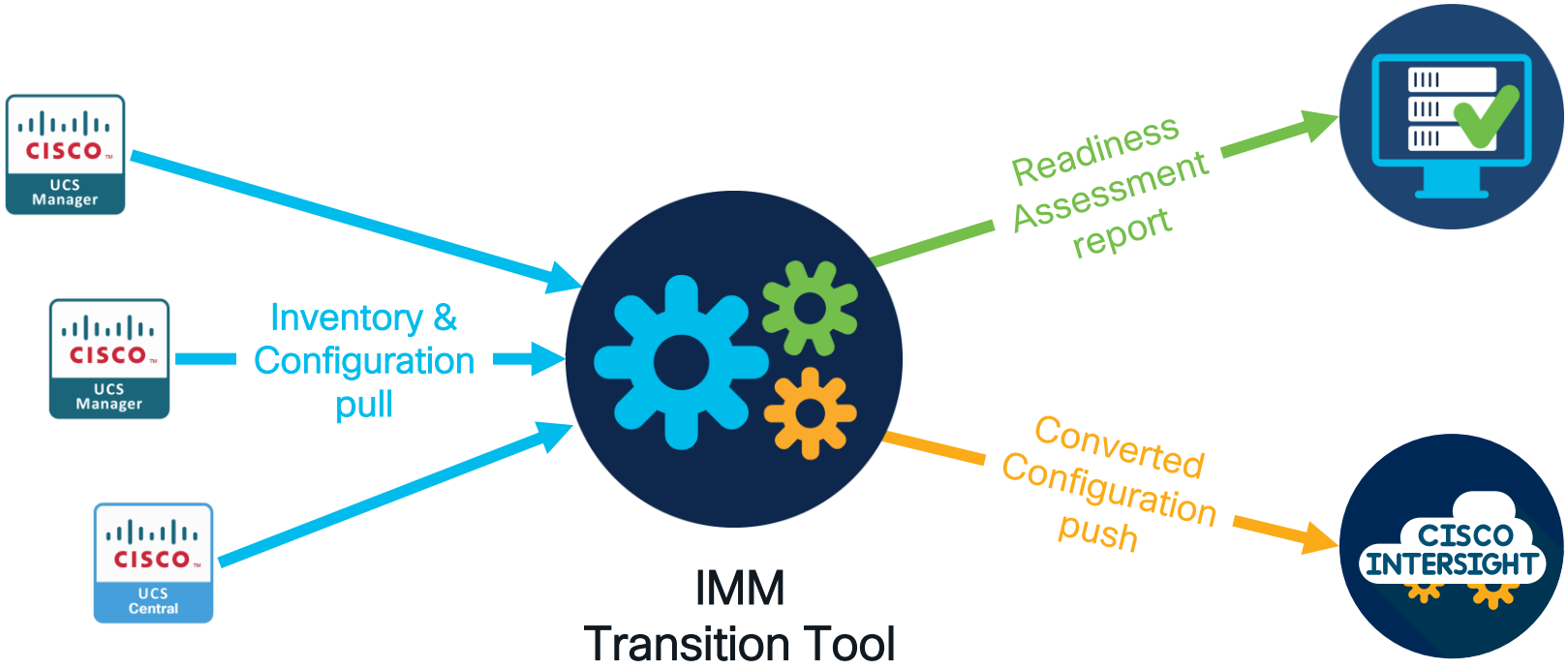




https://intersight.com/apidocs/

Transitioning to Intersight Managed Mode

Introducing the IMM Transition Tool



Primary use cases

Accelerate deployments of UCS X-Series

- **Extends** existing **Service Profile Templates** to Intersight
- Automatically converts related **server policies** (boot, BIOS, LAN/SAN connectivity, etc.)
- Converts **fabric configuration** (VLANs/VSANs, port configuration, etc.)

Move existing servers to IMM domains

- Automatically **converts** existing **Service Profiles** to Intersight Server Profiles
- Maintains all **server identities** (MAC, WWN, etc.)
- Allows **transition** to new server generation (e.g. M3/M4 to M6/M7)

Migrate an entire UCS domain to IMM*

- Assesses **hardware & firmware compatibility**
- Performs **complete conversion** of UCS Manager domain to IMM mode
- **Requires domain downtime**
- Handles **all necessary operations** automatically

** Roadmap*

Additional use cases

Intersight form-factor migration

- Perform **form-factor migration** of policies (between Intersight SaaS, CVA & PVA)
- Clones **org structure** and **policies**, **profiles**, **templates**
- Supports **server**, **domain** & **chassis** policies (no support for HyperFlex & Kubernetes)

Bulk claim of devices to Intersight

- **Automatically claim** various UCS devices (UCSM, CIMC)
- Use CSV input file for providing **credentials**
- Support claiming to Intersight **SaaS** or Connected/Private **Appliance**

Simplify OS Installation and firmware upgrades

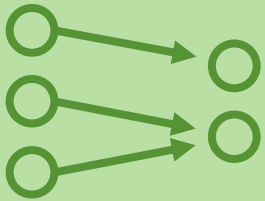
- Use IMM Transition Tool VM as a **Software Repository**
- Allows **hosting of ISO images** or **firmware packages**
- Can be leveraged to easily perform **OS Installation** or **firmware upgrades** on UCS servers

** Roadmap*

Major Features

Identities Preservation

- Conversion/cloning of profiles with **preservation of their identities** (IP, MAC, WWPN, WWNN, UUID)
- User-selectable option in the Transition Settings



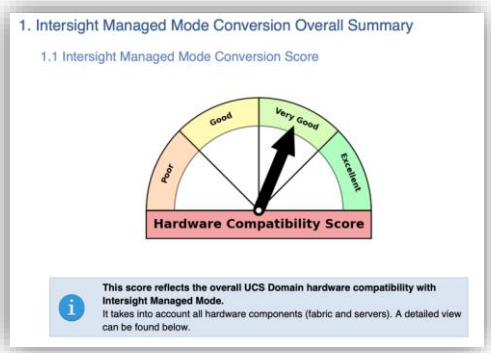
Advanced Organization Mapping

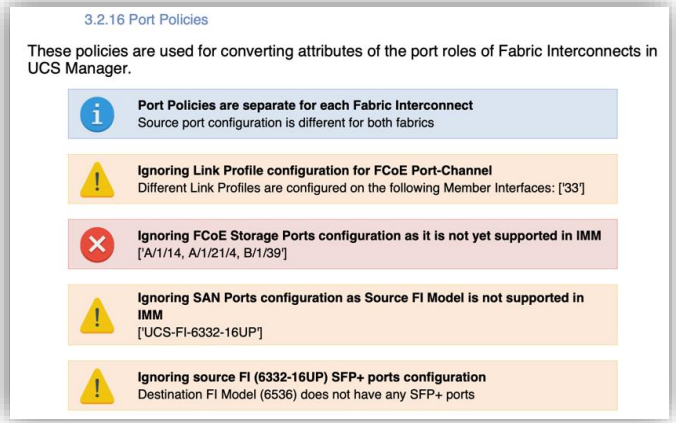
- Gives **more flexibility** to control where converted policies are placed
- Supports **one-to-one** and **many-to-one** mapping

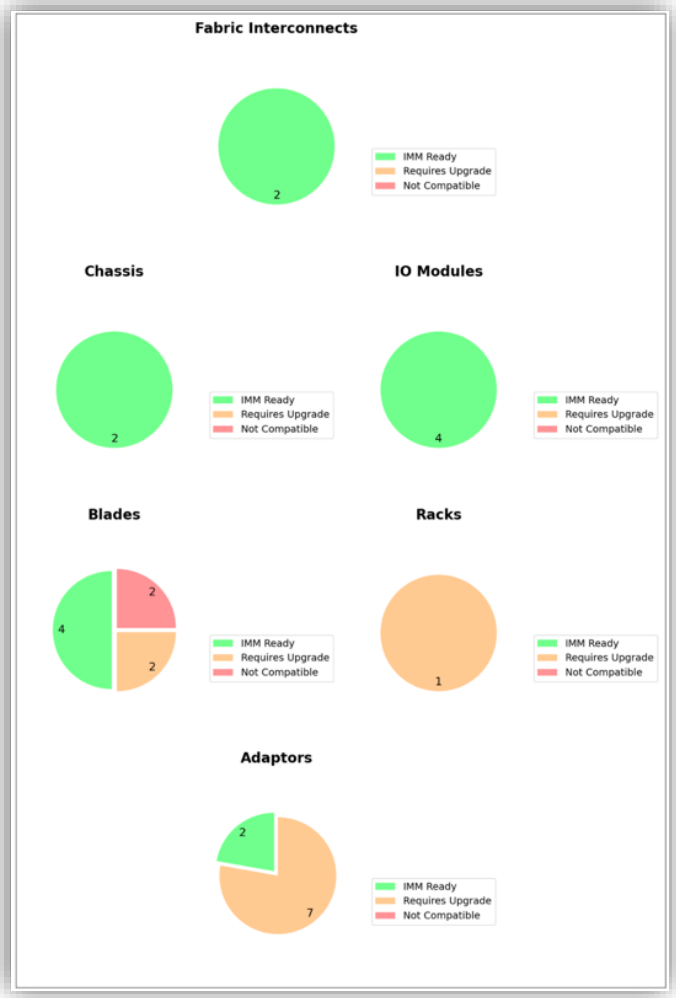
Profile/Template based

- **Selective** conversion/cloning based on profiles/templates
- Only converts/clones **policies attached** to selected profiles/templates

Sample Readiness Report



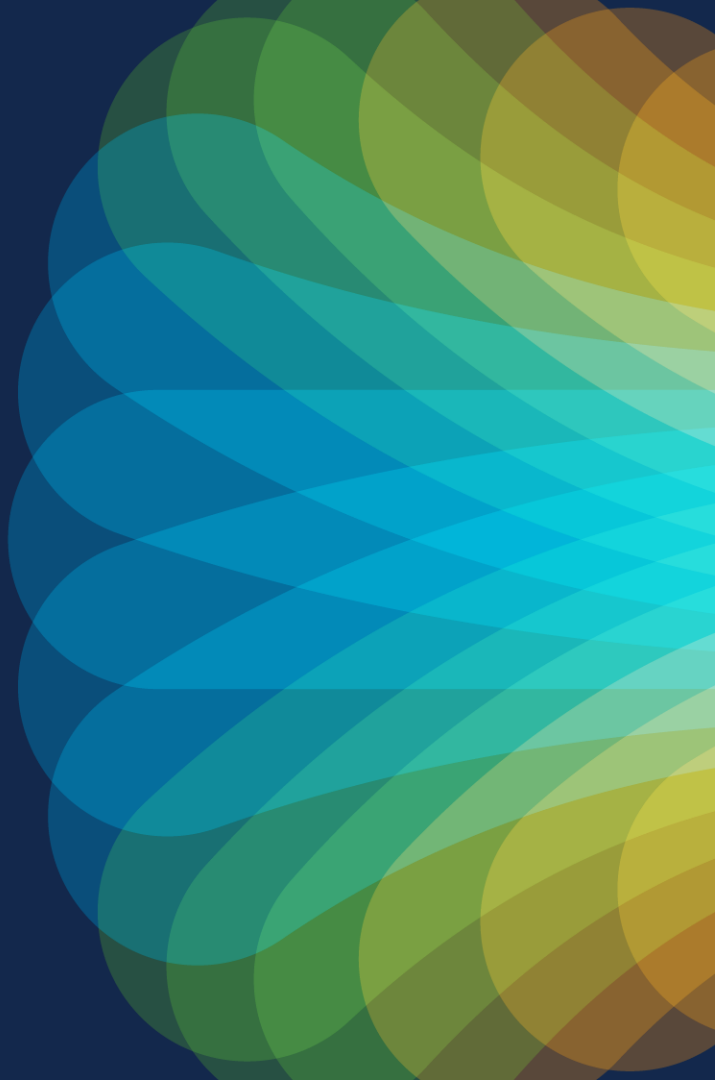




Additional Resources

- IMM Transition Tool demo videos
  - https://www.youtube.com/watch?v=tHJJ-prOrO0
  - https://www.youtube.com/watch?v=Oqmf2CAPxtE
  - https://www.youtube.com/watch?v=duczkclCYrk
- IMM Transition Tool download page
  - https://ucstools.cloudapps.cisco.com/
- IMM Transition Tool Documentation
  - User Guide: https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM-Transition-Tool/User-Guide-4-0/b_imm_transition_tool_user_guide_4_0.html
  - Release Notes: https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM-Transition-Tool/b_imm_tt_rn.html
- Transition CVDs
  - *FlexPod*: https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-manager/transition-a-cisco-ucs-in-flexpod-from-ucs-manager-to-cisco-intersight.html
  - *FlashStack*: https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/transition-flashstack-from-ucs-to-imm-wp.html

Key Takeaways



Summary

- Intersight is much more than UCS Manager/Central
- Same DNA: Policy-based Server & Fabric Management
- Additional features (OS Install, HCL, Advisories)
- Improved Change Control
- Policies everywhere (Domain & Chassis Profiles, natively Multi Domain)
- Modernized Platform (OpenAPI, Redfish, Automated Updates, Feedback, …)
- IMM Transition Tool can help assess readiness and convert config

Intersight Managed Mode is the future of UCS Management

Call to Action

- Adopt Intersight by claiming your existing domains
- Start using IMM in the lab / new deployments
- Consider UCS X-Series as your next-gen server platform
- Generate a Readiness Report with the IMM Transition Tool

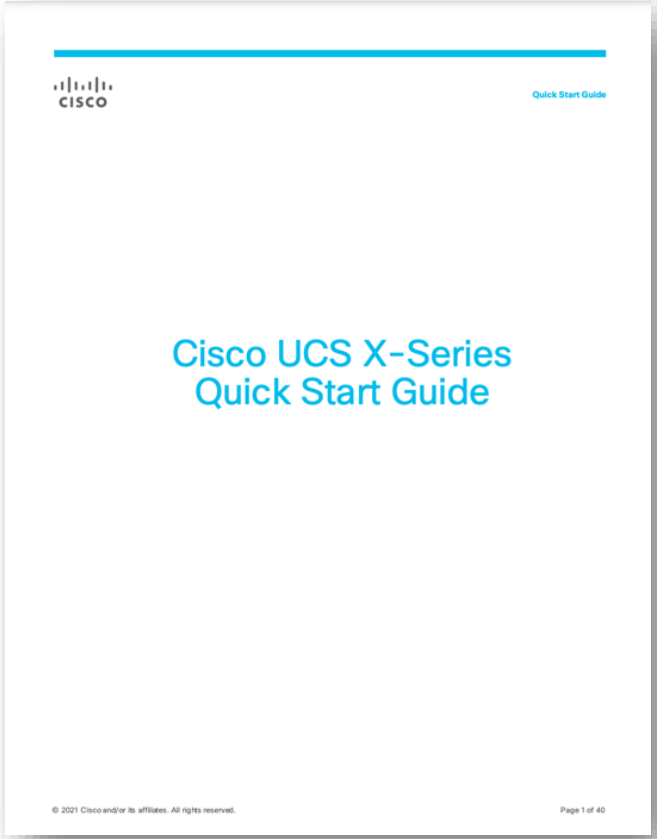
IMM Advantage

- Modernized
- Policies Everywhere
- Simplified
- Safer Operations
- Multi Domain

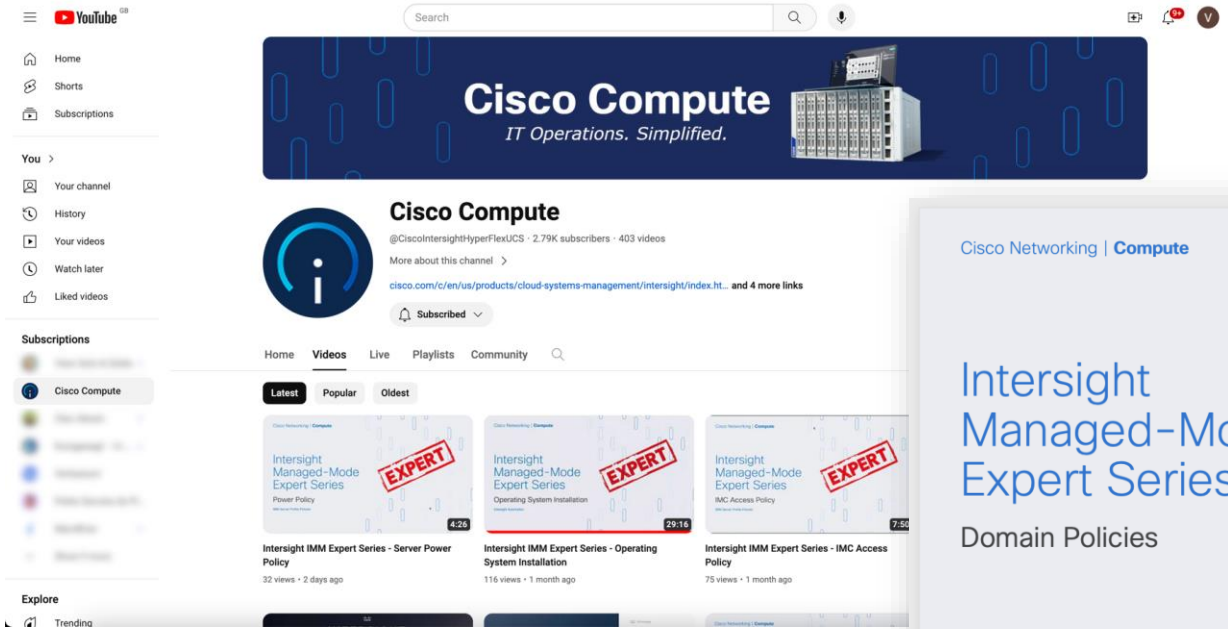
For your reference

X-Series Quick Start Guide

- Complete deployment guide for an X-Series IMM deployment from scratch
- Contains IMM domain, chassis and server configuration steps with all details
- https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-quick-start-guide.html

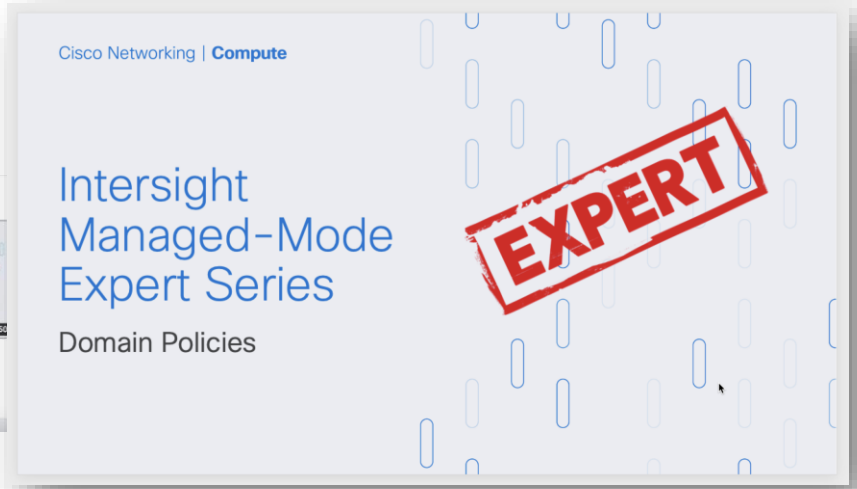


Cisco Compute YouTube Channel



IMM Expert Series

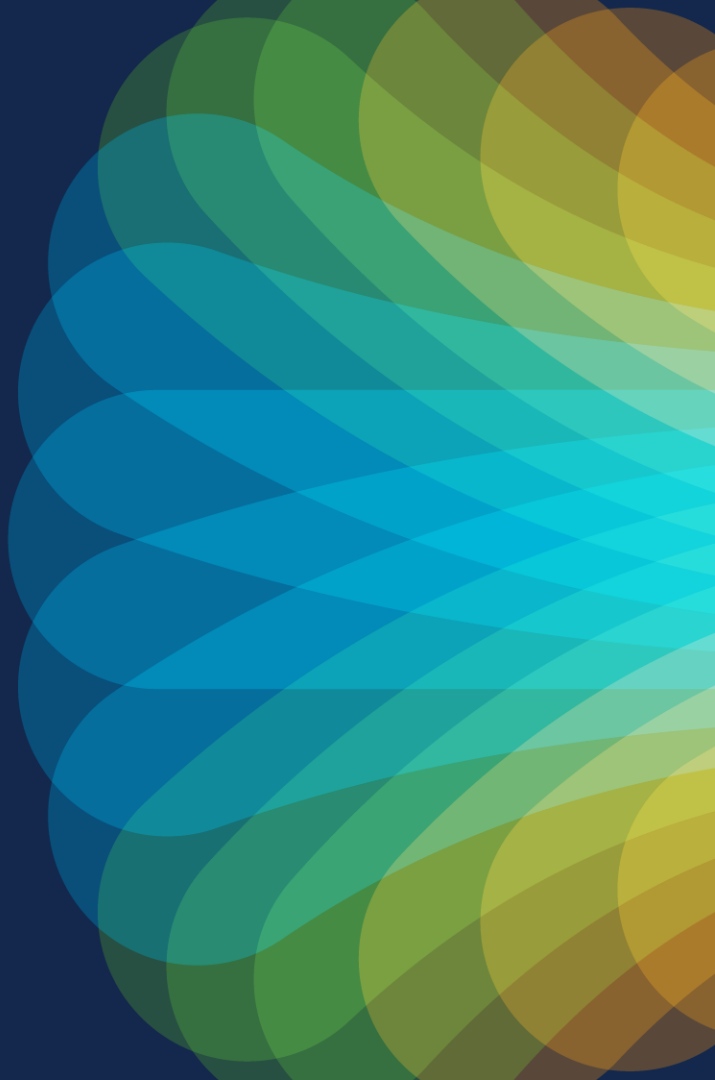
Detailed IMM Training Videos



https://www.youtube.com/@CiscoIntersightHyperFlexUCS

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go