Cisco Intersight Policies

Executive summary

This document is for individuals who are new to Cisco Intersight® and are looking for a summary and definitions of the domain, chassis, and server policies available in Intersight. Information is broken down by policies for servers using Intersight Managed Mode (IMM) and those using Intersight Standalone Mode (ISM). It includes a list of the minimum recommended policies to deploy a server. Detailed instructions on how to use policies are available in the Additional Resources section.

This document is a complementary piece to "Stateless Computing with Cisco UCS® and Cisco Intersight," which describes the core concepts of stateless computing and how policies, profiles, and templates form the foundation of efficient and secure server management.

Cisco Intersight policies are configurations that define specific settings and behaviors for various components within IT infrastructure. Policies help enforce secure deployments and ensure consistency across server configurations. Along with fabric interconnects, profiles, and templates, they are a foundational element of stateless computing and enable flexible and dynamic server management.

Domain policies

In Cisco Intersight, a domain policy allows you to configure various parameters for Cisco Unified Computing System™ (Cisco UCS) fabric interconnects, including port configuration, network control settings, and VLAN and VSAN settings. A domain policy can be assigned to any number of domain profiles to provide a configuration baseline.

- **Certificate Management Policy**
  Allows you to specify the certificate details for an external certificate and attach the policy to server profile or to domain profile. Intersight currently supports Root CA and IMC certificates.
- **Ethernet Network Control Policy**
  Configures the network control settings for a UCS domain; applicable only for the appliance ports defined in a port policy.
- **Ethernet Network Group Policy**
  Configures the allowed VLANs and native VLAN for Ethernet uplink ports, Ethernet uplink port channels, appliance ports, or appliance port channels. This policy is only attached to the domain profile if using a Disjoint Layer-2 (DJL2) use case or an appliance-port use case. If not using an appliance-port use case (and if uplinking Ethernet to a single Layer-2 broadcast domain), then this policy will not be applied to a domain profile. It is most used for disjoint Layer-2 use cases.
- **Flow Control Policy**
  Configures the priority flow control for ports and port channels to enable the no-drop behavior for the CoS defined by the System QoS Policy and an Ethernet QoS policy.

- **Link Aggregation Policy**
  Used to configure link-aggregation properties. Combines multiple network connections in parallel to increase throughput and provide redundancy. Link aggregation is achieved using port channels; a port channel is an aggregation of multiple physical interfaces into a logical interface.
- **Link Control Policy**
  Enables configuration of link control administrative state and configuration (normal or aggressive) mode for ports.
- **Multicast Policy**
  Configures Internet Group Management Protocol (IGMP) snooping and IGMP querier. Each VLAN added in the VLAN policy must have a Multicast policy configured for it in Intersight.
- **Network Connectivity Domain (DNS) Policy**
  Specifies the DNS server settings for IPv4 and IPv6 for the fabric interconnects.
- **NTP (Network Time Protocol) Policy**
  Enables the NTP service to configure a Cisco UCS system that is managed by Cisco Intersight to synchronize the time with an NTP server. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco Intersight configures the NTP details on the endpoint.
- **Port Policy**
  Used for configuring the port parameters such as unified ports that carry Ethernet or Fibre Channel traffic, port roles and speed.
- **SNMP (Simple Network Management Protocol) Policy**
  Configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. This policy supports SNMP versions such as SNMPv1, SNMPv2 (includes v2c), and SNMPv3. Any existing SNMP users or SNMP traps configured previously on the managed devices are removed and replaced with users or traps that you configure in this policy.
- **Switch Control Policy**
  Supports VLAN port count optimization, configuring MAC address aging time, and configuring link-control global settings.
- **Syslog Policy**
  Defines the minimum severity as the logging level from an endpoint. The policy also defines the target destination to store syslog messages, and the hostname or IP address, the port information, and the communication protocol for the remote logging servers.
- **System QoS Policy**
  Assigns a system class to the outgoing traffic; determines the quality of service for the outgoing traffic. All domain profiles must include this policy for successful deployment; may be default settings.
- **VLAN Policy**
  Must include all the VLANs communicating between the UCS domain fabric and upstream switching. Cannot add a server policy (Ethernet Network Group) unless the VLAN is already deployed in the VLAN Policy and domain profile.
- **VSAN Policy**
  Partitions the Fibre Channel fabric into one or more zones. Each zone defines the set of Fibre Channel initiators and Fibre Channel targets that can communicate with each other in a VSAN.

Server policies

Server policies are used to define and manage configurations for Cisco UCS servers. These policies can include settings for server BIOS, local disk configurations, boot security, and maintenance windows, among others. Server policies enhance security by enforcing predefined settings and help ensure consistency, efficiency, and flexibility in server management by allowing administrators to apply the same configuration settings across multiple servers. Server configurations only change if the Intersight administrator updates or changes policies.

Policies are available for the two management modes in Intersight: Intersight Managed Mode (IMM) and Intersight Standalone Mode (ISM). IMM is used for Cisco UCS fabric interconnected systems, and ISM is used for servers not connected to UCS fabric interconnects. Note that Cisco C-Series rack mount servers can be configured as either IMM or ISM. Some of the sever policies are specific to IMM, and others are specific to ISM exclusively. The following summary aids in identifying them so you can ensure you are working with the correct policies.

Server policies for Intersight Managed Mode (IMM)

Minimum policies to deploy a server

- **BIOS Policy**
  Automates the configuration of BIOS settings on servers. You can create one or more BIOS policies that contain a specific grouping of BIOS settings, matching the needs of a server or a set of servers. If you do not specify a BIOS policy for a server, the BIOS settings will default to a set of values for a brand-new bare metal server or to a set of values previously configured using Cisco IMC. If a BIOS policy is specified, its values replace any previously configured values on the server.
- **Boot Order Policy**
  Configures the linear ordering of devices and enables you to change the boot order and boot mode. You can also add multiple devices under various device types, rearrange the boot order, and set parameters for each boot device type.
- **Ethernet Adapter Policy**
  Governs the host-side behavior of the adapter, including how the adapter handles traffic. For each VIC virtual Ethernet interface, you can configure various features, such as Virtual Extensible LAN (VXLAN), Network Virtualization using Generic Routing Encapsulation (NVGRE), Accelerated Receive Flow Steering (ARFS), interrupt settings, and TCP offload settings.
- **Ethernet Network Control Policy**
  This policy can be configured on each vNIC of the LAN Connectivity policy and configures how each vNIC is discoverable on the network using Cisco Discovery Protocol (CDP) and/or Link Level Discovery Protocol (LLDP). Additional settings include MAC registration mode, MAC security, and actions taken on uplink fail behavior.
- **Ethernet Network Group Policy**
  Enables you to manage settings for VLANs on each vNIC on a UCS server. These settings include defining which VLANs are allowed, designating a native VLAN, and specifying an optional QinQ VLAN.
- **IMC Access Policy**
  Allows you to configure your network and associate an IP address from an IP pool with a server. In-band IP address, out-of-band IP address, or both in-band and out-of-band IP addresses can be configured using an IMC Access policy and are supported on drive security, SNMP, syslog, and vMedia policies.

- **LAN Connectivity Policy**
  Determines the connections and the network communication resources between the server and the LAN on the network. You can specify MAC address pools, or static MAC addresses, to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.
- **Local User Policy**
  Defines local user access to the server. You can create one or more local user policies which contain a list of local users that need to be configured.
- **Storage Policy**
  Allows you to create drive groups and virtual drives, and configure both the storage capacity of a virtual drive and the M.2 RAID controllers.
- **Virtual KVM Policy**
  The KVM console is an interface that emulates a direct keyboard, video, and mouse (KVM) connection to the server. It allows you to control the server from a remote location and to map physical locations to virtual drives that can be accessed by the server during this KVM session. Enables specific groupings of virtual KVM properties; lets you specify the number of allowed concurrent KVM sessions, port information, and video encryption options.
- **Virtual Media (vMedia) Policy**
  Enables you to install an operating system on the server using the KVM console and virtual media, mount files to the host from a remote file share, and enable virtual media encryption. You can create one or more virtual media policies, which can contain virtual media mappings for different OS images, and configure up to two virtual media mappings, one for ISO files through CDD and the other for IMG files through HDD.

Optional server policies based on use case

- **Certificate Management Policy**
  Allows you to specify the certificate details for an external certificate and attach the policy to a server profile or to a domain profile. Intersight currently supports Root CA and IMC certificates.
- **Drive Security Policy**
  Enables you to configure security keys either locally or remotely using a KMIP server.
- **Ethernet QoS Policy**
  Assigns a system class to the outgoing traffic for a vNIC. This system class determines the quality of service for the outgoing traffic. For certain adapters, you can also specify additional controls such as burst and rate on the outgoing traffic.
- **FC Zone Policy**
  Allows you to set up access control between hosts and storage devices. This policy is only used for direct attached storage use cases with the fabric interconnect setup in FC-switching mode.
- **Fibre Channel Adapter Policy**
  Governs the host-side behavior of the adapter, including how the adapter handles traffic. You can enable FCP error recovery, change the default settings of queues, and interrupt handling for performance enhancement.
- **Fibre Channel Network Policy**
  Governs the Virtual Storage Area Network (VSAN) configuration for the virtual host-bus adapter (vHBA) interfaces in the SAN Connectivity Policy.

- **Fibre Channel QoS Policy**
  Assigns a system class to the outgoing traffic for a vHBA and determines the quality of service for the outgoing traffic. For certain adapters, you can also specify additional controls such as burst and rate on the outgoing traffic.
- **Firmware Policies**
  Allows the designation of a server firmware bundle version to be attached to the server profile and deployed to the server endpoint. When you deploy the server profile, the server firmware is upgraded.
- **IPMI Over LAN Policy**
  Defines the protocols for remote interfacing with a service processor that is embedded in a server platform. The Intelligent Platform Management Interface (IPMI) enables an operating system to obtain information about the system-health and control-system hardware and directs the Cisco IMC to perform the required actions. You can create an IPMI over LAN policy to manage the IPMI messages through Cisco Intersight.
- **iSCSI Adapter Policy**
  Allows you to configure values for TCP connection timeout, DHCP timeout, and the retry count if the specified LUN ID is busy. This policy is used on iSCSI configured vNICs.
- **iSCSI Boot Policy**
  Allows you to initialize the operating system on FI-attached blade and rack servers from a remote disk across a storage area network (SAN). The remote disk, known as the target, is accessed using TCP/IP and iSCSI boot firmware.
- **iSCSI Static Target Policy**
  Allows you to specify the name, IP address, port, and logical unit number of the primary target for iSCSI boot. You can optionally specify these details for a secondary target as well.
- **LDAP Policy**
  Lightweight Directory Access Protocol (LDAP) stores and maintains directory information in a network. When LDAP is enabled, user authentication and role authorization is performed by the LDAP server for user accounts not found in the local user database. You can enable and configure LDAP servers and LDAP groups.
- **Network Connectivity Policy**
  Enables you to configure and assign IPv4 and IPv6 addresses.
- **NTP Policy**
  Enables the NTP service to configure a Cisco UCS system that is managed by Cisco Intersight to synchronize the time with an NTP server. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco Intersight configures the NTP details on the endpoint.
- **Memory Policy**
  Allows you to enable or disable the blocklisting of dual in-line memory modules (DIMMs).
- **Power Policy**
  Enables the configuration of power redundancy, power profiling, and power restoration for servers. The power profiling setting is only applicable to Cisco UCS X-Series servers.
- **SAN Connectivity Policy**
  A storage area network (SAN) connectivity policy determines the network storage resources and the connections between the server and the storage device on the network. This policy enables you to specify WWPN address pools, or a static WWPN address to add a vHBA. Similarly, you can specify a WWNN pool, or a static WWNN address to configure vHBAs that the servers use to communicate with the SAN.

- **Scrub Policy**
  Allows for the BIOS and/or disk to be scrubbed on the server. Occurs when configured and attached to a server profile, and when the server profile is detached from the server.
- **SD Card Policy**
  Configures the Cisco FlexFlash and FlexUtil secure digital (SD) cards for the Cisco UCS C-Series Standalone M4 and M5 servers, and Cisco UCS C-Series M5 servers in a Cisco Intersight-managed fabric interconnect domain. This policy specifies details of virtual drives on the SD cards. You can configure the SD cards in operating system only, utility only, or operating system + utility modes.
- **Serial Over LAN Policy**
  Enables the input and output of the serial port of a managed system to be redirected over IP. You can create one or more serial over LAN policies which contain a specific grouping of serial over LAN attributes that match the needs of a server or a set of servers.
- **Server Pool Qualification Policy**
  Supports setting domain, server, tag, and hardware qualifiers to logically auto-populate the servers into a server resource pool that can be assigned to the server profile and/or server profile template.
- **SNMP Policy**
  Configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. This policy supports SNMP versions such as SNMPv1, SNMPv2 (includes v2c), and SNMPv3. Any existing SNMP users or SNMP traps configured previously on the managed devices are removed and replaced with users or traps that you configure in this policy. If you have not added any users or traps in the policy, the existing users or traps on the server are removed.
- **Syslog Policy**
  Defines the logging level (minimum severity) to report for a log file collected from an endpoint, the target destination to store the syslog messages, and the hostname/IP address, port information, and communication protocol for the remote logging server(s).
- **Thermal Policy**
  Sets the fan-speed modes on Cisco UCS X-Series servers.

Server policies for Intersight Standalone Mode (ISM)

Cisco® rack mount servers operating in Intersight Standalone Mode—connected directly to Intersight without fabric interconnects—use the following policies:

BIOS	Fibre Channel QoS	SD Card
Boot Order	Firmware	Serial Over LAN
Certificate Management	IPMI Over LAN	SNMP
Drive Security	LAN Connectivity	Storage
Ethernet Adapter	Local User	Syslog
Ethernet QoS	Memory	Thermal
Fibre Channel Adapter	Power	Virtual KVM
Fibre Channel Network	SAN Connectivity	Virtual Media

In addition, the following server policies are applicable only to ISM-managed servers:

- **Adapter Configuration**
  Configures the Ethernet and Fibre-Channel settings for the virtual interface card (VIC) adapter.

- **Device Connector Policy**
  Lets you choose the configuration from Intersight only option to control configuration changes allowed in Cisco IMC. The configuration from Intersight only option is enabled by default.
- **Ethernet Network Policy**
  Enables the configuration of VLAN mode (access or trunk), the QinQ tagging option, and the default native VLAN.
- **LDAP (standalone and domain)**
  Lightweight Directory Access Protocol (LDAP) stores and maintains directory information in a network. When LDAP is enabled, user authentication and role authorization are performed by the LDAP server for user accounts not found in the local user database. You can enable and configure LDAP servers and LDAP groups.
- **Network Connectivity (standalone and domain)**
  Enables dynamic DNS or lets you manually designate IPv4 and IPv6 DNS addresses.
- **NTP (standalone and domain)**
  Enables the NTP service to configure a UCS system that is managed by Cisco Intersight to synchronize the time with an NTP server. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers. When you enable the NTP service, Cisco Intersight configures the NTP details on the endpoint.
- **Persistent Memory**
  Only applicable to Cisco UCS C-Series – special memory (PMem modules) that provide low latency and persistent storage.
- **SMTP**
  Simple Mail Transfer Protocol (SMTP) sends server faults as email alerts to the configured SMTP server.
- **SSH**
  Enables an SSH client to make a secure, encrypted connection. You can create one or more SSH policies that contain a specific grouping of SSH properties for a server or a set of servers.

Chassis policies for Intersight Management Mode

- **IMC Access**
  Allows you to configure your network and associate an IP address from an IP pool with a server. In-band IP address, out-of-band IP address, or both in-band and out-of-band IP addresses can be configured using IMC Access policy and is supported on drive security, SNMP, syslog, and vMedia policies.
- **Power**
  Enables configuration of power redundancy and power allocation for the chassis.
- **SNMP**
  Configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. This policy supports SNMP versions such as SNMPv1, SNMPv2 (includes v2c), and SNMPv3. Any existing SNMP users or SNMP traps configured previously on the managed devices are removed and replaced with users or traps that you configure in this policy. If you have not added any users or traps in the policy, the existing users or traps on the input/output module (IOM) are removed.
- **Thermal**
  Used to set configuration parameters for chassis fans.

Additional resources

Become part of the Cisco Intersight Community to ask questions, share best practices, and learn from other Intersight users. The community is open to everyone. Join the community and explore other Cisco Communities here.

Once you have joined the Intersight Community, get access to the Intersight product and technical teams along with special programs and events by becoming an Intersight Insider. After becoming a community member, ask to become a member on the Intersight Insider Group Hub page.

Creating and managing policies

Multiple instructional materials are available to help you get started with Cisco Intersight. The Cisco Intersight Managed Mode Configuration Guide provides step-by-step instructions and tutorials on creating and assigning policies and profiles in Intersight, including:

Profile configuration

- Configuring UCS Domain Profiles
- Configuring Server Profiles
- Configuring UCS Chassis Profiles

Policy configuration

- Configuring UCS Domain Policies
- Configuring Server Policies
- Configuring UCS Chassis Policies

The Intersight SaaS Help Center provides detailed information on getting started with profiles, policies, and templates. And the Intersight IMM Expert Series on the Cisco Compute YouTube channel provides instructor-led examples on creating individual policies and profiles.

Subscribe to these IMM Expert Series playlists on the Cisco Compute YouTube channel:

- Domain Policies and Domain Profiles
- Server Policies and Server Profiles
- ID Pools
- Use Case Videos

Appendix: Cisco Intersight Policies At-a-Glance

Policy	Chassis	Domain	IMM	ISM
SNMP	×	×	×	×
Power	×		×	×
***IMC Access**	**×**		**×**	
Thermal	×		×	
Certificate Management		×	×	×
Ethernet Network Control Policy		**×**	**×**	**×**
Ethernet Network Group		**×**	**×**	**×**
Syslog		×	×	×
Network Connectivity		×	×	
NTP		×	×	
LDAP (standalone and domain)		×		ISM only
Network Connectivity (standalone and domain)		×		ISM only
NTP (standalone and domain)		×		ISM only
Flow Control		×		
Link Aggregation		×		
Link Control		×		
Multicast		×		

* Minimum recommended policies to deploy a server

Policy	Chassis	Domain	IMM	ISM
Port		×		
Switch Control		×		
System QoS		×		
VLAN		×		
VSAN		×		
***BIOS**			✖	✖
***Boot Order**			✖	✖
***LAN Connectivity**			✖	✖
***Local User**			✖	✖
***Storage**			✖	✖
***Virtual KVM**			✖	✖
***Virtual Media**			✖	✖
Drive Security			×	×
Ethernet Adapter Policy			✖	✖
Ethernet QoS			×	×
Fibre Channel Adapter			×	×
Fibre Channel Network			×	×
Fibre Channel QoS			×	×

Policy	Chassis	Domain	IMM	ISM
Firmware			×	×
IPMI Over LAN			×	×
Memory			×	×
SAN Connectivity			×	×
SD Card			×	×
Serial Over LAN			×	×
FC Zone			×	
iSCSI Adapter			×	
ISCSI Boot			×	
iSCSI Static Target			×	
LDAP			×	
Scrub			×	
Adapter Configuration				ISM only
Device Connector				ISM only
Ethernet Network				ISM only
Persistent Memory				ISM only
SMTP				ISM only
SSH				ISM only