Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers

Common Criteria Operational User Guidance and Preparative Procedures

Version 0.7

10 February 2025

Americas Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Common Criteria Guidance Procedures

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers. This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers TOE certified under Common Criteria.

1.1. Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2. Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining UCS operations.

1.3. Document References

This document makes reference to several Cisco Systems documents. The documents used are shown below.

Links to all configuration guides:

- Cisco Intersight Virtual Appliance and Intersight Assist Getting Started Guide, 1.0.9
  - https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide.pdf
- IMM Fabric - Install and Upgrade Guides
  - https://www.cisco.com/c/en/us/support/servers-unified-computing/intersight/products-installation-guides-list.html
- Cisco Intersight - Appliance Help Center
  - https://intersight.com/help/appliance/getting_started/claim_targets

Table 1: Document References

	Cisco Intersight Virtual Appliance
[1]	Cisco UCS **Site Preparation** Guide http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/site-prep-guide/ucs_site_prep.pdf
[2]	**Release Notes** for Cisco Intersight Virtual Appliance – December 2023 https://intersight.com/help/appliance/whats_new/connected_appliance/2023#december_(1)

[3]	Cisco Intersight Virtual Appliance and Intersight Assist Getting Started Guide, 1.0.9 https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide.html
[4]	Cisco Intersight Virtual Appliance Dashboard Settings https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/m_settings_dashboard.html
[5]	Configuring UCS Domain Policies https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/b_intersight_managed_mode_guide_chapter_0101.html
[6]	Configuring Server Policies https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/b_intersight_managed_mode_guide_chapter_0110.html
[7]	Roles and Privileges https://intersight.com/help/appliance/resources/RBAC#roles_and_privileges
	Fabric Interconnect – Intersight Managed Mode (IMM)
[8]	Cisco UCS **6400** Series Fabric Interconnect Hardware Installation Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6454-install-guide/6454.html Cisco UCS **6500** Series Fabric Interconnect Hardware Installation Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6500-install-guide/b-cisco-ucs-6500-fi-install-guide.html
[9]	Cisco Intersight Managed Mode Configuration Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide.html
[10]	Cisco Intersight Managed Mode Fabric Interconnect **Admin Guide – GUI** https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM-FI-Admin-Guide/b_imm_fi_admin_guide.html Cisco Intersight Managed Mode Fabric Interconnect **Admin Guide – CLI** https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/IMM-FI-Admin-Guide/b_imm_fi_admin_guide/m_imm_fi_admin_guide_device_console_cli.html
	X-Series Modular System
[11]	Cisco UCS **X-Series Modular System**: Install and Upgrade Guides https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-x-series-modular-system/series.html#InstallandUpgrade
[12]	Cisco UCS X-Series Quick Start Guide https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-quick-start-guide.html
	C-Series Rack Servers
[13]	Cisco UCS **C-Series Rack Servers**: Install and Upgrade Guides http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html
	Troubleshooting and Other References

[14]	Cisco Intersight **Troubleshooting** Reference Guide https://intersight.com/help/appliance/troubleshooting
[15]	**Cisco UCS 6536 Fabric Interconnect Data Sheet** https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs6536-fabric-interconnect-ds.html
[16]	Cisco Intersight – **Claim Targets** https://intersight.com/help/appliance/getting_started/claim_targets
[17]	Managing **Firmware** https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/b_intersight_managed_mode_guide_chapter_01000.html
	UCS X9508 Server Chassis and Intelligent Fabric Modules (IFM)
[18]	Cisco UCS X9508 Server Chassis Installation Guide https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/x/hw/x9508/install/b-ucs-x9508-install/m-ucsx-9508-chassis-overview.html

1.4. Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria EAL2+ evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

1.4.1. Supported Configurations

- One Cisco Intersight Virtual Appliance
- Cisco Intersight components
    - One or more Cisco UCS Fabric Interconnects [6454, 64108, and/or 6536]
        - Cisco Intersight Infrastructure Firmware release 4.3(xx)
- One or more Server and Intelligent Fabric Modules (with software loaded from the Cisco Intersight bundle)
    - Modular System configurations:
        - One or more Cisco UCS X9508 Chassis with:
            - One or more Cisco UCS-X Compute Nodes (servers) (210C M6, 210C M7, or 410C M7)
            - One or more Cisco Intelligent Fabric Modules (IFM)
                - For M6 compute nodes: UCSX-I-9108-25G, UCSX-I-9108-100G
                - For M7 compute nodes: UCSX-I-9108-25G-D, UCSX-I-9108-100G-D
    - Rack-Mount Server configurations:
        - One or more Cisco UCS Rack Servers:
            - Any of: C220 M6, C225 M6, C240 M6, C245 M6, C220 M7, or C240 M7

1.4.2. Compatible network adapters (VIC) for Modular System Compute Nodes - M6:

- Cisco UCSX-V4-Q25GME
- Cisco UCSX-V4-PCIME

1.4.3. Compatible network adapters (VIC) for Modular System Compute Nodes – M7:

- Cisco UCSX-ME-V5Q50G-D
- Cisco UCSX-ML-V5Q50G-D
- Cisco UCSX-ML-V5D200G-D
- Cisco UCSX-V4-PCIME

1.4.4. Compatible network adapters (VIC) for Rack Mount Servers

- Cisco UCSC-PCIE-C25Q-04
- Cisco UCSC-PCIE-C100-04
- Cisco UCSC-P-V5Q50G
- Cisco UCSC-P-V5D200G
- Cisco UCSC-M-V25-04
- Cisco UCSC-M-V5Q50G
- Cisco UCSC-M-V100-04
- Cisco UCSC-M-V5D200G

1.5. Operational Environment

1.5.1. Required software for the operational environment:

- Cisco Intersight uses HTML5 on all pages. Intersight does not require any additional plugins beyond your browser's capabilities. Note that that Cisco Intersight runs on the Fabric Interconnect component of the UCS system and the management workstation is used to connect to the UCS and run the Cisco Intersight. Cisco Intersight runs on the following minimum supported browser versions:
  - Google Chrome 62.0.3202.94 or higher
  - Mozilla Firefox 57.0.1 or higher
  - Apple Safari 10.1.1 or higher
  - Microsoft Edge (Chromium) Beta or higher
- SSHv2 Client: Cisco Intersight can be managed remotely via SSHv2.
- NTP Server: An NTP server is a mandatory component of the operational environment that would allow for synchronizing the TOE clocks with an external time source.
- Firewall: The UCS system must be separated from public/untrusted networks by an application-aware firewall such that remote access to the TOE's management interface is prohibited from untrusted networks and only allowed from trusted networks.

1.5.2. Optional software/components for the operational environment:

- Remote Authentication Server: an LDAP server is an optional component for use with the TOE.
- Syslog Server: A syslog server is an optional component for use with the TOE. It is a supplemental storage system for audit logs, but it does not provide audit log storage for the TOE.

1.6. Excluded Functionality

Stand-alone configuration of the C-Series (Rack Mount) Servers is not supported; C-Series servers must be managed by Cisco Intersight.

Direct admin interfaces to CIMC (on X-Series, C-Series servers) is disabled when the servers are integrated with the fabric and will be managed via Cisco Intersight.

IPMI management of CIMC is disabled by default and remains disabled in the evaluated configuration.

Telnet is disabled by default and must remain disabled in the evaluated configuration, SSH must be used instead.

All other functionality is supported in the evaluated configuration.

1.7. Modes of Operation

1.7.1. Cisco Intersight Virtual Appliance

- Booting mode:
    - When booting, the Cisco Intersight normal boot sequence can be interrupted by the Authorised Administrator with direct local access to the serial console port. When the boot sequence is interrupted, Cisco Intersight presents a loader prompt, allowing the administrator to select the image to be booted.
- Intersight Appliance Maintenance Shell mode:
    - The Maintenance Shell CLI can be entered using local console or SSH. This console-based utility helps in troubleshooting and addressing misconfiguration or networking issues during the appliance installation. The Maintenance Shell aims to:
        - Detect and display issues with the installation prerequisites.
        - Enable editing the inputs that are provided during the initial appliance deployment.
        - Assist with continuing the installation after you fix the settings or change inputs during the appliance deployment.
    - For further detail, refer to "Diagnostics" in **[3]**.
- Normal operation mode:

  - There are two forms of normal operation: single-node and multi-node cluster.
    - Setting up a single-node Intersight Virtual Appliance requires an IP address and two DNS records for that IP address. For more information about IP addresses and Hostname requirements, see "IP Address and Hostname Requirements" in **[3]**.
    - Setting up a multi-node cluster for Intersight Virtual Appliance requires three hostnames, three IP addresses, and one DC-CNAME for each hostname. For more information about IP addresses and Hostname requirements, see "IP Address and Hostname Requirements" in **[3]**.
  - Use only HTTPS protocol and fully qualified domain name to access the appliance via the Web user interface.

- Shutdown/Reboot mode:
  - Intersight Virtual Appliance can be rebooted in Intersight Appliance Maintenance Shell mode (CLI). After entering the CLI, the shell will display option [6] Reboot virtual appliance node. This option stops services, reboots the appliance, and restores the services when the appliance reboots.

1.7.2. Cisco Intersight Managed Mode Fabric Interconnect

- Initial Configuration mode:
  - The initial configuration for a Fabric Interconnect can be done by using the serial console when the Fabric Interconnect boots for the first time. This can happen either during factory install, or after the existing configuration is cleared. The configuration wizard enables you to select the management mode and other parameters such as the administrative subnet, gateway, and DNS IP addresses for each Fabric Interconnect. For the management mode, you can choose whether you want to manage the Fabric Interconnect through Cisco UCS Manager or Cisco Intersight. For this evaluation, Cisco Intersight must be selected.
  - After completing the initial configuration of the Fabric Interconnects, they must be claimed for use with the Cisco Intersight platform. For more information about claiming devices in Cisco Intersight, see **[16]** Target Claim.
  - For further information, refer to "Setting Up Fabric Interconnects" in **[9]**.
- Normal operation mode. There are two forms of normal operation:
  - Standalone configuration:

        - Only one IP address and the subnet mask are used for the single management port on the single fabric interconnect.
    - Cluster configuration, a pair of clustered fabric interconnects use the following IP addresses in the same subnet:
        - Management port IP address for fabric interconnect A; Management port IP address for fabric interconnect B. Both fabric interconnects in a cluster configuration must go through the initial setup process.
            - When the second fabric interconnect is set up, it detects the first fabric interconnect as a peer fabric interconnect in the cluster.
            - To use the cluster configuration, the two fabric interconnects must be directly connected together using Ethernet cables between the L1 (L1-to-L1) and L2 (L2-to-L2) high availability ports.
    - For further information, refer to "Setting Up Fabric Interconnects" in **[9]**.

- Device Console mode:
    - Device Console CLI mode can be access via SSH to troubleshoot the devices, or if the devices are not connecting to Cisco Intersight. Device Console CLI also allows the administrator to perform basic maintenance tasks like resetting the admin password.
    - Device Console GUI provides system information such as the model, serial number, and firmware version of the Fabric Interconnects. It allows configuration of the Device Connector. It shows the Inventory details of the Servers and Chassis. To access the Device Console user interface, log in to the Fabric Interconnect using a management IP address or DNS hostname if available. Administrator privileges are required.
    - For further detail, refer to **[10]** **Admin Guide – GUI and CLI**.
- Shutdown/reboot mode:
    - Rebooting can only be done via Device Console CLI mode using "reboot" command. During reboot, running instances are terminated, and unsaved configurations will be lost.

1.7.3. UCS X Chassis and IFM

- IFM is an attached module to the Chassis; therefore, it does not function as a separate entity.
- Booting mode:
    - When booting, no boot sequence is available to be interrupted by anyone with direct local access to the serial console port.

- Initial discovery mode:
    - During discovery, the Chassis (with IFM attached) will auto sync firmware with the Fabric Interconnect if their firmware versions do not match the firmware version of the Fabric Interconnect
- Normal operation mode:
    - During normal operation mode, the Chassis (with IFM attached) is managed by Intersight GUI. For further information, refer to "Chassis and FEX Lifecycle" in **[9]**.
- Power Cycle mode:
    - On the Chassis table page of Intersight GUI, select the chassis, Inventory, Intelligent Fabric Modules, click on the ellipsis and select "Reset Intelligent Fabric Module".

1.7.4. UCS-X Computing Blades

- Booting mode:
    - When booting, no boot sequence is available to be interrupted by anyone with direct local access to the serial console port.
- Normal operation mode:
    - During normal operation mode, the UCS-X Computing Blades are managed by Intersight GUI. For further information, refer to "Server Lifecycle" in **[9]**.
    - CLI mode:
        - In Fabric Interconnect Device Console CLI:
            - show chassis all [to obtain UCSX9508 chassis ID]
            - show server all [to obtain blade number]
                - connect cimc [chassis id]/[server/blade number]
    - via SSH to management IP.
- Shutdown/Reboot mode:
    - On the Servers table page of Intersight GUI, select the UCS-C servers. The following options can be selected via Action > Power:
        - Power off: turn off the power of the server
        - Power cycle: turn off and back on the server
        - Hard Reset: reboot the server
        - Shutdown OS: if the server has an operating system installed, then this option will send a proper shutdown signal to that OS

1.7.5. UCS-C Rack Servers

- Booting mode:
  - When booting, the rack server's normal boot sequence can be interrupted by anyone with direct local access to the serial console port.
  - When the boot sequence is interrupted, the CLI presents options for BIOS Setup, Boot Menu, Diagnostics, CIMC Setup and Network Boot.
  - If none is selected, the CLI will load a UEFI Interactive Shell.
- Normal operation mode:
  - During normal operation mode, the UCS-C Rack Servers are managed by Intersight GUI. For further information, refer to "Server Lifecycle" in **[9]**.
  - CLI mode via Fabric Interconnect:
    - In Fabric Interconnect Device Console CLI:
      - show server all
        - connect cimc [rack id]
    - via SSH to management IP.
- Shutdown/Reboot mode:
  - On the Servers table page of Intersight GUI, select the UCS-C servers. The following options can be selected via Action > Power:
    - Power off: turn off the power of the server
    - Power cycle: turn off and back on the server
    - Hard Reset: reboot the server
    - Shutdown OS: if the server has an operating system installed, then this option will send a proper shutdown signal to that OS

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

2.1. Physical Acceptance

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the

Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also verify that the unit has the following external identification:

Table 2: Evaluated Products and their External Identification

Product Name	External Identification
Cisco UCS X9508 Server Chassis	UCSX-9508
Cisco UCS X210c M6 Compute Node	UCSX-210C-M6
Cisco UCS X210c M7 Compute Node	UCSX-210C-M7
Cisco UCS X410c M7 Compute Node	UCSX-410C-M7
Cisco UCS C220 M6 Rack Server	UCSC-C220-M6
Cisco UCS C225 M6 Rack Server	UCSC-C225-M6
Cisco UCS C240 M6 Rack Server	UCSC-C240-M6
Cisco UCS C245 M6 Rack Server	UCSC-C245-M6
Cisco UCS C220 M7 Rack Server	UCSC-C220-M7
Cisco UCS C240 M7 Rack Server	UCSC-C240-M7

Cisco UCS 6454 Fabric Interconnect	UCS-FI-6454
Cisco UCS 64108 Fabric Interconnect	UCS-FI-64108
Cisco UCS 6536 Fabric Interconnect	UCS-FI-6536
Cisco UCS 9108 25G Intelligent Fabric Module (M6)	UCSX-I-9108-25G
Cisco UCS 9108 100G Intelligent Fabric Module (M6)	UCSX-I-9108-100G
Cisco UCS 9108 25G Intelligent Fabric Module (M7)	UCSX-I-9108-25G-D
Cisco UCS 9108 100G Intelligent Fabric Module (M7)	UCSX-I-9108-100G-D

2.2. Software Acceptance

Step 1 Approved methods for obtaining a Common Criteria evaluated software images:

- First, deploy Cisco Intersight Virtual Appliance and Intersight Assist: Cisco Intersight Virtual Appliance and Intersight Assist is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format. Intersight Virtual Appliance and Intersight Assist OVA must be deployed using VMware vCenter. Software images (see Table 3) are available from Cisco.com at the following: https://software.cisco.com/download/home/
- Second, when the OVA is deployed and can be access via the web browser, the user will be asked to access https://www.intersight.com/pvapp to download the Binary software package Intersight-appliance-bundle-1.0.9-677.bin (see Table 4) to continue with installation.
- Fabric Interconnect and Intelligent Fabric Modules (IFM) ship with software images preinstalled. The IFM (attached on UCS-X Chassis) will synchronize firmware version with Fabric Interconnect during installation. If the firmware version is not the evaluated version, the correct Intersight Managed Mode Fabric Interconnect firmware bundle (See Table 5) can also be downloaded from https://www.intersight.com/pvapp and then upload to the System > Software Repository in the GUI of Cisco Intersight Virtual Appliance. User can then refer to "Upgrading Fabric Interconnect Firmware" in **[17]** and follow the instruction to install the correct version listed in Table 5 using Intersight GUI**.**
- UCS Servers come with basic CIMC. To install the evaluated firmware version listed in Table 6 (UCS-X) and Table 7 (UCS-C), visit https://software.cisco.com/download/home/ to download the correct "Host Upgrade Utility" version in the form of an iso image, and then flash it via the KVM accessible via CIMC.

Step 2 Once the file is downloaded, verify that it was not tampered with by using an SHA512 checksum utility (such as 'sha512sum' on Linux) to compute the SHA512 checksum for the downloaded file and comparing this with the checksum for the image listed in Table 5 below. If the checksums do not match, contact Cisco Technical Assistance Center (TAC) https://mycase.cloudapps.cisco.com/case

Step 3 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. To access the Device Console user interface, which is installed on the Fabric Interconnect, log in to the Fabric Interconnect using a management IP address. You must have administrator privileges to access Device Console UI and CLI. Refer to **[10]** Admin Guide – **GUI** and **CLI**.

- For all Fabric Interconnect (FI) models, use the Intersight GUI to determine the active version, or use the "**show version**" command to display which image is "Active".
    - connect nxos
        - show version
        - exit
- For the Intelligent Fabric Module (IFM), use the "**show firmware**" command in Fabric Interconnect Device Console CLI. Example:
    - show chassis all [to obtain UCSX9508 chassis ID]
    - connect iom [chassis ID]
        - show firmware
- For X-Series servers, use the Fabric Interconnect Device Console CLI to display image version and "Build Sha". First use the "show chassis all" and "show server all" commands to list out the respective inventory and the IDs/numbers; then use "connect" command to access the CLI of the blade; then finally use "version" command to display firmware information (version, Sha). Example:
    - show chassis all
    - show server all
        - connect cimc [chassis id]/[server/blade number]
            - version
- For C-Series servers, use the same procedure as X-Series without [chassis id] in the Fabric Interconnect Device Console CLI. Example:
    - show server all
        - connect cimc [rack id]
            - version

Table 3: OVA Software Image for Cisco Intersight Virtual Appliance and Assist

Cisco Intersight Virtual Appliance and Assist for vSphere	
Release	1.0.9-630
Filename	intersight-appliance-installer-vsphere-1.0.9-630.ova
Release Date	14-Dec-2023
Description	Cisco Intersight Virtual Appliance and Assist for vSphere in deployable virtual machine format (.ova). This is required before installing Cisco Intersight Appliance Software Bundle (.bin) in Table 4.
Size	1796.51 MB
SHA512 Checksum	50bab4a229ce838682ad7d77a7476c33f8b04be3f0908c2aa820694e37926ac07adf0341edb001c2171ee93cc3cabf8d653be2d0b3946e50cb50986b83f08891

Table 4: Binary Software Image for Cisco Intersight Appliance Software Bundle

Cisco Intersight Appliance Software Bundle	
Release	1.0.9-677
Filename	Intersight-appliance-bundle-1.0.9-677.bin
Release Date	07-July-2024
Description	Cisco Intersight Appliance Software Bundle in binary software package format (.bin).
Size	1796.51 MB
SHA512 Checksum	50bab4a229ce838682ad7d77a7476c33f8b04be3f0908c2aa820694e37926ac07adf0341edb001c2171ee93cc3cabf8d653be2d0b3946e50cb50986b83f08891

Table 5: Software Image Bundle for Fabric Interconnects (Intersight infrastructure bundles)

UCS 6500 Series Fabric Interconnects	
Release	4.3(4.240074)
Filename	intersight-ucs-infra-5gfi.4.3.4.240074.bin
Release Date	Sep 3, 2024
Description	Cisco Intersight Infrastructure Bundle - UCS 6500 Series Fabric Interconnects
Size	1932.3 MB

SHA512 Checksum	9afb27d80739e325b704bb8ed76efcd89c46bf620651ac937d3069efe3061716d1d477b0f1796d2df47dcf4262c9b39297292a4f001492e97838fe7f4e9e6488
UCS 6400 Series Fabric Interconnects	
Release	4.3(4.240074)
Filename	ucs-intersight-infra-4gfi.4.3.4.240074.bin
Release Date	Sep 3, 2024
Description	Cisco Intersight Infrastructure Bundle - UCS 6400 Series Fabric Interconnects
Size	1891.6 MB
SHA512 Checksum	8ba0bb3a1360d840521ee0fd2fa48b4406066f55f4248f45ea45f750cb7d47a8e9dd03b17f5ab4753e7787aae5d712f9d62c0280e870528e91ce7224e190c2f4

Table 6: Software Image Bundle for UCS X-Series Server Compute Nodes and Adapters

Cisco UCS X210c M7 Compute Node	
Release	5.2(0.230127)
Filename	intersight-ucs-server-210c-m7.5.2.0.230127.bin
Release Date	Jan 24, 2024
Description	Cisco Intersight Server Bundle – Cisco UCS X210c M7 Compute Node
Size	711.0 MB
SHA512 Checksum	458968cfb83252112ef4c4cb9ab51733bae9316972e6a681ccfe4d8d1aecc3ba6b6b5d1376748fbcf7d3aa95a4e47636562683d7846e8c3c3f25a0d74b7ea2ac
Cisco UCS X210c M6 Compute Node	
Release	5.2(0.230127)
Filename	intersight-ucs-server-210c-m6.5.2.0.230127.bin
Release Date	Jan 24, 2024
Description	Cisco Intersight Server Bundle – Cisco UCS X210c M6 Compute Node
Size	609.5 MB

SHA512 Checksum	0c1874b26c3c3ef6186567b29fedaa9d9fd153ecd30547109bbc6f7dcd99a26df9af34b6c1caa9732ab3c59f631feacd1e3d119813cb8781d6d33ff91ada5319
Cisco UCS X410c M7 Compute Node	
Release	5.2(0.230127)
Filename	intersight-ucs-server-410c-m7.5.2.0.230127.bin
Release Date	Nov 15, 2023
Description	Cisco Intersight Server Bundle – Cisco UCS X410c M7 Compute Node
Size	Jan 24, 2024
SHA512 Checksum	08a93f0b959ed21986cb681212360e99fc94d5e4ad48d9054512ac06b2d0083e573cb3615489037f0e2c4d74ce424ee4235b5d27d0eb8a84e8133ae575cdb9b0

Table 7: Software Image Bundle for UCS C-Series Servers and Adapters

Cisco UCS C220 M6 Rack Server	
Release	4.3(4.240152)
Filename	ucs-c220m6-huu-4.3.4.240152.iso
Release Date	June 04, 2024
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for Intersight based C-Series management.
Size	695.64 MB
SHA512 Checksum	c681132727fc472232be950cebcc9b82aa52ad5ef78538a0ad070a55abfff30a0007ad36105622090ed0973b7580fde7f1277280ec6b8ece07311d2227fc64f0
Cisco UCS C225 M6 Rack Server	
Release	4.3(4.240152)
Filename	ucs-c225m6-huu-4.3.4.240152.iso
Release Date	June 04, 2024
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for Intersight based C-Series management.
Size	676.70 MB
SHA512 Checksum	06f7322170a66de673f3e929bc1a54ef84d753de35c73b0120fed7f260abe1c8904bdcca0a9df6b2e731d902d06d03e58a465cd78e9c092763818ed40891633f

Cisco UCS C240 M6 Rack Server	
Release	4.3(4.240152)
Filename	ucs-c240m6-huu-4.3.4.240152.iso
Release Date	June 04, 2024
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for Intersight based C-Series management.
Size	782.37 MB
SHA512 Checksum	841408859080b22774c3745070fee7231f998319f82847c6338c6fc1fbdf5c5a6d86a4f027f66af313e6867425e54b381a9f2b10fa1db4e4ff76ce0429f1ea75
Cisco UCS C245 M6 Rack Server	
Release	4.3(4.240152)
Filename	ucs-c245m6-huu-4.3.4.240152.iso
Release Date	June 04, 2024
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for Intersight based C-Series management.
Size	688.24 MB
SHA512 Checksum	6a4ea791ff7a0c37e8bdf26d4b3dde3e590bdaff3a68c1ee22f99caa181c2e2f9300a747e3d7219c9e4366f4ac39c7254c0dfff425bfc492eb8f85d5a0c3fdf5
Cisco UCS C220 M7 Rack Server	
Release	4.3(4.240152)
Filename	ucs-c220m7-huu-4.3.4.240152.iso
Release Date	June 04, 2024
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for Intersight based C-Series management.
Size	812.31 MB
SHA512 Checksum	efbb98e5a50e6868b337a09955544a83de37b837236bece008abc1783949bfb0905f2aede6cc349025ae138e5b3410e22d8ec5b10cf865d1dec31bc68ef9b187
Cisco UCS C240 M7 Rack Server	
Release	4.3(4.240152)

Cisco Intersight Virtual Appliance with IMM Fabric and UCS Servers Common Criteria Guidance Procedures

Filename	ucs-c240m7-huu-4.3.4.240152.iso
Release Date	June 04, 2024
Description	Software for the **UCS C-Series rack-mounted servers**. This is software for Intersight based C-Series management.
Size	838.79 MB
SHA512 Checksum	97b09d7c26e6af2ad54c935fed2abef6e12817ad5e6ed6fc269d81f3bd85f14fa0cc096770c61a726e9bdceab183739d17839ecdc5fa0d52a970a6c79671be15

3. Secure Installation

3.1. Physical Installation

Follow the site preparation guide **[1]** for preparation of the physical site, and hardware installation guides as applicable to the configuration of hardware components to be deployed:

- **[8]** for Fabric Interconnects
  - UCS 6400 Series Fabric Interconnect
  - UCS 6500 Series Fabric Interconnect
- **[18]** for
  - UCS X9508 Server Chassis in the "Installation" chapter.
  - Intelligent Fabric Modules in the "Installing and Removing Components" chapter.
- **[11]** for UCS-X Servers.
  - Cisco UCS-X 210C M6 compute node
  - Cisco UCS-X 210C M7 compute node
  - Cisco UCS-X 410C M7 compute node
- **[13]** for UCS-C servers
  - Cisco UCS C220 M6 rack server
  - Cisco UCS C225 M6 rack server
  - Cisco UCS C240 M6 rack server
  - Cisco UCS C245 M6 rack server
  - Cisco UCS C220 M7 rack server
  - Cisco UCS C240 M7 rack server

Refer to Section 2 Step 9 to ensure each of those components are running the CC-evaluated software version.

3.2. Installing Cisco Intersight Virtual Appliance

Note: The hardware required to support the virtual appliance must be deployed within a secure environment, consistent with deployment of the Target of Evaluation (TOE) components.

Cisco Intersight Virtual Appliance is distributed as a deployable virtual machine contained in an Open Virtual Appliance (OVA) file format, ZIP file format, or a TAR file format. Cisco Intersight Virtual Appliance supports VMware High Availability (VMHA) to ensure non-disruptive operation of the virtual appliance. For more information about VMHA, please refer to the documentation on vmware.com.

Intersight Virtual Appliance and Intersight Assist OVA must be deployed using VMware vCenter. The OVA cannot be directly deployed on ESXi servers.

IP addresses and their DNS records need to be set up and provided to complete the deployment of Intersight Virtual Appliance and Intersight Assist OVA. For more information about IP addresses and Hostname requirements, see "IP Address and Hostname Requirements" in **[3]**.

By default, VMware vCenter does not include a Certificate Authority (CA) that validates the Cisco digital signature on the Intersight Virtual Appliance OVA file. The VMware vCenter GUI will indicate that the OVA's certificate is invalid and is not trusted. Although possible, it is recommended that you do not ignore this warning and proceed with the installation. Instead, download and install the appropriate root CA from the table below that will validate the digital signature on the Intersight Virtual Appliance OVA file. Validating the signature ensures that the OVA was both issued by Cisco and has not been modified by a 3rd party.

The root CA certificates listed in the following table are available on Cisco's PKI page.

OVA version	CA Issuer	CA Serial Number	CA Expiration
1.0.9-630	TrustID EV Code Signing CA 4	40:01:7f:9e:01:04:d0:f0:da:98:8d:43:d8:97:43:03	March 18, 2030
1.0.9-588	DigiCert Trusted G4 Code Signing 2021 CA1	08:ad:40:b2:60:d2:9c:4c:9f:5e:cd:a9:bd:93:ae:d9	
1.0.9-499	None	None	None
1.0.9-342	DigiCert Trusted G4 Code Signing 2021 CA1	08:ad:40:b2:60:d2:9c:4c:9f:5e:cd:a9:bd:93:ae:d9	March 18, 2030

For details regarding installing Virtual Appliance, refer to "Installation" in **[3]**

Refer to Table 3: OVA Software Image for Cisco Intersight Virtual Appliance to ensure the TOE is running the CC-evaluated software version.

3.3.Setting up Fabric Interconnects

The initial configuration for a Fabric Interconnect can be referred to "Setting Up Fabric Interconnects" in **[9]**.

After completing the initial configuration of the Fabric Interconnects, they must be claimed in Cisco Intersight. For more information about claiming devices in Cisco Intersight, see **[16]** Target Claim.

Intersight cannot discover any hardware connected to the Fabric Interconnects until its ports are configured, and that is done through a domain profile. After the Fabric Interconnect is claimed in section 2.3, proceed to configure server ports:

- Connect the server ports to both Fabric Interconnects. For example, ports 1 and 2 to FI-A and ports 3 and 4 to FI-B. For UCS-C, 1 SFP cable goes to any Server Port in the FI-A, and 1 SFP cable goes to any Server Port in the FI-B. These Server Ports need to be configured in the Port Policy.
- Configure the server ports on both Fabric Interconnects by using a UCS Domain profile with a Port Policy. Creating a UCS Domain Profile provides detailed information about creating a UCS Domain profile and assigning it to a UCS Fabric Interconnect Domain. Refer to "Configuring UCS Domain Profiles" within [9] to configure a UCS Domain Profile. See section 3.6.2 for more information regarding Port Policy.

After the server ports are configured and applied, all the Server Chassis (with IFM attached) and UCS-C servers that are connected to the Fabric Interconnect are automatically discovered.

3.4.Setting up UCS X Chassis, IFM, and Compute Nodes

UCS-X chassis is automatically claimed and discovered. During discovery, the Server Chassis (with IFM attached) will automatically synchronize firmware with the Fabric Interconnect if their firmware versions do not match the firmware version of the Fabric Interconnect. Because of this, it may take 25-30 minutes for the Server Chassis (with IFM attached) to appear in the GUI.

To view the Server Chassis (with IFM attached) that are discovered in Intersight Virtual Appliance, browse to **Operate -> Chassis**. If they are still not displayed, refresh the browser. For further information, refer to "Chassis and FEX Lifecycle" in **[9]**.

Cisco UCS X compute node is configured and managed using Cisco Intersight Virtual Appliance. For references, see the **[12]** Cisco UCS X-Series Quick Start Guide. After a UCS-X chassis is discovered, the blade servers connected to the UCS-X chassis are automatically claimed and discovered.

The servers that are discovered appear on the Servers page. In Intersight, browse to **Operate -> Servers**. Intersight should have discovered the servers in the domain. If servers are still not displayed, refresh the browser. For further information, refer to "Server Lifecycle" in **[9]**.

3.5.Setting up UCS-C Servers

The UCS-C rack servers connected to the FI are automatically claimed and discovered. For UCS-C servers to be claimed and discovered, they must be in the factory default state.

If the UCS-C server is not automatically discovered, it may not be in the correct firmware version. To correct this, go to the CIMC > Launch vKVM and install

the "Host Upgrade Utility" iso image with the correct firmware version listed in Table 7.

3.6. Network Connectivity for Servers

3.6.1. Port Configurations

For configuration options and procedures related to available port modes and port types, refer to "Creating a Port Policy" within **[5]**. After the Port Policy is configured, the Domain Profile that claimed it has to be deployed in order for the changes to take effect.

3.6.2. Server Ports

For configuration options and procedures related to server ports, refer to Step 8 Port Roles in "Creating a Port Policy" mentioned above.

3.6.3. Protected Management Network

The IT Environment in which the TOE components reside will need to provide a protected network for interconnects from the Intersight to remote authentication servers, remote time servers (NTP), and remote log servers (syslog).

An option for sufficient isolation of the protected management network would be to isolate it from Ethernet traffic of hosted OS instances by assigning separate VLAN(s) from the VLANs assigned to vNICs of any hosted OS, except where the hosted OS is an OS trusted by the TOE to provide remote authentication, time, or logging service.

For configuration options and procedures, refer to "Creating an Ethernet Network Group Policy" within **[5]**.

3.6.3.1. Reserved VLAN Ranges

VLAN IDs from 3915-4042, 4043-4047, 4094, and 4095 are reserved for internal system use, and thus cannot be used.

The maximum number of VLANs allowed per Ethernet Network Policy is 3000.

Whenever the range of reserved VLANs is changed, all Fabric Interconnects must be rebooted. If a Fabric Interconnect boots and its reserved VLAN range does not match what's defined by Intersight, the Fabric Interconnect will be updated and rebooted automatically. For VLANs, refer to "Creating a VLAN Policy" within **[5]**.

Before creating a VLAN policy with VLAN ID, a Multicast Policy needs to be created as a pre-requisite:

- **Step 1:** Log in to Cisco Intersight with your Cisco ID and select admin role.
- **Step 2:** From the **Service Selector** drop-down list, select **Infrastructure Service**.
- **Step 3:** Navigate to **Configure > Policies**, and then click **Create Policy**.

- **Step 4:** Select **Multicast Policy**, and then click **Start**.
- **Step 5:** On the **Policy Details** page, leave everything at default value.
- **Step 6:** Click **Create.**

Procedure To configure VLAN IDs:

- **Step 1:** Log in to Cisco Intersight with your Cisco ID and select admin role.
- **Step 2:** From the **Service Selector** drop-down list, select **Infrastructure Service**.
- **Step 3:** Navigate to **Configure > Policies**, and then click **Create Policy**.
- **Step 4:** Select **VLAN**, and then click **Start**.
- **Step 5:** On the **Policy Details** page, click **Add VLAN** and configure policy details, including VLAN IDs.
- **Step 6:** Under **Multicast Policy***, click **Select Policy.**
- **Step 7:** Click **Add.**

3.6.3.2. Add FI to the VLAN

Before adding the servers to the VLAN, both Fabric Interconnects have to be configured to add the VLAN policy to their current UCS Domain Profile in use:

- **Step 1:** Log in to Cisco Intersight with your Cisco ID and select admin role.
- **Step 2:** From the **Service Selector** drop-down list, select **Infrastructure Service**.
- **Step 3:** Navigate to **Configure > Profiles**, and then select the applicable Fabric Interconnect's UCS Domain Profile.
- **Step 4:** Select **Action > Edit**, and then navigate to **VLAN & VSAN Configuration**.
- **Step 5:** In **VLAN Configuration** of both Fabric Interconnect A and B, select the VLAN policy.
- **Step 6:** Click Next until the end of the dialog, then click **Deploy**. Changes will not be made until deploy is completed.

3.6.3.3. Add UCS Server to VLAN

First, an IP Pool needs to be created before an IMC Access Policy (which claims the VLAN ID) can be created:

- **Step 1:** Log in to Cisco Intersight with your Cisco ID and select admin role.
- **Step 2:** From the **Service Selector** drop-down list, select **Infrastructure Service**.
- **Step 3:** Navigate to **Configure > Pools**, and then click **Create Pool**.
- **Step 4:** Select **IP**, and then click **Start**.
- **Step 5:** On the **IPv4 Details** page, input the Netmask, Gateway, Primary DNS and the optional Secondary DNS as needed.

- **Step 6:** Click **Add IP Blocks** and input the IP subnet range for this Protected Management Network.
- **Step 7:** Repeat for IPv6, or unselect **Configure IPv6 Pool** to skip it.
- **Step 8:** Click **Create.**

Second, an IMC Access Policy needs to be created to claim the VLAN ID:

- **Step 1:** Log in to Cisco Intersight with your Cisco ID and select admin role.
- **Step 2:** From the **Service Selector** drop-down list, select **Infrastructure Service**.
- **Step 3:** Navigate to **Configure > Policies**, and then click **Create Policy**.
- **Step 4:** Select **IMC Access**, and then click **Start**.
- **Step 5:** On the **Policy Details** page, in the **VLAN ID** box, input the VLAN ID.
- **Step 6:** Check or uncheck **IPv4 address configuration** depending on the IP pool configured, repeat for IPv6.
- **Step 7:** Click **Select IP Pool >** Select the **IP Pool.**
- **Step 8:** Click **Create**.

Finally, claim this IMC Access Policy in the applicable UCS Server Profile. To modify the server assignment for the profile, first go to **Configure > Profiles** menu, select the applicable server profile, then **Action > Unassign** the existing server first and then proceed with new server assignment in edit view later.

After unassigning server, edit the UCS Server Profile:

- **Step 1:** From the **Service Selector** drop-down list, select **Infrastructure Service**.
- **Step 2:** Navigate to **Configure > Profiles**, and then select the **UCS Server Profiles** tab.
- **Step 3:** Select the applicable UCS Server Profile.
- **Step 4:** Select **Action > Edit**, and then navigate to **Management Configuration**.
- **Step 5:** In **IMC Access,** select the IMC Access policy.
- **Step 6:** Click Next until the end of the dialog, then click **Deploy**. Changes will not be made until deploy is completed.

3.7. Network Protocols and Cryptographic Settings

3.7.1. Remote Administration Protocols

- Telnet is disabled by default and must remain disabled in the evaluated configuration.

- SSHv2 is enabled be default for the Intersight Virtual Appliance (Maintenance Shell) and cannot be disabled.
- Cisco Intersight does not provide an option to limit which algorithms are enforced for SSH connections, so administrators using SSH should configure their SSH clients to use only the algorithms that are specified for use in the evaluated configuration, including RSA, AES, and SHA-1.

  Cisco Intersight Virtual Appliance provides SSH default key sizes of 2048 which is the evaluated configuration. The following algorithms are allowed for use to SSH to Intersight Virtual Appliance:

  - Encryption Algorithms
    - aes128-ctr,
    - aes192-ctr,
    - aes256-ctr,
    - aes128-gcm@openssh.com,
    - aes256-gcm@openssh.com
  - MAC Algorithms
    - hmac-sha2-256,
    - hmac-sha2-512
  - Key Exchange methods
    - diffie-hellman-group14-sha1,
    - ecdh-sha2-nistp256,
    - ecdh-sha2-nistp384,
    - ecdh-sha2-nistp521
    - curve25519-sha256

  Fabric Interconnect in Intersight Managed Mode provides SSH default key sizes of 2048 which is the evaluated configuration. The following I algorithms are allowed for use to SSH to Fabric Interconnect – Intersight Managed Mode:

  - Encryption Algorithms
    - aes128-ctr,
    - aes192-ctr,
    - aes256-ctr,
    - aes128-gcm@openssh.com,
    - aes256-gcm@openssh.com
  - MAC Algorithms
    - hmac-sha1,
    - hmac-sha2-256,
    - hmac-sha2-512
  - Key Exchange methods
    - diffie-hellman-group14-sha1,
    - diffie-hellman-group16-sha512,
    - ecdh-sha2-nistp256,
    - ecdh-sha2-nistp384,

- ecdh-sha2-nistp521
- curve25519-sha256

Fabric Interconnect provides an HTTPS interface to access the FI Device Connector. The FI supports the following ciphersuites:

TLSv1.2 Allowed Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (P-256)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (P-256))
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (P-256)
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

TLSv1.3 Allowed Cipher Suites:

- TLS_AES_256_GCM_SHA384 (secp521r1)
- TLS_AES_128_GCM_SHA256 (secp521r1)
- TLS_CHACHA20_POLY1305_SHA256 (secp521r1)

UCS-X compute nodes and UCS-C servers in Intersight Managed Mode disable SSH by default. Only Direct KVM Access is available, which can be found in Intersight Virtual Appliance interface. Only SSH for UCS-C servers in Standalone mode (which is not in the scope of this evaluation) can be enabled/disabled if desired using Intersight GUI.

- HTTPS is enabled by default and must remain enabled for remote administrative access to all management functions described in the Security Target. HTTPS is listening by default on TCP port 443. Intersight does not provide an option to limit which algorithms are enforced for HTTPS connections, so administrators using HTTPS should configure their HTTPS clients/browsers to use only the algorithms that are specified for use in the evaluated configuration, including RSA, AES, and SHA.
    - To configure HTTPS, refer to "Certificates" in **[4]**.
        - UCS supports key modulus sizes of 2048 by default, and any larger modulus sizes are permitted in the evaluated configuration. The default key pair is 2048-bit.
    - When the steps above have been applied, the following cipher-suites will be the only ones available for use.

TLSv1.2 Allowed Cipher Suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp521r1)

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp521r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp521r1)

TLSv1.3 Allowed Cipher Suites:

- TLS_AES_256_GCM_SHA384 (secp521r1)
- TLS_AES_128_GCM_SHA256 (secp521r1)

  - When the browser-based HTTPS client using HTML5 Cisco Intersight Client is used, it will also use TLSv1.2 and TLSv1.3, and negotiate the connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, if the browser supports that ciphersuite, otherwise Intersight will negotiate one of the other ciphersuites listed above that allowed in the CC-certified configuration and all use RSA, AES, and SHA. If the browser does not support TLSv1.2 or TLSv1.3 and at least one of the listed ciphersuites, the session negotiation will fail.

3.7.2. Authentication Server Protocols

- LDAP (outbound) for authentication of TOE administrators to remote authentication servers is disabled by default and should only be used with TLS encryption enabled. UCS supports encryption of LDAP connections using TLS (LDAPS). To configure LDAP refer to "Configuring LDAP Settings" within **[4]**. When creating the LDAP provider via GUI, check the "Enable Encryption" checkbox. If encryption is enabled, a trusted root certificate has to be added. For more information, see "Certificates" in **[4]**

3.7.3. Logging and Alerting Protocols

- Syslog (outbound) for transmission of UCS syslog events to a remote syslog server is disabled by default but can be enabled in the evaluated configuration (to enable transmission of all events to a remote syslog server including failure messages that are not stored locally) with the understanding that syslog traffic is transmitted unencrypted, so any protection from unauthorized disclosure or modification while in transit must be provided by the operational environment.
- To configure syslog, refer to "Configuring External Syslog" in **[4]**
- To enable the transmitting of syslog messages to remote syslog servers:
  - Log in to Cisco Intersight with your Cisco ID and select **admin role**.

- From the Service Selector drop-down list, choose System, and navigate to **Settings > NETWORKING > External Syslog**.
- Navigate to **Configure > Policies**, and then click **Create Policy**.
- Click **Add External Syslog Server**
- Update the following fields as needed
  - **Enable External Syslog** radio button.
    - Hostname/IP Address
    - Port number
    - Protocol (TLS)
    - Minimum Severity of Alarms to Report, from Infor to Warning.
- Click **Save**.

3.7.4. VSAN

- VSAN is not in the scope of this evaluation. However, Intersight allows an administrator to configure VSAN policies and incorporate VSAN appliances in their deployment.
- If TOE administrators choose to enable VSAN functionality, Cisco recommends following Cisco procedures to configure VSAN policies.

4. Secure Configuration

4.1. User Roles

User can switch between accounts or roles in Cisco Intersight without logging out of the application. If you are logged into multiple accounts or roles, the **Profile** menu in the Intersight dashboard provides the option to **Switch Account or Role**. In the **Select Account and Role** window, select the account (or role) that you want to switch to. You will be logged in to the new account.

All roles include read access to all configurations on the system, and all roles except Read-Only can modify some portion of the system state. A user assigned a role can modify the system state in that user's assigned area. For more information see [7] "Roles and Privileges" and Section 7 - Security Parameters for the Administrative Roles of this document.

To change the role, navigate to **Settings > ACCESS & PERMISSIONS > Users**, and select the user that you want to change the role for, and click the **Edit** icon. In the **Edit User** window, select the role and click **Save**.

4.1.1. Default Roles and Privileges

More details about default roles can be found in the Security Target. The system contains the following default user roles:

- Account Administrator
- Read-Only
- Device Technician
- Device Administrator
- User Access Administrator
- Server Administrator

Note: HyperFlex Cluster Administrator is also a default user role. However, the role is only applicable to HyperFlex Clusters, which are not in scope of this evaluation.

Privileges give their holder access to specific system resources and permission to perform specific tasks. Privileges can be added to the default roles. Table 5 in the Security Target lists each privilege and the user role given that privilege by default.

4.1.2. Custom Roles and Modification of Default Roles

New custom roles can be created, deleted, or modified to add or remove any combination of privileges. Default roles can be deleted or modified except the 'admin' and 'read-only' roles. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role.

For example, the default Server Administrator and Device Administrator roles have different set of privileges, but a new custom Server and Device Administrator role can be created that combines the privileges of both roles. To create a User Defined Role, refer to "Adding a Role" in **[4]**.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

LDAP servers return the roles in the user profile attributes.

Refer to **[7]** "Roles and Privileges" for more information about UCS roles and privileges.

4.1.3. User Role Functions following Failure or Operational Error

In the case of failure or operational error including security relevant events that prevent the user role from performing their privilege, every role must contact the Organization's Account Administrator as soon as possible to maintain the TOE's security.

An Account Administrator can find troubleshooting steps can be found at **[14] Cisco Intersight Troubleshooting Reference Guide** which are shown in the sub-sections below (from 4.1.3.1 to 4.1.3.7)**.** If the Organization's Account Administrator still cannot remediate the issue to maintain security, the Account Administrator should contact Cisco Technical Assistance Center (TAC) https://mycase.cloudapps.cisco.com/case as soon as possible for assistance.

4.1.3.1. Problem: Device Connection to Intersight is unsuccessful

If device connection to Intersight is unsuccessful, check for the following in the Device Connector UI in IMM Fabric Interconnect:

- A network connection to the Intersight platform is established from the Device Connector in the endpoint.
- Intersight Management is enabled in the Device Connector.
- A valid CA-signed certificate presented by the Intersight portal exists.
- DNS is configured, and the DNS name is resolved.
- NTP is configured
- If a firewall is introduced between the managed device and Intersight or the rules for an existing firewall was changed, thus impacting the connectivity, ensure that the rules permit traffic through the firewall.
- If you use an HTTP proxy to route traffic out of your premises, and if you have made changes to the HTTP proxy server's configuration, ensure that you change the Device Connector's configuration accordingly. This is required because Intersight does not automatically detect HTTP proxy servers.

After you ensure that the items listed above are in place, you can log into the managed device and navigate to the Device Connector Admin page.

From the Admin page, you can find details about the specific connectivity error as observed by the Device Connector. For more information, see Device Connection.

4.1.3.2. Problem: Unable to Launch vKVM Session

Before initiating a vKVM session, ensure that:

- vKVM is enabled on the server. vKVM can be enabled from the Cisco IMC or using the Virtual KVM Policy. For more information, see Creating a Virtual KVM Policy in [6] Configuring Server Policies.
- The number of Active sessions does not exceed the configured limit in the Virtual KVM policy. Existing vKVM sessions can be viewed and if required, terminated from the Sessions tab.

4.1.3.3. Problem: Unable to Launch Tunneled vKVM Session

Before initiating a vKVM session, ensure that:

- vKVM is enabled in the account and on the server. vKVM can be enabled using the Virtual KVM Policy. For more information, see Creating a Virtual KVM Policy in [6] Configuring Server Policies.
- There are no other active Tunneled vKVM sessions and the number of Active sessions does not exceed the configured limit in the Virtual KVM policy. Existing Tunneled vKVM and vKVM sessions can be viewed and if required, terminated from the Sessions tab.

4.1.3.4. Problem: Chassis discovery is unsuccessful with an error "Fabric port configuration failed"

When a chassis IOM is connected to the port that was repurposed (earlier connected to the rack server and now connected to IOM) without disconnecting the rack server from Intersight, you will get an error.

To overcome this problem, perform the following:

- You must decommission the server before connecting an IOM to the Fabric Interconnect port to which the rack server was previously connected.
- When one adapter port of the rack server is connected to Fabric Interconnect port and the same port is repurposed to connect to an IOM, you must unconfigure the specific port through domain profile deployment and reconfigure the same Fabric Interconnect port with server role.

4.1.3.5. Problem: Rack Server discovery is unsuccessful with an error "Unable to configure rack server" or "Retry of rack server connection failed"

When a rack server adapter is connected to the port that was repurposed (earlier connected to the IOM and now connected to rack server) without disconnecting the IOM port from Intersight, you will get an error.

To overcome this problem, perform the following:

- You must decommission the chassis only when you are fully disconnecting the IOM.
- When one IOM port is removed from the Fabric Interconnect port and the same port is repurposed to connect to a rack server, you must unconfigure the specific IOM port through domain profile deployment and reconfigure the same IOM port with server role.

4.1.3.6. Problem: “Profile in validating state” warning message seen for all applicable policies

The following warnings can be seen in different use cases:

Warning 1: “The policy is attached to profile ESXI-SP-1-1 which is in Validating state. Ensure that the profile deployment completes and retry."

Warning 2: "The policy is attached to multiple profiles which are in Validating/Configuring state. Ensure that the profile deployments complete and retry."

The use cases are:

- Case 1: Policy is being attached to a Server Profile Template and one or more of the existing derived profiles of the Template are being deployed.
    - Workarounds/Solution: Retry attaching the policy to the Template after some time.
- Case 2: New profiles are being derived from a Server Profile Template but one or more of the existing derived profiles of the Template are being deployed.
    - Workarounds/Solution: This is a known issue tracked by CSCwh89356. The policies attached to the Template and the derived profiles will be out of sync. For the profile with warnings, you can detach and reattach to the same Template. This will sync the Template to the derived profile.
- Case 3: Policy is being edited while one or more of the profiles that it is already attached to are being deployed.
    - Workarounds/Solution: This is a valid error. Policy attached to a profile being deployed cannot be edited. Try to edit the policy after some time.

- Case 4: Policy is being attached to a profile while one or more of the profiles that it is already attached to are being deployed.
    - Workarounds/Solution: Retry attaching the policy to the Profile after some time.

4.1.3.7. Problem: LAN or SAN Connectivity Policy attach warning: "Adapter slot 2, configured in the policy, is not present in the server."

This is due to policy configuration mismatch with the assigned server. Rediscover the server and try again or change the server assignment to a compatible server.

4.2. Passwords

4.2.1. Virtual Appliance Password Policy

To configure password policy for local users in Intersight Virtual Appliance:

- Log in to Cisco Intersight with your Cisco ID and select **admin role**.
- From the Service Selector drop-down list, choose System, and navigate to **Settings > AUTHENTICATION > Local Users**.
    - User can view the details of the existing password policy
- Navigate to **Configure > Configure Local Users**
- Configure the password policy by updating the following password policy options as needed.
    - CC Evaluated Configuration:
        - Length of Password: Minimum 12.
        - Must not be identical to the username or reverse username
        - Does not contain more than three repeating characters, such as aaabbb
        - Does not contain dictionary words
        - At least three of the following: lower case letters, upper case letters, digits, special characters
            - Upper Case Characters: Minimum 1 (required)
            - Lower Case Characters: Minimum 1 (required)
            - Digits: Minimum 1 (required)
            - Special characters: Minimum 0 (optional) and not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign)
        - The administrator must configure Max Consecutive Incorrect Login Attempts Allowed (Default is 5).
            - Note: Lockout for Admin User is “false” by default and can be set to “true” if needed.
        - The administrator must configure lockout period. Default is 900 seconds (15 minutes). The account is automatically unlocked after the configured lockout time period elapses.
- Click **Save**.

- For more information, refer to "Configuring Password Policy for Local Users" in **[4]**.

4.2.2. Virtual Appliance Resetting Password of Local Users

To reset the password for local users in Intersight Virtual Appliance:

- Log in to Cisco Intersight with your Cisco ID and select **admin role**.
- From the Service Selector drop-down list, choose System, and navigate to **Settings > ACCESS & PERMISSIONS > Users**.
- Select the local user to reset the password.
- Click the pencil icon and change the password.
- Click **Save**.

Note: When an Account Administrator resets the password for the local "admin" user, only the GUI password is changed. The SSH password of the local "admin" user remains unchanged. The local "admin" user must log into the appliance using the newly reset password. Once the local "admin" user is logged in, a prompt appears that mandates the local "admin" user to change the password, which then resets both the GUI and the SSH passwords.

- For more information, refer to "Resetting the Password of Local Users" in **[4]**.

4.2.3. Fabric Interconnect Password Policy

Fabric Interconnects prevent users from choosing insecure passwords, each password for local user accounts must meet the following requirements:

- Must contain at least 12 characters.
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must contain at least three of the following:
    - Lower case letters
    - Upper case letters
    - Digits
    - Special characters
- Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank.

This requirement applies to the local password database and on the password selection functions provided by the TOE, but remote authentication servers may have pre-configured passwords which do not meet the quality metrics.

The requirements above are enforced by UCS for CLI and GUI accounts. IPMI also supports password-based authentication, but IPMI is disabled by default and must remain disabled in the CC-evaluated configuration.

For more information, refer to "Fabric Interconnect Password Guidelines" within to "Setting Up Fabric Interconnects" in **[9]**.

4.3. Clock Management

It is mandatory to have at least one Network Time Protocol (NTP) configured in Cisco Intersight Virtual Appliance to enable synchronizing the time on the appliance with the NTP servers. An administrator must have the admin or server-maintenance privilege to be able to configure the system's use of an NTP server. To add an NTP server via the GUI:

- Log in to Cisco Intersight with your Cisco ID and select **admin role**.
- From the Service Selector drop-down list, choose System, and navigate to Settings > NETWORKING > NTP.
- Click **Configure**.
- Click **Add NTP Server**.
- Click + New Server. Enter the following information:
  - **Server Name:** Server hostname or IP address
  - **Symmetric Key Type:** Type of symmetric key to use for this server
  - **Symmetric Key ID:** Positive integer that identifies a cryptographic key used to authenticate NTP messages
  - **Symmetric Key Value:** Value of the symmetric key
- Click Save.

4.4. Identification and Authentication

4.4.1. Local and Remote Authentication

Intersight can be configured to use any of the following authentication methods:

- Local authentication (password);
  - Authorized administrators with the or admin privileges may configure local authentication.

- Remote authentication (LDAP)
    - A "Bind DN" and its password need to be created on LDAP server so that the Intersight Virtual Appliance can authenticate against the LDAP server.
    - Authorized administrators with the admin privileges may configure remote authentication. Refer to "Configuring LDAP Settings" in **[4]** for more details.

Note: At the login page of the GUI, "Local" or "LDAP" authentication has to be specified. A local user and LDAP user may have the same username, password, and the same roles and privileges.

4.4.2. Delete a User

Intersight can be configured to use any of the following authentication methods:

- Local account:
    - Log in to Cisco Intersight with your Cisco ID and select **admin role**.
    - From the Service Selector drop-down list, choose System, and navigate to Settings > ACCESS & PERMISSIONS > Users.
    - Check the box next to the user to be deleted.
    - Click the trash can icon.
    - Click **Delete**.
- Remote authentication (LDAP)
    - Remove on LDAP Server.

Note: Deleting a User does not automatically log the user out of the current session. The following steps need to be taken to terminate the current session of the user being deleted:

- Log in to Cisco Intersight with your Cisco ID and select **admin role**.
- From the Service Selector drop-down list, choose System, and navigate to System, and navigate to Sessions.
- Check the box next to the session of the deleted user to be terminated.
- Click the trash can icon.
- Click **Terminate**.

5. Security Relevant Events

The Audit Log is stored centrally on the primary Intersight instance and replicated to secondary instances (if present). For the most complete view audited events, across all devices, and to view the auditable events defined in the Security Target, administrators should review the Audit Log. Note: Cisco Intersight does not generate audit events specific to startup or shutdown of the audit log or system event log because those logs cannot be stopped or started. However, booting/rebooting or shutting down Cisco Intersight are audited events and can be used to satisfy this requirement. Configuration of syslog servers is audited within the local audit log. Failed authentication attempts are logged to Intersight.

5.1. Reviewing, Sorting, and Filtering Audited Events

Using the Intersight GUI, administrators with any privilege level can review, sort and filter audited events based on record identifier (ID); affected object; or user.

- To perform sorting:
    - From the Service Selector drop-down list, choose System, and navigate to **Audit Logs**
        - Click on any one of the tabs to sort by that field:
            - Date/Time
            - Affected Object
            - User ID
- To perform filtering:
    - From the Service Selector drop-down list, choose System, and navigate to Audit Logs
        - Click on the "Add Filter" box and enter desired filter parameters on the Filter page.

For more information about logging refer to "Configuring External Syslog" in **[4]**.

Additional audit logs, relevant to startup, shutdown, reboot, etc., can be found in the Tech Support Bundle. The administrator (any role except Account administrator, User Access Administrator, Audit log viewer, Integrated Systems Administrator/Operator) can navigate to the Tech Support Bundle using these steps:

- From the Service Selector drop-down list, choose System, and navigate to **Tech Support Bundle**
    - Click on Collect Appliance Tech Support Bundle in the center screen.
    - Download the tech support bundle when generation is complete.

- Uncompress the bundle and look in the following locations in this example (date numbers will be different):
  - 20240811211326_intersight_ts.tar\20240811211326_intersight_ts\20240811211326_intersight_intersight.cc.local_ts.tar\20240811211326_intersight_intersight.cc.local_ts\intersight.cc.local\system\last.log

5.2. Deleting Audit Records

Audit Log Retention Period is configurable. The time is in months, for which Audit Logs are retained. The allowed range is between 6 months and 48 months. The system default is 48 months. Audit Logs older than the specified retention period are automatically deleted. It is not possible for administrators with any privilege to edit, purge or delete records.

The Audit logs deletion task is set to run on a daily basis at 6.00 AM UTC, and all the audit logs that meet the retention period set in this field will automatically start getting deleted at this time. Once deleted, audit logs cannot be retrieved.

To configure the length of time (Retention Period) before Audit Logs are deleted of a specific user, specify “Audit Logs Retention Period (Months) in Account Details configuration. For more information , refer to “Configure Account Settings” in **[4]**.

6. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. Table 8 identifies the requirements and the associated security measures of the authorized users.

Table 8: Environment Objectives

Env. Security Objectives (From the Security Target)	**IT Environment Security Objective Definition** (From the Security Target)	**Responsibility of the Administrators**
OE.ADMIN	Personnel measures are in place to ensure well trained and trusted administrators are authorized to manage the TOE.	The authorized administrators must be trained, and access rights are limited to those with the necessary trust and qualifications.
OE.BOUNDARY	The TOE must be separated from public networks by an application aware firewall.	The authorized administrators are responsible for deploying and maintaining an application aware firewall to separate the TOE from public networks and ensuring it is appropriately configured to filter traffic.
OE.PHYSICAL	The operational environment of the TOE shall have a physical security policy preventing unauthorized physical access to the TOE. The policy must document physical security controls including access control, physical separation of hardware, and monitoring policies to	The authorized administrators must establish and enforce a physical security policy, which includes access control, physical separation of hardware, and monitoring policies to prevent unauthorized physical access to the TOE.

	ensure no unauthorized physical access to the TOE is allowed.	
OE.POWER	The operational environment of the TOE shall incorporate a power management strategy using UPS or backup generators to ensure that power continues to flow under any adverse conditions.	The authorized administrators must implement a power management strategy that includes UPS or backup generators to maintain TOE operations during power failures.
OE.REDUNDANT_NET	The operational environment of the TOE shall provide redundant network links to protect against network administrator operator error or network equipment failure.	The authorized administrators must ensure the establishment of redundant network links to mitigate downtime and maintain TOE connectivity in case of operator error or equipment failure.
OE.REMOTE_SERVERS	The operational environment of the TOE shall optionally provide remote authentication servers, SNMP servers, and/or NTP servers, and will protect communications between the TOE and the servers.	When using remote authentication servers, SNMP, and/or NTP servers, the authorized administrator must implement secure communication channels to protect data in transit between these servers and TOE.

7. Security Parameters for the Administrative Roles

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. Table 9 identifies the requirements and the associated security measures of the authorized users.

Table 9: Secure Parameters for Administrative Accounts

Administrative Interfaces	Administrative Roles	Permissions	Secure Parameters
Cisco Intersight Virtual Appliance			
GUI via Virtual Appliance WebUI	Account Administrator Read-Only Server Administrator	Refer to section Summary of Roles and Privileges within [7]	See section 2.7.2 for authentication server protocols and 3.2.1 for local authentication
CLI via ESXi console	Account Administrator	All permissions with no restrictions.	See section 3.2.1
CLI via SSH	Account Administrator	All permissions with no restrictions.	See section 2.7.1 for remote administration protocols and 3.2.1 for local authentication
Fabric Interconnects			
GUI via Virtual Appliance WebUI	Account Administrator Read-Only Server Administrator	Refer to section Summary of Roles and Privileges within [7]	See section 2.7.2 for authentication server protocols and 3.2.1 for local authentication
CLI via SSH	Account Administrator	All permissions with no restrictions.	See section 3.2.2
IFM, UCS-X Chassis			
Graphical User Interface (GUI) via	Account Administrator Read-Only	Refer to section Summary of	See section 2.7.2 for authentication

Virtual Appliance WebUI	Server Administrator	Roles and Privileges within [7]	server protocols and 3.2.1 for local authentication
CLI via Fabric Interconnect CLI	Account Administrator	All permissions with no restrictions.	See section 3.2.2
UCS-X Computing Node			
Graphical User Interface (GUI) via Virtual Appliance WebUI	Account Administrator Read-Only Server Administrator	Refer to section Summary of Roles and Privileges within [7]	See section 2.7.2 for authentication server protocols and 3.2.1 for local authentication
vKVM via Virtual Appliance WebUI	Account Administrator	All permissions with no restrictions.	See section 2.7.2 and 3.2.1 for local authentication
CLI via Fabric Interconnect CLI	Account Administrator	All permissions with no restrictions.	See section 3.2.2
CLI via SSH	Account Administrator Server Administrator	Refer to section Summary of Roles and Privileges within [7]	See section 2.7.1 for remote administration protocols
UCS-C Rack Server			
Graphical User Interface (GUI) via Virtual Appliance WebUI	Account Administrator Read-Only Server Administrator	Refer to section Summary of Roles and Privileges within [7]	See section 2.7.2 for authentication server protocols and 3.2.1 for local authentication
vKVM on Virtual Appliance WebUI	Account Administrator	All permissions with no restrictions.	See section 2.7.2 for authentication server protocols and 3.2.1 for local authentication

CLI via Fabric Interconnect CLI	Account Administrator	All permissions with no restrictions.	See section 3.2.2
CLI via SSH	Account Administrator Server Administrator	Refer to section Summary of Roles and Privileges within [7]	See section 2.7.1 for remote administration protocols

8. Related Documentation

Use this document in conjunction with the Unified Computing documentation at the following location:

- https://www.cisco.com/c/en/us/support/servers-unified-computing/intersight/series.html

The following sections provide sources for obtaining documentation from Cisco Systems.

8.1. Obtaining Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see *Cisco Support & Downloads*, which also lists all new and revised Cisco technical documentation of specific products at:

https://www.cisco.com/c/en/us/support/index.html

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

8.2. Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Contact Cisco** in the toolbar and select **Feedback**. After you complete the form, click Submit to send it to Cisco.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

9. Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in

the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com