



# Cisco Intersight™ Feature Overview

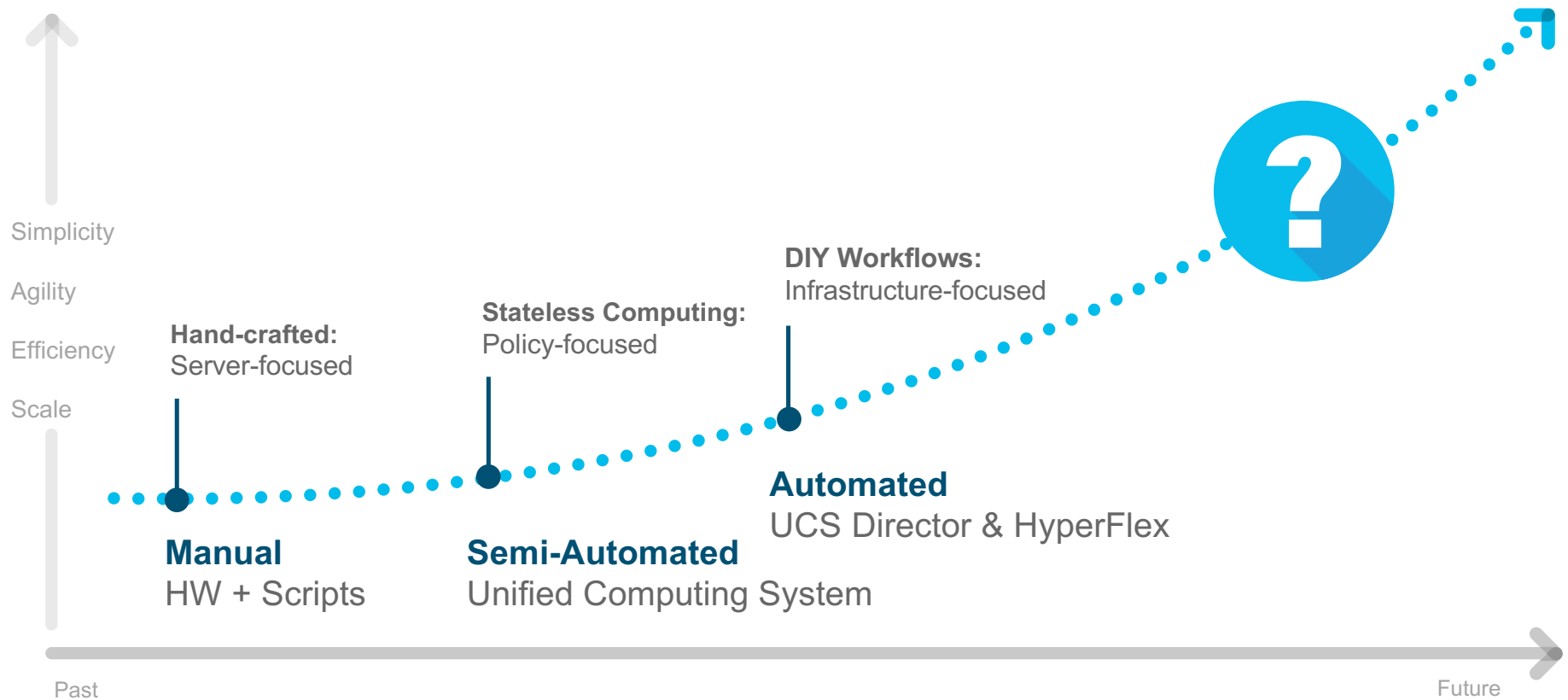
## Standalone Management for UCS C-Series Servers

January 2018

# Agenda

- Overview
- Monitoring/Fault Reporting
- Device Addition / Registration
- Policies and Profiles
- Firmware Upgrades

# Operational Evolution



# UCS Standalone Management Simplification

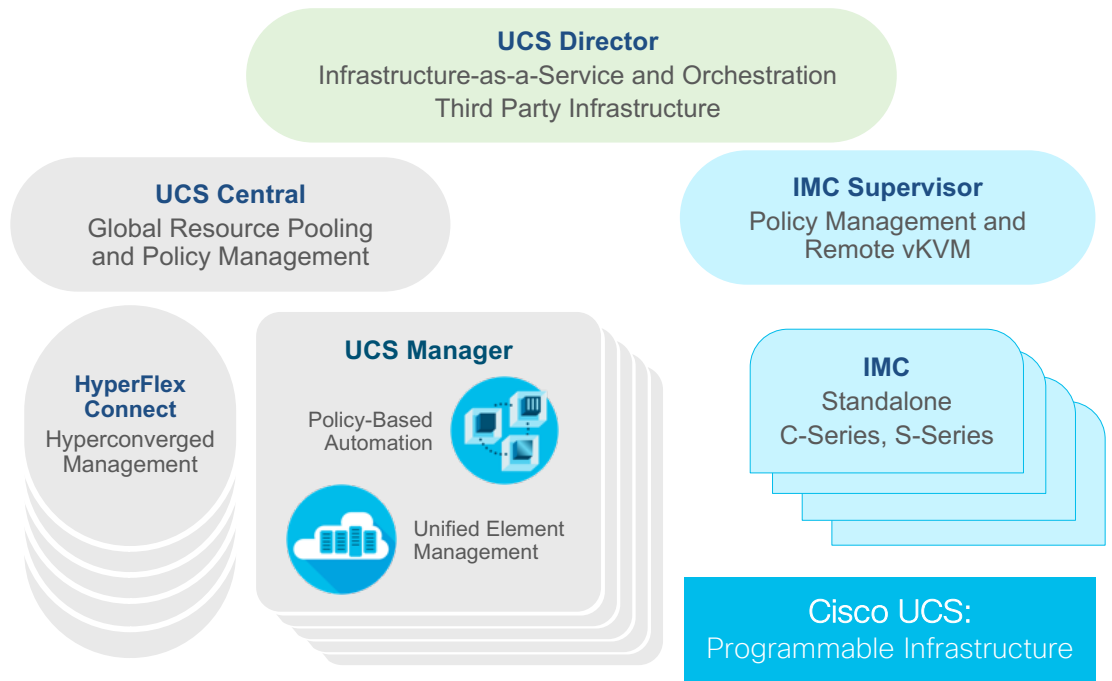
## Cisco Intersight Core Features and Functionality

### Familiar Capabilities from IMCS

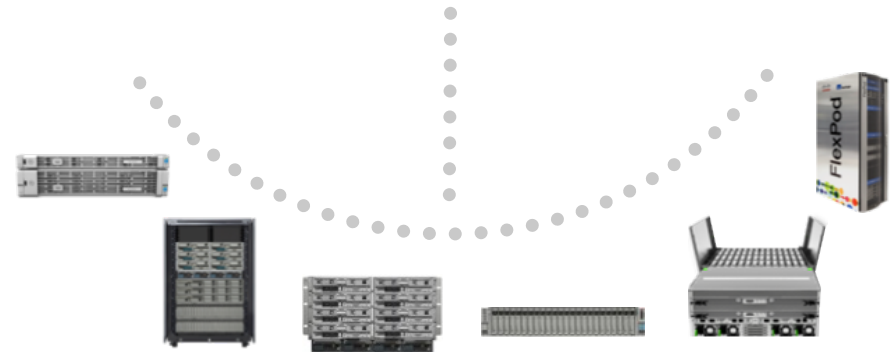
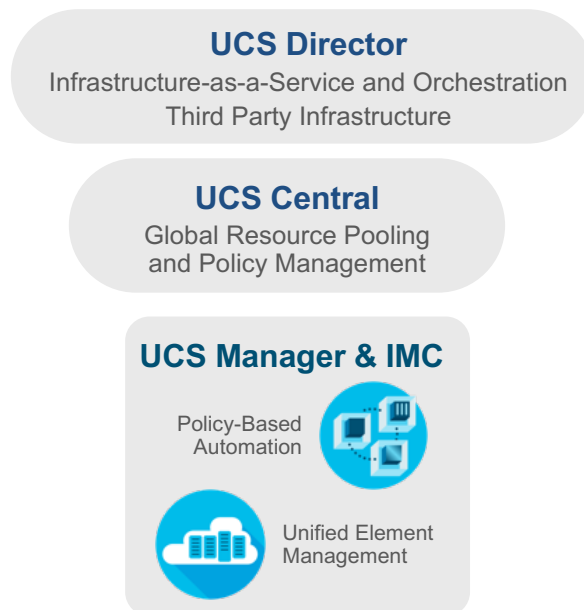
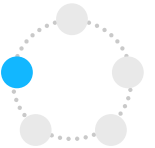


- Platform Hardware Inventory
- Hardware Health Status
- vKVM Launcher (Incl. vMedia)
- Firmware Inventory + Management
- Call-Home (Email Alerting)
- Cisco Smart Call Home
- Policy/Profile Based Framework
- **C-Series + HX Standalone Only**

### Cisco Intersight Enhanced Functionality



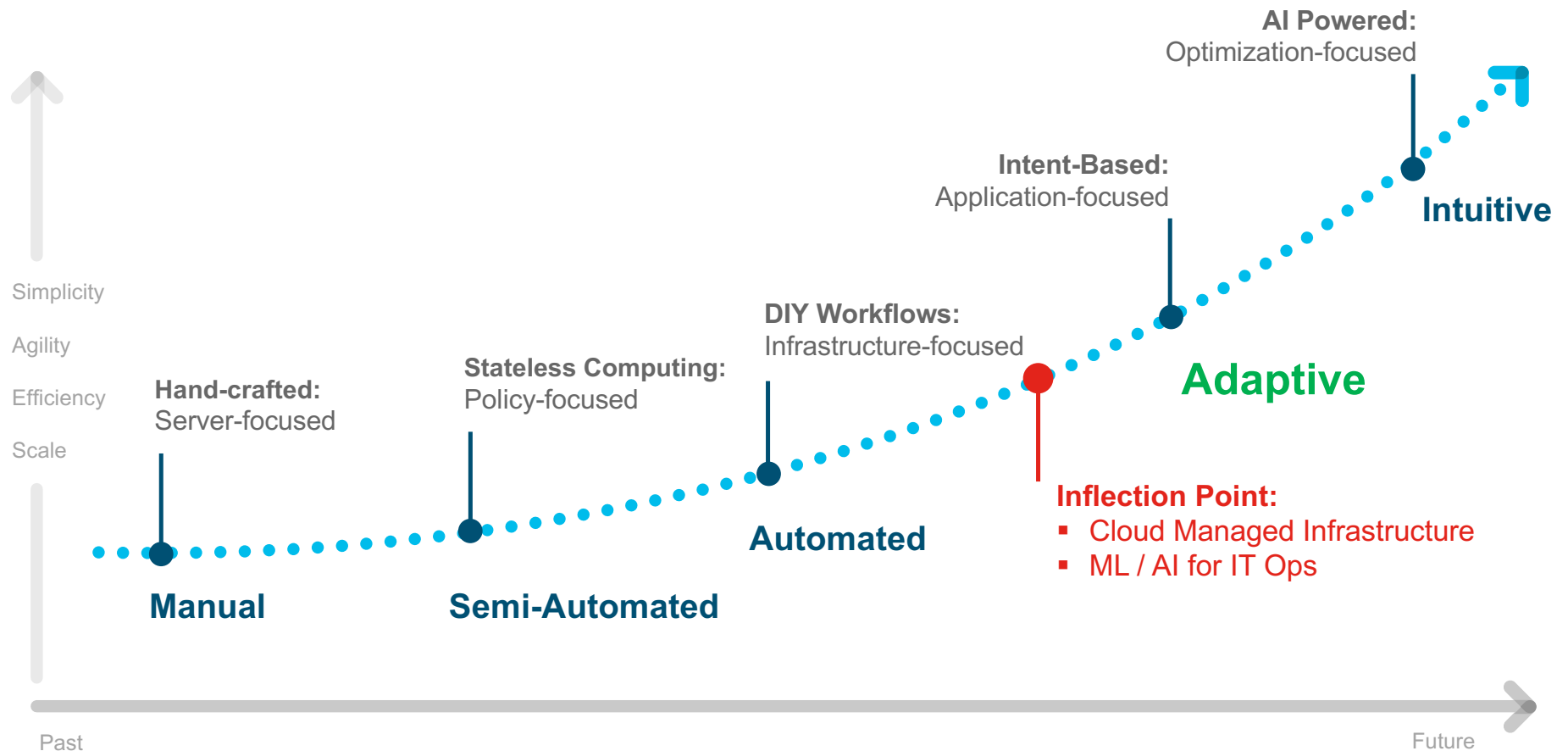
# SaaS-Delivered



## Consumption Models

Cisco hosted  
Service provided, customer hosted

# A New Era of Adaptive Systems Management



# UCS Standalone Management Simplification

## Core Differences – IMC Supervisor vs Intersight

### Cisco IMC Supervisor

- On-Premise Virtual Appliance
- Feature / appliance upgrades require user intervention and downtime
- Fixed bundle licensing – 1000 servers max per appliance
- REST XML API
- Database backup / redundancy requires multiple appliances and manual intervention

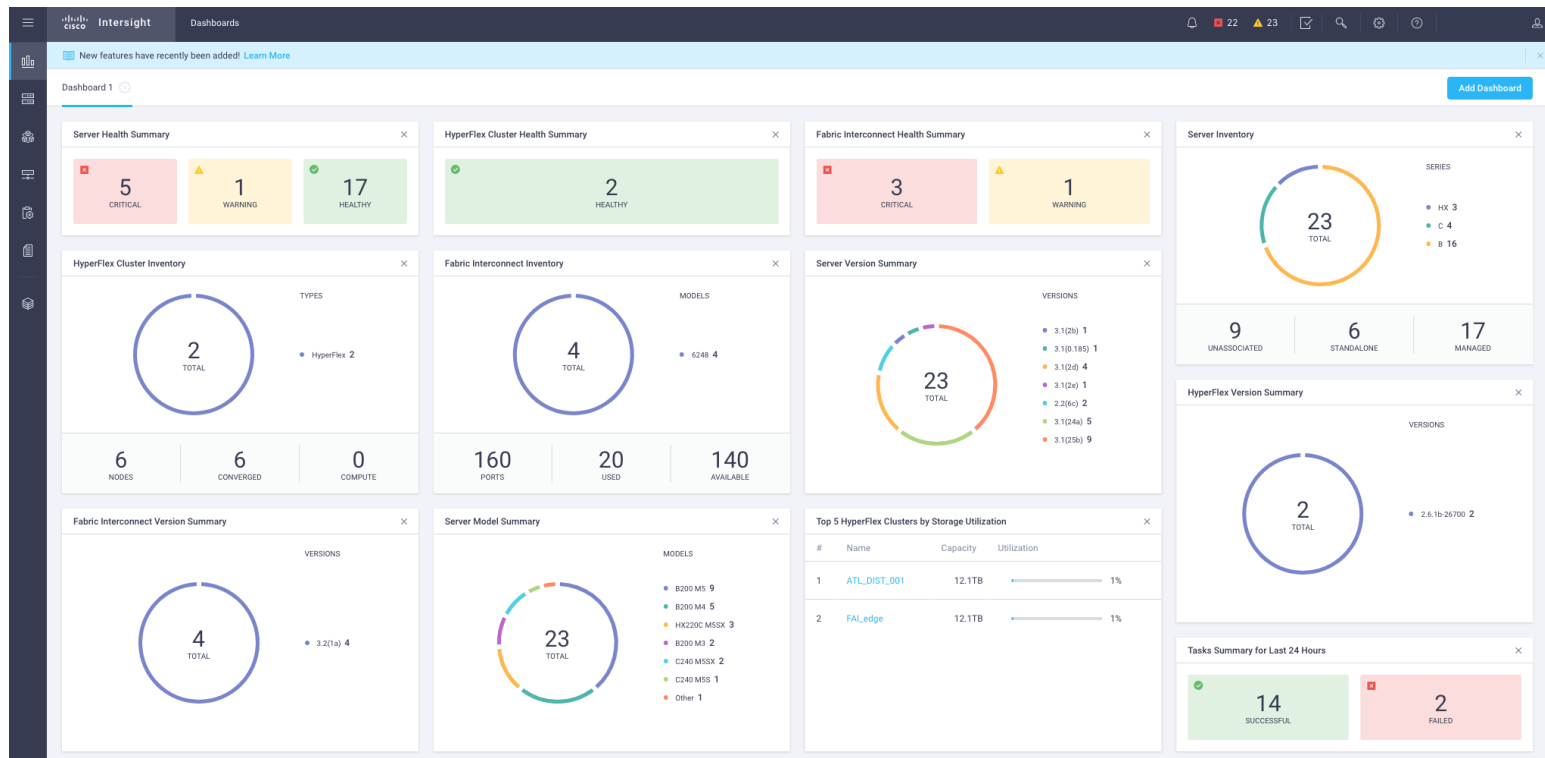
### Cisco Intersight

- Cloud-based centralized management
- Features and upgrades pushed through the cloud to streamline availability
- SaaS / Subscription based model licensing – Smart Licensing support
- RESTFUL JSON API (Odata)
- Cloud based redundancy - autonomously
- Cisco Hyperflex Installation
- Customizable dashboards
- Telemetry Data Collection / Recommendation Engine

# Monitoring / Fault Reporting / Server Actions



# Cisco Intersight Dashboard



- Customizable dashboard to show overall faults / health / inventory for all managed infrastructure
- Can create unique dashboards for individual Intersight users
- Can add / remove widgets as desired
- Can click on various widgets for more detailed information

# Cisco Intersight Fault List

Severity	Date/Time	Code	Source Type	Source Name	Component	Message
	Jan 18, 2018 8:38 AM	UCS-F0743	Standalone Ser...	C240-WZP213...	sys/rack-unit-1	PS_RDNDNT_MODE: Power Supply redundancy is lost: Reseat or replace Power Supply

1 - 1 of 1

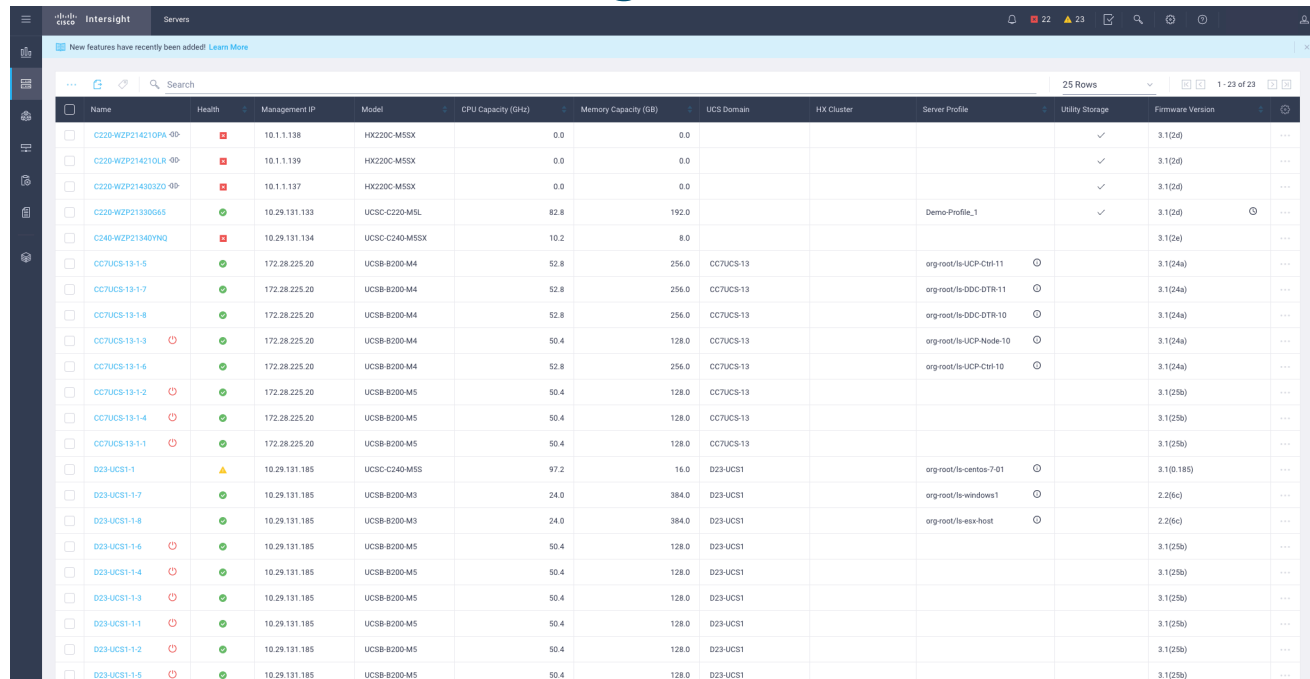
The screenshot shows the Cisco Intersight interface with the 'Alarms' panel open. The panel displays a list of faults with columns for severity, code, timestamp, and description. The faults are categorized by severity: Critical (red square), Warning (yellow triangle), and Information (blue circle). The faults listed are:

- UCS-F0276** (Critical): Jan 23, 2018 2:47 PM. ether port 2/1 on fabric interconnect B oper state: link-down, reason: Link failure or not-connected
- UCS-F0279** (Warning): Jan 23, 2018 1:30 PM. ether port 1/31 on fabric interconnect B oper state: sfp-not-present
- UCS-F0689** (Warning): Jan 19, 2018 4:09 PM. Assignment of service profile UCP-Node-10 to server sys/chassis-1/blade-3 failed
- UCS-F0156** (Warning): Jan 18, 2018 6:04 PM. Server, vendor(Disco Systems Inc), model(UCSB-B200-M5), serial(F0H21347DEK) in slot 1/3 presence: mismatch
- UCS-F0842** (Warning): Jan 18, 2018 8:38 AM. P2\_PRESENT: Processor 2 missing. Please reseat or replace Processor 2
- UCS-F0743** (Critical): Jan 18, 2018 8:38 AM. PS\_RDNDNT\_MODE: Power Supply redundancy is lost: Reseat or replace Power Supply
- UCS-F0395** (Warning): Jan 17, 2018 4:57 PM. Fan 1 in Fan Module 1-2 under chassis 1 speed: upper-non-critical
- UCS-F0397** (Warning): Jan 17, 2018 4:53 PM. Fan 2 in Fan Module 1-4 under chassis 1 speed: upper-non-recoverable
- UCS-F0397** (Warning): Jan 17, 2018 4:53 PM. Fan 2 in Fan Module 1-3 under chassis 1 speed: upper-non-recoverable
- UCS-F0397** (Warning): Jan 17, 2018 4:53 PM. Fan 2 in Fan Module 1-2 under chassis 1 speed: upper-non-recoverable

The panel also includes a 'View All' link at the bottom.

- All device faults can be accessed from any Intersight page (image to the right shows access from dashboard)
- Clicking on a particular fault provides additional fault details, remediation steps if available
- Tabs available for All / Critical / Warning fault levels
- Fault tab shows UCS fault code, timestamp, and fault details

# Cisco Intersight Servers Tab



Name	Health	Management IP	Model	CPU Capacity (GHz)	Memory Capacity (GB)	UCS Domain	HX Cluster	Server Profile	Utility Storage	Firmware Version
C220-WZP214210PA-00	❌	10.1.1.138	HK220C-M5SX	0.0	0.0				✓	3.1(2d)
C220-WZP214210LJ-00	❌	10.1.1.139	HK220C-M5SX	0.0	0.0				✓	3.1(2d)
C220-WZP21430320-00	❌	10.1.1.137	HK220C-M5SX	0.0	0.0				✓	3.1(2d)
C220-WZP21330565	✅	10.29.131.133	UCSC-C220-M5L	82.8	192.0			Demo-Profile_1	✓	3.1(2d)
C240-WZP21340YNQ	❌	10.29.131.134	UCSC-C240-M5SX	10.2	8.0					3.1(2e)
CC7UCS-13-1-5	✅	172.28.225.20	UCSB-E200-M4	52.8	256.0	CC7UCS-13		org-root/ls-UCP-Ctrl-11	⊙	3.1(24a)
CC7UCS-13-1-7	✅	172.28.225.20	UCSB-E200-M4	52.8	256.0	CC7UCS-13		org-root/ls-DDC-DTR-11	⊙	3.1(24a)
CC7UCS-13-1-8	✅	172.28.225.20	UCSB-E200-M4	52.8	256.0	CC7UCS-13		org-root/ls-DDC-DTR-10	⊙	3.1(24a)
CC7UCS-13-1-3	⚠️	172.28.225.20	UCSB-E200-M4	50.4	128.0	CC7UCS-13		org-root/ls-UCP-Node-10	⊙	3.1(24a)
CC7UCS-13-1-6	✅	172.28.225.20	UCSB-E200-M4	52.8	256.0	CC7UCS-13		org-root/ls-UCP-Ctrl-10	⊙	3.1(24a)
CC7UCS-13-1-2	⚠️	172.28.225.20	UCSB-E200-M5	50.4	128.0	CC7UCS-13				3.1(25b)
CC7UCS-13-1-4	⚠️	172.28.225.20	UCSB-E200-M5	50.4	128.0	CC7UCS-13				3.1(25b)
CC7UCS-13-1-1	⚠️	172.28.225.20	UCSB-E200-M5	50.4	128.0	CC7UCS-13				3.1(25b)
D23-UCS1-1	⚠️	10.29.131.185	UCSC-C240-M5S	97.2	16.0	D23-UCS1		org-root/ls-centos-7-01	⊙	3.1(0.185)
D23-UCS1-1-7	✅	10.29.131.185	UCSB-E200-M3	24.0	384.0	D23-UCS1		org-root/ls-windows1	⊙	2.2(6c)
D23-UCS1-1-8	✅	10.29.131.185	UCSB-E200-M3	24.0	384.0	D23-UCS1		org-root/ls-esx-host	⊙	2.2(6c)
D23-UCS1-1-6	⚠️	10.29.131.185	UCSB-E200-M5	50.4	128.0	D23-UCS1				3.1(25b)
D23-UCS1-1-4	⚠️	10.29.131.185	UCSB-E200-M5	50.4	128.0	D23-UCS1				3.1(25b)
D23-UCS1-1-3	⚠️	10.29.131.185	UCSB-E200-M5	50.4	128.0	D23-UCS1				3.1(25b)
D23-UCS1-1-1	⚠️	10.29.131.185	UCSB-E200-M5	50.4	128.0	D23-UCS1				3.1(25b)
D23-UCS1-1-2	⚠️	10.29.131.185	UCSB-E200-M5	50.4	128.0	D23-UCS1				3.1(25b)
D23-UCS1-1-5	⚠️	10.29.131.185	UCSB-E200-M5	50.4	128.0	D23-UCS1				3.1(25b)

- Main server tab shows all servers managed by Cisco Intersight, and provides basic Health/Model/IP info
  - Desired column details can be added/removed as user sees fit
- Clicking on any server name dials in to that server – detailed server overview / inventory information (details on next few slides)

# Cisco Intersight Server Overview

The screenshot displays the Cisco Intersight interface for a server. The top navigation bar includes the Cisco Intersight logo, the 'Servers' tab, and various system status icons (notifications, alarms, search, settings, etc.). A blue banner at the top indicates that new features have been added, with a 'Learn More' link.

The main content area is divided into several sections:

- Details:** A sidebar on the left showing the server's health status as 'Healthy' (green checkmark). It also lists basic information: Name (C220-WZP21330G65), Serial (WZP21330G65), PID (UCSC-C220-M5L), Vendor (Cisco Systems Inc), and Revision.
- Properties:** A central section displaying the server's model (Cisco UCSC-C220-M5L) and a 3D front view image. Below the image, there are controls for 'Power' (on) and 'Locator LED' (off). A 'Health Overlay' toggle is also present.
- Alarms:** A section on the right showing 'All (0)' alarms.
- Server Actions:** A dropdown menu on the far right containing various management actions: Power Off, Power Cycle, Shut Down OS, Hard Reset, Reboot IMC, Turn On Locator, Launch KVM, Launch Cisco IMC, Add/Edit Asset Tags, and Add/Edit User Label.

Below the 3D image, a table lists the server's hardware specifications:

Property	Value
CPU	2
Threads	72
Cores	36
Enabled Cores	36
Total Memory (GB)	192.0
Speed (GHz)	82.8
ID	1
Adapters	1
NICs	2
HBAs	2
UUID	A19EFD0F-C126-44AE-89B6-64DC1ED60A22
Firmware	3.1(2d)

- Server name, model, serial number, and other basic properties are displayed
- Health overlay for front/back/top views can be turned on/off as needed
- Alarms/Faults visible on right hand side
- Server Actions available as well – IMC crosslaunch, vKVM (coming soon), power operations, tagging


# Cisco Intersight Server Inventory

















The screenshot displays the Cisco Intersight Server Inventory interface. The top navigation bar includes the Cisco Intersight logo, the 'Servers' tab, and a notification banner stating 'New features have recently been added! Learn More'. The left sidebar contains a tree view of server components: Motherboard, CIMC, CPUs (with Processor 1 and Processor 2 selected), Memory, Adapters, Storage, Controllers, and LUN. The main content area is titled 'Processor 1' and shows its state as 'Operable'. Below this, the 'Key Identifiers' section lists 'Presence' as 'Equipped'. The 'Resources' section provides detailed specifications for the processor, including CPU Stepping (4), Speed (2.3 GHz), Model (Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz), Number of Threads (36), Number of Cores (18), and Number of Cores Enabled (18). The 'Hardware' section on the right lists 'Architecture' as Xeon, 'Socket Designation' as CPU1, and 'Vendor' as Intel(R) Corporation.

Component	Value
State	Operable
Key Identifiers	
Presence	Equipped
Resources	
CPU Stepping	4
Speed (GHz)	2.3
Model	Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz
Number of Threads	36
Number of Cores	18
Number of Cores Enabled	18
Hardware	
Architecture	Xeon
Socket Designation	CPU1
Vendor	Intel(R) Corporation

- Detailed information for all server peripherals – CPUs, memory, adapters, storage, etc
- Can dial in to specific peripheral for additional component information
- Server Actions tab available here as well

# Cisco Intersight - Server Actions

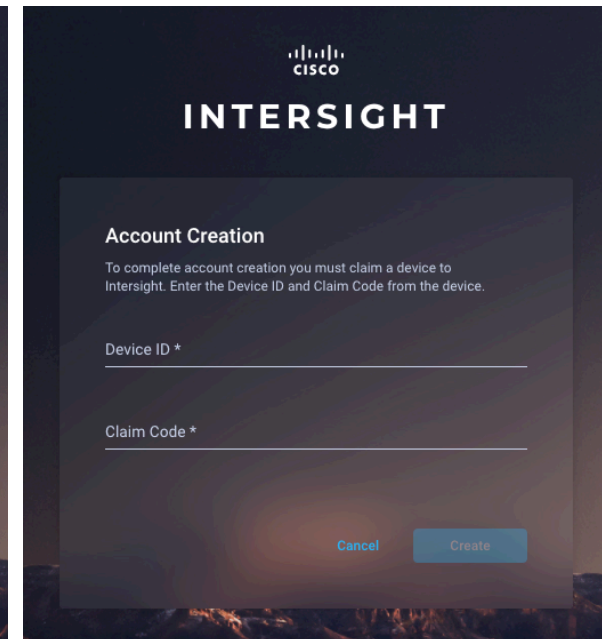
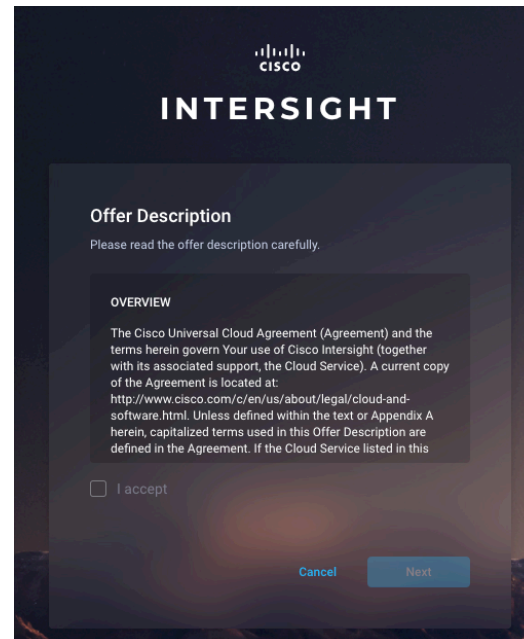
- Available Server Actions
  - Launch IMC
  - Launch KVM (coming soon)
  - Power ON/OFF
  - Shutdown
  - Reboot
  - Power Cycle
  - Hard Reset Server
- Server actions can be accessed from main servers page by clicking the  icon

<input type="checkbox"/>	<a href="#">C220-WZP21330G65</a>		10.29.131.133	UCSC-C220-M5L	82.8	192.0			Demo-Profile_1	✓	3.1(2d)		...
<input type="checkbox"/>	<a href="#">C240-WZP21340YNQ</a>		10.29.131.134	UCSC-C240-M5SX	10.2	8.0					3.1(2e)		Power Off
<input type="checkbox"/>	<a href="#">CC7UCS-13-1-5</a>		172.28.225.20	UCSB-B200-M4	52.8	256.0	CC7UCS-13		org-root/ls-UCP-Ctrl-11		3.1(24a)		Power Cycle
<input type="checkbox"/>	<a href="#">CC7UCS-13-1-7</a>		172.28.225.20	UCSB-B200-M4	52.8	256.0	CC7UCS-13		org-root/ls-DDC-DTR-11		3.1(24a)		Shut Down OS
<input type="checkbox"/>	<a href="#">CC7UCS-13-1-8</a>		172.28.225.20	UCSB-B200-M4	52.8	256.0	CC7UCS-13		org-root/ls-DDC-DTR-10		3.1(24a)		Hard Reset
<input type="checkbox"/>	<a href="#">CC7UCS-13-1-3</a> 		172.28.225.20	UCSB-B200-M4	50.4	128.0	CC7UCS-13		org-root/ls-UCP-Node-10		3.1(24a)		Reboot IMC
<input type="checkbox"/>	<a href="#">CC7UCS-13-1-6</a>		172.28.225.20	UCSB-B200-M4	52.8	256.0	CC7UCS-13		org-root/ls-UCP-Ctrl-10		3.1(24a)		Launch KVM
<input type="checkbox"/>	<a href="#">CC7UCS-13-1-2</a> 		172.28.225.20	UCSB-B200-M5	50.4	128.0	CC7UCS-13				3.1(25b)		Launch Cisco IMC

- Server actions can also be access on server properties page for any given endpoint

# Accounts Creation / Device Claim

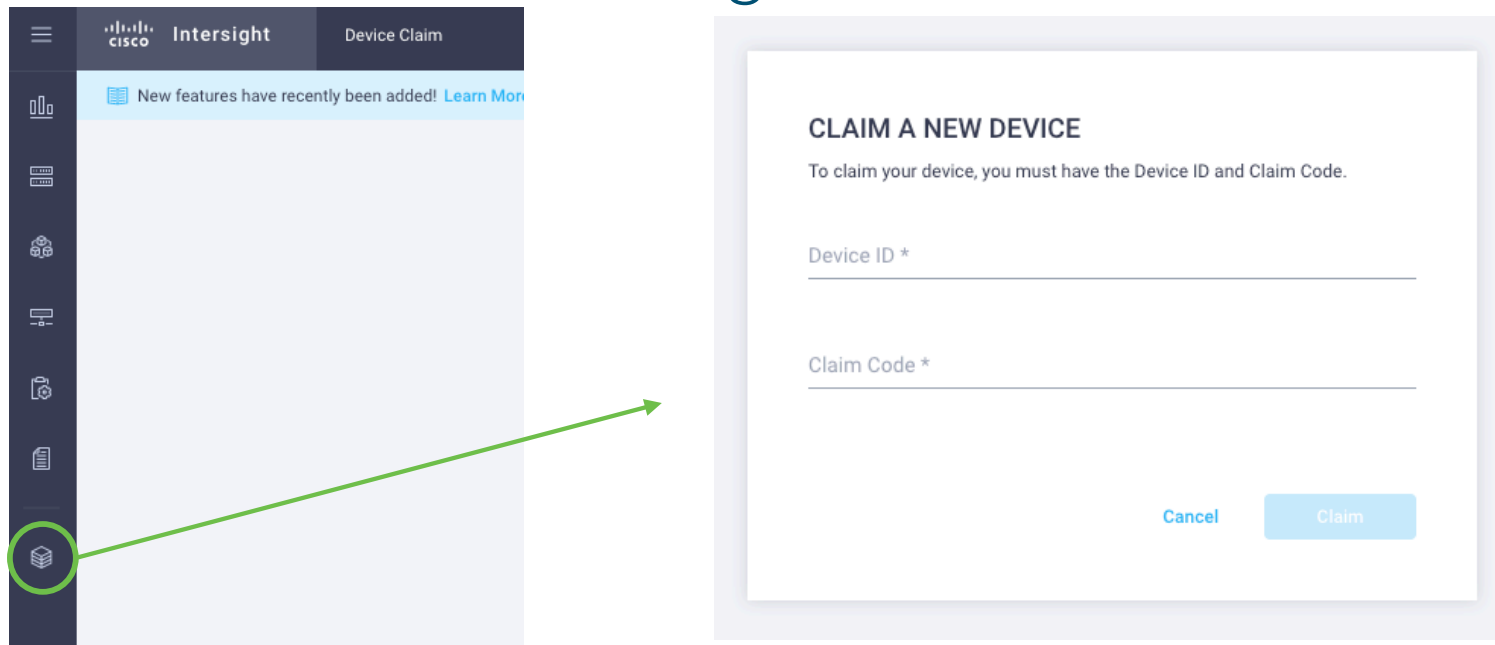
# Cisco Intersight Account Creation



- Users navigate to <https://www.intersight.com> and sign into portal with cisco.com ID/password – required
- Can create new account or sign into existing account
- Existing account accessed with account number
- New accounts created with device ID / claim code (IMC/UCSM/HX Cluster) – must accept offer agreement first
- Must claim a single device to create account



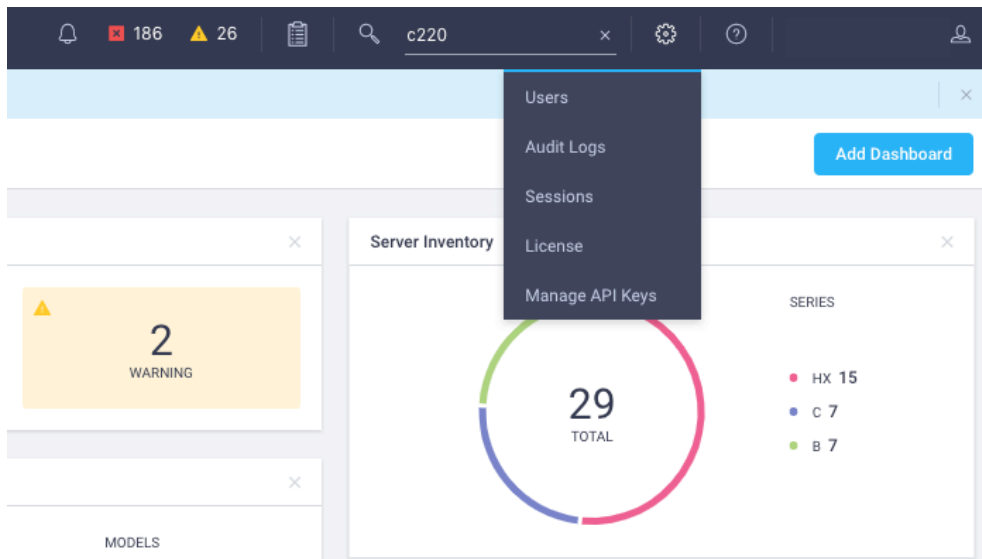
# Cisco Intersight Device Claim



- Additional devices can be claimed from Devices tab – each device has a unique device ID and claim code
- Devices must be running supported firmware version that includes Intersight Device Connector
- **??? List of FW versions (think there is a slide for this)**
- Devices are claimed one at a time, bulk claim is a work in progress

# Cisco Intersight Account Settings

# Cisco Intersight Account Settings



- Actions available from account settings tab
  - User List / adding new users – admin/read-only
  - Audit logs across appliance
  - Active user sessions
  - Licensing
  - Manage API keys

# Server Policies and Profiles

# Cisco Intersight Server Policies Overview

- Individual Server policies are created within the policies tab
- Policies can also be created on the fly when creating a Server Profile
- Available server policies
  - LDAP policy
  - Serial Over LAN Policy
  - NTP Policy
  - BIOS Policy
  - Disk Group Policy (coming soon)
  - Storage Policy (coming soon)
  - Network Connectivity Policy
  - Virtual KVM Policy
  - SMTP Policy
  - SNMP Policy (coming soon)
  - IPMI Over LAN Policy
  - SSH Policy
  - Local User Policy
  - Precision Boot Order Policy
- Server Policies must be assigned to Server Profile before they can be associated with a server and deployed

# Cisco Intersight Server Profiles Overview

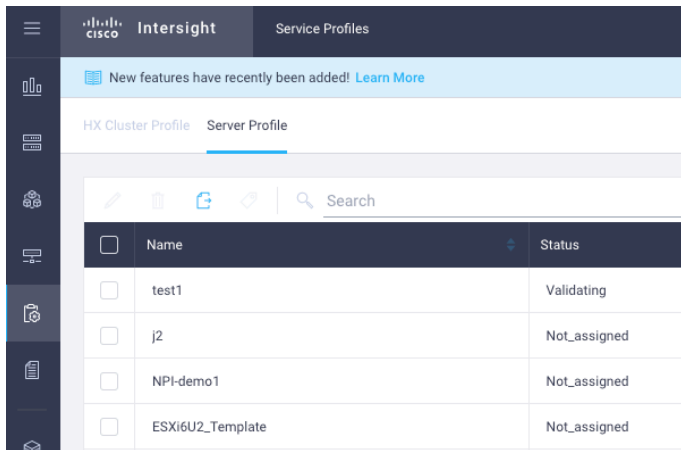
- Individual Server profiles are created within the Profiles tab
- Users select desired policies to include in profile
- Users can also create new policies within profile setup
- A profile can only be assigned to a single server
- Profiles can be cloned and assigned to additional endpoints
- Profiles can be exported to CSV file and tagged for better organization
- Profile summary page will show list of profiles, status and the endpoint they are associated with

The screenshot displays the Cisco Intersight web interface. The top navigation bar includes the Cisco Intersight logo and the 'Service Profiles' tab. A notification banner at the top states 'New features have recently been added! Learn More'. Below the navigation bar, there are tabs for 'HX Cluster Profile' and 'Server Profile', with 'Server Profile' being the active tab. A 'Create Profile' button is located in the top right corner of the main content area. The main content area features a table with the following columns: Name, Status, Server, Server Health, and Last Update. The table contains two rows of data. The first row shows 'Demo-Profile\_1' with a status of 'Ok', assigned to server 'C220-WZP21330G65', with a health status of 'Ok' (indicated by a green checkmark), and updated '25 minutes ago'. The second row shows 'Demo-Profile' with a status of 'Not Assigned', no server assigned, and updated '30 minutes ago'. The table has a search bar and pagination controls at the bottom, showing '25 Rows' and '1 - 2 of 2'.

Name	Status	Server	Server Health	Last Update
Demo-Profile_1	Ok	C220-WZP21330G65	Ok	25 minutes ago
Demo-Profile	Not Assigned			30 minutes ago

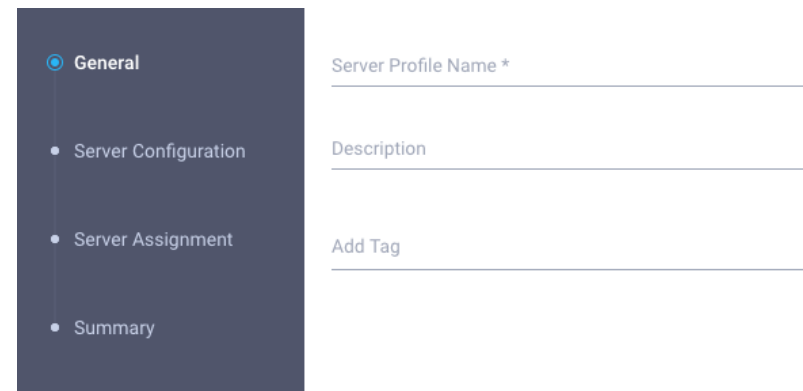
# Cisco Intersight – Creating a Server Profile

- Navigate to Profiles tab, and select Server Profiles



	Name	Status
<input type="checkbox"/>	test1	Validating
<input type="checkbox"/>	j2	Not_assigned
<input type="checkbox"/>	NPI-demo1	Not_assigned
<input type="checkbox"/>	ESXi6U2_Template	Not_assigned

- Click “Create Profile” and provide profile name and description (if desired)



- General
- Server Configuration
- Server Assignment
- Summary

Server Profile Name \*

Description

Add Tag

# Cisco Intersight – Creating a Server Profile (cont'd)

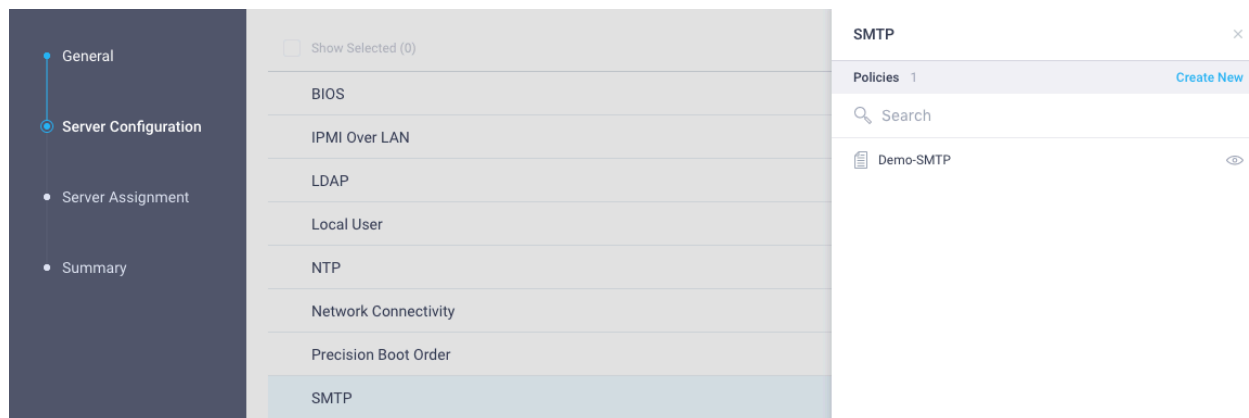
- Select desired policies to include in profile



The screenshot shows the 'Server Configuration' tab selected in the left sidebar. The main area displays a list of available policies under the heading 'Show Selected (0)'. The policies listed are BIOS, IPMI Over LAN, LDAP, Local User, NTP, and Network Connectivity. Each policy has a document icon to its right.

Show Selected (0)	
BIOS	
IPMI Over LAN	
LDAP	
Local User	
NTP	
Network Connectivity	

- Available Policies can be expanded



The screenshot shows the 'Server Configuration' tab selected in the left sidebar. The main area displays a list of available policies under the heading 'Show Selected (0)'. The policies listed are BIOS, IPMI Over LAN, LDAP, Local User, NTP, Network Connectivity, Precision Boot Order, and SMTP. The SMTP policy is highlighted in blue. To the right of the list, a modal window titled 'SMTP' is open, showing a search bar and a list of policies. The list contains one entry: 'Demo-SMTP' with an eye icon to its right.


Show Selected (0)	
BIOS	
IPMI Over LAN	
LDAP	
Local User	
NTP	
Network Connectivity	
Precision Boot Order	
SMTP	

**SMTP** ×  
**Policies** 1 [Create New](#)  
  

Demo-SMTP



# Cisco Intersight – Creating a Server Profile (cont'd)

- View properties for chosen policy by clicking on the  icon


< Demo-SMTP ×

**General**

Name	Demo-SMTP
Usage	0

**Main**


Enable SMTP	true
Minimum Severity	warning
SMTP Port	25
Mail Alert Recipients	user1@cisco.com
SMTP Server Address	172.25.234.127

- 
- Can also create new policy within profile setup

SMTP ×

Policies 1 Create New

 Search

 Demo-SMTP 

# Cisco Intersight – Creating a Server Profile (cont'd)

- Assign Profile to Server (can assign later as well)

The screenshot shows the 'Server Assignment' step in the Cisco Intersight configuration process. On the left, a sidebar contains a navigation menu with 'General', 'Server Configuration', 'Server Assignment' (selected), and 'Summary'. The main area has two radio buttons: 'Assign Server' (selected) and 'Assign Server Later'. Below them is a 'Show Assigned' toggle switch. A table displays a list of servers with columns for Health, Name, Model, and Management IP. The table shows 3 rows of data. At the bottom right, there are pagination controls showing '1 - 3 of 3'.

Health	Name	Model	Management IP
✓	C220-WZP21330G65	UCSC-C220-M5L	10.29.131.133
✗	C240-WZP21340YNQ	UCSC-C240-M5SX	10.29.131.134
✗	C240-WZP21380035	UCSC-C240-M5SX	10.29.131.135

- Review then Save and Deploy Profile

The screenshot shows the 'General' configuration page for a Server Profile. On the left, a sidebar contains a navigation menu with 'General' (selected), 'Server Configuration', 'Server Assignment', and 'Summary'. The main area displays the following information:

- General**
- Server Profile Name: Demo-profile2
- Assigned Server: C240-WZP21380035
- Management IP: 10.29.131.135
- Server Profile Status: Not Deployed
- Management Platform: IMC

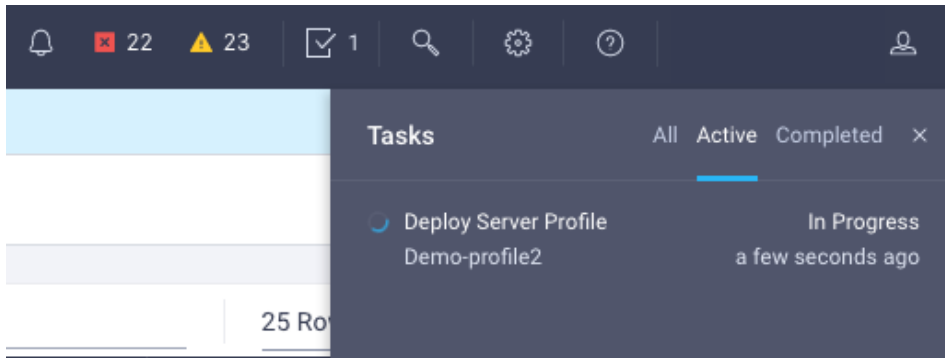
Below this information, there is a section for 'Configuration' and 'Errors (0)'. The 'Configuration' section is expanded, showing the following settings:

- BIOS: Demo-BIOS
- NTP: Demo-NTP
- SMTP: Demo-SMTP

At the bottom of the page, there are three buttons: 'Save & Close', 'Previous', and 'Save & Deploy'.

# Cisco Intersight – Creating a Server Profile (cont'd)

- View running tasks in task list

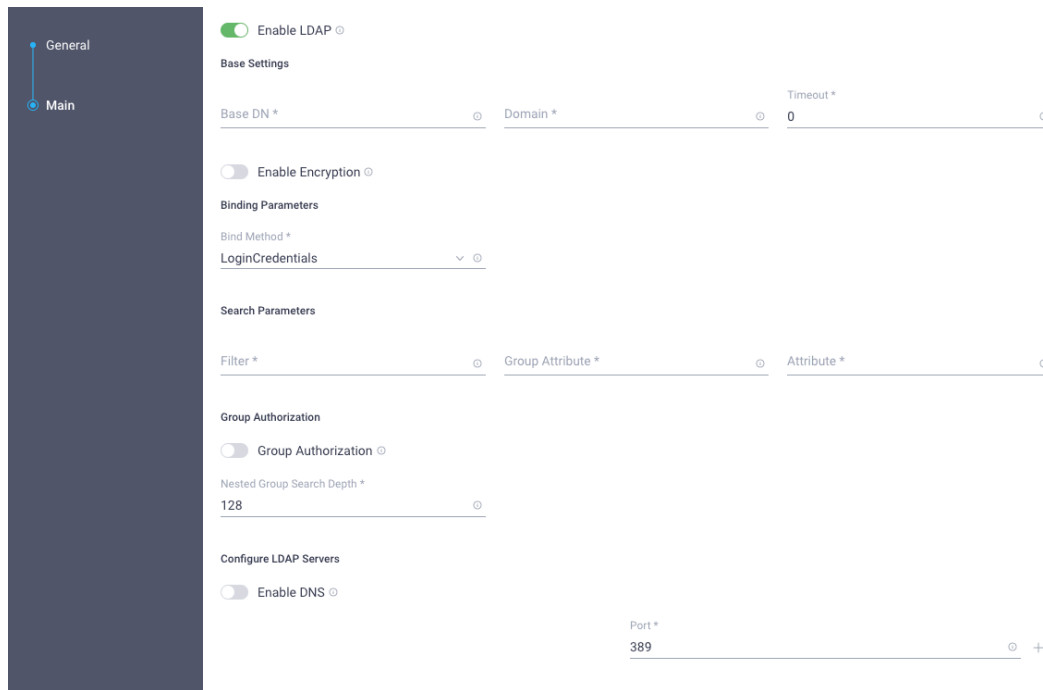


- Click on desired task for more details

New features have recently been added! <a href="#">Learn More</a>				
Details		Execution Flow		Results
Status	Success <span>✓</span>	Progress <div><div></div></div> 100%		
Name	Deploy Server Profile	Deploy NTP Policy <span>✓</span>		<span>✓</span> Deploy NTP Policy Completed
Source Name	Demo-profile2	Deploy SMTP Policy <span>✓</span>		<span>✓</span> Deploy SMTP Policy Completed
Source Type	Server Profile	Deploy BIOS Policy <span>✓</span>		<span>✓</span> Deploy BIOS Policy Completed
Target Name	UCSC-C240-M5SX	Validate SMTP Policy <span>✓</span>		<span>✓</span> Validate SMTP Policy Completed
Target Type	Rack Server	Validate NTP Policy <span>✓</span>		<span>✓</span> Validate NTP Policy Completed
Start Time	Jan 25, 2018 8:22 AM	Validate BIOS Policy <span>✓</span>		<span>✓</span> Validate BIOS Policy Completed
End Time	Jan 25, 2018 8:23 AM			
Duration	00:01:12			

# Server Policies

# Intersight Server Policies – LDAP Policy



**General**

**Main**

☒ Enable LDAP

**Base Settings**

Base DN \* Domain \* Timeout \*

☐ Enable Encryption

**Binding Parameters**

Bind Method \* LoginCredentials

**Search Parameters**

Filter \* Group Attribute \* Attribute \*

**Group Authorization**

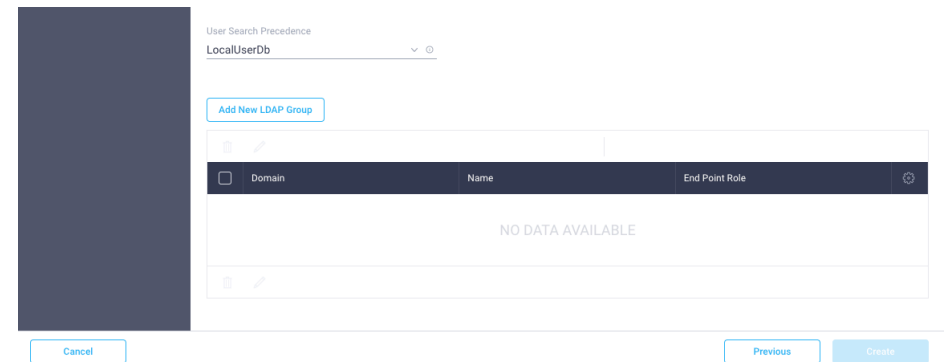
☐ Group Authorization

Nested Group Search Depth \* 128

**Configure LDAP Servers**

☐ Enable DNS

Port \* 389



User Search Precedence LocalUserDb

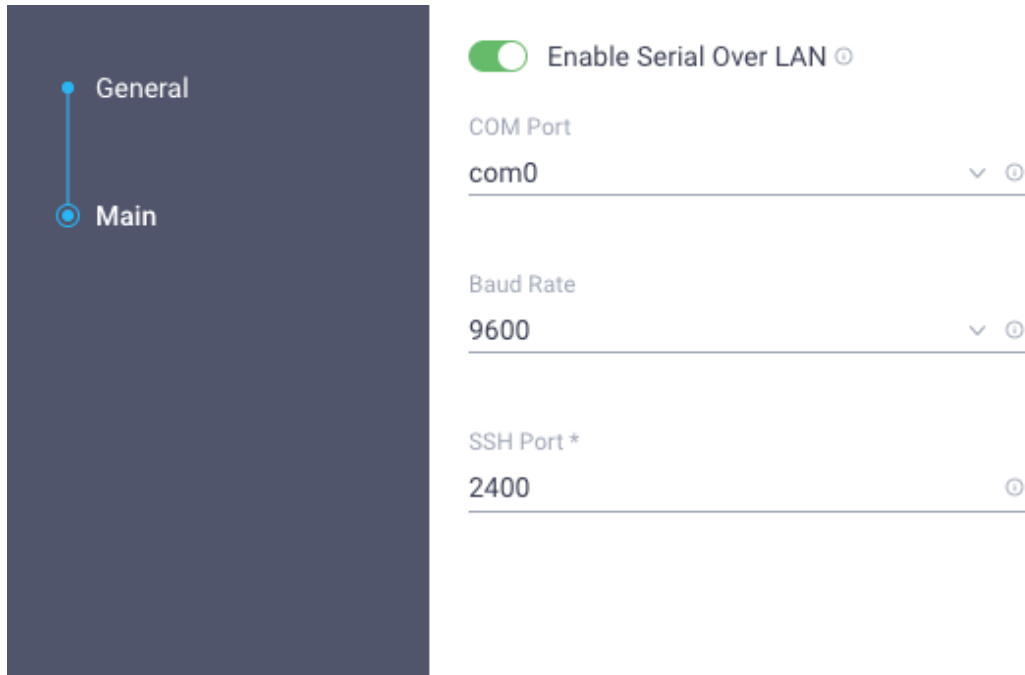
Add New LDAP Group

Domain	Name	End Point Role
NO DATA AVAILABLE		

Cancel Previous Create

- LDAP Policy includes the following
  - Base Settings
  - Encryption settings (if desired)
  - Search parameters
  - Group Authorization and search depth
  - LDAP Server / DNS config
  - Ability to create LDAP Groups

# Intersight Server Policies – Serial Over LAN Policy

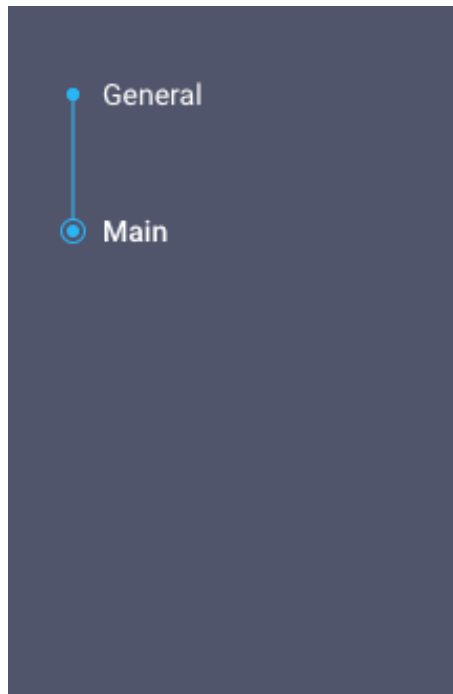


The screenshot shows the 'Main' configuration page for a policy. On the left, a dark sidebar contains a vertical menu with 'General' and 'Main' options. 'Main' is selected, indicated by a blue dot and a line. The main content area is white and contains the following settings:

- Enable Serial Over LAN**: A green toggle switch is turned on, followed by the text 'Enable Serial Over LAN' and a help icon (i).
- COM Port**: A dropdown menu showing 'com0' with a downward arrow and a help icon (i).
- Baud Rate**: A dropdown menu showing '9600' with a downward arrow and a help icon (i).
- SSH Port \***: A text input field showing '2400' with a help icon (i).

- Serial Over LAN enables input/output of serial port on managed endpoint to be redirected via an SSH session over IP
- Allows users to reach host console via CIMC

# Intersight Server Policies – NTP Policy



☒ Enable NTP ⓘ

NTP Server ⓘ ⓘ

NTP Server ⓘ ⓘ

NTP Server ⓘ ⓘ

NTP Server ⓘ ⓘ

- Cisco IMC synchronizes time with the host by default
- Network Time Protocol (NTP) allows the Cisco IMC to sync the time with an NTP Server
- Must enable NTP and specify IP/DNS info for at least one NTP server (max of 4 servers allowed)

# Intersight Server Policies – BIOS Policy

The screenshot shows the Intersight BIOS Policy configuration page. On the left is a dark sidebar with a navigation menu containing 'General' and 'Policy Details', with 'Policy Details' being the active selection. The main content area has a yellow warning banner at the top stating 'The BIOS settings will be applied only on next host reboot.' Below this is a list of BIOS categories: 'Input-Output', 'LOM and PCIe Slots Configuration', 'Memory' (which is expanded), 'Power/Performance', 'Processor', 'Security', 'Serial Configuration', and 'Server Management'. The 'Memory' section is open, showing three settings: 'Above 4G Decoding' set to 'platform-default', 'NUMA' set to 'platform-default', and 'SelectMemory RAS configuration' set to 'platform-default'. Each setting has a dropdown arrow and a refresh icon.

General

Policy Details

⚠ The BIOS settings will be applied only on next host reboot.

- + Input-Output
- + LOM and PCIe Slots Configuration
- Memory
  - Above 4G Decoding: platform-default
  - NUMA: platform-default
  - SelectMemory RAS configuration: platform-default
- + Power/Performance
- + Processor
- + Security
- + Serial Configuration
- + Server Management

- BIOS policy allows users to set complete set of BIOS tokens across an endpoint
- All tokens use platform-defaults for desired endpoint unless otherwise specified
- BIOS Policy works in forgiveness mode
  - any tokens that are not found or applicable to chosen endpoint are ignored



# Intersight Server Policies – Disk Group Policy

The screenshot shows the 'Main' configuration page for a 'Disk Group Policy'. On the left is a dark sidebar with 'General' and 'Main' tabs, where 'Main' is selected. The main content area is titled 'Virtual Drive Configuration' and includes a 'RAID Level' dropdown set to 'Raid1' and a 'Number of Slots per Span' input set to '2'. Below this is the 'Local Disk Configuration' section, which contains a 'Disk Group (Span 0)' header, two 'Slot Number \*' input fields (both marked 'Required'), a '+ Dedicated Hot Spares' section with a toggle switch, and two other toggle switches: 'Enable Disk Encryption' (with a descriptive note) and 'Set Disks in JBOD state to Unconfigured Good' (with a descriptive note).

Coming soon!!!!

- Disk Group Policy allows users to carve out disk groups to be used with virtual drives
- Disk groups can be configured to use encryption when SEDs are used
- JBOD disks can be set to Unconfigured Good
- Disks can also be assigned as dedicated hot spares
- Selected RAID level will populate minimum number of disks required for group
- Disk Group policy cannot be deployed by itself, must be assigned to storage policy

# Intersight Server Policies – Storage Policy

Coming soon!!!!

The screenshot displays the 'Drive Configuration' section of the Intersight Server Policies interface. The 'Main' tab is selected, showing options for 'Enable Drive Security' (disabled), 'Global Hot Spares' (disabled), 'Unused Disks State' (UnconfiguredGood selected), 'Secure Drive' (disabled), and 'Retain Virtual Drives' (enabled). A green arrow points from the 'Add Virtual Drives' button in the 'Drive Configuration' section to the 'Add Virtual Drives' dialog box on the right.

**Add Virtual Drives**

Virtual Drive Name \*  Size \*

Disk Group \*  Access Policy

Read Policy  Write Policy

IO Policy  Drive Cache

☐ Expand to Available ☐ Set as Boot Drive

- Allows users enable drive security (disabled by default)
- Configure disks to be used as global hot spares (across RAID groups)
- Configure unused disks as UG/JBOD
- Create virtual drives with desired Disk Group(s)
- Can expand virtual drive to use all available space, and also set virtual drive as boot drive
- Retain existing virtual drives if desired

# Intersight Server Policies – Network Connectivity Policy

**General**

**Policy Details**

**Common Properties**

☐ Enable Dynamic DNS ⓘ

**IPv4 Properties**

☐ Obtain IPv4 DNS Server Addresses from DHCP ⓘ

Preferred IPv4 DNS Server \* ⓘ

Alternate IPv4 DNS Server ⓘ

☐ Enable IPv6 ⓘ

- Additional Cisco IMC connectivity options
  - Configure Dynamic DNS
  - Enable IPv6 (Static or DHCP)
  - Enable VLAN

# Intersight Server Policies – Virtual KVM Policy



General

Main

☒ Enable Virtual KVM ⓘ

Max Sessions \*

4 ⓘ

Remote Port \*

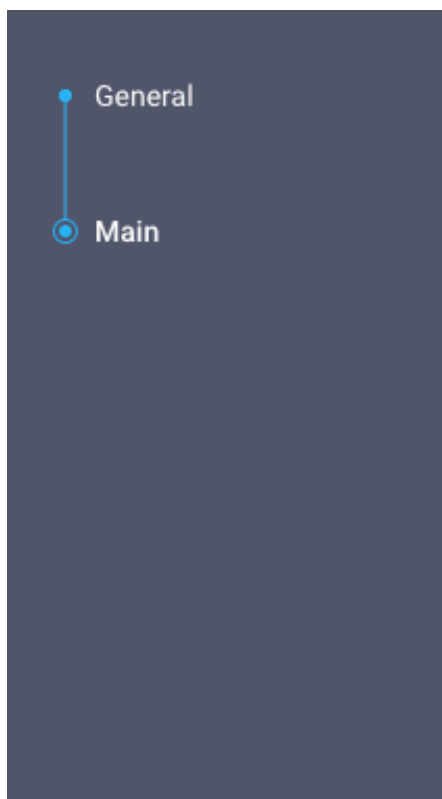
2068 ⓘ

☒ Enable Video Encryption ⓘ

☒ Enable Local Server Video ⓘ

- Configure max # of vKVM sessions (4 is max allowed)
- Remote port (default is 2068)
- Video Encryption / Local Server Video (both enabled by default)

# Intersight Server Policies – SMTP Policy



☒ Enable SMTP ⓘ

SMTP Server Address ⓘ

SMTP Port  
25 ⓘ

Minimum Severity  
critical ▼ ⓘ

Mail Alert Recipients \* ⓘ +

- Simple Mail Transfer Protocol (SMTP)
- Allows for email-based notification of server faults to recipients without depending on SNMP
- System uses SMTP to send server faults as email alerts for the configured SMTP server

# Intersight Server Policies – SNMP Policy

Coming soon!!!!

**General**

**Main**

☒ Enable SNMP

SNMP Port: 161

Access Community String:

SNMP Community Access: Disabled

Trap Community String:

System Contact \*:

System Location \*:

SNMP Engine Input ID:

**SNMP Users**

[Add SNMP User](#)

<input type="checkbox"/>	Name	Security Level	Auth Type	Privacy Type
NO DATA AVAILABLE				

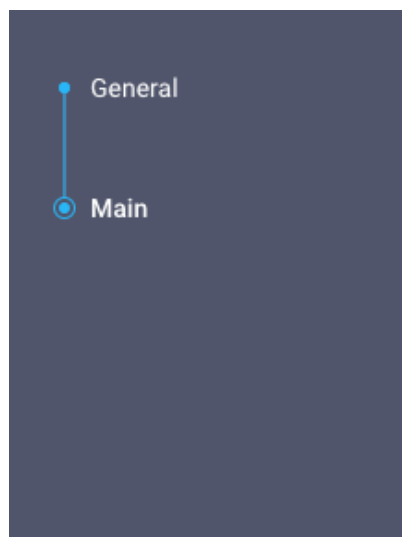
**SNMP Trap Destinations**

[Add SNMP Trap Destination](#)

<input type="checkbox"/>	Enable	SNMP Version	Trap Type	User	Destination Address	Port
NO DATA AVAILABLE						

- Simple Network Management Protocol (SNMP)
- Allows users to view server configuration/status and sends fault/alert information in the form of SNMP traps
- Users can configure SNMP as desired – some parameters are optional
- Can add SNMP users with desired security level
- SNMP traps can be configured as SNMP v2/v3

# Intersight Server Policies – IPMI over LAN Policy



☒ Enable IPMI Over LAN ⓘ

Privilege Level

admin

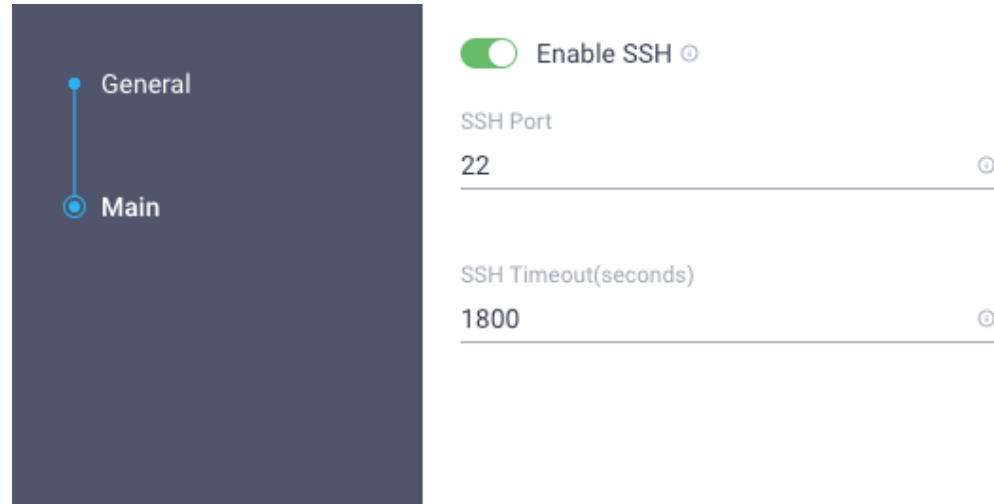


Encryption Key



- Intelligent Platform Management Interface (IPMI)
- Allows server Operating System to access system details via Cisco IMC
- Users can query system for overall health/sensor data
- Power operations for system

# Intersight Server Policies – SSH Policy



General

Main

☒ Enable SSH ⓘ

SSH Port

22 ⓘ

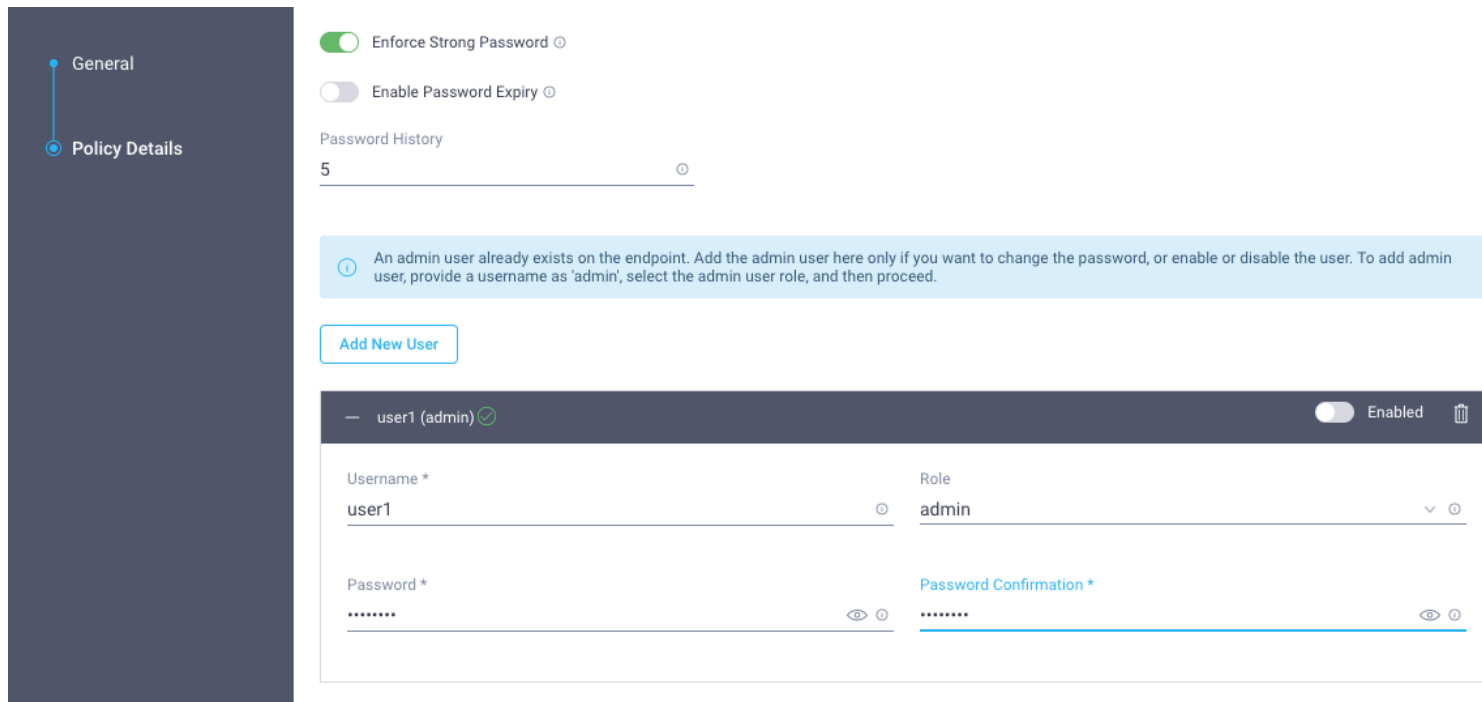
SSH Timeout(seconds)

1800 ⓘ

- Secure Socket Shell (SSH)
- Allows communication with the Cisco IMC over SSH port (CLI)



# Intersight Server Policies – Local User Policy



General

Policy Details

☒ Enforce Strong Password ⓘ

☐ Enable Password Expiry ⓘ

Password History

5 ⓘ

ⓘ An admin user already exists on the endpoint. Add the admin user here only if you want to change the password, or enable or disable the user. To add admin user, provide a username as 'admin', select the admin user role, and then proceed.

Add New User

— user1 (admin) ✓ Enabled ⓘ

Username \*

user1 ⓘ

Role

admin ⓘ

Password \*

..... ⓘ

Password Confirmation \*

..... ⓘ

- Local admin user hidden from user list by default – can add user “admin” again if wishing to disable user or change password
- User roles are admin, user, read-only
- Configure password expiry details if desired
- Configure password history

# Intersight Server Policies – Precision Boot Order Policy

The screenshot displays the 'Policy Details' tab for a Precision Boot Order Policy. On the left, a sidebar shows 'General' and 'Policy Details' with 'Policy Details' selected. The main area is titled 'Boot Mode' and shows 'Configured Boot Mode' as 'Legacy' (selected) with a radio button, and 'Unified Extensible Firmware Interface (UEFI)' as an option. Below this is an 'Add Boot Device' button. The boot devices are listed in a table:

Device Name *	MAC Address	Port	Slot
pxe-lom0		0	L
uefi-shell			
HDD			MRAID

Each device entry has a toggle switch set to 'Enabled' and icons for delete, up, and down arrows.

- Configure legacy vs UEFI boot mode (including UEFI secure boot)
- Add boot devices and configure boot order
- Enable / disable particular devices

# Firmware Upgrades

# Intersight – Firmware Upgrades

...				
Search				
<input type="checkbox"/>	Power On	Health	Management IP	Model
<input type="checkbox"/>	Power Off	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Power Cycle	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Shut Down OS	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Hard Reset	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Reboot IMC	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Turn On Locator	✓	Unavailable	UCSB-B200-M4
<input type="checkbox"/>	Turn Off Locator	✓	Unavailable	UCSC-C220-M5SX
<input type="checkbox"/>	Upgrade Firmware	✗	172.22.249.75	UCSC-C220-M5SX
<input type="checkbox"/>	D23-UCS1-1-8	✓	10.29.131.185	UCSB-B200-M3
<input type="checkbox"/>	D23-UCS1-1-7	✓	10.29.131.185	UCSB-B200-M3
<input type="checkbox"/>	D23-UCS1-1	⚠	10.29.131.185	UCSC-C240-M5S
<input checked="" type="checkbox"/>	C240-WZP21340YNQ	✗	10.29.131.134	UCSC-C240-M5SX

## Upgrade Firmware

Network Share Utility Storage

NFS CIFS HTTP/S

Remote IP \*

Remote Share \*

Remote File Name \*

Firmware will be installed and the device will be rebooted immediately.

Cancel Upgrade

## Upgrade Firmware

Network Share Utility Storage

Utility storage includes FlexUtil cards for the M5 servers.

Firmware Version \*  
3.1(2b)

Image Name ucs-c240m5-huu-3.1.2b.iso

Release Date October 5, 2017

Size 487 MB

Supported Models UCSC-C240-M5S, UCSC-C240-M5L, UCSC-C240-M5SX, UCSC-C240-M5SN

Description Cisco UCS Host Upgrade Utility

On clicking upgrade below, firmware download to FlexUtil will begin immediately. Installation will start on the first boot after the download has successfully completed. Installation can be initiated once the server Firmware Status is "Ready for Upgrade" by performing a Host Reboot on the server.

Cancel Upgrade

- Firmware upgrades available via Network Share or Utility Storage
- Network upgrades reboot host immediately and begin upgrade
- Utility Storage upgrades are staged – firmware is downloaded and then upgrades on next reboot

