IMM Checklist

This guide is divided into several worksheets. There are three Cisco UCS® deployment types covered. You will see these deployment variations in the Cisco Intersight® policy creation settings in the left Navigation Menu. Cisco HyperFlex® Clusters and Kubernetes Clusters are not included in this guide.

If you are using this guide to enter and retail values for the same policy more than once, create another worksheet and copy over the relevant fields to populate them from the original worksheet for the first policy implmementation.

1. Column Definitions detail the values entered in the worksheet columns for the three Cisco UCS deployment types covered. They are specific to policy considerations. Not all policies are reflected in the deployment types; only those relevant to secure configurations have values populated. If the policy is not relevant to system hardening or security, then it is listed as Not Applicable (N/A).

2. Initial setup worksheets are for relevant secure settings in PVA/CVA configurations during deployment of the on-premises appliances and for the initial setup of fabric-interconnect-based (FI-based) IMM deploymets that require FI IMM selection during first boot with console access.

3. Account Settings have some common configurations for PVA/CVA/SaaS Intersight deployments using the account admin user. The worksheets are broken out between SaaS (Software as a Service) settings and local on-premises settings for PVA and CVA, to capture the differences.

4. Cisco UCS Server

This is for servers deployed and managed by IMM with and without fabric interconnects (FIs). Some settings apply specifically to standalone servers; others apply to FI-attached servers only; most apply to either.

5. Cisco UCS Domain

Thes is for servers deployed and managed by FIs operating in IMM.

6. Cisco UCS Chassis

These are settings specific to the chassis in chassis-based Cisco UCS domain deployments.

API References: Cisco Intersight API Docs and Overview - Intersight - Cisco DevNet

IMM Checklist

The columns in the configuration and settings worksheets are categorized as follows:

Configuration	Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call
Name of the settings being used in the Initial Setup worksheets and the Account Settings worksheet.	Only used in the Cisco UCS® Server, Domain, and Chassis worksheets. The name of the policy from the deployment type and policy creation menu.	The recommended setting in the configuration or policy being discussed	Item description. This provides additonal information on the setting.	The security aspect being affected, e.g., user management, authentication, or encryption.	The relative importance of configuring the option. For example, secure LDAP for identity provider would be P1.	Any applicable API calls that can be used to set or retrieve values for the specific configuration.
				Network	P0 - Immediate	
				Management - Users	P1 - Day 1	
				Management - Policies	P2 - Day 2	
				Management - Hardware	P3 - Optional	
				Management - Software		
				Configuration - User		
				Configuration - Policy		
				Configuration - Software		
				Configuration - Hardware		

IMM Checklist

PVA-CVA version	1.0.9-1.1.0				
Configuration	**Setting**	**Description**	**Feature/Component**	**Implementation Priority**	**Notes**
Environment Preqs					
DNS A Record		FQDN record for appliance	Network	P0	
DNS CNAME (Alias)		Alias for appliance device connector	Network	P0	
DNS PTR		Reverse lookup for A Record	Network	P0	
Port Availabliity					
TLS	TCP 443	TLS Single-node and Multi-node	Network	P0	
VM comms	TCP 2379	Multi-node only appliance VM intercommunication	Network	P0	
VM comms	TCP 6443	Multi-node only appliance VM intercommunication	Network	P0	
VM comms	TCP 2380	Multi-node only appliance VM intercommunication	Network	P0	
VM comms	TCP 9092	Multi-node only appliance VM intercommunication	Network	P0	
VM comms	TCP 9100	Multi-node only appliance VM intercommunication	Network	P0	
VM comms	TCP 10250	Multi-node only appliance VM intercommunication	Network	P0	
Name resolution	UDP 53	DNS Single-node and Multi-node	Network	P0	
Time	UDP 67	NTP Single-node and Multi-node	Network	P0	
Time	UDP 68	NTP Single-node and Multi-node	Network	P0	
Service Access URLs					
Tools	tools.cisco.com:443	Required for all servers for Smart Licensing.	Network	P0	
Downloads	download-ssc.cisco.com	Access to Cisco Software download site(s).	Network	P0	
Downloads	dl.cisco.com	Access to Cisco Software download site(s).	Network	P0	
Downloads	dll.cisco.com	Access to Cisco Software download site(s).	Network	P0	

IMM Checklist

PVA-CVA version	1.0.9-1.1.0				
Configuration	**Setting**	**Description**	**Feature/Component**	**Implementation Priority**	**Notes**
Downloads	dl2.cisco.com	Access to Cisco Software download site(s).	Network	P0	
API access	api.cisco.com	Access to Cisco Software download site(s).	Network	P0	
SSO	cloudsso.cisco.com:443	Access to Cisco SSO login accounts	Network	P0	
Region URLs for Endpoints					
North America	intersight.com	intersight-aws-us-east-1	Network	P0	
	us-east-1.intersight.com		Network	P0	
NA Device Connector URL	svc.intersight.com		Network	P0	
	svc.us-east-1.intersight.com		Network	P0	
	svc-static1.intersight.com		Network	P0	
	ucs-connect.com		Network	P0	
Europe	eu-central-1.intersight.com	intersight-aws-eu-central-1	Network	P0	
EU Device Connector URL	svc.eu-central-1.intersight.com		Network	P0	
	svc-static1.eu-central-1.intersight.com		Network	P0	
HTTPS Proxy					
Proxy hostname/IP		If using an HTTPS proxy, complete these fields.	Configuration - Software	P0	
Proxy port			Configuration - Software	P0	
Proxy user			Configuration - Software	P0	
Proxy password			Configuration - Software	P0	

IMM Checklist

PVA-CVA version	1.0.9-1.1.0				
Configuration	**Setting**	**Description**	**Feature/Component**	**Implementation Priority**	**Notes**
Passwords		Hard passwords are default and 8 characters minimum. Enter the following.	Configure settings for admin user to the PVA		No 3x repeated characters, no forward/ reverse usernames, no dictionary words, none of the following: $,?,=
Lowercase		At least one.	Configuration - User	P0	
Uppercase		At least one.	Configuration - User	P0	
Number(s)		At least one.	Configuration - User	P0	
Special Character(s)		At least one.	Configuration - User	P0	
Password change count		Max times a password can be changed in the change interval.	Configuration - User	P0	
Change interval		Timeframe used by change count.	Configuration - User	P0	
No-change interval		Min hours a local user must wait to change passwords.	Configuration - User	P0	
Change during interval		Capability to change password during the change interval.	Configuration - User	P0	
Default passwords changed?		Do not leave any defaults.	Configuration - User	P0	

IMM Checklist

Server Models	M5/M6/M7/M8
FI Models	6300/6400/6500 series
FI Software Version	4.3+

These are relevant security settings for first-time setup of Fabric Interconnect pairs in Cisco Intersight® Managed Mode (IMM). See the Cisco UCS X-Series quick start for more details if needed: Cisco UCS X-Series Quick Start Guide - Cisco. Note that this checklist assumes console access to the hardware. You can follow this process from the UI once an IP has been assigned. This guide goes through the console entries without using the UI.

Configuration	Setting	Description	Feature/Component	Implementation Priority	Notes
Config and Mgmt Mode					
Config Method	Console	Configure by console	Configuration - Software	P0	
Mgmt Mode	Intersight	Verify IMM	Configuration - Software	P0	
Enforce Strong Password	Yes	Strong password is enforced. Enter password here	Configuration - Software	P0	
Fabric node to select first	A		Configuration - Hardware	P0	
FI A					
IP Assignment FI-A		IP address for mgmt FI A	Network	P0	
Netmask		Netmask in xxx.xxx.xxx.xxx format.	Network	P0	
Gateway		Subnet gateway.	Network	P0	
DNS		One or more name servers	Network	P0	
Confirm	Yes	After confirmation autoreboot.	Configuration - Software	P0	
FI B					
IP Assignment FI-B		IP address for mgmt FI B	Network	P0	
User peer fabric?	Yes	The information from FI-A will be imported for use in FI-B.	Configuration - Software	P0	

IMM Checklist

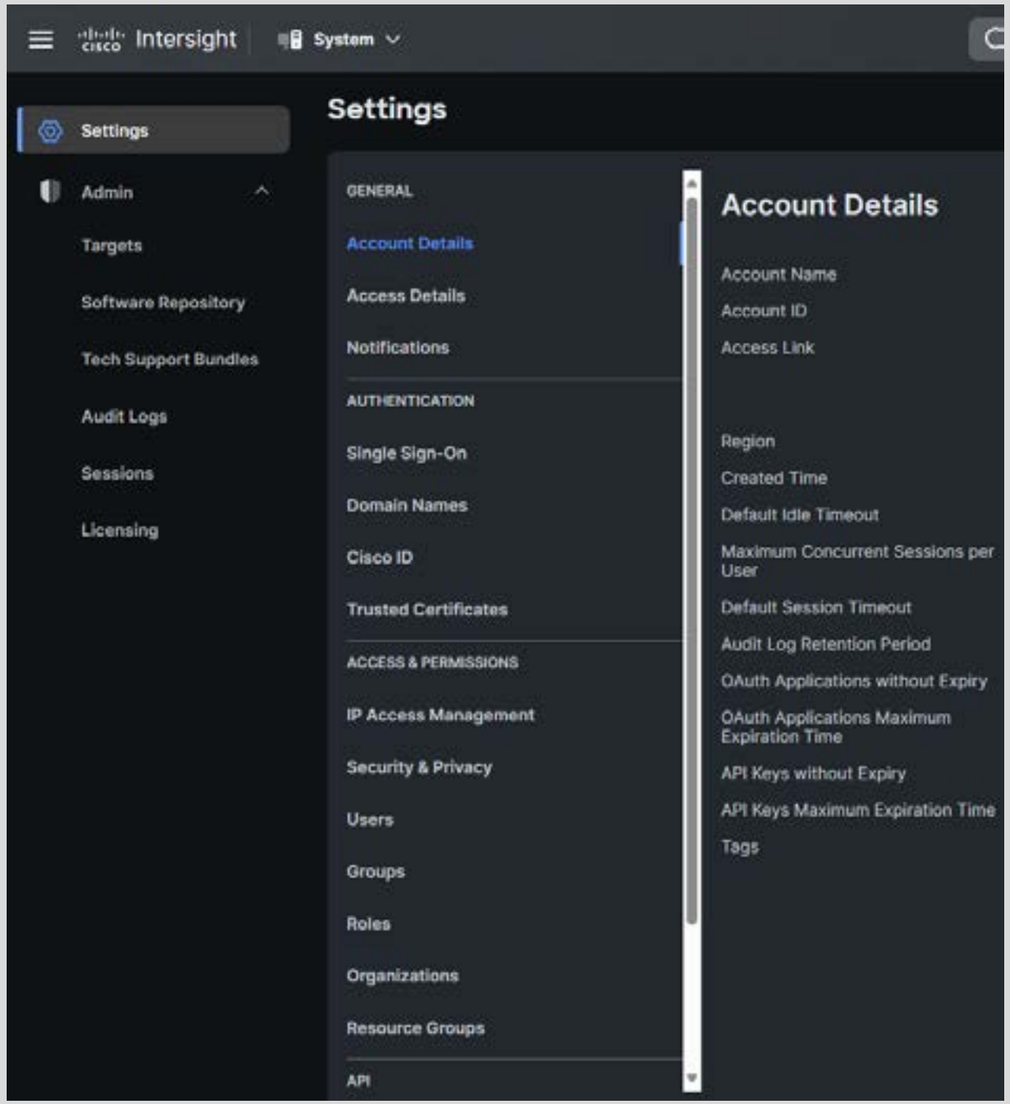
Configuration	Setting	Description	Feature/Component	Implementation Priority	Notes
Device Connector UI					
Device ID		Record this value	Configuration - Hardware	P0	
Claim Code		Record this value. It has a TTL of 2 minutes before a new code is generated.	Configuration - Hardware	P0	
Intersight (SaaS/PVA/CVA)					
Claim Target		Settings-->Admin--Targets-->Claim New Target	Management - Hardware	P0	
Firmware					
Firmware upgrade needed?		Does FW need to be updated to a new version for known fixes?	Management - Software	P2	
FW current version		Current FW version	Management - Software	P2	
FW upgrade version		Firmware upgrade version	Management - Software	P2	

IMM Checklist

Account Admin User Settings

These values can be found in the account admin system settings.

API References: Cisco Intersight API Docs and Overview - Intersight - Cisco DevNet.



IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
Account Details (Configure as account admin)						
Default Idle Timeout (seconds)	1800	This is the idle login timeout for the UI. The default is 1800 seconds (30 mins). The max value is 18000 seconds (5 hours) and the min value is 300 seconds (5 minutes).	Management - User	P1	iam/SessionLimits	
Default Session Timeout (seconds)	57600	This is the session timeout when your session will be terminated, even if active, to re-authenticate. The default is 57600 seconds (16 hours). The max value is 31536000 (1 year) and the min value is 300 seconds (5 mins). Consider reducing the timeout to 10800 seconds (3 hours).	Management - User	P1	iam/SessionLimits	
Max Concurrent Sessions per User	32	This is how many independent login sessions can be opened by the same user. Depending on shared responsibilities in your organization, consider reducing this to a lower value (e.g., 8).	Management - User	P1	iam/SessionLimits	
Audit Log Retention Period	48	The length of time in months before audit records rotate (i.e., begin truncation).	Configuration - Software	P2	aaa/RetentionPolicies	
OAuth Applications without Expiry	Disable	OAuth (Open Authorization) is an open standard for authorization that enables third-party applications to access user information without needing to expose user passwords. It's a protocol that allows an end user's account information to be used by third-party services.	Configuration - Software	P2	iam/AppRegistrations	
OAuth Applications Max Expiration Time (Days)	180	The default for third-party service access via OAuth is 180 days. Consider lowering this depending on the services being used.	Configuration - Software	P2	iam/AppRegistrations	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
API Keys Expiry	360	The maximum time in days before API keys need to be renewed. The default is 360 days. Consider lowering this depending on the proliferation of API- based applications in your organization.	Configuration - Software	P1	iam/ApiKeys	
Notifications (add rule)						
email		E-mail address for notification recipient.	Management - Software	P3	notification/ AccountSubscriptions	
severity	Warning	Select the severity of the alert; choose Warning to get broader coverage.	Management - Software	P3	notification/ AccountSubscriptions	
Single Sign-On (add identity provider)						
Identity provider		Add a new identity provider (IDP) (e.g., Active Directory LDAP)	Configuration - Software	P2	iam/Idps	
Domain name		Domain name(s) assocated with the IDP.	Configuration - Software	P2	iam/DomainNameInfos	
Skip warning during login	Disable	Show warnings for unverified domains on login.	Configuration - Software	P2	iam/Idps	
Single Log Out (SLO)	Enable	Single log out is a feature of SSO systems that allows the user to log out of all applications and sessions with a single action. This includes terminating all user sessions for the browser that initiated the logout.	Configuration - Software	P2	iam/Idps	
Domain Names						
IDP domain name		Verified domain names for the Identity Provider (IDP).	Configuration - Software	P2	iam/DomainNameInfos	
Cisco ID						

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
MFA	Enable	Require multifactor authentication (MFA) for Cisco ID-based users.	Configuration - Software	P0	iam/IdpReferences	
Trusted Certificates						
Add TLS/SSL certificate	N/A	Add trusted certificates as needed.	Configuration - Software	P2	iam/TrustPoints	
IP Access Management						
Enable IP Access Management	Enable	Enable IP access management to restrict access to the Cisco Intersight® portal to only trusted users by defining IP addresses and/or ranges that are permitted.	Configuration - Software	P0	iam/pAccessManagements	
Security and Privacy						
Data Collection	Enable	Allow tech-support bundle collection.	Configuration - Software	P0	techsupportmanagement/CollectionControlPolicies	
Allow Tunneled vKVM Launch	Enable	Allow tunneled (over secure device connector) vKVM connections for claimed devices.	Configuration - Software	P0	kvm/TunneledKvmPolicies	
Allow Tunneled vKVM Configuration	Enable	Allow tunneled (over secure device connector) vKVM connections for claimed devices.	Configuration - Software	P0	kvm/TunneledKvmPolicies	
Users						
Add user(s)	N/A	Add users with appropriate roles.	Management - User	P0	iam/Users	
Groups						
Add group(s)	N/A	Add groups to segment users in logical roles.	Management - User	P1	iam/UserGroups	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
Roles						
Create role(s)	N/A	Add custom roles if needed. Assign privileges. Go to Groups/Users and adjust role(s) if needed.	Management - User	P3	iam/Permissions	
Organizations						
Create organization(s)	N/A	Add organizations to logically segmented resource groups so that hardware is assigned to the correct personnel.	Management - Software	P2	organization/Organizations	
Resource Groups						
Create resource group(s)	N/A	Use the custom option to select specific hardware to add to resource groups that can be assigned to an organization.	Management - Hardware	P2	resource/Groups	
API Keys						
API Key Purpose	OpenAPI Schema v3	Do not choose deprecated schemas.	Management - Software	P0	iam/ApiKeys	
Key Never Expires	Disable	Allow the API key to expire for security reasons. See the API Keys Expiry setting in Account Details (Configure) above.	Management - Software	P0	iam/ApiKeys	

IMM Checklist

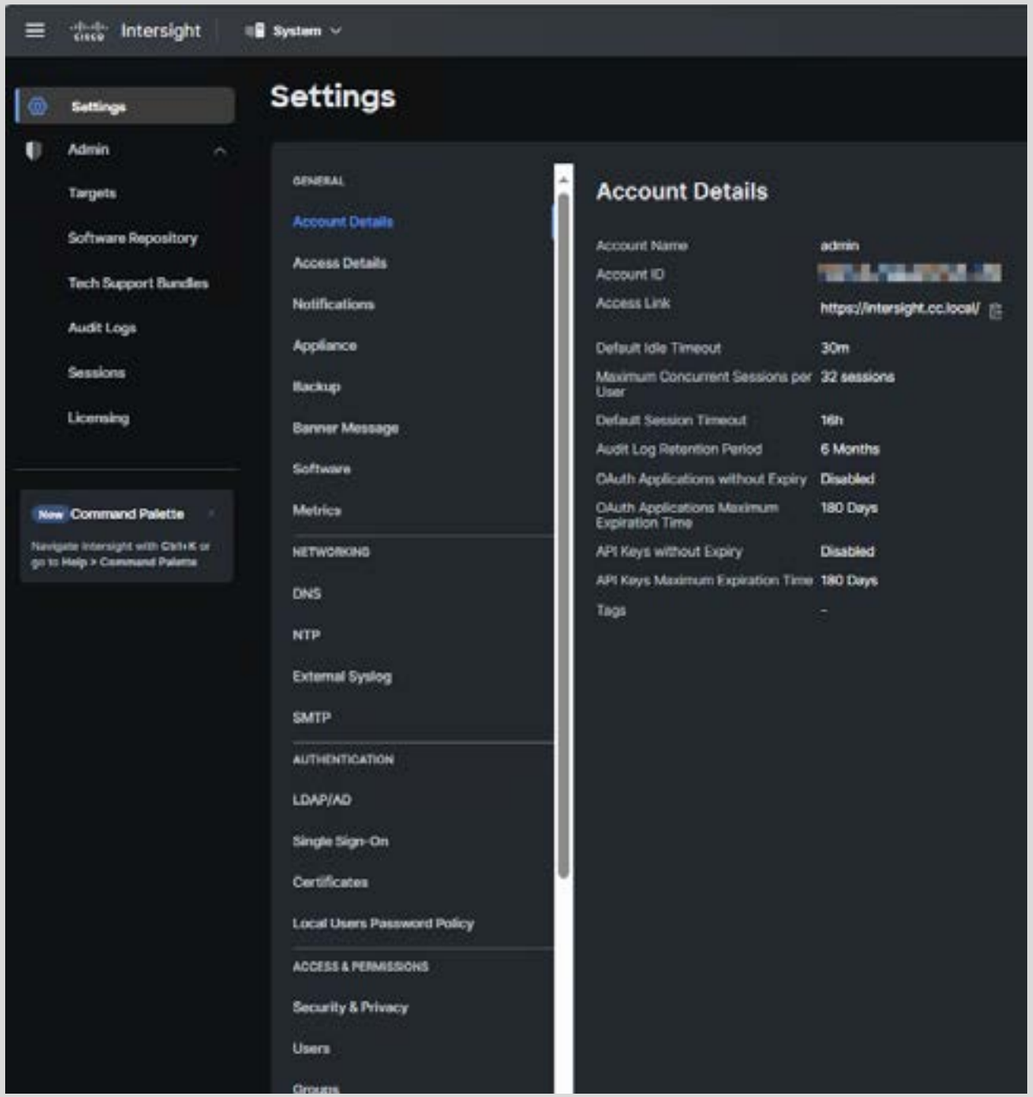
Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
OAuth 2.0		**OAuth (Open Authorization)** is an open standard for authorization that enables third-party applications to access user information without needing to expose user passwords. It's a protocol that allows an end user's account information to be used by third-party services.				
Application name		Name of the application needing auth. E.g., the Intersight Mobile App.	Management - Software	P3	iam/AppRegistrations	
Expiration Time	180	Create OAuth v2 credentials to grant third-party applications access to Intersight. Depending on the function, keep expiry time to a minimum.	Configuration - Software	P3	iam/AppRegistrations	
Webhooks		A webhook is an HTTP request, triggered by an event in a source system and sent to a destination system, often with a payload of data.				
Enable	Disable	Enable only if needed for sending events to a remote application via POST.	Configuration - Software	P3	notification/ AccountSubscriptions	
Secret		The secret key is a value shared between the webhook producer and consumer.	Configuration - Software	P3	notification/ AccountSubscriptions	

IMM Checklist

Account Admin User Settings

These values can be found in the account admin system settings.

API References: Cisco Intersight API Docs and Overview - Intersight - Cisco DevNet.



IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
Account Details (Configure as account admin)						
Default Idle Timeout (seconds)	1800	This is the idle login timeout for the UI. The default is 1800 seconds (30 mins). The max value is 18000 seconds (5 hours) and the min value is 300 seconds (5 minutes).	Management - User	P1	iam/SessionLimits	
Default Session Timeout (seconds)	57600	This is the session timeout when your session will be terminated, even if active, to re-authenticate. The default is 57600 seconds (16 hours). The max value is 31536000 (1 year) and the min value is 300 seconds (5 mins). Consider reducing the timeout to 10800 seconds (3 hours).	Management - User	P1	iam/SessionLimits	
Max Concurrent Sessions per User	32	This is how many independent login sessions can be opened by the same user. Depending on shared responsibilities in your organization, consider reducing this to a lower value (e.g., 8).	Management - User	P1	iam/SessionLimits	
Audit Log Retention Period	48	The length of time in months before audit records rotate (i.e., begin truncation).	Configuration - Software	P2	aaa/RetentionPolicies	
OAuth Applications without Expiry	Disable	OAuth (Open Authorization) is an open standard for authorization that enables third-party applications to access user information without needing to expose user passwords. It's a protocol that allows an end user's account information to be used by third-party services.	Configuration - Software	P2	iam/AppRegistrations	
OAuth Applications Max Expiration Time (Days)	180	The default for third-party service access via OAuth is 180 days. Consider lowering this number depending on the services being used.	Configuration - Software	P2	iam/AppRegistrations	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
API Keys Expiry	360	The maximum time in days before API keys need to be renewed. The default is 360 days. Consider lowering this number depending on the proliferation of API-based applications in your organization.	Configuration - Software	P1	iam/ApiKeys	
Notifications (add rule)						
email		E-mail address for notification recipient.	Management - Software	P3	notification/ AccountSubscriptions	
severity	Warning	Select the severity of the alert; choose Warning to get broader coverage.	Management - Software	P3	notification/ AccountSubscriptions	
Banner Message		Customized login banner.				
Show banner message before login	Enable	Turn the banner on	Management - Software	P2	/iam/BannerMessages	
Banner Title	WARNING	Set an alert message or similar	Management - Software	P2	/iam/BannerMessages	
Banner Message		Enter a message	Management - Software	P2	/iam/BannerMessages	
DNS (Configure)		For the appliance				
IPv4 Server(s)		Name servers	Network	P0	networkconfig/Policies	
Enable IPv6		Enable IPv6 is needed.	Network	P0	networkconfig/Policies	
IPv6 Server(s)		Name servers	Network	P0	networkconfig/Policies	
NTP (Configure)		For the appliance				
Add NTP server(s)		Time servers	Network	P0	networkconfig/Policies	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
External Syslog (Configure)		For the appliance, add external syslog server				
Enable External Syslog Server	Enable	Allow external syslog	Management - Software	P2	appliance/ ExternalSyslogSettings	
Web Server Access Logs	Enable	Transfer access logs	Management - Software	P2	appliance/ ExternalSyslogSettings	
Audit Logs	Enable	Transfer audit logs	Management - Software	P2	appliance/ ExternalSyslogSettings	
Alarms	Enable	Transfer alarms	Management - Software	P2	appliance/ ExternalSyslogSettings	
Hostname or IP		Syslog server identity	Management - Software	P2	appliance/ ExternalSyslogSettings	
Port		Syslog port	Management - Software	P2	appliance/ ExternalSyslogSettings	
Protocol	TLS	Use secure transport	Management - Software	P2	appliance/ ExternalSyslogSettings	
Minimum SEL severity	Warning	Select minimum alert level	Management - Software	P2	appliance/ ExternalSyslogSettings	
SMTP (Configure)		For the appliance alerts				
Enable SMTP	Enable	Allow SMTP	Management - Software	P2	smtp/Policies	
Server Address		Server FQDN or IP	Management - Software	P2	smtp/Policies	
Server Port		Email port	Management - Software	P2	smtp/Policies	
Sender email		Email for PVA sender	Management - Software	P2	smtp/Policies	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
TLS	Enable	Enable secure transport	Management - Software	P2	smtp/Policies	
Certificate		TLS certificate	Management - Software	P2	smtp/Policies	
Authentication Enable	Enable	Authenticated user	Management - Software	P2	smtp/Policies	
Username			Management - Software	P2	smtp/Policies	
Password			Management - Software	P2	smtp/Policies	
LDAP/AD (configure)		Identity provider for users. Use LDAPS.				
Name		Friendly LDAP IDP name	Management - Software	P2	iam/LdapPolicies	
Base DN		LDAP attribute	Management - Software	P2	iam/LdapPolicies	
Bind DN		LDAP attribute	Management - Software	P2	iam/LdapPolicies	
Group Attribute		LDAP attribute	Management - Software	P2	iam/LdapPolicies	
Password			Management - Software	P2	iam/LdapPolicies	
Nested group search	Enable	LDAP search attribute	Management - Software	P2	iam/LdapPolicies	
Enable encryption	Enable	Use secure LDAP	Management - Software	P2	iam/LdapPolicies	
LDAP server		LDAP FQDN	Management - Software	P2	iam/LdapPolicies	
Port	636	Secure LDAP port	Management - Software	P2	iam/LdapPolicies	
Single Sign-On (Add identity provider.)						
Identity provider		Add a new identity provider (IDP) (e.g., Active Directory LDAP)	Configuration - Software	P2	iam/Idps	
Domain name		Domain name(s) assocated with the IDP.	Configuration - Software	P2	iam/DomainNameInfos	
Skip warning during login	Disable	Show warnings for unverified domains on login.	Configuration - Software	P2	iam/Idps	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
Single Log Out (SLO)	Enable	Single log out is a feature of SSO systems that allows the user to log out of all applications and sessions with a single action. This includes terminating all user sessions for the browser that initiated the logout.	Configuration - Software	P2	iam/Idps	
Certificates						
Add Trusted Certificate (SSL/TLS)		Enter trusted certificate	Management - Software	P2	iam/TrustPoints	
SSL certificate create CSR		PVA-CVA certificate for secure management sessions	Management - Software	P2	iam/TrustPoints	
Org		Certificate Signing Request Field	Management - Software	P2	iam/TrustPoints	
Org Unit		Certificate Signing Request Field	Management - Software	P2	iam/TrustPoints	
Locality		Certificate Signing Request Field	Management - Software	P2	iam/TrustPoints	
State		Certificate Signing Request Field	Management - Software	P2	iam/TrustPoints	
Country		Certificate Signing Request Field	Management - Software	P2	iam/TrustPoints	
Email		Certificate Signing Request Field	Management - Software	P2	iam/TrustPoints	
Modulus	4096	Key depth	Management - Software	P2	iam/TrustPoints	
SSL certificate create self-signed		PVA-CVA certificate for secure management sessions.This will replace the current certificate.	Management - Software	P2	iam/TrustPoints	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
Local Users Password Policy (Configure)						
Minimum length of password	8	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Minimum number of required uppercase characters	1	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Minimum number of required lowercase characters	1	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Minimum number of required numeric characters	1	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Minimum number of special characters	1	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Number of previous passwords disallowed	5	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Minimum number of characters different from previous password	2	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Minimum days allowed between password changes	0	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Time duration for incorrect login attempts (seconds)	1800	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Max consecutive incorrect login attempts allowed	3	Password policy	Management - User	P2	iam/LocalUserPasswordPolicies	
Enable lockout for admin user	Disable	Be careful with admin lockout.	Management - User	P2	iam/LocalUserPasswordPolicies	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
Security and Privacy						
Data Collection	Enable	Allow tech-support bundle collection.	Configuration - Software	P0	techsupportmanagement/ CollectionControlPolicies	
Allow Tunneled vKVM Launch	Enable	Allow tunneled (over secure device connector) vKVM connections for claimed devices.	Configuration - Software	P0	kvm/TunneledKvmPolicies	
Allow Tunneled vKVM Configuration	Enable	Allow tunneled (over secure device connector) vKVM connections for claimed devices.	Configuration - Software	P0	kvm/TunneledKvmPolicies	
Users						
Add user(s)	N/A	Add users with appropriate roles.	Management - User	P0	iam/Users	
Groups						
Add group(s)	N/A	Add groups to segment users into logical roles.	Management - User	P1	iam/UserGroups	
Roles						
Create role(s)	N/A	Add custom roles if needed. Assign privileges. Go to Groups/Users and adjust role(s) if needed.	Management - User	P3	iam/Permissions	
Organizations						
Create organization(s)	N/A	Add organizations to logically segmented resource groups so that hardware is assigned to the correct personnel.	Management - Software	P2	organization/Organizations	
Resource Groups						
Create resource group(s)	N/A	Use the custom option to select specific hardware to add to resource groups that can be assigned to an organization.	Management - Hardware	P2	resource/Groups	

IMM Checklist

Configuration	Setting	Description	Feature/Component	Implementation Priority	API call	Notes
API Keys						
API Key Purpose	OpenAPI Schema v3	Do not choose deprecated schemas.	Management - Software	P0	iam/ApiKeys	
Key Never Expires	Disable	Allow the API key to expire for security reasons. See the API Keys Expiry setting in Account Details (Configure) above.	Management - Software	P0	iam/ApiKeys	
OAuth 2.0		OAuth (Open Authorization) is an open standard for authorization that enables third-party applications to access user information without needing to expose user passwords. It's a protocol that allows an end user's account information to be used by third-party services.				
Application name		Name of the application needing auth. E.g., the Cisco Intersight® Mobile App.	Management - Software	P3	iam/AppRegistrations	
Expiration Time	180	Create OAuth v2 credentials to grant third-party applications access to Intersight. Depending on the function, keep expiry time to a minimum.	Configuration - Software	P3	iam/AppRegistrations	
Webhooks		A webhook is an HTTP request, triggered by an event in a source system and sent to a destination system, often with a payload of data.				
Enable	Disable	Enable only if needed for sending events to a remote application via POST.	Configuration - Software	P3	notification/ AccountSubscriptions	
Secret		The secret key is a value shared between the webhook producer and consumer.	Configuration - Software	P3	notification/ AccountSubscriptions	

IMM Checklist

Component type	Models	Software Version	Reference for BIOS	Note
Cisco UCS® standalone rack server, Cisco UCS FI-attached rack server, Cisco UCS FI- attached blade server and chassis	M5/M6/M7/M8	FW FI 4.3+, or Cisco Intersight® Server bundles 5.6+	Cisco UCS Server BIOS Tokens in Intersight Managed Mode - Introduction to Intersight Managed Mode Server Bios Tokens [Cisco Intersight] - Cisco	If you select any Cisco preconfigured policies (e.g., BIOS or Ethernet Adapter) you will be unable to change individual items until the policy is created. Once done, you can edit the policy. Only settings in the policies relevant to security are specifically cited here.

Policies in Cisco Intersight provide different configurations for UCS servers, including BIOS settings, firmware versions, disk group creation, Simple Mail Transfer Protocol (SMTP), Intelligent Platform Management Interface (IPMI) settings, and more. A policy that is once configured can be assigned to any number of servers to provide a configuration baseline. Policies in Cisco Intersight are native to the application and are not directly imported from the UCS Systems. Policy-based configuration with Server Profiles is a Cisco Intersight Essentials license tier functionality.

The Server Policy creation wizard in Cisco Intersight has two pages:

General—The general page allows you to select the organization and enter a name for your policy. Optionally, include a short description and tag information to help identify the policy. Tags must be in the key:value format. For example, Org: IT or Site: APJ.

Policy Details—The policy details page has properties that are applicable to standalone UCS servers, FI-attached UCS servers, or both. You can view these properties separately for **All Platforms, Cisco UCS Servers (Standalone)**, and **Cisco UCS Servers (FI-Attached)** by clicking on these options.

Server Policies can be imported as part of importing configuration details (server profiles and policies) of a Cisco C-Series Standalone server from Cisco IMC. For more information, see Importing a Server Profile.

API References: Cisco Intersight API Docs and Overview - Intersight - Cisco DevNet.

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Adapter Configuration						
Enable LLDP	Disable	Link Layer Discovery Protocol. This is generally safe but can allow users to gain insight into devices present on their LAN segment.	Network	P1	vnic/EthAdapterPolicies	
BIOS		https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/Intersight/IMM_BIOS_Tokens_Guide/b_IMM_Server_BIOS_Tokens_Guide/b_UCS_BIOS_Tokens_Guide_chapter_01.html				
Boot Options						
Cisco Provided BIOS preconfiguration	Select a config, edit as needed.	Choose a server profile that matches what you are deploying and use the Cisco selected preconfigured BIOS settings for that type of deployment.	Configuration - Software	P1	boot/PrecisionPolicies	
Preconfig Selected		Record the profile for preconfig selected		P1	boot/PrecisionPolicies	
IPv4 PXE support	Disable	PXE support is potentially unsafe since it relies on the physical security of the system. It is subject to rogue DHCP attacks, MITM attacks, or image capture that may contain hard-coded domain credentials.	Network	P1	boot/PrecisionPolicies	
IPv6 PXE support	Disable	PXE support is potentially unsafe since it relies on the physical security of the system. It is subject to rogue DHCP attacks, MITM attacks, or image capture that may contain hard-coded domain credentials.	Network	P1	boot/PrecisionPolicies	
Power on Password	Enable	Secure the system from boot on theft using a power on password.	Configuration - Software	P1	boot/PrecisionPolicies	
IPv4 HTTP support	Disable	HTTP boot support is potentially unsafe if DNS or the boot image is compromised. It is also subject to MITM attacks. All of these are LAN-based issues.	Network	P1	boot/PrecisionPolicies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
IPv6 HTTP support	Disable	HTTP boot support is potentially unsafe if DNS or the boot image is compromised. It is also subject to MITM attacks. All of these are LAN-based issues.	Network	P1	boot/PrecisionPolicies	
Intel® Directed IO				N/A		
LOM and PCIe Slots						
External SSC Enable	Enable	This option allows you to Enable/Disable the Clock Spread Spectrum of the external clock generators. This can reduce EMI.	Configuration - Hardware	P1	bios/Policies	
PCIe ROM CLP	Disable	PCI ROM Command Line Protocol (CLP) controls the execution of different Option ROMs such as PxE and iSCSI that are present in the card. By default, it is disabled.	Configuration - Software	P1	bios/Policies	
PCIe PLL SSC	Enable	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading.	Configuration - Hardware	P1	bios/Policies	
Main				N/A		
Memory						
BME DMA Mitigation	Disable	Allows you to disable the PCI BME bit to mitigate the threat from an unauthorized external DMA	Configuration - Software	P1	bios/Policies	
CPU SMEE	Enable	Allows the processor to use the Secure Memory Encryption Enable (SMEE) function, which provides memory encryption support.	Configuration - Software	P1	bios/Policies	
DRAM Scrub Time	24 hours	The value that represents the number of hours to scrub the whole memory.	Configuration - Hardware	P1	bios/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
SNP Memory Coverage	Enable	This option selects the operating mode of the Secured Nested Paging (SNP) Memory and the reverse Map Table (RMP). The RMP is used to ensure a one-to-one mapping between system physical addresses and guest physical addresses.	Configuration - Hardware	P1	bios/Policies	
SNP Memory Size to Cover in MiB	8192	Allows you to configure SNP memory size.	Configuration - Hardware	P1	bios/Policies	
SEV-SNP Support	Enable	Allows you to enable the Secure Nested Paging feature.	Configuration - Software	P1	bios/Policies	
Secured Encrypted Virtualization	Enable	Enables running encrypted virtual machines (VMs) in which the code and data of the VM are isolated.	Configuration - Software	P1	bios/Policies	
SMEE	Enable	Allows the processort to use the Secure Memory Encryption Enable (SMEE) function, which provides memory encryption support.	Configuration - Software	P1	bios/Policies	
Transparent Secure Memory Encryption	Enable	Provides transparent hardware memory encryption of all data stored on system memory.	Configuration - Hardware	P1	bios/Policies	
PCI				N/A		
Power and Performance				N/A		
Processor						
Transparent Secure Memory Encryption (TSME)	Enable	Provides hardware memory encryption of all the data stored on system DIMMs that is invisible to the OS and slightly increases the memory latency. Cisco UCS C245 M8 Rack Server only.	Configuration - Hardware	P1	bios/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
SVM Mode	Enable	Allows the processor to use AMD Secure Virtual Machine Technology. Cisco UCS C225 M6, C245 M6, and C245 M8 rack servers only.	Configuration - Software	P1	bios/Policies	
Core Watchdog Timer Enable	Enable	Enables or disables CPU watchdog timer.	Configuration - Software	P1	bios/Policies	
QPI		Intel QuickPath Interconnect		N/A		
Security						
Trust Domain Extensions (TDX)	Enable	Intel security extensions. Only for Intel-based systems.	Configuration - Hardware	P1	bios/Policies	
TDX Secure Arbitration Mode (SEAM) Loader	Enable	Intel security extensions. Only for Intel -based systems.	Configuration - Hardware	P1	bios/Policies	
Serial Port						
Serial A Enable	Disable	Whether serial port A is enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
Server Management				N/A		
Trusted Platform						
Total Memory Encryption (MK-TME)	Enable	MK-TME allows you to have multiple encryption domains with one key. Different memory pages can be encrypted with different keys.	Configuration - Software	P1	bios/Policies	
Software Guard Extensions (SGX)	Enable	Allows you to enable Software Guard Extensions (SGX) feature.	Configuration - Software	P1	bios/Policies	
Total Memory Encryption (TME)	Enable	Allows you to provide the capability to encrypt the entirety of the physical memory of a system.	Configuration - Software	P1	bios/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Select Owner EPOCH Input Type		Allows you to change the seed for the security key used for the locked memory region that is created.	Configuration - Software	P1	bios/Policies	
SGX Auto MP Registration Agent		Allows you to enable the registration authority service to store the platform keys.	Configuration - Software	P1	bios/Policies	
SGX Epoch 0		Allows you to define the SGX EPOCH owner value for the EPOCH number designated by 0.	Configuration - Software	P1	bios/Policies	
SGX Epoch 1		Allows you to define the SGX EPOCH owner value for the EPOCH number designated by 1.	Configuration - Software	P1	bios/Policies	
SGX Factory Reset	Enable	Allows the system to perform SGX factory reset on subsequent boot.	Configuration - Software	P1	bios/Policies	
SGX PubKey Hashnwhere n ranges from 0 to 3.	0	Allows you to set the Software Guard Extensions (SGX) value.	Configuration - Software	P1	bios/Policies	
SGX Write Enable	Enable	Allows you to enable SGX Write feature.	Configuration - Software	P1	bios/Policies	
SGX Package Information In-Band Access	Disable	Allows you to enable SGX Package Info In-Band Access.	Configuration - Software	P1	bios/Policies	
SGX QoS	Enable	Allows you to enable SGX QoS.	Configuration - Software	P1	bios/Policies	
SHA-1 PCR Bank	Enable	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 1 or SHA-1 PCR Bank allows to enable or disable TPM security.	Configuration - Software	P1	bios/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
SHA256 PCR Bank	Enable	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 256-bit or SHA-256PCR Bank allows to enable or disable TPM security.	Configuration - Software	P1	bios/Policies	
SHA384 PCR Bank	Enable	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 384-bit or SHA-384PCR Bank allows to enable or disable TPM security.	Configuration - Software	P1	bios/Policies	
Trusted Platform Module State	Enable	Whether to enable or disable the Trusted Platform Module (TPM), which is a component that securely stores artifacts that are used to authenticate the server.	Configuration - Hardware	P1	bios/Policies	
Trust Domain Extension (TDX)	Enable	Whether to enable or disable the Trust Domain Extension (TDX), which protects the sensitive data and applications from unauthorized access. To enable Trust Domain Extension, ensure that: Total Memory Encryption (TME) is Enabled. Software Guard Extensions (SGX) is Enabled. Multikey Total Memory Encryption (MK-TME) is Enabled. LIMIT CPU PA to 46 Bits token is Disabled.	Configuration - Software	P1	bios/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
TDX Secure Arbitration Mode Loader	Enable	Whether to enable or disable the TDX Secure Arbitration Mode (SEAM) Loader, which helps to verify the digital signature on the Intel TDX module and load it into the SEAM-memory range. To enable Trust Domain Extension, ensure that: Total Memory Encryption (TME) is Enabled. Software Guard Extensions (SGX) is Enabled. Multikey Total Memory Encryption (MK-TME) is Enabled. LIMIT CPU PA to 46 Bits token is Disabled. TDX is enabled.	Configuration - Software	P1	bios/Policies	
TPM Pending Operation	None	Trusted Platform Module (TPM) Pending Operation option allows you to control the status of the pending operation.	Configuration - Software	P1	bios/Policies	
TPM Minimal Physical Presence	Disable	Whether to enable or disable TPM Minimal Physical Presence, which enables or disables the communication between the OS and BIOS for administering the TPM without compromising the security.	Configuration - Software	P1	bios/Policies	
Intel Trusted Execution Technology Support	Enable	Whether to enable or disable Intel Trusted Execution Technology (TXT), which provides greater protection for information that is used and stored on the business server.	Configuration - Software	P1	bios/Policies	
Security Device Support	Enable	It controls the entire TPM functionality.	Configuration - Hardware	P1	bios/Policies	
DMA Control Opt-In Flag	Enable	Enabling this token enables Windows 2022 Kernel DMA Protection feature. The OS treats this as a hint that the IOMMU should be enabled to prevent DMA attacks from possible malicious devices.	Configuration - Software	P1	bios/Policies	
LIMIT CPU PA to 46 Bits	Enable	Limits CPU physical address to 46 bits to support the older Hyper-v CPU platform.	Configuration - Hardware	P1	bios/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
USB						
All USB Devices	Disable	Whether all physical and virtual USB devices are enabled or disabled	Configuration - Hardware	P1	bios/Policies	
Legacy USB Support	Disable	Whether the system supports legacy USB devices.	Configuration - Hardware	P1	bios/Policies	
Make Device Non Bootable	Enable	Whether the server can boot from a USB device.	Configuration - Hardware	P1	bios/Policies	
USB Port Front	Disable	Whether the front panel USB devices are enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
USB Port Internal	Enable	Whether the internal USB devices are enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
USB Port KVM	Disable	Whether the USB Port KVM devices are enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
USB Port Rear	Disable	Whether the USB port rear devices are enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
USB Port SD Card	Enable	Whether the SD card drives are enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
USB Port VMedia	Disable	Whether the virtual media devices are enabled or disabled.	Configuration - Hardware	P1	bios/Policies	
Boot Order		The Boot Order policy configures the linear orderin?g 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.				
Boot mode UEFI or Legacy		Select BIOS type	Configuration - Software	P1	boot/PrecisionPolicies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Secure Boot	Enable	Enable secure boot	Configuration - Software	P1	boot/PrecisionPolicies	
Certificate Management		In Intersight Managed Mode, the Certificate Management policy allows you to specify the certificate details for an external certificate and attach the policy to servers. Cisco Intersight currently supports the following certificates: Root CA certificates: A Root CA certificate is necessary for HTTPS boot authentication. You can deploy a maximum of 10 Root CA certificates using the Certificate Management Policy. For a successful boot, at least one valid and unexpired Root CA certificate is required. Note: In Intersight Managed Mode servers, removing a server profile will delete the Root CA certificates from the CIMC. However, for C-Series servers in Standalone mode, the Root CA certificates are not automatically removed. You must manually delete them from CIMC or perform a factory reset on the server. Additionally, when you export the profile of a C-Series server in Standalone mode, the certificate management policy will not be included. IMC certificates: This option is available only for Intersight Managed Mode servers.				
IMC certficate (Paste in field)		Management Console certificate.	Management - Software	P1	certificatemanagement/Policies	
IMC Private Key (Paste in field)		Management Console private key	Management - Software	P1	certificatemanagement/Policies	
Enable IMC certificate	Enable	Activate IMC certificate	Management - Software	P1	certificatemanagement/Policies	
Root CA Name		Root certificate authority name	Management - Software	P1	certificatemanagement/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Root CA Certificate (Paste in field)		Root certificate	Management - Software	P1	certificatemanagement/Policies	
Enable Root CA	Enable	Activate Root CA	Management - Software	P1	certificatemanagement/Policies	
Device Connector		Device Connector Policy lets you choose the Configuration from Intersight only option to control configuration changes allowed from Cisco IMC. The Configuration from the Intersight-only option is enabled by default. You will observe the following changes when you deploy the Device Connector policy in Intersight: Validation tasks will fail: If Intersighl Read-only mode is enabled in the claimed device. If the firmware version of the Cisco UCS Standalone C-Series Servers is lower than 4.0(1). If Intersight Read-only mode is enabled, firmware upgrades will be successful only when performed from Intersight. Firmware upgrade performed locally from Cisco IMC will fail. IPMI over LAN privileges will be reset to read-only level if Configuration from Intersight only is enabled through the Device Connector policy, or if the same configuration is enabled in the Device Connector in Cisco IMC.				
Configuration from IS only	Enable	Enables configuration lockout on the endpoint. IMM only. Stand-alone servers only.	Management - Software	P1	deviceconnector/Policies	
Drive Security		Drive Security Policy enables you to configure security keys either locally or remotely using a KMIP server.				
Remote Key Mgmt (KMS)						
Primary KMS		KMS server IP or FQDN	Management - Software	P1	storage/DriveSecurityPolicies	
Secondary KMS		KMS server IP or FQDN	Management - Software	P1	storage/DriveSecurityPolicies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
KMS Root CA Certificate		KMS root certificate	Management - Software	P1	storage/DriveSecurityPolicies	
Enable KMS Authentication	Enable	Activate remote KMS	Management - Software	P1	storage/DriveSecurityPolicies	
Manual Key						
New Security Passphrase		Security passphrase	Management - Software	P1	storage/DriveSecurityPolicies	
Ethernet Adapter		An 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 like Virtual Extensible LAN (VXLAN), Network Virtualization using Generic Routing Encapsulation (NVGRE), Accelerated Receive Flow Steering (ARFS), Interrupt settings, and TCP Offload settings. The Ethernet Adapter policy includes the recommended settings for the virtual Ethernet interface, for each supported server operating system. Operating systems are sensitive to the settings in these policies. In general, the storage vendors require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.				
Cisco® Provided Ethernet adapter preconfiguration		Choose a server profile that matches what you are deploying and use the Cisco selected preconfigured BIOS settings for that type of deployment.	Network	P1	vnic/EthAdapterPolicies	
Preconfig selected		Selected precofigured setup	Network	P1	vnic/EthAdapterPolicies	
Enable advanced filtering		Activate advanced filtering	Network	P1	vnic/EthAdapterPolicies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Ethernet Network		An Ethernet Network policy sets the rules for the port to handle network traffic. This policy determines whether the port can carry single VLAN (Access) or multiple VLANs (Trunk) traffic.		N/A		
Ethernet Network Control		Ethernet Network Control policies configure the network control settings for the UCS Domain. This policy is applicable only for the Appliance Ports defined in a Port Policy and for the vNICs defined in a LAN Connectivity Policy, on FI-Attached UCS Servers.				
CDP enable	Disable	Enable Cisco Discovery Protocol. Disable if unneeded.	Network	P1	fabric/EthNetworkControlPolicies	
MAC Security Forge Allow/Deny	Enable	Determines whether forged MAC addresses are allowed or denied when packets are sent from the server to the switch. This can be: Allow– All server packets are accepted by the switch, regardless of the MAC address associated with the packets. This is the default option. Deny– After the first packet has been sent to the switch, all other packets must use the same MAC address or they will be silently rejected by the switch. In effect, this option enables port security for the associated vNIC.	Network	P1	fabric/EthNetworkControlPolicies	
Ethernet Network Group		An Ethernet Network Group policy enables you to manage settings for VLANs on a UCS Server. These settings include defining which VLANs are allowed, designating a Native VLAN, and specifying a QinQ VLAN.				

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Enable QinQ tunnelling	Enable	QinQ tunneling is a technique that enables a service provider to segregate the traffic of different customers in their infrastructure, while still giving the customer a full range of VLANs for their internal use by adding a second 802.1Q tag to an already tagged frame1. The 802.1Q tunneling expands the VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets2. A port configured to support 802.1Q tunneling is called a tunnel port2. This should be enabled in multitenant secure networks.	Network	P1	fabric/EthNetworkGroupPolicies	
Ethernet QoS		An Ethernet Quality of Service (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 like burst and rate on the outgoing traffic.		N/A		
FC Zone		Fiber Channel settings		N/A		
Fibre Channel Adapter		Fiber Channel settings		N/A		
Fibre Channel Network		Fiber Channel settings		N/A		
Fibre Channel QoS		Fiber Channel settings		N/A		
Firmware		Firmware installation behavior.				
Stand Alone - Advanced Mode		Values for standalone FW policy only. FW updates are important for patching known security issues and reducing the attack surface of your system.				
Rack Server Model		The UCS model you are using.	Management - Hardware	P1	firmware/Policies	
Firmware version		The FW for the UCS model you are using.	Management - Software	P1	firmware/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Exclude Drives		Check to exclude drive FW	Management - Hardware	P1	firmware/Policies	
Exclude Storage Controllers		Check to exclude Storage Conroller FW	Management - Hardware	P1	firmware/Policies	
UCS Server FI-attached - **Advanced Mode**		Values for UCS FI-attached FW policy only				
Rack Server Model		The UCS model you are using.	Management - Hardware	P1	firmware/Policies	
Firmware version		The FW for the UCS model you are using.	Management - Software	P1	firmware/Policies	
Exclude Drives		Check to exclude drive FW	Management - Hardware	P1	firmware/Policies	
Exclude Storage Controllers		Values for UCS FI-attached FW policy only	Management - Hardware	P1	firmware/Policies	
IMC Access		The 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 IMC Access Policy and is supported on Drive Security, SNMP, Syslog, and vMedia policies.				
Out of band mgmt	Enable	Enable or disable. In general it is more secure to deploy with an isolated management network, which would place out-of -band management at an advantage over in-band management. OOBM uses the management port, while IBM uses the uplink port and IP addresses typically in the host address space.	Management - Software	P1	access/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
IPMI Over LAN		The IPMI over LAN policy defines the protocols for 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.				
Enable or disable	Enable	Default is set to enable for admin user. It is recommended to disable unless needed. If enabled use a read-only user unless edits are required.	Management - Software	P1	ipmioverlan/Policies	
Privilege Level	Read-only	You can assign these privileges to the IPMI sessions on the server: admin–You can create admin, user, and read-only sessions on servers with the “Administrator” user role. read-only–You can only create read-only IPMI sessions on servers with the “Read-only” user role. user–You can create user and read-only sessions, but not admin sessions on servers with the “User” role. NOTE: This configuration is supported only on Cisco UCS C-Series Standalone and C-Series Intersight Managed Mode Servers. The value of the Privilege field must match exactly the role assigned to the user attempting to log in. For example, if this field is set to read-only and a user with the admin role attempts to log in through IPMI, that login attempt will fail.	Management - User	P1	ipmioverlan/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Encryption Key		The encryption key to use for IPMI Communication. The key must have an even number of hexadecimal characters and not exceeding 40 characters. You can use “00” to disable the encryption key use. If the encryption key specified is less than 40 characters, then the IPMI commands must add zeroes to the encryption key to achieve a length of 40 characters.	Management - Software	P1	ipmioverlan/Policies	
iSCSI Adapter		iSCSI settings.		N/A		
iSCSI Boot		iSCSI settings for boot.				
Static Configuration	Select Static	Preset connection information you enter here.	Configuration - Software	P1	vnic/IscsiBootPolicies	
Authentication CHAP or Mutual CHAP	Mutual CHAP	Mutual CHAP is recommended as the most secure method.	Configuration - Software	P1	vnic/IscsiBootPolicies	
iSCSI Static Target		Setting up the static target policy for iSCSI boot.				
Name		The static iSCSI target name. This policy needs to be created to use iSCSI boot with CHAP.	Configuration - Software	P1	vnic/IscsiStaticTargetPolicies	
IP address			Configuration - Software	P1	vnic/IscsiStaticTargetPolicies	
Port			Configuration - Software	P1	vnic/IscsiStaticTargetPolicies	
LUN ID			Configuration - Software	P1	vnic/IscsiStaticTargetPolicies	
LAN Connectivity		A 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.		N/A		

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
LDAP		Lightweight Directory Access Protocol (LDAP) stores and maintains directory information in a network. When LDAP is enabled in the Cisco IMC, 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, and configure LDAP servers and LDAP groups.				
Enable Encryption	Enable	Encrypts communication between endpoints and the LDAP server(s).	Configuration - Software	P1	iam/LdapPolicies	
Bind method	Login Credentials	The authentication (credentialed) method. Select login credentials.	Configuration - Software	P1	iam/LdapPolicies	
Group authentication	Enable	Group authorization is checked for users not in the local user database.	Configuration - Software	P1	iam/LdapPolicies	
Local User		The Local User policy automates the configuration of local user preferences. You can create one or more Local User policies which contain a list of local users that need to be configured. By default IPMI access is granted for all users. Adjust the IPMI policy as needed.				

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Enforce Strong Password	Enable	The password must have a minimum of 8 and a maximum of 20 characters. This is an Intersight platform limitation. The password must not contain the User Name. The password must contain characters from three of the following four categories: English uppercase characters (A through Z). English lowercase characters (a through z). Base 10 digits (0 through 9). Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, , =, ‘’). These rules are meant to define a strong password for the user, for security reasons. [[Please note: these requirements are not consistent with previous password requirements - OK?]]	Management - User	P1	iam/EndPointUserPolicies	
Enable Password Expiry	Enable	Set expiration to enable.	Management - User	P1	iam/EndPointUserPolicies	
Expiry Duration	180 days	Days until password expired.	Management - User	P1	iam/EndPointUserPolicies	
Expiry Notification	15 days	Days before expiry to notify the user.	Management - User	P1	iam/EndPointUserPolicies	
Password History	5	Retain the most “old passwords” possible: 5.	Management - User	P1	iam/EndPointUserPolicies	
Password Expiry Grace Period	0	Days that the expired password can still be used, set to 0.	Management - User	P1	iam/EndPointUserPolicies	
Network Connectivity		Sets DHCP/IPv4/IPv6		N/A		
NTP		Set up Network Time Protocol for clock sync.				
Enable	Enable	Enable NTP for time sensitive security methods.	Network	P1	ntp/Policies	
Server(s)		Time servers, use NIST public servers if not running your own.	Network	P1	ntp/Policies	
Timezone		Set timezone.	Network	P1	ntp/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Persistent Memory		Meeting pre-requisites, some UCS systems with Intel Optane® storage allow for perisistent memory capability. This policy referes to “Managed from Intersight” perisistet memeory policies.				
Enable Security Passphrase	Enable	Set the passphrase for persistent memory module configuration.	Configuration - Hardware	P1	memory/ PersistentMemoryPolicies	
Power		Power profiling and redundancy		N/A		
SAN Connectivity		vHBA setup		N/A		
Scrub		Scrub is typically used in server decommissions that will result in re-use of the system. It is distinct from the data sanitization in server secure erase. This policy determines what happens to local data and to the BIOS settings on a server during the discovery process, when the server is re-acknowledged, or when the server is disassociated from a service profile. Local disk scrub policies only apply to hard drives that are managed by Intersight and do not apply to other devices such as USB drives.				
Disk	Enable	Enable disk scrub	Configuration - Hardware	P1	compute/ScrubPolicies	
BIOS	Enable	Enable BIOS scrub	Configuration - Software	P1	compute/ScrubPolicies	
SD Card		Enable SD-based virtual drive (VD) to be available to the host.		N/A		
Serial Over LAN		Serial console access over the network.				
Enable or Disable Serial over LAN	Disable	Disable to reduce attack surface.	Configuration - Software	P1	sol/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
SMTP		Mail server capability for automated alerts based on system event log severity.				
Enable or disable	Enable	Enable	Management - Software	P1	smtp/Policies	
SMTP server		IP or FQDN of the SMTP server	Management - Software	P1	smtp/Policies	
SMTP port		SMTP server port for communications	Management - Software	P1	smtp/Policies	
Minimum severity	Warning	System Event Log severity for the alert. Set to warning to get all relevant alerts that might be security related.	Management - Software	P1	smtp/Policies	
Alert sender		Endpoint name	Management - Software	P1	smtp/Policies	
Alert reciever (email)		Alert recipient	Management - Software	P1	smtp/Policies	
SNMP		The 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.				
Enable or disable	Enable	Enable for monitoring system state	Management - Software	P1	snmp/Policies	
SNMP version select	v3	v3 is the most secure	Management - Software	P1	snmp/Policies	
SSH		The SSH policy 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.				

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Enable or disable	Disable	Disable to reduce attack surface unless required.	Management - Software	P1	ssh/Policies	
Storage		The Storage policy allows you to create drive groups, virtual drives, configure the storage capacity of a virtual drive, and configure the M.2 RAID controllers.				
Secure JBOD disk slots		Enter the secure drive slots in use (SED).	Management - Hardware	P1	storage/StoragePolicies	
Syslog		The 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).				
Minimum Severity	Warning	Use at least Warning level to get potentially security-related alerts.	Management - Software	P1	syslog/Policies	
Syslog server address		FQDN or IP of remote logging server.	Management - Software	P1	syslog/Policies	
Syslog server port		Syslog server communication port.	Management - Software	P1	syslog/Policies	
Thermal		Fan policy		N/A		
Virtual KVM		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.				
Enable video encryption	Enable	Enables encryption on all video information sent through KVM. The Video Encryption is enabled by default.	Configuration - Software	P1	kvm/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Allow tunneled vKVM	Enable	Allows vKVM traffic to be tunneled over the secure Device Connector connection.	Configuration - Software	P1	kvm/Policies	
Virtual Media		The Virtual Media 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 could 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.				
Enable Virtual Media Encryption	Enable	Select this option to enable the appearance of virtual drives on the boot selection menu after mapping the image and rebooting the host. This property is enabled by default. Systems running FW 4.2 or greater cannot disable this.	Configuration - Software	P1	vmedia/Policies	

IMM Checklist

Component type	Models	Software Version	Note
Cisco UCS® domain IMM	M5/M6/M7/M8	FW FI 4.3+, or Cisco Intersight® Server bundles 5.6+	Only settings in the policies relevant to security are specifically cited here.

Domain policies in Cisco Intersight allow you to configure various parameters for 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. Domain policies in Cisco Intersight are a new feature, and native to the application. Policy-based configuration with Domain Profiles is a Cisco Intersight Essentials feature, and is supported on Cisco UCS B-Series M5 and M6 servers and Cisco UCS C-Series M5, M6, M7, and M8 servers, and Cisco UCS X-Series M6 and M7 servers that are in a UCS Domain.

The Domain Policy creation wizard in Cisco Intersight has two pages:

General—The general page allows you to select the organization and enter a name for your policy. Optionally, include a short description and tag information to help identify the policy. Tags must be in the key:value format. For example, Org:IT or Site APJ

Policy Details—The policy-details page has properties that are applicable to UCS Domain Policies.

API References: Cisco Intersight API Docs and Overview - Intersight - Cisco DevNet.

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Ethernet Network Control		Ethernet Network Control policies configure the network control settings for the UCS Domain. This policy is applicable only for the Appliance Ports defined in a Port Policy and for the vNICs defined in a LAN Connectivity Policy, on FI-Attached UCS Servers.				
CDP enable	Disable	Enable Cisco Discovery Protocol. Disable if unneeded.	Network	P1	fabric/EthNetworkControlPolicies	
MAC Security Forge Allow/ Deny	Allow	Determines whether forged MAC addresses are allowed or denied when packets are sent from the server to the switch. This can be: Allow– All server packets are accepted by the switch, regardless of the MAC address associated with the packets. This is the default option. Deny– After the first packet has been sent to the switch, all other packets must use the same MAC address, or they will be silently rejected by the switch. In effect, this option enables port security for the associated vNIC.	Network	P1	fabric/EthNetworkControlPolicies	
LLDP Transmit	Disable	Link Layer Discovery Protocol. This is generally safe but can allow users to gain insight into devices present on their LAN segment.	Network	P1	fabric/EthNetworkControlPolicies	
LLDP Receive	Disable	Link Layer Discovery Protocol. This is generally safe but can allow users to gain insight into devices present on their LAN segment.	Network	P1	fabric/EthNetworkControlPolicies	
Eithernet Network Group		An Ethernet Network Group policy enables you to manage settings for VLANs on a UCS Server. These settings include defining which VLANs are allowed, designating a Native VLAN, and specifying a QinQ VLAN.		N/A		

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Flow Control		Configure the Priority Flow Control for each port, to enable the no-drop behavior for the CoS defined by the System QoS Policy and an Ethernet QoS policy. In Auto and On priorities, the Receive and Send link level flow control will be Off.		N/A		
Link Aggregation		This policy can be used to configure Link Aggregation properties.		N/A		
Link Control		This policy enables configuration of link control administrative state and configuration (normal or aggressive) mode for ports.		N/A		
Multicast Policy		The multicast policy is used to configure Internet Group Management Protocol (IGMP) snooping and IGMP querier.				
IGMP Snooping	Enable	IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic to control delivery of IP multicasts. Network switches with IGMP snooping listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast transmission. If a network does not enable IGMP snooping, attackers could exploit this fact in a denial-of-service (DoS) attack.	Network	P1	fabric/MulticastPolicies	
Network Connectivity		The Network Connectivity policy enables you to configure and assign IPv4 and IPv6 addresses.		N/A		
NTP		Set up Network Time Protocol for clock sync.				
Enable	Enable	Enable NTP for time sensitive security methods.	Network	P1	ntp/Policies	

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Server(s)		Time servers; use NIST public servers if not running your own.	Network	P1	ntp/Policies	
Timezone		Set timezone.	Network	P1	ntp/Policies	
Port		FI Port configuration settings.		N/A		
SNMP		The 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.				
Enable or disable	Enable	Enable for monitoring system state	Management - Software	P1	snmp/Policies	
SNMP version select	v3	v3 is the most secure.	Management - Software	P1	snmp/Policies	
Switch Control		The Switch Control policy supports VLAN port count optimization, configuring MAC address aging time, and configuring Link Control Global settings.		N/A		
Syslog		The 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).				

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
Minimum Severity	Warning	Use at least Warning level to get potentially security-related alerts.	Management - Software	P1	syslog/Policies	
Syslog server address		FQDN or IP of remote logging server.	Management - Software	P1	syslog/Policies	
Syslog server port		Syslog server communication port.	Management - Software	P1	syslog/Policies	
System QoS		A System Quality of Service (QoS) policy assigns a system class to the outgoing traffic. This system class determines the quality of service for the outgoing traffic.		N/A		
VLAN		VLAN policies create a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic. You can create VLANs and Private VLANs using the VLAN policy.		N/A		
VSAN		With the VSAN policy, you can create Virtual SANs (VSANs) to isolate devices physically connected to the same SAN fabric. VSANs improve security and stability in Fibre Channel fabrics and let you create several logical SANs over a common physical infrastructure.		N/A		

IMM Checklist

Component type	Models	Software Version	Note
Cisco UCS® Blade System Chassis in IMM	9508	FW FI 4.3+, or Cisco Intersight® Server bundles 5.6+	Only settings in the policies relevant to security are specifically cited here.

Chassis policies in Cisco Intersight allow you to configure various parameters of the chassis, including IP pool configuration, VLAN settings, SNMP authentication, and SNMP trap settings. A chassis policy can be assigned to any number of chassis profiles to provide a configuration baseline for a chassis.

To view the Chassis Policies table view, from the **Service Selector** drop-down list, choose **Infrastructure Service**. Navigate to **Configure > Policies**.

The Chassis Policy creation wizard in Cisco Intersight has two pages:

General—The general page allows you to select the organization and enter a name for your policy. Optionally, include a short description and tag information to help identify the policy. Tags must be in the key:value format. For example, Org:IT or Site APJ

Policy Details—The policy details page has properties that are applicable to Cisco UCS® Chassis Policies. Chassis Policies can also be cloned (using the **Policy Clone** wizard) with properties that are similar to the existing policies. The clone policy action is available on both the policies list and detailed views. For more information, see Cloning a Policy.

API References: Cisco Intersight API Docs and Overview - Intersight - Cisco DevNet.

IMM Checklist

Policy Name	Setting	Description	Feature/Component	Implementation Priority	API Call	Notes
IMC Access		The IMC Access policy allows you to configure your network and associate an IP address from an IP Pool with a server. In-Band IP addresses, Out-Of-Band IP addresses, or both In-Band and Out-Of-Band IP addresses can be configured using IMC Access Policy and are supported on Drive Security, SNMP, Syslog, and vMedia policies.				
Out-of-band Mgmt	Enable	Enable or disable. In general it is more secure to deploy with an isolated management network that would place out-of-band management at an advantage over in-band management. OOBM uses the management port, while IBM uses the uplink port and IP addresses typically in the host address space.	Management - Software	P1	access/Policies	
Power		This policy enables configuration of power redundancy and power allocation for chassis.		N/A		
SNMP		The SNMP policy configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. This policy supports such SNMP versions 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.				
Enable or disable	Enable	Enable for monitoring system state	Management - Software	P1	snmp/Policies	
SNMP version select	v3	v3 is the most secure.	Management - Software	P1	snmp/Policies	
Thermal		Sets chassis fan control.		N/A		