

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

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

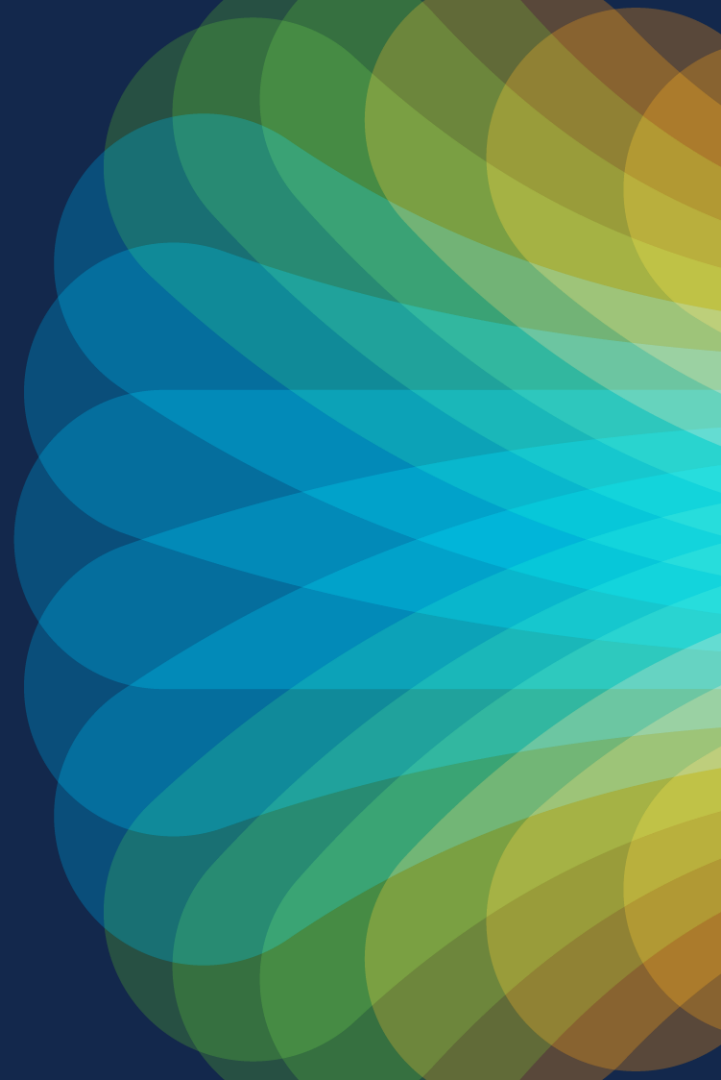
Session non-objectives

- 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



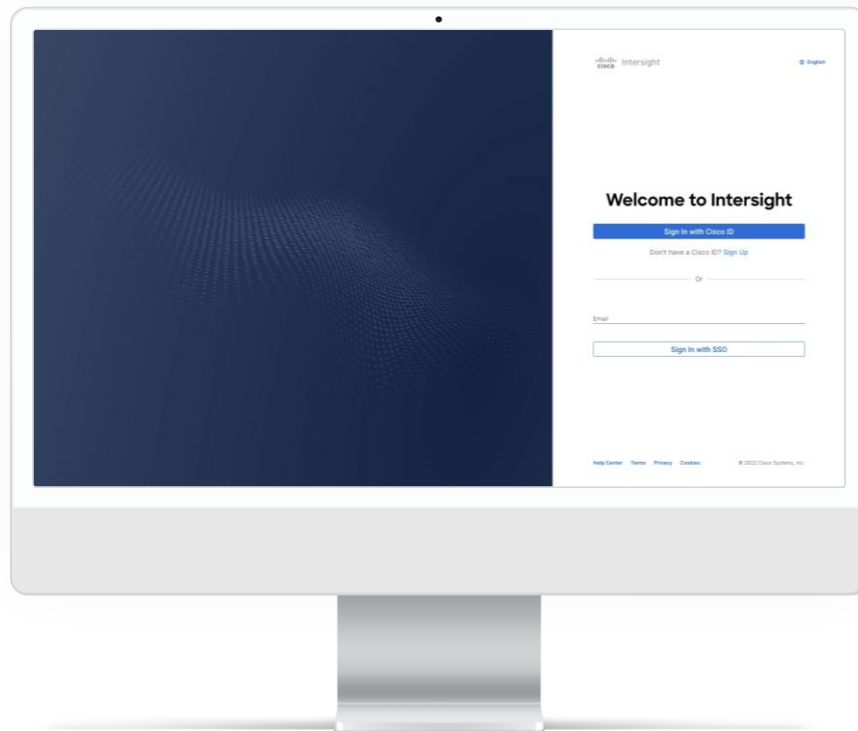
Automate

Networking and computing deployments and configuration

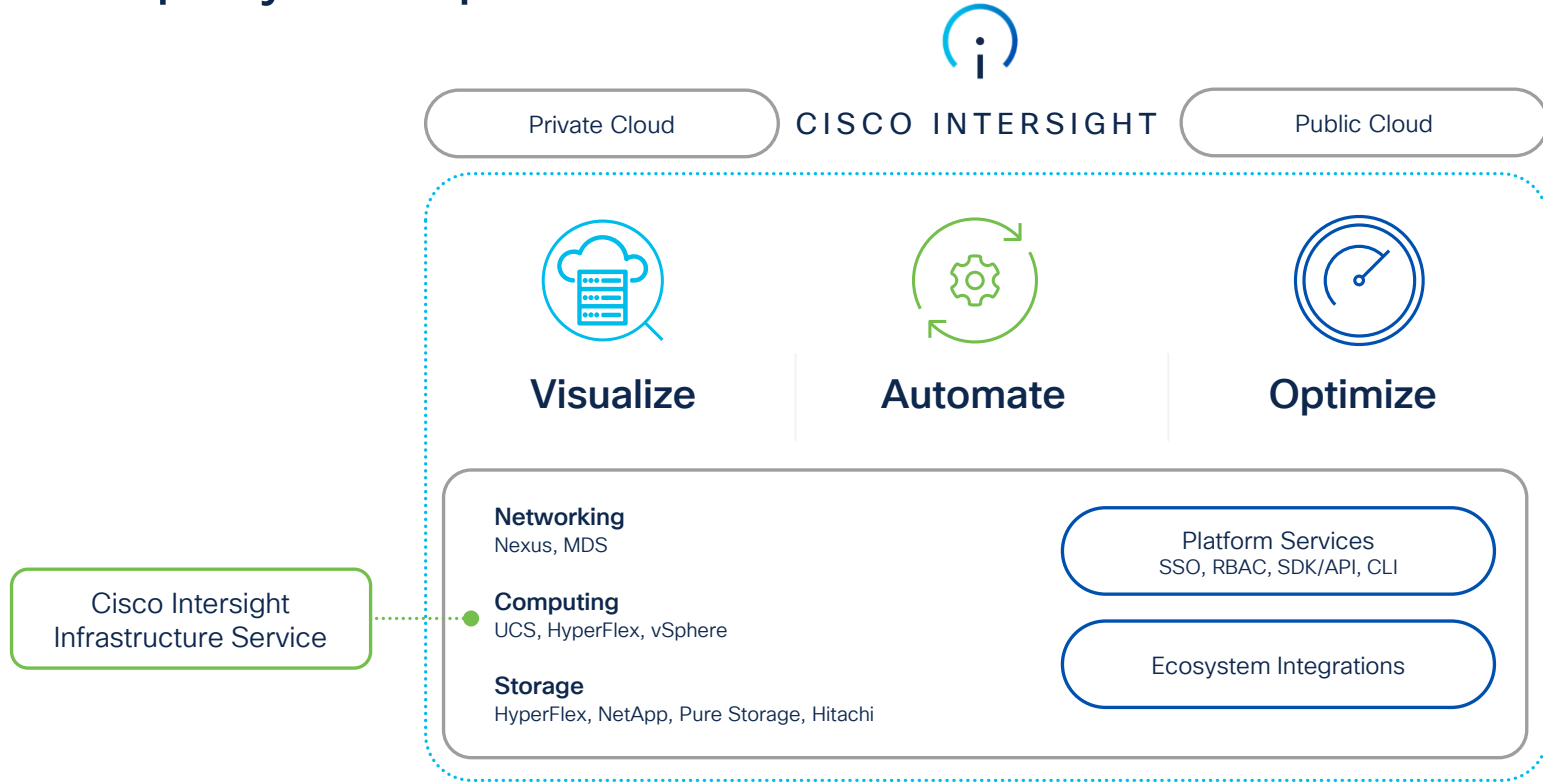


Optimize

Performance, cost, and user experience



Simplify IT Operations



SaaS | Connected Virtual Appliance | Private Virtual Appliance

Cisco Inter sight Infrastructure Service (IIS)



UCSM Provider



Global Policies



Proactive RMAs
Connected TAC



Advisories



Hardware
Compatibility List

Inter sight Infrastructure Service (IIS)

UCS Manager

Fabric Interconnect

Fabric Interconnect

UCS B-Series

UCS C-Series

Traditional UCS domain

IMC

Cisco UCS C-Series

Benefits

Fabric Interconnect

Fabric Interconnect

UCS X-Series

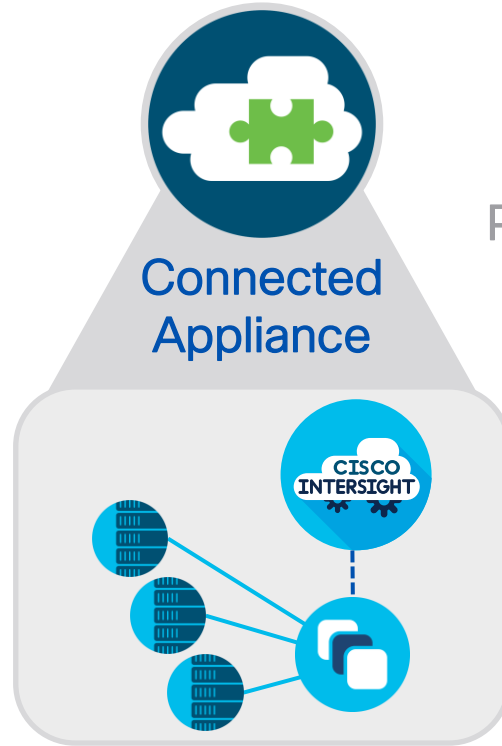
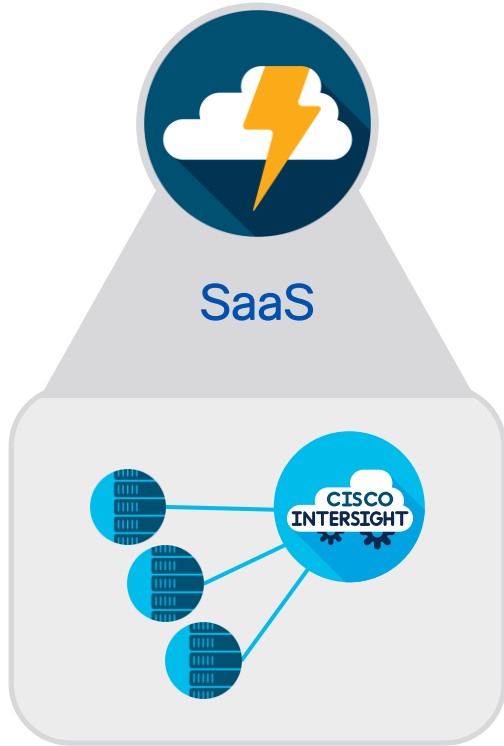
UCS B-Series

UCS C-Series

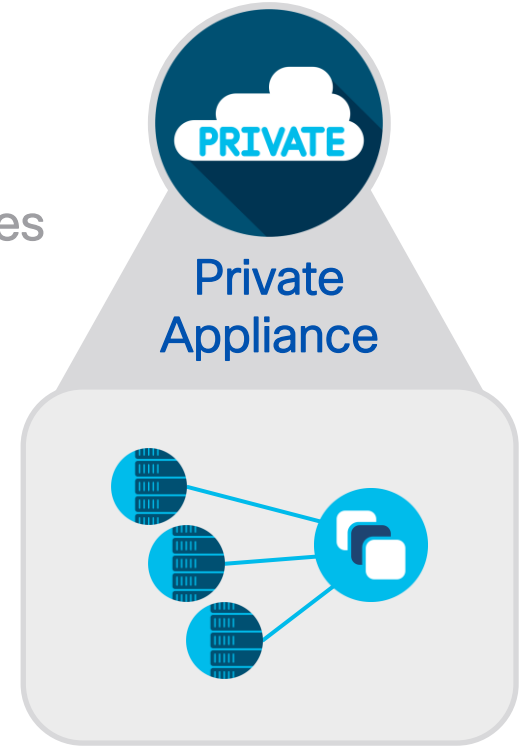
Modernized UCS domain

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

Intersight Deployment Modes

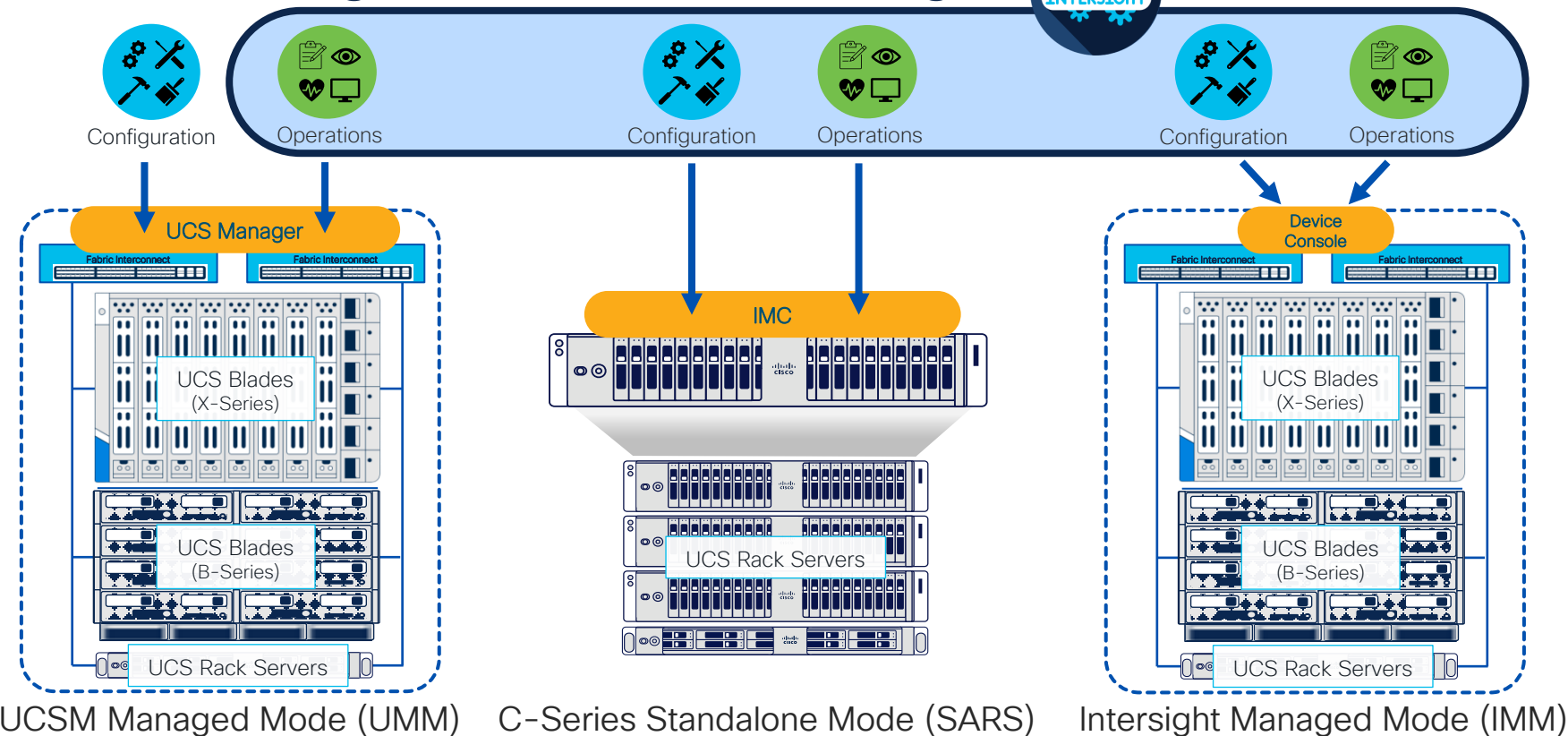


On
Premises



What is Intersight Managed Mode?

UCS Management with Intersight

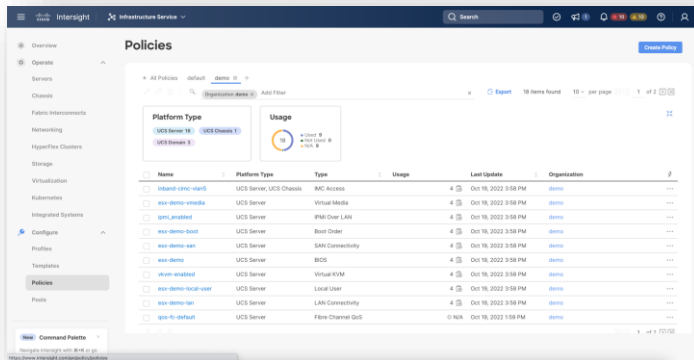
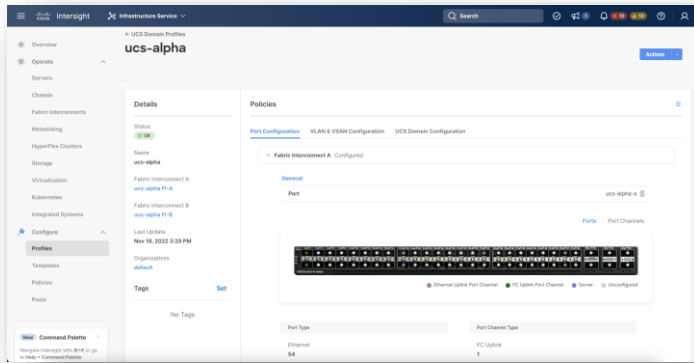


UCSM Managed Mode (UMM)

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)

CISCO *Live!*



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

1  {
2    "@odata.context": "/redfish/v1/$metadata#Thermal.Thermal",
3    "@odata.id": "/redfish/v1/Chassis/FCH22347N7W/Thermal",
4    "@odata.type": "#Thermal.v1_6_2.Thermal",
5    "Description": "Represents the properties for Temperature",
6    "Id": "Thermal",
7    "Name": "Thermal",
8    "Status": {
9      "Health": "OK",
10     "State": "Enabled"
11   },
12   "Temperatures": [
13     {
14       "@odata.id": "/redfish/v1/Chassis/FCH22347N7W/Thermal#/Temperatures/0",
15       "MemberId": "0",
16       "Name": "TEMP_SENS_FRONT",
17       "PhysicalContext": "Front",
18       "ReadingCelsius": 22,
19       "Status": {
20         "Health": "OK",
21         "State": "Enabled"
22       },
23       "UpperThresholdCritical": 75,
24       "UpperThresholdFatal": 85
25     },
26     {
27       "@odata.id": "/redfish/v1/Chassis/FCH22347N7W/Thermal#/Temperatures/1",
28       "MemberId": "1",
29       "Name": "TEMP_SENS_REAR",
30       "PhysicalContext": "Back",
31       "ReadingCelsius": 33,
32       "Status": {
33         "Health": "OK",
34         "State": "Enabled"
35       },
36       "UpperThresholdCritical": 75,
37       "UpperThresholdFatal": 85
38     }
39   ]
40 }
```


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

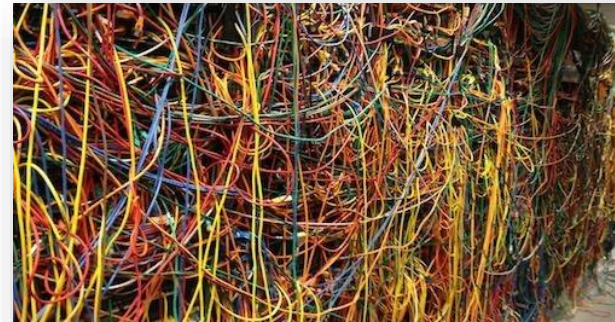
- **Configuration consistency** for domains
- **Decoupling** of firmware / software features
- **Improved Change Control** with Assign/Deploy steps
- **Better policy scale** – not limited by FI resources

When should you start using IMM?

Hardware refresh



New domain deployment / Greenfield



How to use Intersight Managed Mode?

Setting up a domain in Intersight Managed 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):
```

Management mode



Device Console – System Information

The screenshot shows the Cisco Device Console interface for a device named 'ucs-bravo'. The top navigation bar includes the Cisco logo, the title 'DEVICE CONSOLE', and the device name. Below this, a secondary navigation bar contains four tabs: 'SYSTEM INFORMATION', 'DEVICE CONNECTOR', 'INVENTORY', and 'DIAGNOSTIC DATA'. The 'SYSTEM INFORMATION' tab is selected and highlighted with a red box. The main content area is divided into two columns, each representing a Fabric Interconnect. The left column is for 'Fabric Interconnect A (Primary)' and the right column is for 'Fabric Interconnect B (Subordinate)'. Each column contains a table of system information, including Health status, Management IPs, Model, Serial number, Firmware Version, Available Memory, and Total Memory. Both interconnects show a 'Healthy' status and identical hardware specifications.

Fabric Interconnect A (Primary)		Fabric Interconnect B (Subordinate)	
Health	Healthy	Health	Healthy
Management IPs	10.60.5.31	Management IPs	10.60.5.32
Model	UCS-FI-6454	Model	UCS-FI-6454
Serial	FDO23290UBT	Serial	FDO2327063Z
Firmware Version	9.3(5)I42(3b)	Firmware Version	9.3(5)I42(3b)
Available Memory	50.38 MiB	Available Memory	50.38 MiB
Total Memory	62.76 MiB	Total Memory	62.76 MiB

Device Console – Device Connector


The screenshot displays the Cisco Device Console interface for a device named 'ucs-bravo'. The top navigation bar includes 'SYSTEM INFORMATION', 'DEVICE CONNECTOR' (which is the active tab), 'INVENTORY', and 'DIAGNOSTIC DATA'. Below the navigation bar, a descriptive text states: 'The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit [Help Center](#)'.

The main content area is titled 'Device Connector' and features a 'Settings' gear icon and a 'Refresh' circular arrow icon. A toggle switch for 'ACCESS MODE' is set to 'ALLOW CONTROL'. A diagram illustrates the connection flow: 'Device Connector' (represented by a monitor icon) connects via a dotted line to 'Internet' (represented by a globe icon), which then connects via another dotted line to 'Intersight' (represented by a cloud icon). Below this diagram, a green bar with a checkmark and the text 'Claimed' indicates the device's status.

On the right side, the 'Device ID' is displayed as 'FD023290UBT&FD02327063Z' with a copy icon. Below this, the 'Claimed to Account' section shows a redacted account name with an information icon and an 'Unclaim' button.

The bottom left corner of the interface shows the version number '1.0.11-4206'.

Device Console - Inventory

 **DEVICE CONSOLE** | ucs-bravo

SYSTEM INFORMATION

DEVICE CONNECTOR

INVENTORY

DIAGNOSTIC DATA

Servers

Chassis
















Fabric Extender

5 items found

10 per page

1 of 1

⚙️

Name	Health	Status	PID	Serial	User Label	⚡
 ucs-bravo-1-1	 Critical	 Active	UCSB-B200-M5	FCH22347N7W	-	...
 ucs-bravo-1-3	 Healthy	 Active	UCSB-B200-M5	FCH223570ND	-	...
 ucs-bravo-1-4	 Healthy	 Active	UCSB-B200-M5	FCH223570BY	-	...
 ucs-bravo-2-1	 Healthy	 Active	UCSB-B200-M5	FCH22347M5Q	-	...
 ucs-bravo-2-2	 Healthy	 Active	UCSB-B200-M5	FCH22347N5N	-	...

Power On

Turn On Locator

Launch KVM

Launch API Explorer

Generate Tech Support Bundle

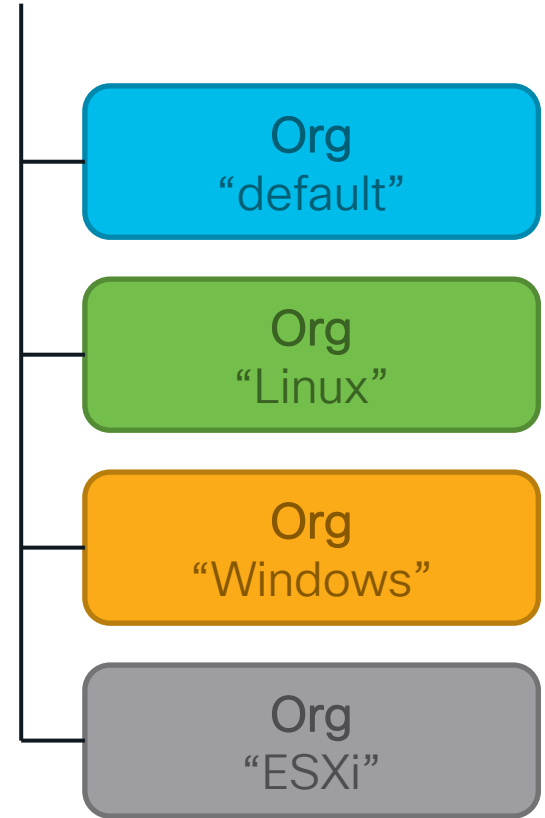
And... that's it!

Everything else is done on



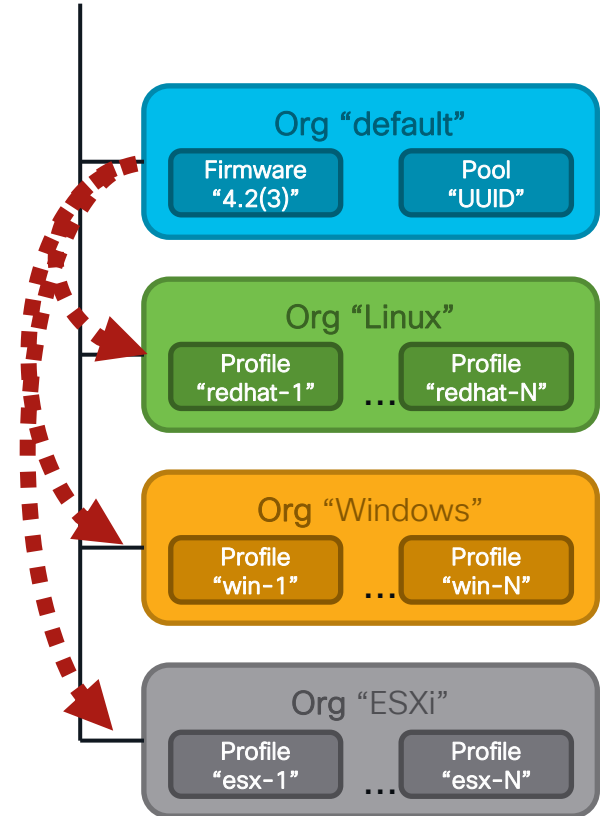
Organizations in Intersight

- **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



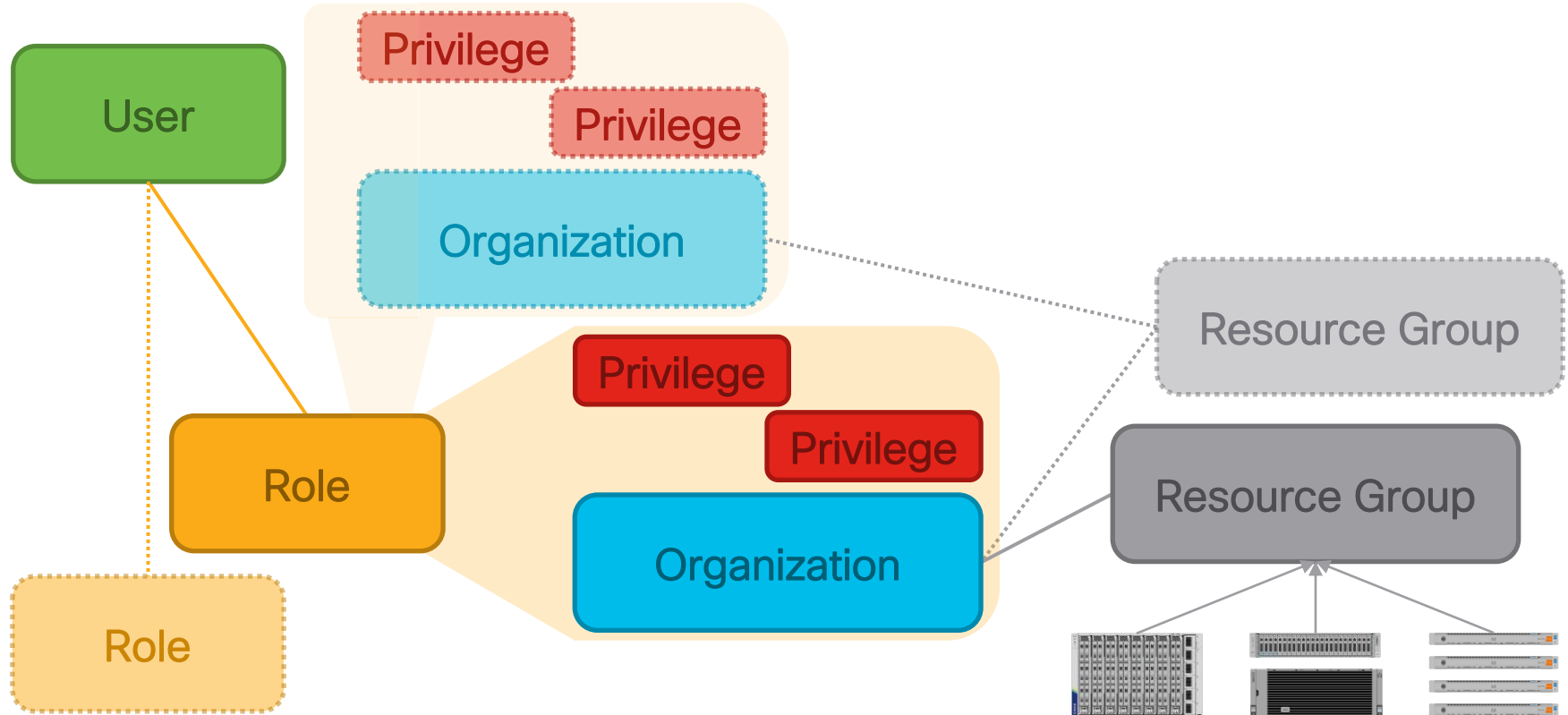
Organization Sharing

- 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



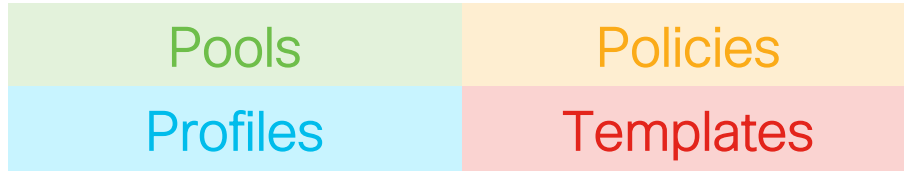
<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/imm-con-sharing-across-organization-cloning-wp.html>

Role-Based Access Control with Intersight



Policy-based Model

- **Similar** to UCS Manager / Central



- **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



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**

IMM Policies

Key differences with UCS Manager/Central



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

IMM Profiles & Templates

Key differences with UCS Manager/Central



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**



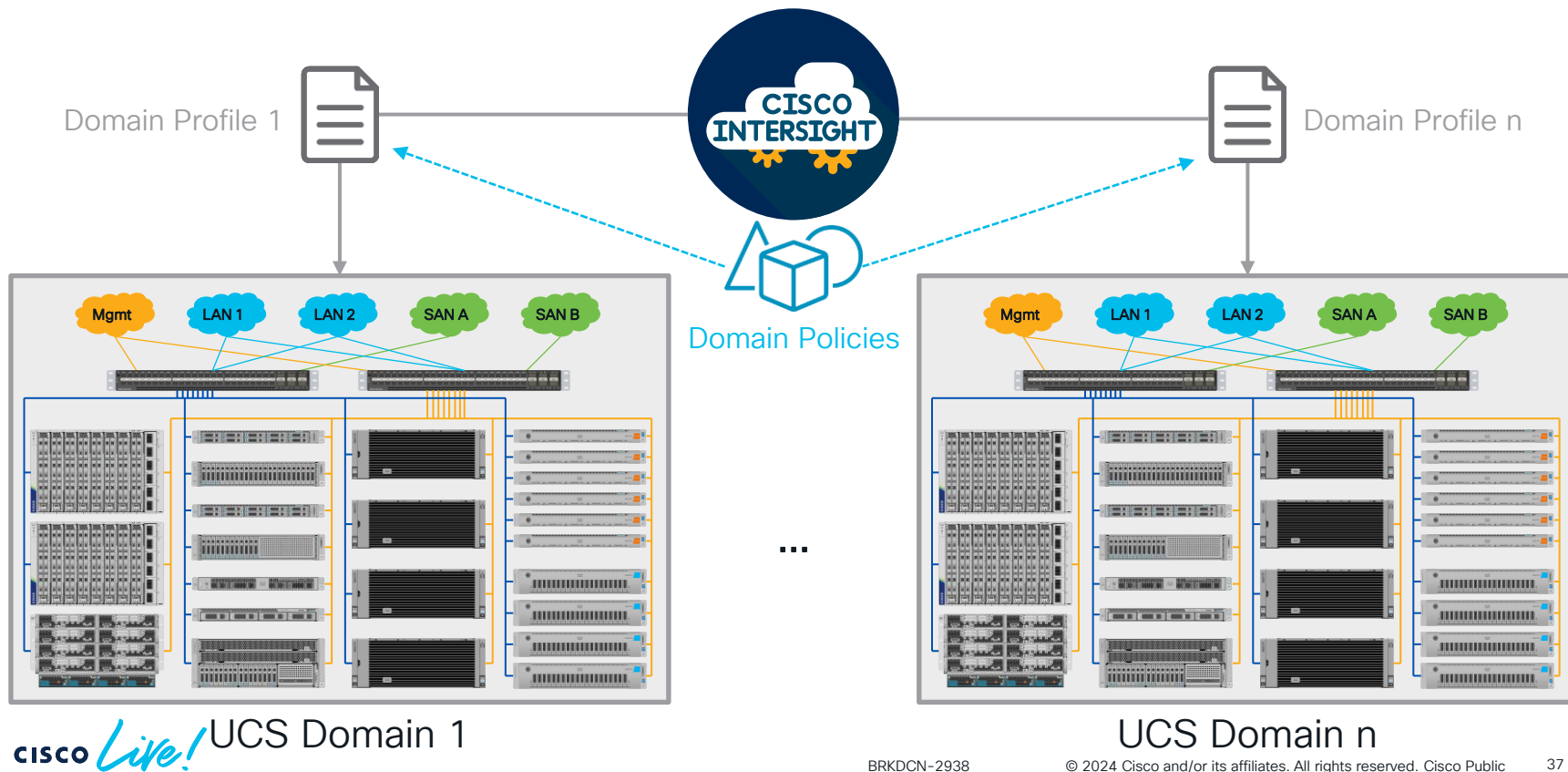
Changed

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

Managing UCS Domains

UCS Domain Profiles

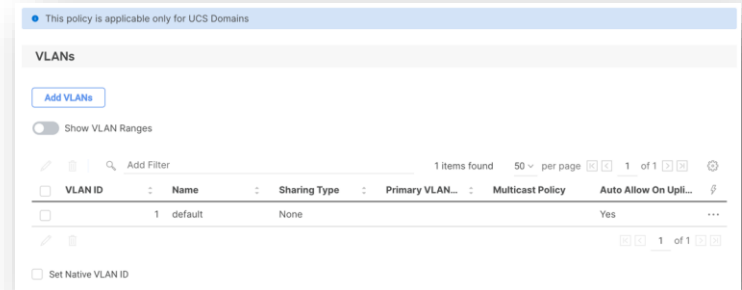
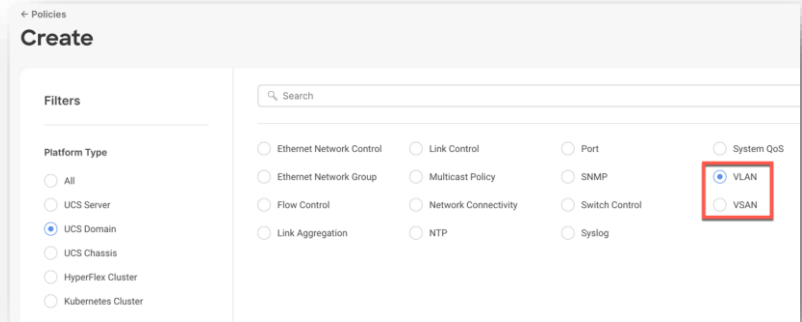
Policy-based configuration of the UCS fabric



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

Port Roles
Configure port roles to define the traffic type carried through a unified port connection.

[Port Roles](#) [Port Channels](#) [Pin Groups](#)

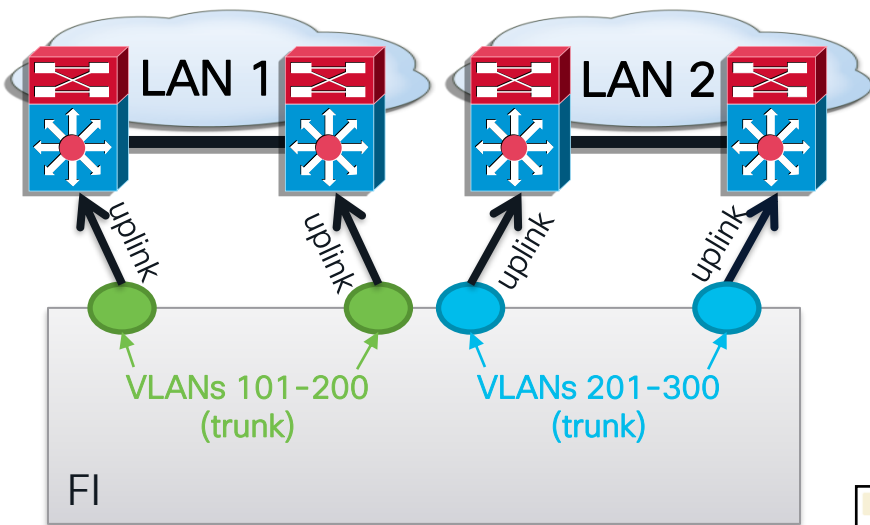
[Configure](#) Selected Ports -



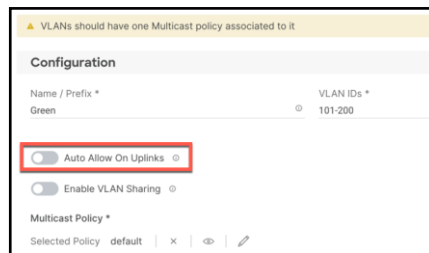
[Export](#)

<input type="checkbox"/>	Name	Type	Role	Connected Dev...	Device Number	Port Channel	Mode
<input type="checkbox"/>	port 1	FC	FC Uplink Port Cl			FC Uplink Port Cl	
<input type="checkbox"/>	port 2	FC	FC Uplink Port Cl			FC Uplink Port Cl	
<input type="checkbox"/>	port 3	FC	Unconfigured			-	

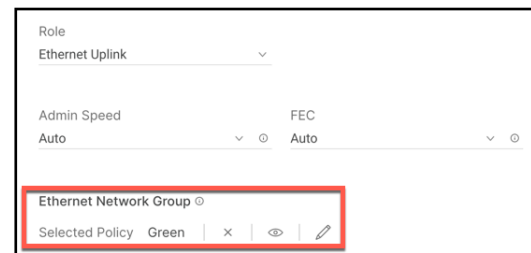
Disjoint Layer 2 configuration in IMM



- 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

Switching Mode

Ethernet ☐ FC ☐

☒ End Host ☐ Switch ☒ End Host ☐ Switch

VLAN Port Count

☐ Enable VLAN Port Count Optimization

System Reserved VLANs

By default, the reserved VLAN Start ID is 3915 and a range of 128 VLANs starting from this ID cannot be used in any VLAN policy. To change the default range, configure the Reserved VLAN Start ID and Reserved VLAN End ID.

Reserved VLAN Start ID * 3915 Reserved VLAN End ID 4042

2 x 3915

MAC Address Table Aging Time

Default Custom Never

This option sets the default MAC address aging time to 14500 seconds for the Default mode.

Unidirectional Link Detection (UDLD) Global Settings

Message Interval 15 7 - 90

Recovery Action ☒ None ☐ Reset

Fabric port-channel vHBA

☐ Enable the fabric port-channel vHBA reset

UCS Domain Profiles

System Settings Policies

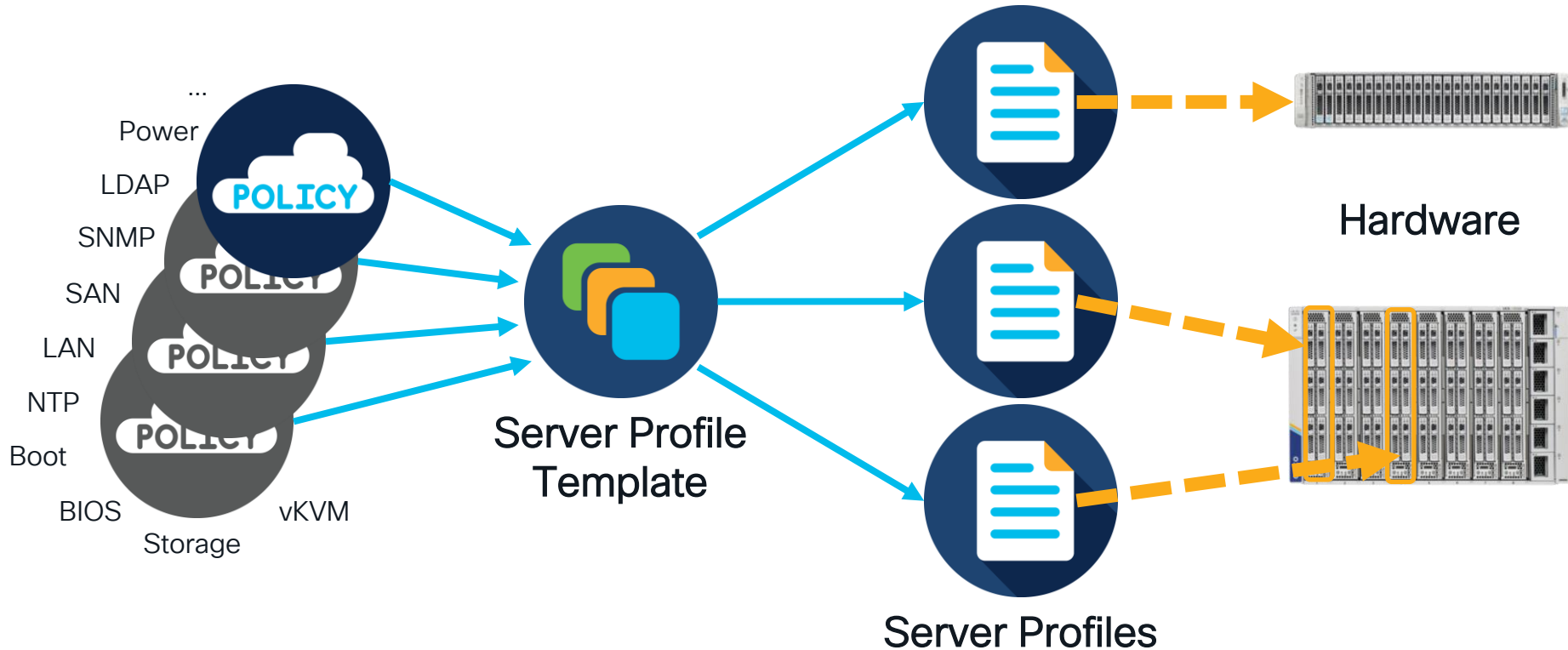
- These policies define the Fabric Interconnects configuration
Similar to Domain Group settings in UCS Central.
 - **Network Connectivity Policy**: Defines DNS settings
 - **NTP Policy**: NTP & Timezone settings
 - **System QoS Policy**: QoS classes settings
 - **Switch Control Policy**: VLAN compression, 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)

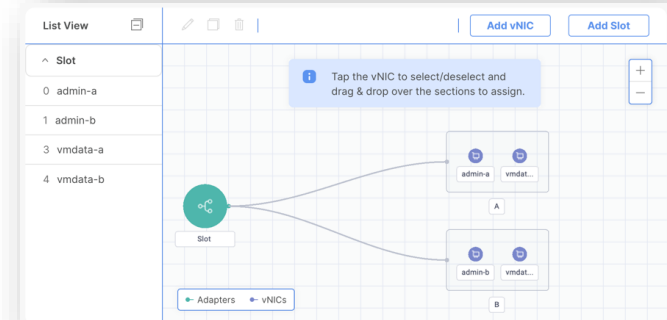
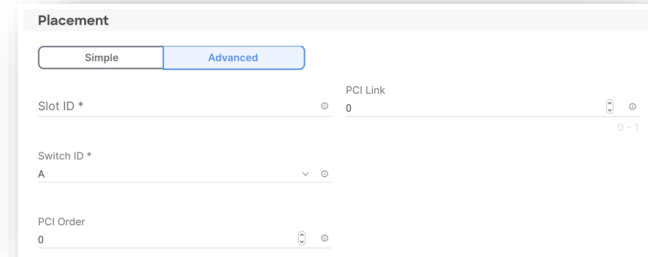
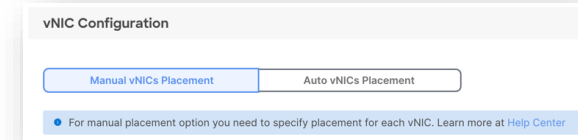
Storage Policy: All in One!

- **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

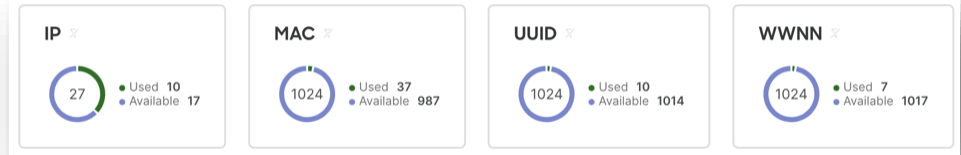
The screenshot shows a web-based configuration interface for storage policy. At the top, there are three tabs: 'All Platforms' (selected and highlighted with a red box), 'UCS Server (Standalone)', and 'UCS Server (FI-Attached)'. Below the tabs is a 'General Configuration' section. It includes a toggle for 'Use JBOD drives for Virtual Drive creation' (disabled), and two dropdown menus for 'Unused Disks State' (set to 'No Change') and 'Default Drive State' (set to 'Unconfigured Good'). Below this is an 'M.2 RAID Configuration' section with three rows, each with a toggle set to 'Enable': 'M.2 RAID Configuration', 'MRAID/RAID Controller Configuration' (highlighted with a red box), and 'MRAID/RAID Single Drive RAID0 Configuration'. At the bottom, there are 'Cancel', 'Back', and 'Create' buttons.

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, WWP, 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 identifiers 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**

Select LAN Connectivity

Policy "lan_esxi" will be changed to "lan_esxi_2".
Changing the LAN Connectivity Policy may result in change of identities "MAC, IQN, iSCSI Boot IP" if the pool ranges configured in the new policy do not include the existing identities.

8 items found 10 per page 1 of 1

lan_esxi	lan_esxi_2
data1	-
data2	-
iscsi1	iscsi1
iscsi2	iscsi2
mgmt1	mgmt1
mgmt2	mgmt2
vmotion1	vmotion1
vmotion2	vmotion2

1 of 1

CancelSelect

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

The screenshot displays the IMC configuration interface. At the top, the 'In-Band Configuration' section is highlighted with a red box and has a toggle switch set to 'Enabled'. Below this, the 'VLAN ID' is set to 105, with a range of 4 - 4093. The 'IPv4 address configuration' checkbox is checked, and the 'IPv6 address configuration' checkbox is unchecked. The 'IP Pool' is set to 'cimc-bravo'. At the bottom, the 'Out-Of-Band Configuration' section is also highlighted with a red box and has a toggle switch set to 'Enabled'.

* In roadmap

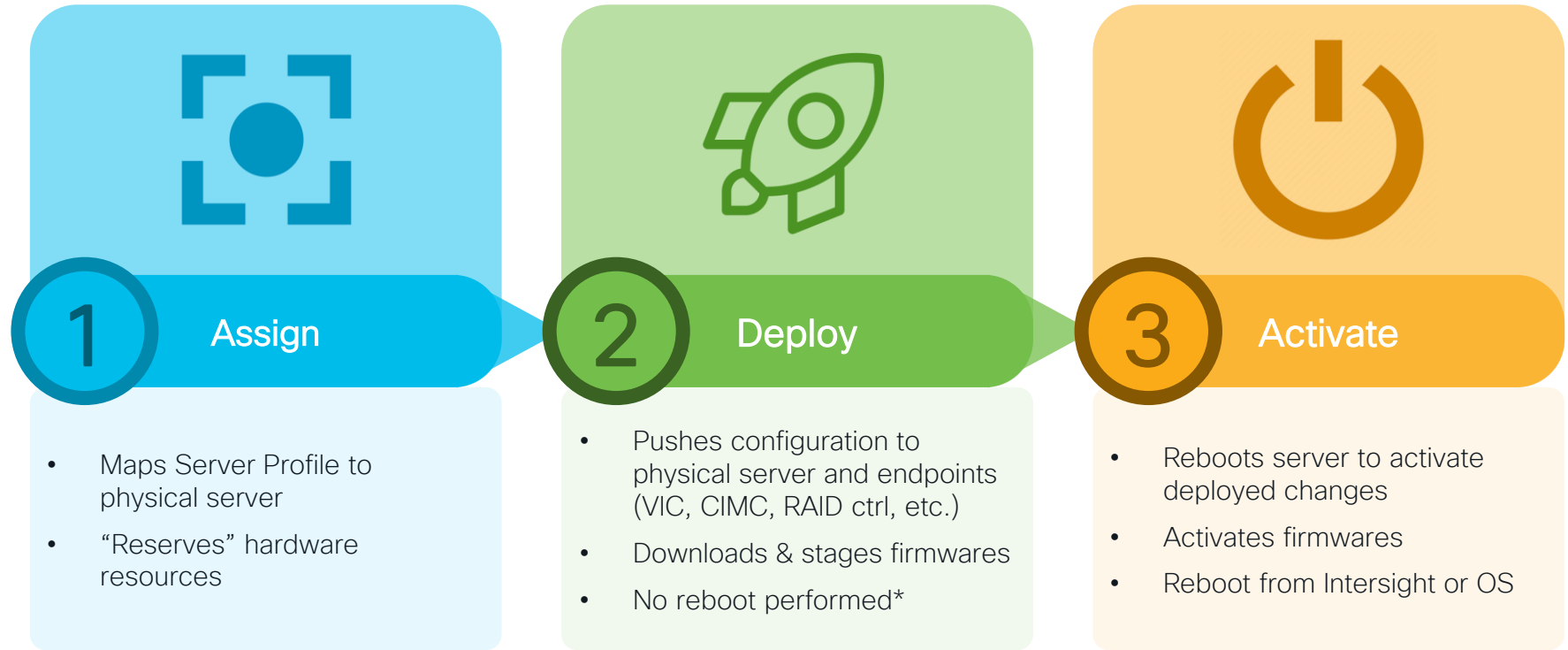
Firmware Policy

- 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

The screenshot shows the 'Advanced Mode' configuration for a Firmware Policy. At the top, there is a toggle switch for 'Advanced Mode' which is turned on. Below this is a blue information banner that reads: 'You can add a maximum of six server models.' The main configuration area is a table with two columns: 'Server Model *' and 'Firmware Version *'. The first row shows 'UCSX-210C-M7' and '5.2(0.230092)'. The second row shows 'UCSB-B200-M5' and '4.2(3g)'. Each row has a dropdown arrow, a refresh icon, and a trash icon. A plus sign is visible at the bottom right of the table, indicating the ability to add more models.

Server Model *	Firmware Version *
UCSX-210C-M7	5.2(0.230092)
UCSB-B200-M5	4.2(3g)

Improved change control



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**

Name	Status
esx-demo-1	OK
esx-demo-2	Inconsistent
esx-demo-3	Not Deployed

Details

Status
Inconsistent

Inconsistency Reason

Pending Changes

Name
esx-demo-1

User Label
-

Target Platform
UCS Server (FI-Attached)

Template Name

Configuration

General Identifiers Connectivity

Inconsistency Reason

Impact Type

1 Pending Changes 1 Activate Requires Reboot 1

BIOS

Firmware

IMC Access Policy

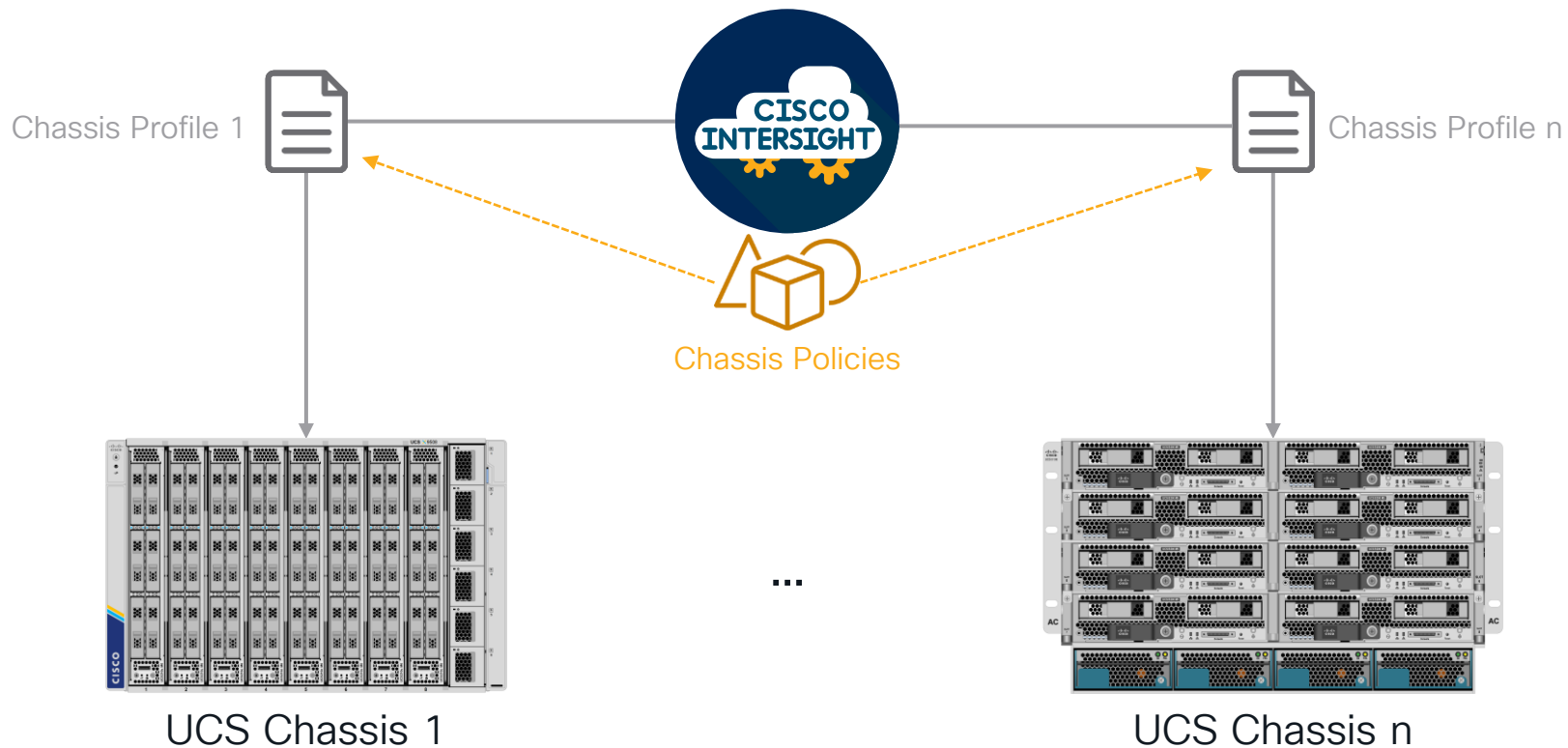
LAN Connectivity Activate Requires Reboot Changed View Changes

View Changes LAN Connectivity		
Display	Changes Only	Last Deployed Settings
IQN Pool	iqn-demo	-
Enable Azure Stack Host QoS	No	Yes

Managing UCS Chassis

UCS Chassis Profiles

Policy-based configuration of the UCS chassis



UCS Chassis Profiles

Chassis Policies

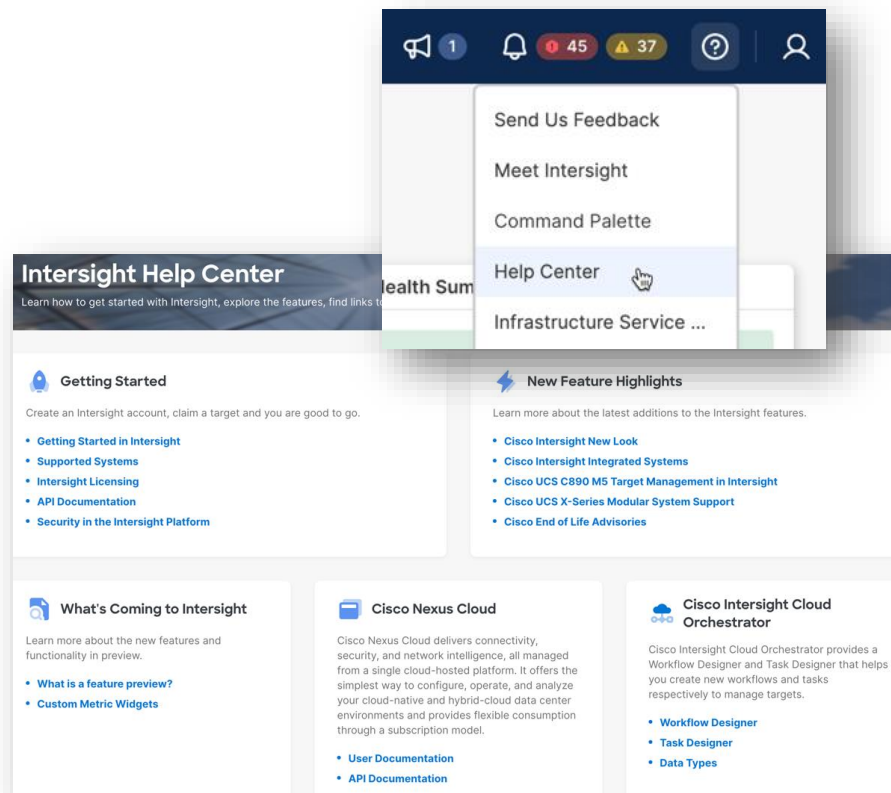


- **Chassis policies** – to support per-chassis settings (different from UCSM)
 - IMC Access Policy: Defines VLAN/IP address for chassis CMC (used by SNMP)
 - Power Policy: Configures power management (redundancy & power budget)
 - SNMP Policy: SNMP settings
 - Thermal Policy: Fan control settings
- 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

Clone Details

Policy Name *
esx-demo_CLONE

Organization *
default
demo
test-org

Description

← Requests
Clone BIOS Policy

Details

Status
Success

Name
Clone BIOS Policy

Execution Flow

- Process Clone Result
- Check Clone Status
- Start Clone Processing

Attached Policy and Pool Behaviour

☐ Use policies and pools in the destination organization with the same name, clone if not found

☒ Clone all policies and pools into the destination organization

Suffix Name *
Required

Server Assignment

Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later

Number of Clones *
1

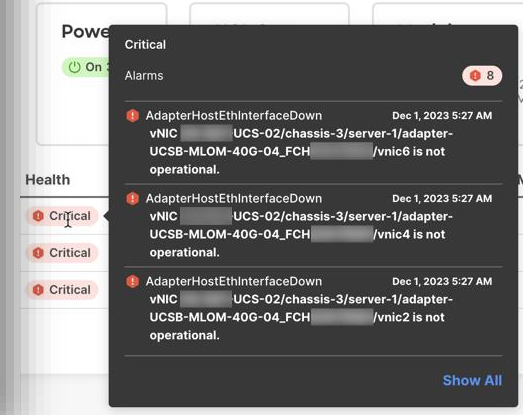
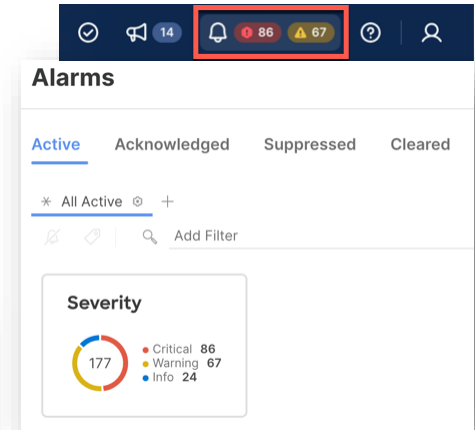
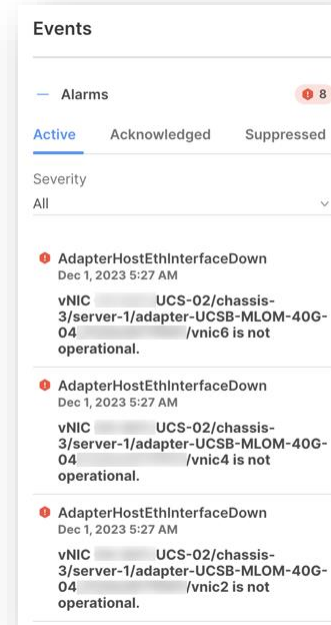
Where is my FSM?

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

The screenshot shows the Cisco Lifecycle Services (CLS) interface. The top navigation bar has a red box around the 'Requests' icon. The main content area displays a table of requests with columns: Name, Status, Initiator, Target Type, Target Name, Start Time, Duration, ID, and Execution Type. A summary card shows 69 items found, 12 per page, and 1 of 6 pages. The table lists requests like 'Chassis Inventory' and 'Chassis Discovery'. A detailed view for 'Blade Discovery' is shown on the right, including a 'Details' section with fields like ID, Target Type, Target Name, Source Type, Source Name, Initiator, Start Time, and End Time, and an 'Execution Flow' section listing steps like 'Sync Server View Inventory', 'Inventory Server Power', 'Power Off Server', etc.

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

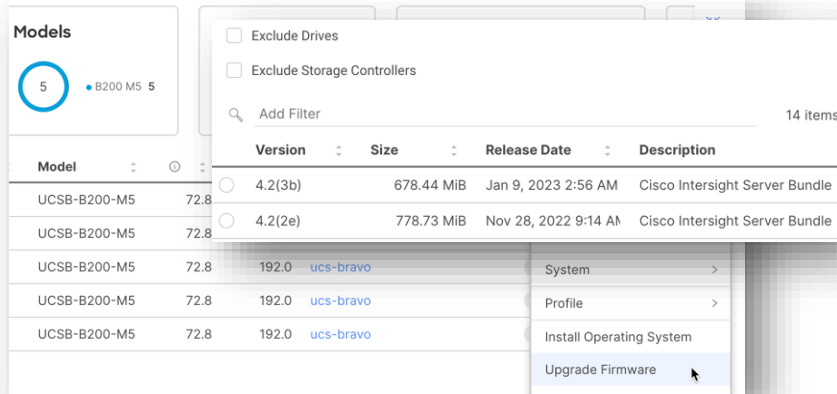
- Temporarily mutes alarms notifications
- Useful during maintenance window or other planned activities (upgrades, etc.)
- Suppressed alarms can still be seen under the “Suppressed” tab in the Alarms drawer
- Applicable at physical server level

The image shows two screenshots from a management interface. The top screenshot is a dialog box titled "Start Alarm Suppression". It contains the text: "All maintenance alarms for the server 'ucs-bravo-1-1' will be suppressed. Refer to the [Help Center](#) for details about the specific alarms that will be suppressed." Below this is a "Description" field with the value "ESXi + firmware upgrade". At the bottom are "Cancel" and "Start" buttons. To the right of the dialog is a vertical menu with options: Power, System, Profile, Install Operating System, Upgrade Firmware, Launch vKVM, Launch Tunneled vKVM, Start Alarm Suppression (highlighted with a mouse cursor), Open TAC Case, Set License Tier, and Collect Tech Support Bundle. The bottom screenshot shows the "Alarms" drawer. It has tabs for Active, Acknowledged, Suppressed (selected), and Cleared. The "Suppressed" tab shows a list of alarms, all with a "Healthy" status. A tooltip is visible over the "Healthy" status of the second alarm, "ucs-bravo-1-1". The tooltip text reads: "Healthy", "Alarm Suppression started Jan 25, 10:05 PM with the description 'ESXi + firmware upgrade'. For more information, see [Help Center](#).", "Alarms" (with a count of 1), and "SuppressionEnabled a few seconds ago", "Suppression is enabled on ucs-bravo/chassis-11/redfish/v1/Systems/FCH22347N7W for reason: ESXi + ...".

Managing Firmwares

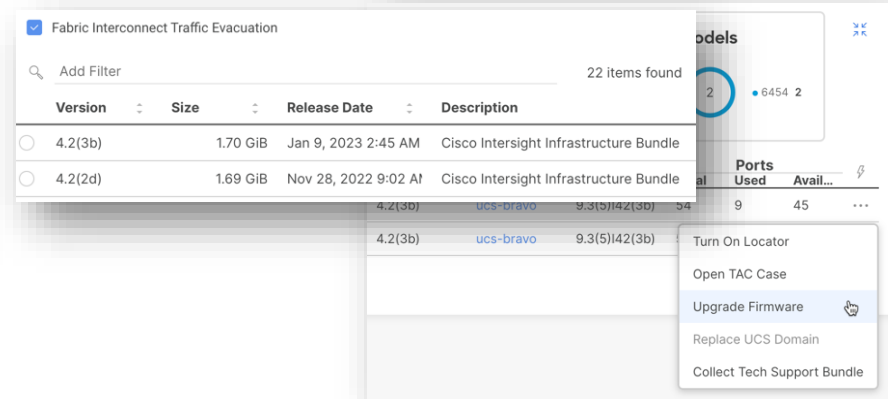
UCS Servers

- 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

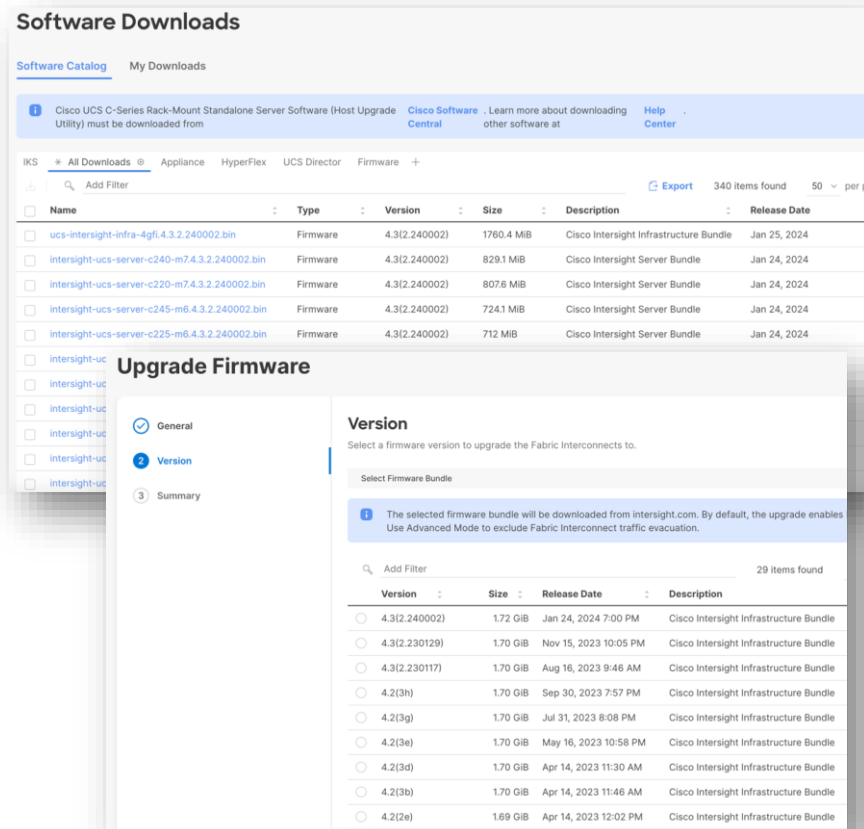
- Similar to UCS Manager Auto-Install
- User acknowledgement for each FI reboot
- Integration of fabric Traffic Evacuation



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



Software Downloads

Software Catalog My Downloads

1 Cisco UCS C-Series Rack-Mount Standalone Server Software (Host Upgrade Utility) must be downloaded from Cisco Software Central. Learn more about downloading other software at Help Center

IKS All Downloads Appliance HyperFlex UCS Director Firmware +

Add Filter Export 340 items found 50 per page

Name	Type	Version	Size	Description	Release Date
ucs-intersight-infra-4gfi.4.3.2.240002.bin	Firmware	4.3(2.240002)	1760.4 MiB	Cisco Intersight Infrastructure Bundle	Jan 25, 2024
intersight-ucs-server-c240-m7.4.3.2.240002.bin	Firmware	4.3(2.240002)	829.1 MiB	Cisco Intersight Server Bundle	Jan 24, 2024
intersight-ucs-server-c220-m7.4.3.2.240002.bin	Firmware	4.3(2.240002)	807.6 MiB	Cisco Intersight Server Bundle	Jan 24, 2024
intersight-ucs-server-c245-m6.4.3.2.240002.bin	Firmware	4.3(2.240002)	724.1 MiB	Cisco Intersight Server Bundle	Jan 24, 2024
intersight-ucs-server-c225-m6.4.3.2.240002.bin	Firmware	4.3(2.240002)	712 MiB	Cisco Intersight Server Bundle	Jan 24, 2024

Upgrade Firmware

General Version Summary

Version

Select a firmware version to upgrade the Fabric Interconnects to.

Select Firmware Bundle

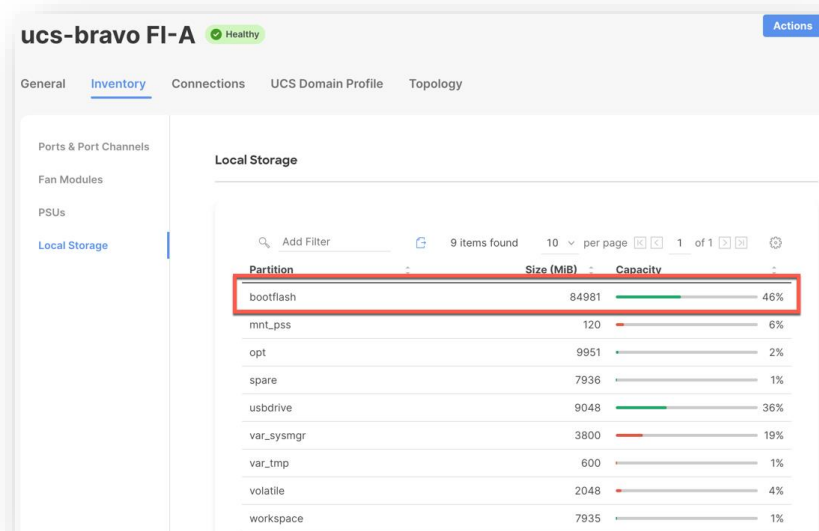
The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.

Add Filter 29 items found

Version	Size	Release Date	Description
4.3(2.240002)	1.72 GiB	Jan 24, 2024 7:00 PM	Cisco Intersight Infrastructure Bundle
4.3(2.230129)	1.70 GiB	Nov 15, 2023 10:05 PM	Cisco Intersight Infrastructure Bundle
4.3(2.230117)	1.70 GiB	Aug 16, 2023 9:46 AM	Cisco Intersight Infrastructure Bundle
4.2(3h)	1.70 GiB	Sep 30, 2023 7:57 PM	Cisco Intersight Infrastructure Bundle
4.2(3g)	1.70 GiB	Jul 31, 2023 8:08 PM	Cisco Intersight Infrastructure Bundle
4.2(3e)	1.70 GiB	May 16, 2023 10:58 PM	Cisco Intersight Infrastructure Bundle
4.2(3d)	1.70 GiB	Apr 14, 2023 11:30 AM	Cisco Intersight Infrastructure Bundle
4.2(3b)	1.70 GiB	Apr 14, 2023 11:46 AM	Cisco Intersight Infrastructure Bundle
4.2(2e)	1.69 GiB	Apr 14, 2023 12:02 PM	Cisco Intersight Infrastructure Bundle

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



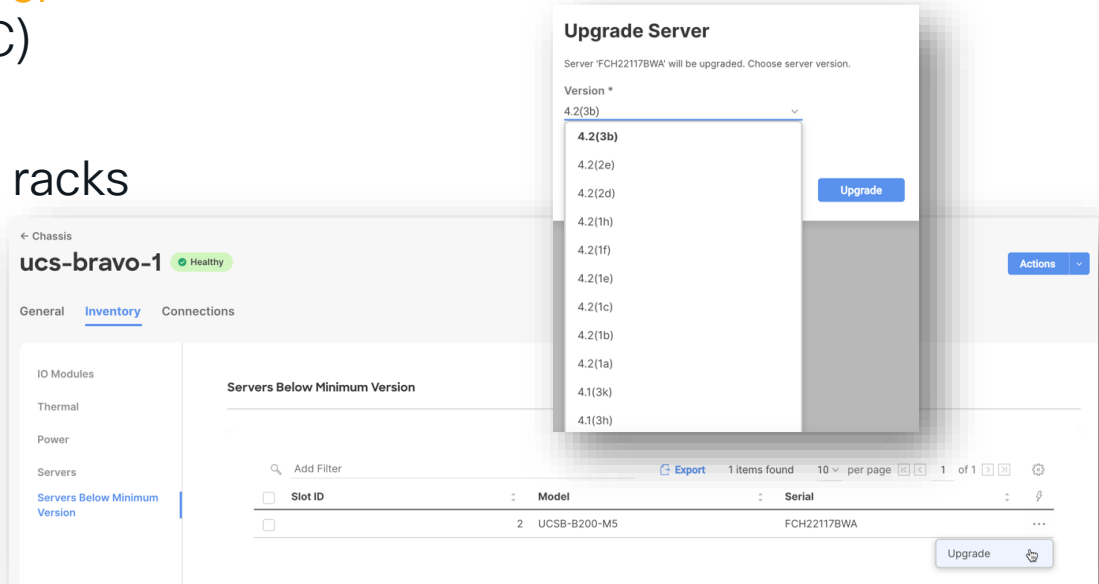
```
ucs-bravo-A# list-firmware-cache
DOWNLOADED DATE      IDENTIFIER
2023-09-13            650216eb65676131019d57ad
2023-10-30            653f6ea3656761310100d082
2023-11-02            6543c63e656761310112aeba
2023-11-19            655a7771656761310121512d
2023-11-19            655a77f56567613101215368
2023-11-19            655a8bd9656761310121a9aa
2023-11-20            655bd6bd6567613101276637
2023-11-22            655e0f9265676130057f6761
2023-12-11            6576dd556567613101d09d47
2024-01-24            65b1355d65676130059f01b7

IMAGE NAME
ucs-intersight-infra-4gfi.4.3.2.230117.bin
intersight-ucs-server-b200-m5.4.2.3f.bin
intersight-ucs-server-b200-m5.5.1.0.230054.bin
intersight-ucs-server-210c-m6.5.2.0.230092.bin
intersight-ucs-server-b200-m5.5.2.0.230100.bin
intersight-ucs-server-c220m5.4.3.2.230270.bin
ucs-intersight-infra-4gfi.4.3.2.230129.bin
intersight-ucs-server-b200-m5.5.1.0.230073.bin
intersight-ucs-server-b200-m5.4.2.3b.bin
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
```

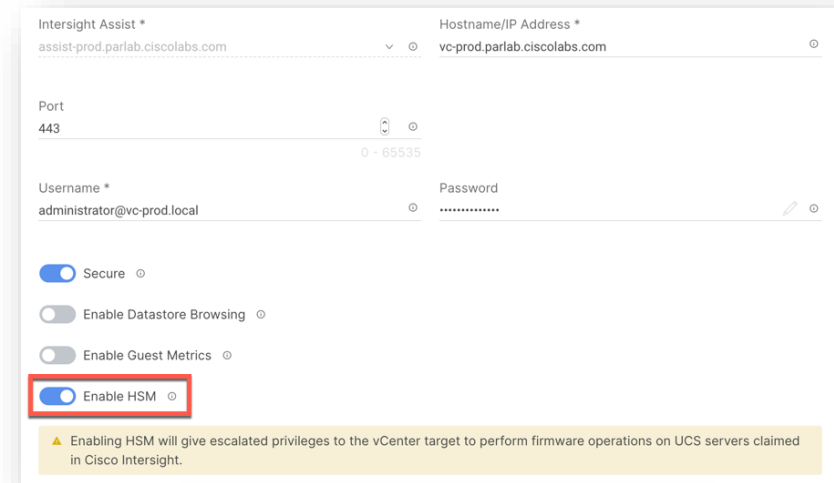
Handling Servers below minimum version

- **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



Intersight Assist *
assist-prod.parlab.ciscolabs.com

Hostname/IP Address *
vc-prod.parlab.ciscolabs.com

Port
443

Username *
administrator@vc-prod.local

Password

☒ Secure

☐ Enable Datastore Browsing

☐ Enable Guest Metrics

☒ Enable HSM

▲ Enabling HSM will give escalated privileges to the vCenter target to perform firmware operations on UCS servers claimed in Cisco Intersight.

Select Firmware and Drivers Addon

Select the hardware support manager
Intersight HSM via intersight-cva.complablab - v

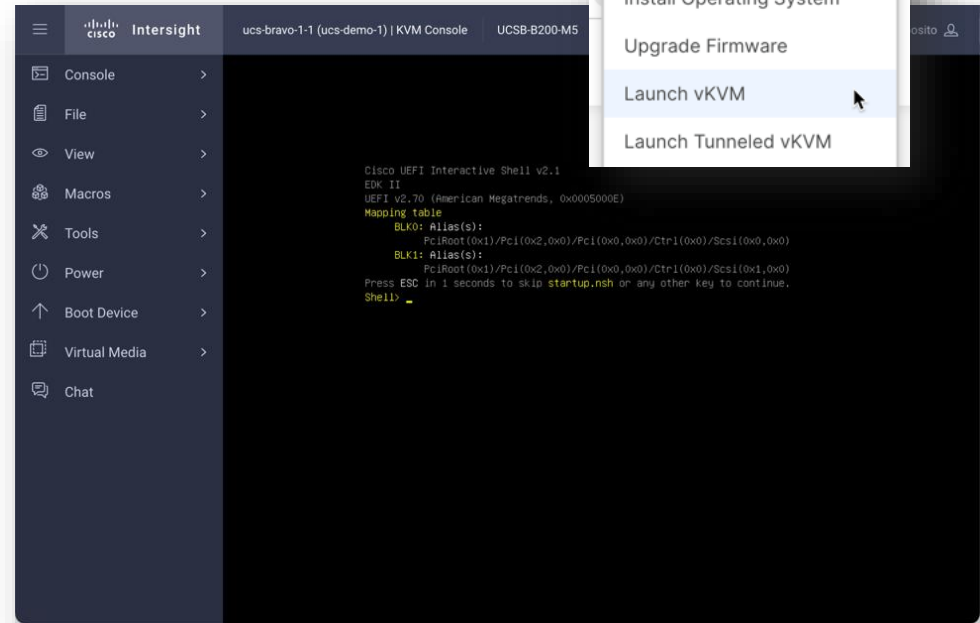
Hardware Support Manager

Select a firmware and driver addon

Addon name	Addon version	Supported ESXi versions
<input type="radio"/> CR-4.2(1f)	4.2(1f)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(3f)	4.1(3f)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(3d)	4.1(3d)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(3c)	4.1(3c)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(3b)	4.1(3b)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(2f)	4.1(2f)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(2g)	4.1(2g)	7.0.0, 7.0.1, 7.0.2, 7.0.3
<input type="radio"/> CR-4.1(2f)	4.1(2f)	7.0.0, 7.0.1, 7.0.2, 7.0.3

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

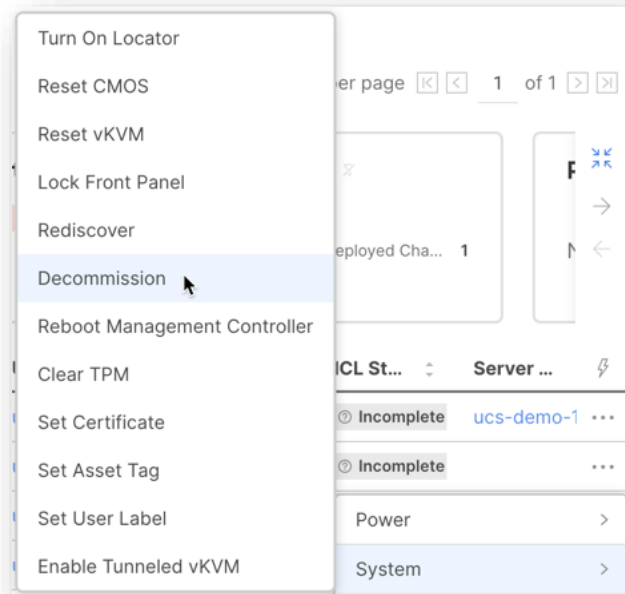


New Cisco vKVM with M5*/M6/M7 servers

** 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 reseal (hot plug) operation
- Action performed from Chassis view
- Resetting secondary slot for X410c M7 is not necessary

Power Cycle Chassis Slot

Selected slot in Chassis 'ucs-bravo-2' will be Power Cycled

 This operation should be used as a last resort to recover a non-responding device. Device management will be interrupted. Allow time for management services to come up following the power cycle.

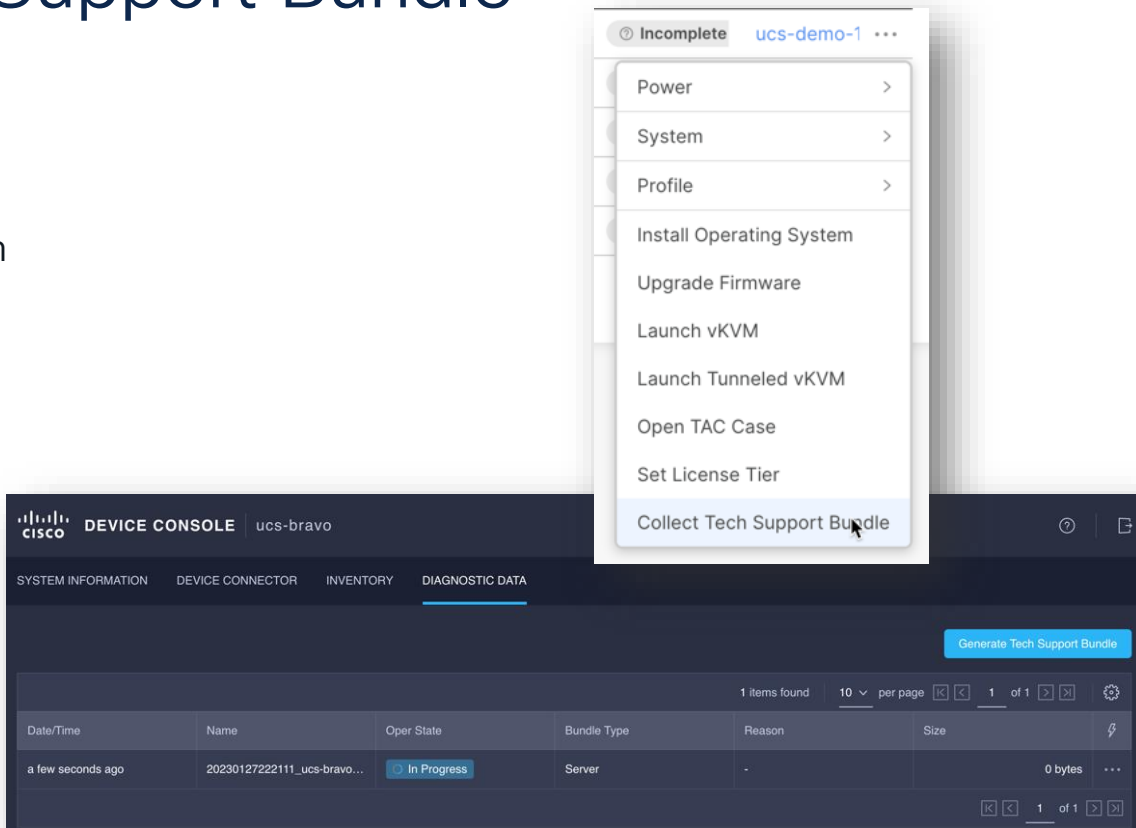
Slot ID *

1

CancelPower Cycle

Collecting a Tech Support Bundle

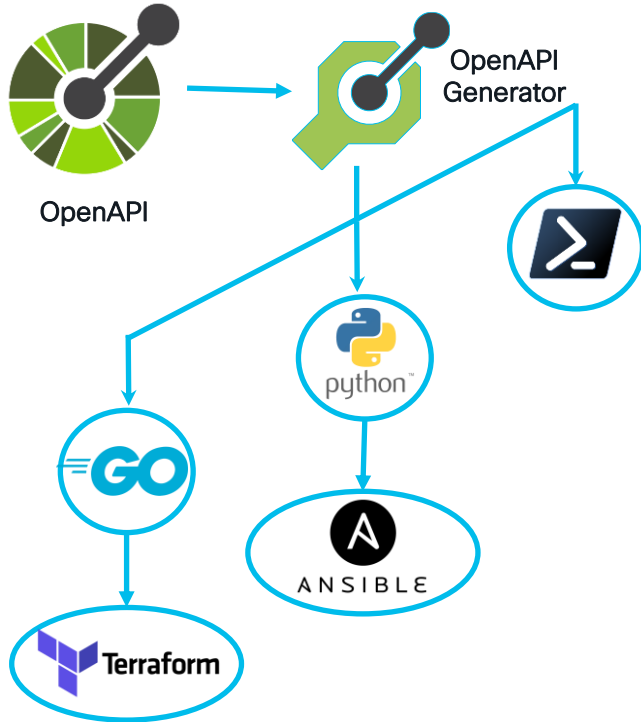
- **From Intersight**
 - Action menu of the equipment
 - Download under System → Tech Support Bundles
- **From Device Console**
 - Action menu of the equipment under Inventory
 - Download under Diagnostic Data
- **Connected TAC**
 - Automated with SaaS and Connected Appliance



The screenshot displays the Cisco Device Console interface for a device named 'ucs-bravo'. The 'DIAGNOSTIC DATA' tab is selected, showing a table with one entry: a bundle named '20230127222111_ucs-bravo...' in an 'In Progress' state. An action menu is open over the table, listing various options, with 'Collect Tech Support Bundle' highlighted at the bottom. The interface also includes a 'Generate Tech Support Bundle' button and pagination controls.

Date/Time	Name	Oper State	Bundle Type	Reason	Size
a few seconds ago	20230127222111_ucs-bravo...	In Progress	Server	-	0 bytes

API is the new UI



CISCO *Live!*

Service: Intersight

API Reference v1.0.11-10513

GET /api/v1/compute/Blades

Parameters: \$filter { string } query

Filter criteria for the resources to return. A URI with a \$filter query option identifies a subset of the entries from the Collection of Entries. The subset is determined by selecting only the Entries that satisfy the predicate expression specified by the \$filter option. The expression language that is used in \$filter queries supports references to properties and literals. The literal values can be strings enclosed in single quotes, numbers and boolean values (true or false).

Sorterby { string } query

Determines what properties are used to sort the collection of resources.

Stop { integer } query

Specifies the maximum number of resources to return in the response.

Sskip { integer } query

Specifies the number of resources to skip in the response.

Sselect { string } query

Specifies a subset of properties to return.

Sexpand { string } query

Specify additional attributes or related resources to return in addition to

REST Client

GET /api/v1/compute/Blades

+ Query Parameter

Send 200 Success

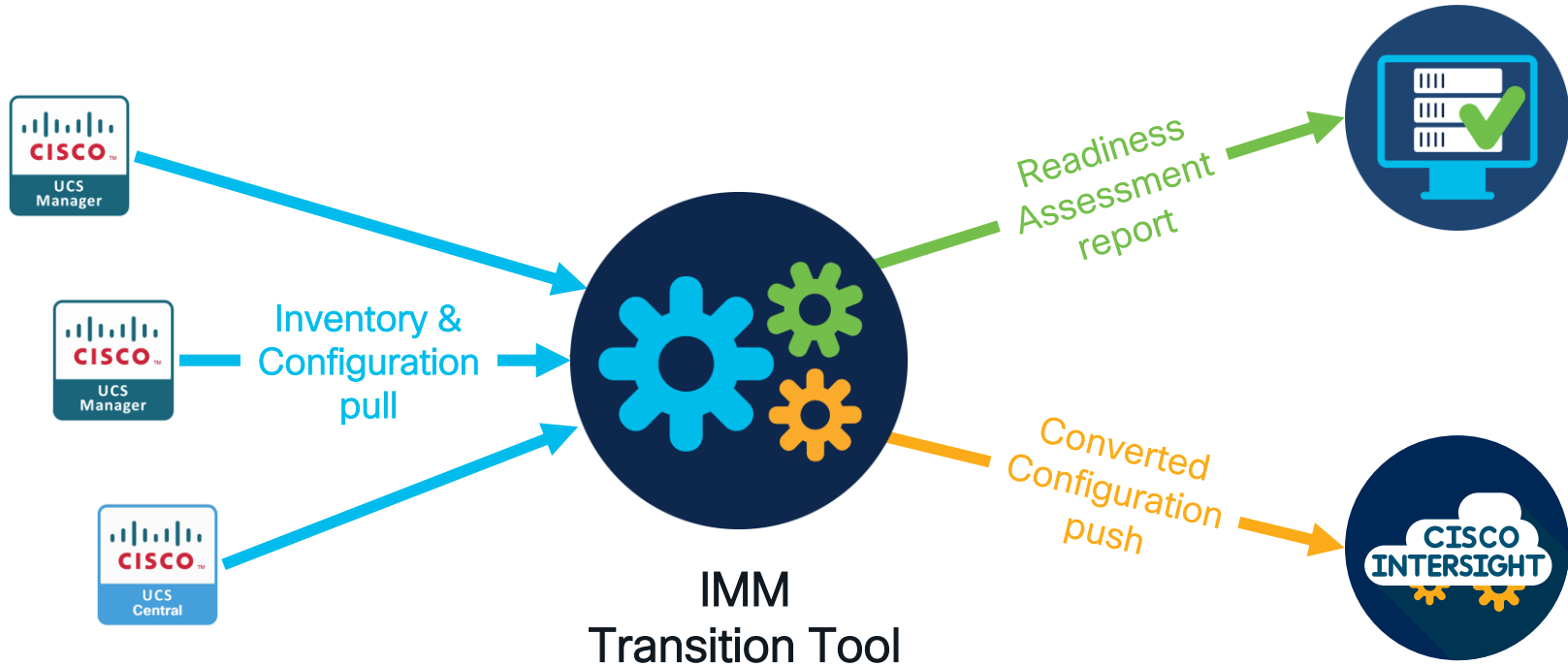
Response Text

```
1 {
2   "ObjectType": "compute.Blade.List",
3   "Results": [
4     {
5       "AccountMoid": "5984328b3e95200001",
6       "Adapters": [
7         {
8           "ClassId": "mo.MoRef",
9           "Moid": "63cd99456176752d31c83",
10          "ObjectType": "adapter.Unit",
11          "link": "https://www.intersight.com/.../api/v1/compute/Adapters/63cd99456176752d31c83",
12        }
13      ],
14      "AdminPowerState": "",
15      "AlarmSummary": {
16        "ClassId": "compute.AlarmSummary",
17        "Critical": 0,
18        "Health": "Healthy",
19        "Info": 0,
20        "ObjectType": "compute.AlarmSummary",
21        "Warning": 0
22      },
23      "Alerts": [],
24      "Ancestors": [
25        {
26          "ClassId": "mo.MoRef",
27          "Moid": "63cd99456176752d31c83",
28          "ObjectType": "equipment.Chassis",
29          "link": "https://www.intersight.com/.../api/v1/compute/Chassis/63cd99456176752d31c83",
30        }
31      ],
32      "AssetTag": ""
33    }
34  ]
35}
```

<https://intersight.com/apidocs/>

Transitioning to Intersight Managed Mode

Introducing the IMM Transition Tool



Primary use cases

1

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.)

2

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)

3

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

Additional use cases

4

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)

5

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**

6

Simplify OS Installation and firmware upgrades

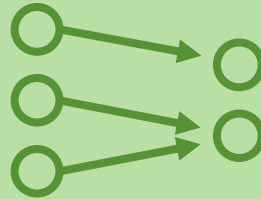
- Use IMM Transition Tool VM as a **Software Repository**
- Allows **hosting of ISO images** or **firmware packages**
- Can be leveraged to easily perform **OS Installation** or **firmware upgrades** on UCS servers

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



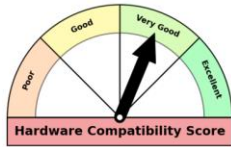
Profile/Template based

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

Sample Readiness Report

1. Intersight Managed Mode Conversion Overall Summary

1.1 Intersight Managed Mode Conversion Score



This score reflects the overall UCS Domain hardware compatibility with Intersight Managed Mode. It takes into account all hardware components (fabric and servers). A detailed view can be found below.

3.2.16 Port Policies

These policies are used for converting attributes of the port roles of Fabric Interconnects in UCS Manager.



Port Policies are separate for each Fabric Interconnect

Source port configuration is different for both fabrics



Ignoring Link Profile configuration for FCoE Port-Channel

Different Link Profiles are configured on the following Member Interfaces: ['33']



Ignoring FCoE Storage Ports configuration as it is not yet supported in IMM

['A/1/14, A/1/21/4, B/1/39']



Ignoring SAN Ports configuration as Source FI Model is not supported in IMM

['UCS-FI-6332-16UP']



Ignoring source FI (6332-16UP) SFP+ ports configuration

Destination FI Model (6536) does not have any SFP+ ports

Fabric Interconnects



IMM Ready
Requires Upgrade
Not Compatible

Chassis



IMM Ready
Requires Upgrade
Not Compatible

IO Modules



IMM Ready
Requires Upgrade
Not Compatible

Blades



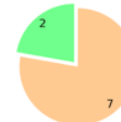
IMM Ready
Requires Upgrade
Not Compatible

Racks



IMM Ready
Requires Upgrade
Not Compatible

Adaptors

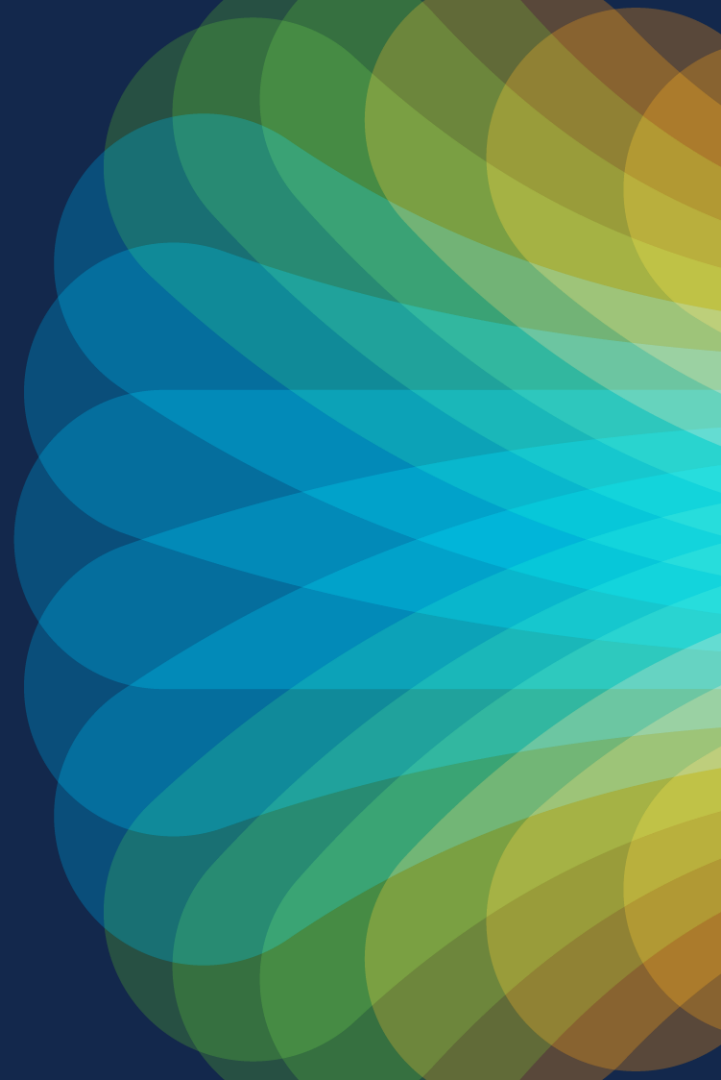


IMM Ready
Requires Upgrade
Not Compatible

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



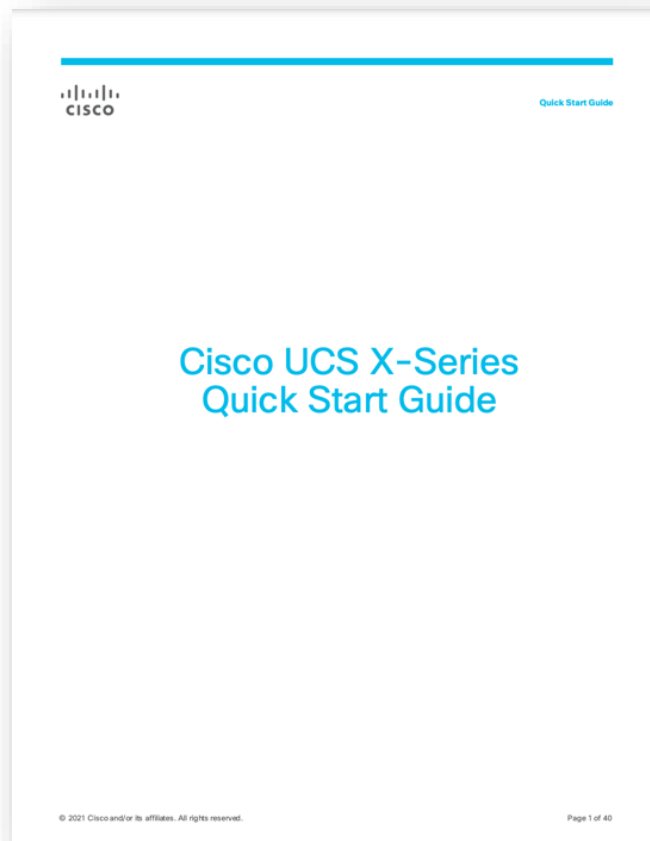
Safer Operations



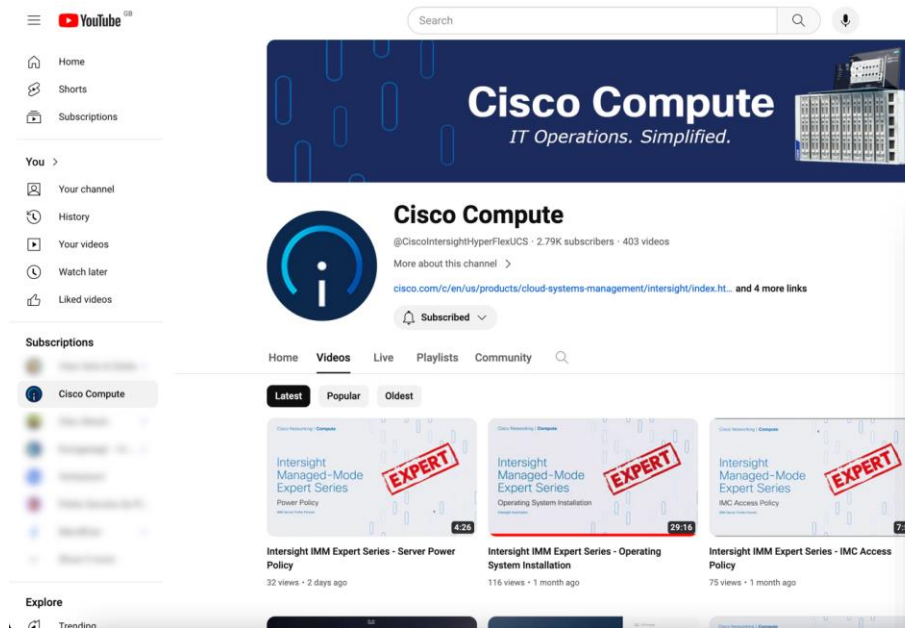
Multi Domain

X-Series Quick Start Guide

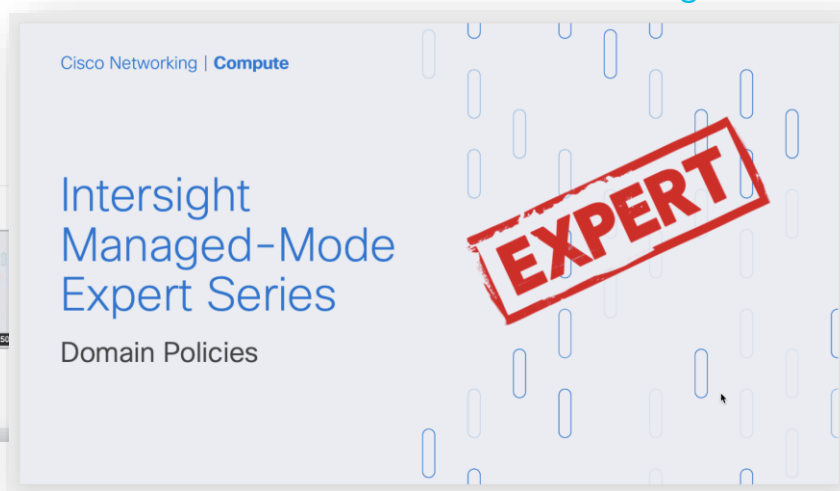
- **Complete deployment guide** for an X-Series IMM deployment from scratch
- Contains IMM domain, chassis and server configuration steps with all details
- <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-quick-start-guide.html>



Cisco Compute YouTube Channel



IMM Expert Series
Detailed IMM Training Videos



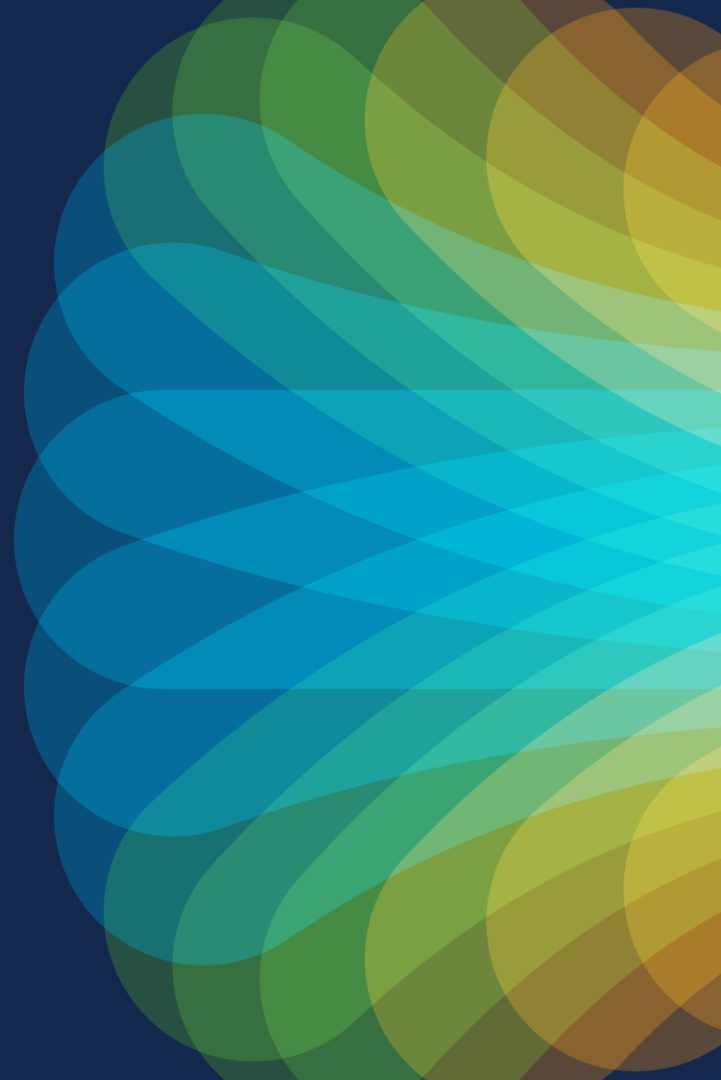
<https://www.youtube.com/@CiscoIntersightHyperFlexUCS>



The bridge to possible

Thank you

CISCO *Live!*



The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, including blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go