

Security Hardening Benchmark for Cisco FirePower Devices

STND-78-2143-Security Hardening Benchmark for Cisco FirePower Devices | Version 1.9

Revision Date: 16/5/2024

Approved By: Head of Department (HOD), Cloud Enablement Services (CES)

Information Classification: Restricted, Sensitive (Normal)

This document contains proprietary information that is confidential to the Synapxe Pte Ltd. Disclosure of this document in full or in part, may result in material damage to the Synapxe Pte Ltd. Written permission must be obtained prior to the disclosure of this document to a third party. Any hardcopy of this document, printed or photocopied, is considered an uncontrolled copy. The original, signed-off document is the controlled copy.

Table of Contents

1	1 Purpose						
2							
3		FIREPOWER MANAGEMENT CENTRE (FMC)					
	3.1	General Security Control List					
	3.2	Health Monitoring	3				
	3.3	Management Access Control List	4				
4	FIRE	EPOWER THREAT DEFENSE (FTD)	7				
	4.1	General Security Control List	7				
	4.2	Health Monitoring	8				
	4.3	Management Access Control List	9				
5	FIRE	EPOWER CHASSIS MANAGER (FCM)	11				
	5.1	General Security Control List	11				
	5.2	Health Monitoring	12				
	5.3	Management Access Control List	13				
6	Ref	erences/Records	16				
7	7 Revision History						

1 Purpose

This document contains the baseline security controls for the Cisco FirePower devices.

2 Scope

This hardening baseline applies to the Cisco FirePower devices deployed in the H-Cloud network infrastructure.

3 10.FIREPOWER MANAGEMENT CENTRE (FMC)

3.1 General Security Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
3.1.1	Hostname	Device Hostname should be unique and consistent across H-Cloud <system name=""> host names should conform to the H- Cloud Naming Convention.</system>	<pre>< DataCenterLocation > - < NetworkZone > - <institution cluster="">-< DevicePurpose >< Running Numbers ></institution></pre>	Login via GUI System > Maangement Interfaces > Shared Settings > Hostname > Save
3.1.2	Warning Banner	Standard login banner containing the authorized use legal disclaimer are to be configured to all security devices where possible.	Banner Message: THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL. ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.	System > Configuration > Login Banner > Custom Login Banner > THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL. ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.
3.1.3	Clock and NTP	Devices must be configured to synchronize with the authorized H-Cloud NTP servers and set to SGT time zone.	H-Cloud NTP Servers IP Address All devices in HDC1 and HDC2 to configure the below NTP servers. 1. 10.247.2.11 2. 10.247.2.12 3. 10.247.34.11 4. 10.247.34.12	System > Configuration > Time Synchronization > Server Time via NTP: Enabled Set My Clock: via NTP: Use the authenticated NTP server only: Enabled Add NTP Server <ntp address="" ip="" server=""> Authentication Settings Key Type: SHA-1</ntp>

				Key Number: <key number=""> Key Value: <key value=""> Save</key></key>
3.1.4	Syslog	All security devices, must be configured to log errors and activity to the H-Cloud syslog servers.	H-Cloud Syslog Servers IP Address List of servers to configure for HDC1 devices: For Audit Log: 1. 10.247.20.161 OIP For eStreamer: 2. 10.234.241.x [IP and Port will be advised by ASOC during ASOC onboarding] 3. 10.247.20.161 OIP List of servers to configure for HDC2 devices: For eStreamer: 1. 10.234.245.x [IP and Port will	System > Configuration > Audit Log > Send Audit Log to Syslog: Enabled Host: <syslog address="" ip="" server=""> Facility: LOCAL7 Severity: INFO Save Syslog Configuration via eStreamer Login to FMC via GUI System > Integration > Other Integrations > eStreamer In eStreamer Event Configuration: Select Connection Events > Save Create Client > Add <ip address=""></ip></syslog>
			be advised by ASOC during ASOC onboarding] 2. 10.247.32.231 OIP	Save and Deploy

3.2 Health Monitoring

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
3.2.1	SNMP Settings	SNMP is an application layer protocol that helps the exchange of management information between the network devices.	H-Cloud EG Servers IP Address List of servers to configure for HDC1 devices: 1. 10.247.22.53 2. 10.247.22.54 3. 10.247.22.55 4. 10.247.22.56 List of servers to configure for HDC2 devices: 1. 10.247.54.53 2. 10.247.54.54 3. 10.247.54.55 4. 10.247.54.56 Username: <eg username=""> Password: ****** Version: v3 Authentication Type: SHA Privacy Protocol: AES128</eg>	Configure SNMP User System > Configuration > SNMP > SNMP Version: Version3 Add User: Username: <username> Authentication: MD5 Authentication Password:***** Verify Password: ***** Configure Access List System > Configuration > Access List > Add/Delete/Edit Rules IP Address: <snmp ip="" server=""> Port: SNMP Add > Save</snmp></username>
3.2.2	Health Monitor Alerts	Configure an alert response that governs the Firepower Management Center's communication with the SNMP, syslog, or email server where	Please refer to 3.1.3 for Syslog and 3.2.1 for SNMP Settings.	To Configure Monitor Alert Policies > Actions > Alerts > Create Alert SNMP/Syslog To Create SNMP Alert Name: <server>_SNMP Trap Server: <snmp ip="" server=""> Version: V3 User Name: <username></username></snmp></server>

you send the health alert. Authentication Protocol: SHA Password: ****** Privacy Protocol: DES Password: ****** To Create Syslog Alert Name: <server>_SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Health Monitor Alert System > Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" interface="" limit="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" status<="" th="" usage=""><th></th></health></syslog></server>	
Privacy Protocol: DES Password: ****** To Create Syslog Alert Name: <server>_SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert Name: <health <health="" alarms="" alert="" appliance="" backlog="" card="" cluster="" configuration="" cpu="" database="" disk="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" monitor="" name:="" process="" reset="" status="" td="" usage=""><td></td></health></syslog></server>	
Privacy Protocol: DES Password: ****** To Create Syslog Alert Name: Server>_SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" heartbeat="" module:="" modules="" na="" normal="" reco="" reset="" select="" severity:="" status="" status<="" td="" usage=""><td></td></health></syslog>	
Protocol: DES Password: ****** To Create Syslog Alert Name: <server> SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Health Monitor Alert System > Health > Monitor Alert Name: <health <health="" aler<="" alert="" name:="" td=""><td></td></health></syslog></server>	
Protocol: DES Password: ****** To Create Syslog Alert Name: <server> SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Health Monitor Alert System > Health > Monitor Alert Name: <health <health="" aler<="" alert="" name:="" td=""><td></td></health></syslog></server>	
Protocol: DES Password: ****** To Create Syslog Alert Name: <server> SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Health Monitor Alert System > Health > Monitor Alert Name: <health <health="" aler<="" alert="" name:="" td=""><td></td></health></syslog></server>	
Password: ****** To Create Syslog Alert Name: <server> SySLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert Na Severity: Critical/Normal/Error/Reco Module: Select below Modules Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Haslth Monitor Process Host Limit</syslog></server>	
To Create Syslog Alert Name: <server>_SYSLOG Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert Name: <health <health="" alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" name:="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health></syslog></server>	
Name: <server>_SYSLOG Host: <\$yslog Server IP Address> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert to System > Health Alert Name: <health <health="" alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" name:="" normal="" process="" recoto="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health></server>	
Name: <server>_SYSLOG Host: <\$yslog Server IP Address> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert to System > Health Alert Name: <health <health="" alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" name:="" normal="" process="" recoto="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health></server>	
Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert System > Health > Monitor Alert Name: <health <health="" alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" name:="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health></syslog>	
Host: <syslog address="" ip="" server=""> Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert System > Health > Monitor Alert Name: <health <health="" alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" name:="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health></syslog>	
Port: 514 Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alert Name: <health <health="" <module:="" alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" name:="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health>	
Facility: Local7 Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alerts > S Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health>	
Severity: INFO To Create Heath Monitor Alert System > Health > Monitor Alerts > S Health Alert Name: < Health Alert Na Severity: Critical/Normal/Error/Reco Module: Select below Modules Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
To Create Heath Monitor Alert System > Health > Monitor Alerts > S Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health>	
System > Health > Monitor Alerts > S Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health>	
System > Health > Monitor Alerts > S Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health>	
Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td></td></health>	
Health Alert Name: <health alarms="" alert="" appliance="" backlog="" below="" card="" cluster="" configuration="" cpu="" critical="" database="" disk="" error="" failover="" ha="" hardware="" health="" heartbeat="" host="" limit<="" module:="" modules="" monitor="" na="" normal="" process="" reco="" reset="" select="" severity:="" status="" td="" usage=""><td>ave</td></health>	ave
Severity: Critical/Normal/Error/Reco Module: Select below Modules Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Severity: Critical/Normal/Error/Reco Module: Select below Modules Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	me>
Module: Select below Modules Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Appliance Heartbeat Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	vereu
Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Backlog Status CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
CPU Usage Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Card Reset Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Disk Status Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Cluster/Failover Status Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Configuration Database Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Disk Status Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Disk Usage Hardware Alarms HA Status Health Monitor Process Host Limit	
Hardware Alarms HA Status Health Monitor Process Host Limit	
HA Status Health Monitor Process Host Limit	
Health Monitor Process Host Limit	
Host Limit	
meriace status	
Memory Usago	
Memory Usage	
Power Supply	
Process Status	
RRD Server Process	
Security Intelligence	
Smart License Monitor	
Time Series Data Monitor	
Time Synchronization Status	
Time Synchronization Status	
ALL A STREET	
Alert: <server>_SYSLOG/<server>_S</server></server>	NIVIP

3.3 Management Access Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
3.3.1	Restrict Remote Access	Access-list is used to secure the management access to the system by IP and port.	H-Cloud PAM Servers (HTTPS, SSH) 1. 10.247.22.62 2. 10.247.22.20-10.247.22.22 3. 10.247.22.39-10.247.22.43 4. 10.247.22.126-10.247.22.133 5. 10.247.22.24 6. 10.247.22.79 7. 10.247.54.62 8. 10.247.54.20 9. 10.247.54.39-10.247.54.43	System > Configuration > Access-list > Add/Delete/Edit Rules > Save IP Address: <pam address="" ip="" server="" utility=""> Port: <ssh https="" snmp=""></ssh></pam>
			10. 10.247.54.122-10.247.54.129 11. 10.247.54.24 12. 10.247.54.77-10.247.54.79 13. 10.247.22.80-10.247.22.81	

3.3.2 Session Timeout	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	## Cloud Security Utility Servers [HTTPS, SSH] 1. 10.247.22.4 2. 10.247.54.4 Security Compliance Server [HTTPS, SSH] 1. 10.247.17.62 2. 10.247.22.135 Algosec Server [HTTPS, SSH] 1. 10.247.126.25-10.247.126.27 [Optional] EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
Cuttrps_ssH 1. 10.247.22.4 2. 10.247.32.4 2. 10.247.32.4 2. 10.247.32.4 2. 10.247.32.4 2. 10.247.32.4 2. 10.247.32.4 2. 10.247.32.5 2. 10.	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	(HTTPS, SSH) 1.	Browser Settings:
3.3.2 Session Timeout account light to a	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	1. 10.247.22.4 2. 10.247.54.4 Security Compliance Server (HTTPS, SSH) 1. 10.247.17.62 2. 10.247.22.135 Algosec Server (HTTPS, SSH) 1. 10.247.126.25-10.247.126.27 [Optional] EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
Security Compliance Server (INTE), SSH) 1. 10.247.17.02 2. 10.247.22.135	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	Security Compliance Server (HTTPS, SSH) 1.	Browser Settings:
Session To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions. Shell Settings: Shell Timeout (Minutes): 15 Shell Settings: Shell Settin	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	(HTTPS, SSH) 1.	Browser Settings:
3.3.2 Session To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions. Shell Settinas: Browser Session Timeout (Minutes): 15 Shell Settinas: Shell Settinas: Shell Timeout (Minutes): 15 Shell Settinas: Shell Timeout (Minutes):	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	2. 10.247.22.135 Algosec Server [HTTPS, SSH] 1. 10.247.126.25-10.247.126.27 [Optional] EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
Session To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions. Shell Timeout (Minutes): 15 Shell Settings: Shell Settings: Shell Settings: Shell Timeout (Minutes): 15 Shell Settings: Sh	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	[HTTPS, SSH] 1. 10.247.126.25-10.247.126.27 [Optional] EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
Session To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions. Shell Timeout (Minutes): 15 Shell Settings: Shell Settings: Shell Settings: Shell Timeout (Minutes): 15 Shell Settings: Sh	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	[HTTPS, SSH] 1. 10.247.126.25-10.247.126.27 [Optional] EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
Session To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions. Shell Timeout (Minutes): 15 Shell Settings: Shell Timeout (Minutes): 15	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	[Optional] EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
3.3.2 Session Timeout Session	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	1. 10.247.17.106 2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
3.3.2 Session Timeout To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions. 3.3.3 Web GUI By default, GUI uses a default self-signed certificate in Secure the information between GUI and your jumphost, its recommended to replace the certificate with a trusted certificate authority. All certificate authority. All certificate authority. Disperment 2023 may use integrated Health information Systems for "Organization". PKI Certificate Installation via CUI Login to FMC via CUI Bignet PKI Certificate > Cer	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	2. 10.247.49.98 Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings:	Browser Settings:
### Browser Session Timeout (Minutes): ### Browser Session Timeout (Minutes): ### Browser Session Timeout (Minutes): ### Browser Session Timeout (Minutes): 15 ### Browser Session Timeout (Minutes): 15 ### Sell Settings: ### Shell Settings: ### Shell Settings: ### Shell Settings: ### Shell Setting	Ті	Timeout	account login to secure the device from unauthorized users to exploit the	Browser Session Timeout (Minutes): 15 <u>Shell Settings:</u>	Browser Settings:
### Strower Session Timeout (Minutes): ### Strower Session Timeout (Minutes): ### Strower Session Timeout (Minutes): ### Shell Settings: ### Shell Settings: ### Shell Settings: ### Shell Settings: ### Shell Settings: ### Shell Settings: ### Shell Settings: ### Shell Settings: #			account login to secure the device from unauthorized users to exploit the	Browser Session Timeout (Minutes): 15 <u>Shell Settings:</u>	
from unauthorized users to exploit the unattended sessions. Shell Settings: Shell Timeout (Minutes): 15 Shell Settings: Shell Timeout (Minutes): 15 Shell Timeout (Minutes): 15 Shell Settings: Shell Timeout (Minutes): 15 Shell Timeout (Minutes): 16 Shell Timeout (Minutes): 15 Shell Timeout (Minutes): 16 System > Configuration > HTPS Certificate > Incoming the factor of State of Province: Solical State of Province: Solical State of Province: Soli	3.3.3 W	Web GUI	from unauthorized users to exploit the	Shell Settings:	
Shell Timeout (Minutes): 15 Shell Timeout (Minutes): 16 Shel	3.3.3 W	Web GUI	-		
3.3.3 Web GUI By default, GUI uses a default self-signed certificate. To secure the information between GUI and your jumphost, it is recommended to replace the certificate with a trusted certificate authority. Note: Certificates generated before OI September 2023 may use Integrated Health Information Systems for "Organization". Note: Certificates generated before OI September 2023 may use Integrated Health Information Systems for "Organization". Note: Certificate authority. Note: Certificate senerated before OI September 2023 may use Integrated Health Information Systems for "Organization". PKI Certificate Installation via GUI System > Configuration > HITPS Certificate > Import HITPS Server Certificate > Save PKI Certificate Installation via GUI System > Configuration > HITPS Certificate > Import HITPS Server Certificate > Save PKI Certificate Installation via GUI System > Configuration > HITPS Certificate > Import HITPS Server Certificate > Save PKI Certificate Installation via GUI System > Configuration > HITPS Certificate > Import HITPS Server Certificate > Import HITPS Server Certificate > Save PKI Certificate Installation via GUI System > Configuration > HITPS Certificate > Import HITPS Server Server Certificate > Import HITPS Server Server Certificate > Import HITPS Server Ser	3.3.3 W	Web GUI		onen rimeout (iviiliutes). 13	
default self-signed certificate. To secure the information between GUI and your jumphost, it is recommended to replace the certificate with a trusted certificate authority. **Note: Certificate sepenated before 01 September 2023 may use Integrated Health Information Systems for "Organization".** **Note: Certificates generated before 01 September 2023 may use Integrated Health Information Systems for "Organization".** **PKI Certificate Installation via GUI Systems Configuration > HTTPS Certificate > Server Certificate > Server Certificate > Server Certificate > Server Certificate = Server Certificate = Server Certificate in the more opposite the certificate content, way to quit and save the editor press it to insert then copy paste the certificate in the copy paste i	3.3.3 W	Web GUI			, , ,
the information between GUI and your jumphost, it is recommended to replace the certificate with a trusted certificate authority. Note: Certificates generated before 01 September 2023 may use Integrated Health Information Systems for "Organization". PKI Certificate Installation via GUI System > Certificate > Save PKI Certificate Installation via GUI System > Certificate > Save PKI Certificate Installation via GUI System > Certificate > Save PKI Certificate Installation via GUI System > Certificate > Save PKI Certificate Installation via GUI System > Certificate > Server Certificate > Save PKI Certificate Installation via GUI System > Certificate > Server Certificate installation via GUI System > Certificate installation via GUI System > Certificate > Server Certificate installation via GUI System > Certificate installation via GUI HEXPORT Login to FMC via CLI HEXPORT #Expert #Sudo su Hed Jett'ss! #ivi <new certificate="" copy="" editor="" entertificate="" file.="" gui="" i="" in="" insert="" installation="" or="" paste="" press="" system="" the="" then="" to="" via=""> Certificate installation via GUI System > Certificate > Server Certificate > Server Certificate > Server Certificate installation via GUI HEXPORT Login to FMC via CLI HEXPORT #Expert #Sudo su Hed Jett'ss! #ivi <new certificate="" gui="" installation="" system="" via=""> Certificate > Server Certificate > Se</new></new>					
between GUI and your jumphost, it is recommended to replace the certificate with a trusted certificate with a trusted certificate authority. **Note: Certificates generated before 01 September 2023 may use Integrated Health Information Systems for "Organization".** **PKI Certificate Installation via GUI System > Configuration > HTPS Certificate > Import of the certificate > Server Ce					Generate New CSR
recommended to replace the certificate with a trusted certificate authority. Note: Certificates generated before 01 September 2023 may use Integrated Health Information Systems for "Organization". PKI Certificate Installation via GUI System > Configuration > HTTPS Certificate > Import HTTPS Server Certificate > Import HTTPS Server Certificate > Save PKI Certificate Installation via GUI System > Configuration > HTTPS Certificate > Import HTTPS Server Certificate > Import HTTPS Server Certificate > Save PKI Certificate Installation via GUI System > Configuration > HTTPS Certificate > Import HTTPS Server Certi				Organizational Unit: HCLOUD	=
with a trusted certificate authority. Note: Certificates generated before OI September 2023 may use Integrated Health Information Systems for "Organization". PKI Certificate Installation via GUI System > Configuration > HTTPS Certificate > Import HTTPS Server Certificate > Server Certificate > Save PKI Certificate Installation via CUI HExpert #Sudo su #cd /etc/ssl/ #vi <new #mv="" #pmtool="" 1.="" 15="" 3.3.4="" :wq="" <hostname="" _certificate="" a="" accounts="" admin="" and="" apply="" be="" breakfix.="" certificate="" certname.crt="" characters="" check="" common="" contain="" content,="" copy="" dranactional="" editor="" enabled="" file.="" for="" gui="" hcloud="" https="" i="" in="" insert="" local="" locally="" minimum="" must="" name:="" new="" of="" password="" paste="" policy="" press="" quit="" restart="" save="" server.crt="" service="" strength="" the="" then="" to="" unit:="" used="" –="">. HCloud.healthgrp.com.sg HCloud.healthgrp.com.sg HCloud.healthgrp.com.sg PKI Certificate Installation via GUI System > Configuration > Import HTTPS Server Certificate > Import H</new>			recommended to		Locality or City: SG
## Distribution of the property of the new certificate file. In editor press i to insert then copy paste the certificate content, way to quit and save the editor #mv certificate file. In editor press i to insert then copy paste the certificate content, way to quit and save the editor #mv certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate file. In editor press i to insert then copy paste the certificate installation via CLI Login to FMC					
Systems for "Organization". PKI Certificate Installation via GUI System > Configuration > HTTPS Certificate > Import HTTPS Server Certificate > Server Certificate > Save PKI Certificate Installation via CUI Login to FMC via CLI #Expert #Sudo su #cd /etc/ssl/ #vi <new_certname>.crt - to create new certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor #mv certname.crt to server.crt - to apply the new certificate #pmtool restart https - to restart GUI service 3.3.4 Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally Must contain a minimum of 15 characters System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username></new_certname>			certificate authority.		
PKI Certificate Installation via GUI System > Configuration > HTTPS Certificate > Import HTTPS Server Certificate > Server Certificate > Save				, ,	
Import HTTPS Server Certificate > Server Certificate > Server Certificate > Save PKI Certificate Installation via CLI Login to FMC via CLI #Expert #Sudo su #cd /etc/ssl/ #vi <new_certname>.crt – to create new certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor #mv certname.crt to server.crt – to apply the new certificate #pmtool restart https – to restart GUI service </new_certname>				, , , , , , , , , , , , , , , , , , ,	
PKI Certificate Installation via CLI Login to FMC via CLI #Expert #Sudo su #cd /etc/ssl / #vi <new_certname>.crt – to create new certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor #mv certname.crt to server.crt – to apply the new certificate #pmtool restart https – to restart GUI service #pmtool restart https – to restart GUI service System > Users > Create User > Save User Save User Name: <username> Configuration: User Name: <username> Configuration: User Name: <username> Password: ***** Password: *****</username></username></username></new_certname>					Import HTTPS Server Certificate > Server
Local Accounts					
#Sudo su #cd /etc/ssl/ #vi <new_certname>.crt – to create new certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor #mv certname.crt to server.crt – to apply the new certificate #pmtool restart https – to restart GUI service 3.3.4 Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally #Sudo su #cd /etc/ssl/ #vi <new_certname>.crt – to create new certificate #pmtool restart https – to restart GUI service System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username></new_certname></new_certname>					
#cd /etc/ssl/ #vi <new_certname>.crt – to create new certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor #mv certname.crt to server.crt – to apply the new certificate #pmtool restart https – to restart GUI service 3.3.4 Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally #cd /etc/ssl/ #vi <new_certname>.crt – to create new certificate #pmtool restart https – to restart GUI service System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username></new_certname></new_certname>					·
certificate file. In editor press i to insert then copy paste the certificate content, :wq to quit and save the editor #mv certname.crt to server.crt – to apply the new certificate #pmtool restart https – to restart GUI service 3.3.4 Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally Description in the ditor press i to insert then copy paste the certificate editor #mv certname.crt to server.crt – to apply the new certificate #pmtool restart https – to restart GUI service System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username>					#cd /etc/ssl/
3.3.4 Local Accounts Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally Local Accounts Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally Accounts Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally Local Accounts Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally					certificate file. In editor press i to insert then
the new certificate #pmtool restart https – to restart GUI service 3.3.4 Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally Local admin accounts used for breakfix. Password strength check must be enabled for locally the new certificate #pmtool restart https – to restart GUI service System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username>					quit and save the editor
#pmtool restart https – to restart GUI service 3.3.4 Local Accounts Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally #pmtool restart https – to restart GUI service System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username>					
3.3.4 Local Accounts Accounts Basword Strength Check must be enabled for locally Local admin accounts Basword Policy Characters System > Users > Create User > Save User Configuration: User Name: <username> Password: *****</username>					#pmtool restart https – to restart GUI
Password strength check must be enabled for locally 1. Must contain a minimum of 15 characters 1. Must contain a minimum of 15 User Configuration: User Name: <username> Password: *****</username>	3.3.4 Lo	Local	Local admin accounts	Password Policy	
check must be characters User Name: <username> enabled for locally Password: *****</username>	A	Accounts		Must contain a minimum of 15	<u>User Configuration:</u>
·			check must be	characters	User Name: <username></username>
			authenticated users.	2. Must include characters from at	Confirm Password: ****
categories: Minimum Password Length: 16				_	Minimum Password Length: 16
Days Until Password Expiration: 365				A. Upper case (A through Z);	Days Until Password Expiration: 365 Days Before LDA Expiration Warning: 5

			B. Lower case (a through z);	
			C. Digits (0-9); D. Special Characters (!, \$, #, %, etc.).	ole: Administrator
			Password expiration must be 365days	
			4. Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.	
			5. Not be reused for at least 5 generations	
			6. Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.	
			7. Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.	
			Must not be identical to the username or the reverse of the username.	
			9. Account lockout after 5 consecutive failed authentication attempts	
3.3.5	External Authenticatio n	To secure that only H- Cloud Security Engineers are able to	List of servers to configure for HDC1 OI	/stem > Users > External Authentication > dd/Delete/Edit External Authentication bject >Save and Apply
		access and make changes to the device configuration through LDAP or RADIUS authentication.	2. 10.245.152.19 Au [HISADDCVPUTL02.hcloud.healt hgrp.com.sg] De 3. 10.244.152.19 Se	external Authentication Object: authentication Method: <ldap radius=""> ame: <authentication name=""> escription: <optional> erver Type: <ms active="" directory="" irectory="" openldap="" oracle="" other=""></ms></optional></authentication></ldap>
			List of servers to configure for HDC2 devices: PC 1. 10.245.152.19	rimary Server: ost Name/IP Address: <ip hostname=""> ort: ackup Server (Optional)</ip>
			hgrp.com.sg] Ho 2. 10.244.152.19 Po [HISADDCVPUTL04.hcloud.healt hgrp.com.sg]	ost Name/IP Address: <ip hostname=""> ort:</ip>
			[HISADDCVPUTL03.hcloud.healt hgrp.com.sg] [Optional] hc	DAP-Specific Parameters: ase DN= cloud,DC=healthgrp,DC=com,DC=sg ase Filter =
			hcloud,DC=healthgrp,DC=com,DC=sg	(memberOf=CN=IHIS_PAMSECREAD,OU=H oud roups,DC=hcloud,DC=healthgrp,DC=com,D
			(m ou Gr	roups,DC=hcloud,DC=healthgrp,DC=com,D
				esg)) ser Name: <service account=""></service>

		Password: ***** Confirm Password: *****
		-

4 FIREPOWER THREAT DEFENSE (FTD)

4.1 General Security Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
4.1.1	Hostname	Device Hostname should be unique and consistent across H-Cloud <system name=""> host names should conform to the H- Cloud Naming Convention.</system>	<pre>< DataCenterLocation > - < NetworkZone > - <institution cluster="">-< DevicePurpose >< Running Numbers ></institution></pre>	Login via CLI >configure network hostname <hostname></hostname>
4.1.2	Warning Banner	Standard login banner containing the authorized use legal disclaimer are to be configured to all security devices where possible.	Banner Message: THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL. ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.	Platform Settings > Platform_HIS_ <zone> > Banner > Save > Deploy THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEMS ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL. ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT</zone>
4.1.3	Clock and NTP	Devices must be configured to synchronize with the authorized H-Cloud NTP servers and set to SGT time zone.	H-Cloud NTP Servers IP Address All devices in HDC1 and HDC2 to configure the below NTP servers. 1. 10.247.2.11 2. 10.247.2.12 3. 10.247.34.11 4. 10.247.34.12	Platform Settings > Time Synchronization > Set My Clock > via NTP from Management Server > Save
4.1.4	Syslog	All security devices, must be configured to log errors and activity to the H- Cloud syslog servers.	H-Cloud Syslog Servers IP Address List of servers to configure for HDC1 devices: 1. 10.247.126.25 UDP/514 Algosec [Optional] 2. 10.247.20.161 TCP/9003 OIP 3. 10.247.0.9 UDP/514 CSA [Optional] List of servers to configure for HDC2 devices: 1. 10.247.126.25 UDP/514 Algosec [Optional]	Platform Settings > Platform_HIS_ <zone> > Syslog > Deploy Logging Setup Enable Logging: Yes Enable Logging on the failover standby unit: Yes Memory Size of the Internal Buffer: 4096 Enable Logging to FMC: Yes Logging Level: Informational Logging Destinations Click Add/Delete/Edit Logging Destination: Syslog Servers</zone>

Event Lists Click Add/Delete/Edit Name: <event list="" name=""> Severity/Event Class: Click Add/Delete/Edit and select from the list of events (Optional) Message ID: Click Add/Delete/Edit and select from the list of Message ID Sysloa Settinas: Facility: Local20 Enable Timestamp on Syslog Messages Timestamp Format: Legacy (MM dd yy HH:mm:ss) Enable Syslog Device ID: Enable > Hostname Syslog Servers: Allow user traffic to pass when TCP syslog server is down > Enable Message Queue Size(messages): 512 ADD Syslog Server: IP Address: <syslog address="" ip="" server=""> Protocol: <tcp udp=""> Port: <port #=""> Save</port></tcp></syslog></event>		2. 10.247.32.231 TCP/9003 OIP 3. 10.247.32.9 UDP/514 CSA [Optional]	Click Add/Delete/Edit Name: <event list="" name=""> Severity/Event Class: Click Add/Delete/Edit and select from the list of events (Optional) Message ID: Click Add/Delete/Edit and select from the list of Message ID Syslog Settings: Facility: Local20 Enable Timestamp on Syslog Messages Timestamp Format: Legacy (MM dd yy HH:mm:ss) Enable Syslog Device ID: Enable > Hostname Syslog Servers: Allow user traffic to pass when TCP syslog server is down > Enable Message Queue Size(messages): 512 ADD Syslog Server: IP Address: <syslog address="" ip="" server=""> Protocol: <tcp udp=""></tcp></syslog></event>
--	--	---	---

4.2 Health Monitoring

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
4.2.1	SNMP Settings	SNMP is an application layer protocol that helps the exchange of	H-Cloud EG, OIP and CSPC Servers IP Address List of servers to configure for HDC1	Platform Settings > Platform_HIS_ <zone> SNMP > Deploy Enable SNMP Serves > Tick</zone>
		management information between the network devices.	devices: 1. 10.247.22.53 2. 10.247.22.54 3. 10.247.22.55 4. 10.247.22.56 5. 10.247.209.10 6. 10.247.20.170 List of servers to configure for HDC2 devices:	Add Users: Security Level: <noauth auth="" priv=""> Username: <username> Encryption Password Type: <cleartext encrypted=""> Auth Algorithm Type: <md5 sha=""> Authentication Password: ***** Confirm: *****</md5></cleartext></username></noauth>
			1. 10.247.54.53 2. 10.247.54.54 3. 10.247.54.55 4. 10.247.54.56 5. 10.247.218.10 6. 10.247.32.232 Username: <eg username=""></eg>	Add SNMP Management Hosts: IP Address: <snmp ip="" server=""> SNMP Version: 3 Username: <username> Enable: Poll and Trap Port: 162</username></snmp>

			Password: ***** Version: v3 Authentication Type: SHA	<u>Delete SNMP Management Hosts:</u> Select IP Address > Delete
			Privacy Protocol: AES128	
4.2.2	Health Monitor Alerts	Configure an alert response that	Please refer to 3.1.3 for Syslog and 3.2.1 for SNMP Settings.	System > Health > Policy > Save
		governs the		Policy Run Time Interval: 5mins
		Firepower		AMP for Endpoints Status: ON
		Management		AMP for Firepower Status: ON
		Center's		Appliance Heartbeat: ON
		communication		Automatic Application Bypass Status: ON
		with the		Backlog Status: ON
		SNMP, syslog, or		Card Reset: OFF
		email server where		Cluster/Failover Status: ON
		you send the health		CPU Usage
		alert.		Disk Status: ON
				Disk Usage: ON
				Critical Threshold %: 90
				Warning Threshold %: 85
				2HD Critical Threshold %: 99
				2HD Warning Threshold %: 97
				Hardware Alarms: ON
				HA Status: ON
				Health Monitor Process
				Host Limit: ON
				Inline Link Mismatch Alarms: ON
				Interface Status: ON
				Intrusion and File Event Rate: ON
				ISE Connection Status Monitor
				Link State Propagation: ON
				Local Malware Analysis: ON
				Memory Usage:
				Critical Threshold %: 90
				Warning Threshold %: 80
				Platform Faults
				Power Supply: ON
				Process Status: ON
				Realm
				Reconfiguring Detection: ON
				RRD Server Process: ON
				Security Intelligence: ON
				Smart License Monitor: ON
				Threat Data Updates on Devices: ON
				Time Series Data Monitor: ON
				Time Synchronization Status: ON
				URL Filtering Monitor: ON
				User Agent Status Monitor
				VPN Status
<u> </u>				

4.3 Management Access Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
4.3.1	Restrict	Access-list is used to	H-Cloud PAM Servers (HTTPS, SSH)	Devices > Platform Settings > Policy Name>
	Remote	secure the	1. 10.247.22.62	Secure Shell > Add/Delete/Edit > Save
	Access	management access	2. 10.247.22.20-10.247.22.22	
		to the system by IP	3. 10.247.22.39-10.247.22.43	IP Address: <pam address="" ip="" server="" utility=""></pam>
		and port.	4. 10.247.22.126-10.247.22.132	Interface: <diagnostic management=""></diagnostic>
			5. 10.247.22.24	
			6. 10.247.22.77-10.247.22.79	

		7. 10.247.54.62 8. 10.247.54.20-10.247.54.22 9. 10.247.54.39-10.247.54.43 10. 10.247.54.122-10.247.54.129	***Alternate Method: Login to FTD via CLI and Execute below command via clish >configure ssh-access-list <ip< th=""></ip<>
		11. 10.247.54.24 12. 10.247.54.77-10.247.54.79 13. 10.247.22.80-10.247.22.81	Address/Subnet mask> To verify the configuration
		H-Cloud Security Utility Servers (HTTPS, SSH) 1. 10.247.22.4 2. 10.247.54.4	>show ssh-access-list
		Security Compliance Server (HTTPS, SSH) 1. 10.247.17.62 2. 10.247.22.135	
		Algosec Server (HTTPS, SSH) 1. 10.247.126.25-10.247.126.27 [Optional]	
		EVMS Scanner IP (HTTPS, SSH) 1. 10.247.17.106 2. 10.247.49.98	
Session Timeout	To limit the length of account login to secure the device from unauthorized users to exploit the unattended sessions.	Browser Settings: Browser Session Timeout (Minutes): 15 Shell Settings: Shell Timeout (Minutes): 15	Devices > Platform Settings > Policy Name> Timeout > 15(mins) > Save
Local	Local admin accounts used for breakfix. Password strength check must be enabled for locally authenticated users.	Password Policy 1. Must contain a minimum of 15 characters 2. Must include characters from at least 2 of the following 4 categories: E. Upper case (A through Z); F. Lower case (a through z); G. Digits (0-9); H. Special Characters (!, \$, #, %, etc.). 3. Password expiration must be 365days 4. Must pass a password dictionary check. For example, the password must not be	Login to FTD via CLI configure user add <username> <basic config=""></basic></username>
	Timeout	Timeout account login to secure the device from unauthorized users to exploit the unattended sessions. Local Accounts Local admin accounts used for breakfix. Password strength check must be enabled for locally	Session

			in any order, such as passwordABC or password321. 8. Must not be identical to the username or the reverse of the username. 9. Account lockout after 5 consecutive failed authentication attempts	
4.3.4	External Authenticatio n	To secure that only H-Cloud Security Engineers are able to access and make changes to the device configuration through LDAP or RADIUS authentication.	H-Cloud LDAP Servers IP Address List of servers to configure for HDC1 devices: 1. 10.244.152.18 [HISADDCVPUTL03.hcloud.healt hgrp.com.sg] 2. 10.245.152.19 [HISADDCVPUTL02.hcloud.healt hgrp.com.sg] 3. 10.244.152.19 [HISADDCVPUTL04.hcloud.healt hgrp.com.sg] [Optional] List of servers to configure for HDC2 devices: 1. 10.245.152.19 [HISADDCVPUTL02.hcloud.healt hgrp.com.sg] 2. 10.244.152.19 [HISADDCVPUTL04.hcloud.healt hgrp.com.sg] 3. 10.244.152.19 [HISADDCVPUTL04.hcloud.healt hgrp.com.sg] 3. 10.244.152.18 [HISADDCVPUTL03.hcloud.healt hgrp.com.sg] [Optional] Base DN: hcloud,DC=healthgrp,DC=com,DC=sg Port: 636/TCP	Devices > Platform Settings > Policy Name > External Authentication Select the External Authentication Profile: Enable For Authentication Profile, refer to FMC External Authentication Settings.

5 FIREPOWER CHASSIS MANAGER (FCM)

5.1 General Security Control List

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
5.1.1	Hostname	should be unique Ne and consistent <ir< td=""><td>< DataCenterLocation > - < NetworkZone > - <institution cluster="">-< DevicePurpose >< Running Numbers ></institution></td><td>Login via CLI Firepower-chassis-A# scope system Firepower-chassis-A /system # set name <hostname> Firepower-chassis-A /system* # commit-buffer</hostname></td></ir<>	< DataCenterLocation > - < NetworkZone > - <institution cluster="">-< DevicePurpose >< Running Numbers ></institution>	Login via CLI Firepower-chassis-A# scope system Firepower-chassis-A /system # set name <hostname> Firepower-chassis-A /system* # commit-buffer</hostname>
5.1.2	Warning Banner	Standard login banner containing the authorized use legal disclaimer are to be configured to	Banner Message: THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL	Firepower-chassis# scope security Firepower-chassis / security # scope banner Firepower-chassis / security / banner # create pre-login-banner

		all security devices where possible.	PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS COMPUTER SYSTEM ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES MONITORED AND RECORDED BY SYSTEM PERSONNEL. ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT.	Firepower-chassis /security/banner/pre- login-banner* # set message Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort. Enter prelogin banner: >THIS SYSTEM IS SOLELY FOR THE USE OF AUTHORIZED USERS FOR OFFICIAL >PURPOSES. YOU HAVE NO EXPECTATION OF PRIVACY IN ITS USE AND TO ENSURE >THAT THE SYSTEM IS FUNCTIONING PROPERLY, INDIVIDUALS USING THIS >COMPUTER SYSTEM ARE SUBJECT TO HAVING ALL OF THEIR ACTIVITIES >MONITORED AND RECORDED BY SYSTEM PERSONNEL. > >ANY UNAUTHORIZED ACCESS IS LIABLE TO PROSECUTION UNDER THE COMPUTER MISUSE ACT. >ENDOFBUF Firepower-chassis /security/banner/pre- login-banner* # commit-buffer Firepower-chassis /security/banner/pre- login-banner #
5.1.3	Clock and NTP	Devices must be configured to synchronize with the authorized H-Cloud NTP servers and set to SGT time zone.	H-Cloud NTP Servers IP Address All devices in HDC1 and HDC2 to configure the below NTP servers. 1. 10.247.2.11 2. 10.247.2.12 3. 10.247.34.11 4. 10.247.34.12	Platform Settings > NTP > Time Synchronization > Use NTP Server > Add >Save <ntp address="" ip="" server=""></ntp>
5.1.4	Syslog	All security devices, must be configured to log errors and activity to the H- Cloud syslog servers.	H-Cloud Syslog Servers IP Address List of servers to configure for HDC1 devices: 1. 10.247.20.161 OIP List of servers to configure for HDC2 devices: 1. 10.247.32.231 OIP	Platform Settings > Syslog > Remote Destinations > Save Server1 Admin State: Enable Level: Information Hostname/IP Address: <syslog address="" ip="" server=""> Facility: Local7</syslog>

5.2 Health Monitoring

SN	Controls	Purpose	Required Settings -All settings are mandatory unless listed as Optional.	Configuration Reference -The instructions are purely for reference purpose and may differ across different product versions.
5.2.1	SNMP Settings	SNMP is an application layer	H-Cloud EG Servers IP Address	Devices > Platform Settings > SNMP > Save
		protocol that helps the exchange of	List of servers to configure for HDC1 devices:	Admin State: Enable
		management	1. 10.247.22.53	Add User
		information	2. 10.247.22.54	Username: <username></username>
		between the	3. 10.247.22.55	Auth Type: SHA
		network devices.	4. 10.247.22.56	Encryption Password Type: Use AES-128:
			5. 10.247.20.170	Enable
				Password: ****
			List of servers to configure for HDC2	Confirm Password: *****
			devices:	Privacy Password: ****
			1. 10.247.54.53	Confirm Privacy Password: ****
			2. 10.247.54.54	
			3. 10.247.54.55	Add SNMP Traps:
			4. 10.247.54.56	Hostname/IP Address: 2.2.2.2

	5. 10.247.32.232	Community/Username: <username></username>	
		Port: 162	
	Username: <eg username=""></eg>	Version: V3	
	Password: *****	Type: <traps informs=""></traps>	
		V3 Privilege: <auth noauth="" priv=""></auth>	
	Version: v3		
	Authentication Type: SHA	Save	
	Privacy Protocol: AES128		

5.3 Management Access Control List

SN	Controls	Purpose	Required Settings	Configuration Reference
"			-All settings are mandatory unless	-The instructions are purely for reference
			listed as Optional.	purpose and may differ across different
				product versions.
5.3.1	Restrict	Access-list is used to	H-Cloud PAM Servers (HTTPS, SSH)	Devices > Platform Settings > Access-list >
	Remote	secure the	1. 10.247.22.62	Add > Save
	Access	management access	2. 10.247.22.20-10.247.22.22	
		to the system by IP	3. 10.247.22.39-10.247.22.43	IP Address: <pam address="" ip="" server="" utility=""></pam>
		and port.	4. 10.247.22.126-10.247.22.132	Prefix Length: /32
			5. 10.247.22.24 6. 10.247.22.77-10.247.22.79	Protocol: <https snmp="" ssh=""></https>
			7. 10.247.54.62	
			8. 10.247.54.20-10.247.54.22	
			9. 10.247.54.39-10.247.54.43	
			10. 10.247.54.122-10.247.54.129	
			11. 10.247.54.24	
			12. 10.247.54.77-10.247.54.79	
			13. 10.247.22.80-10.247.22.81	
			14. 10.247.54.81-10.247.54.82	
			H-Cloud Security Utility Servers	
			(HTTPS, SSH)	
			1. 10.247.22.4	
			2. 10.247.54.4	
			Security Compliance Server	
			(HTTPS, SSH)	
			1. 10.247.17.62	
			2. 10.247.22.135	
			EVMS Scanner IP (HTTPS, SSH)	
			1. 10.247.17.106	
			2. 10.247.49.98	
5.3.2	Session	To limit the length of	Browser Settings:	Firepower-chassis # scope security
	Timeout	account login to	Browser Session Timeout (Minutes):	Firepower-chassis /security # scope default-
		secure the device	15	auth
		from unauthorized	Shall Sallian	Firepower-chassis /security/default-auth #
		users to exploit the unattended sessions.	Shell Settings: Shell Timeout (Minutes): 15	set session-timeout seconds 900 Firepower-chassis /security/default-auth #
		unattended sessions.	Shell Timeout (Willutes). 13	commit-buffer
5.3.3	Web GUI	By default, the device	Country Name: SG	Firepower-chassis # scope security
5.5.5	**ED GOI	uses a default self-	State of Province: SG	Firepower-chassis /security # create
		signed certificate. To	Locality or City: SG	trustpoint firepower chain
		secure the	Organization: SYNAPXE	Firepower-chassis /security # set certchain
		information between	Organizational Unit: H-CLOUD	,
		GUI and your jump	Common Name: <hostname>. H-</hostname>	Copy and paste the CA Cert Binary one line
		host, it is	Cloud.healthgrp.com.sg	at a time
		recommended to		
		replace the certificate		enter "ENDOFBUF" at the end of the line
		with a trusted	Note: Certificates generated before	Financia de cario de caracte de c
		certificate authority.	01 September 2023 may use	Firepower-chassis /security # commit-buffer

			Integrated Health Information	Firepower-chassis /security # scope keyring
			Systems for "Organization".	firepower_cert Firepower-chassis /security # set trustpoint firepower_chain #set cert
				Copy and paste the Signed Cert Binary one line at a time
				enter "ENDOFBUF" at the end of the line
				#commit-buffer #scope system #scope services
				#set https keyring firepower_cert #commit buffer
5.3.4	Local Accounts	Local admin accounts used for breakfix.	Password Policy	System > Users > Add/Delete/Edit User > Save
	Accounts	Password strength	Must contain a minimum of 15	
		check must be enabled for locally	characters	User Name:
		authenticated users.	Must include characters from at least 2 of the following 4	First Name: Last Name:
			categories:	Email: example@example.com (Optional) Phone Number: +XXXXXXXXXX (Optional)
			I. Upper case (A through Z); J. Lower case (a through z);	Password: ***** Confirm Password: *****
			K. Digits (0-9); L. Special Characters (!, \$, #,	Account Status: <active inactive=""> User Role: Read-Only</active>
			%, etc.).	Admin Operations
			Password expiration must be 365days	AAA Account Expires: (Optional)
			4. Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.	Expiry Date: (mm/dd/yyyy) 12months
			5. Not be reused for at least 5 generations	
			Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.	
			7. Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.	
			8. Must not be identical to the username or the reverse of the username.	
			Account lockout after 5 consecutive failed authentication attempts	
5.3.5	External Authenticatio	To secure that only H- Cloud Security	H-Cloud LDAP Servers IP Address	Platform Settings > AAA > LDAP/RADIUS/TACACS > Add/Delete/Edit >
	n	Engineers are able to access and make	List of servers to configure for HDC1 and HDC2 devices:	Save
		changes to the device configuration through	1. 10.247.0.11 2. 10.247.32.11	Add RADIUS Servers IP addreses: <pri ip="" nps=""></pri>
		LDAP or RADIUS authentication.	Port: 1812	Order: 1 Key: xxxx
				Confirm Key: xxxx

		Authorization: 1812 Timeout: 5
		Retires: 1 IP addreses: <sec ip="" nps=""></sec>
		Order: 1 Key: xxxx
		Confirm Key: xxxx Authorization: 1812
		Timeout: 5 Retires: 1
		Save
		Set Authentication to Radius as Primary System > User Management > Settings Default Authentication : RADIUS
		Save

6 References/Records

The following is the list of references used for this document:

FirePower Management Centre

Firepower Management Centre Configuration Guide Version 7.2

Last Modified: 01 September 2022

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72.html

FirePower Chassis Manager

Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide Version 2.12

Last Modified: 09 December 2022

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/2120/webguide/b_GUI_FXOS_ConfigGuide_2120.html

ICT Security Policy

HIM-ICT Security Policy Version 1.5

Last Modified: 29 Nov 2023

https://healthtech-im.intranet.ihis/Pages/HIM-ISP/Purpose.aspx

7 Revision History

Document Title: Security Hardening Benchmark for Cisco FirePower Devices

Document ID: STND-78-2143- Security Hardening Benchmark for Cisco FirePower

Devices

Document Owner: Cloud, Platform Services

Document Approver: Head of Department (HOD), Cloud Enablement Services (CES)

Information Classification: Restricted, Sensitive (Normal)

Special Instructions: NA

Version	Revision Date	Summary of Changes	Documented By	Reviewed By
1.0	23-Jul-2021	Initial Document	Marie Ann CadizSam Lee	Ho Bee Huat
1.1	16-Aug-2021	Update: -Restrict Remote Access: added HDC1 and HDC2 Jump Host IPsLocal Accounts 1.Password expiration must be 365days 2.Not be reused for at least 5 generations	-Marie Ann Cadiz -Sam Lee	Ho Bee Huat
1.2	15-Sep-2021	Update: -Restrict Remote Access: added HDC1 and HDC2 Jump Host IPs Syslog: removed old MSS IP and updated to use TCP/514 for ELK and Splunk.	-Marie Ann Cadiz -Sam Lee	Ho Bee Huat
1.3	10-Oct-2021	Update: -Restrict Remote Access - Syslog	-Marie Ann Cadiz -Sam Lee	Ho Bee Huat
1.4	24-Jan-2022	Update: -Document Approver -4.2 Health Policy updated Configuration/Variable with the alert modules5.1 Restrict Remote Access, added EG Server IPs and management ports -5.2 Session Timeout, updated Browser and Shell Timeout to 15mins5.5 External Authentication, Added Radius Servers.	-Marie Ann Cadiz -Sam Lee	Kenneth Chew
1.5	20-May-2022	Update: -Individual Hardening Guide for FMC, FTD and FCM4.1.3 Added Event Lists	-Marie Ann Cadiz -Sam Lee	Kenneth Chew
1.6	1-Aug-2022	Update: -3.3.1 Restrict Remote Access, Updated PAM Servers and added Algosec Servers -3.3.5 External Authentication, updated 3 rd LDAPS Server as Optional.	-Marie Ann Cadiz -Sam Lee	-Kenneth Chew -Stephen Tan

Version	Revision Date	Summary of Changes	Documented By	Reviewed By
		-4.3.1 Restrict Remote Access, added Algosec Servers -4.3.4 External Authentication, updated 3 rd LDAPS Server as Optional.		
1.7	13-Jan-2023	-Annual Review Completed Update: -3.3.1 Restrict Remote Access, added EVMS Scanner IP -3.1.3 Syslog, Syslog Configuration via eStreamer -4.3.1 Restrict Remote Access, Added EVMS Scanner IP and alternative Method via CLI -5.3.1 Restrict Remote Access, Added EVMS Scanner IP	-Mohamed Refain -Marie Ann Cadiz	-Connie Tham -Stephen Tan -Terence Lee
1.8	01-Aug-2023	-Annual Review Completed Update: -Synapxe Template -Document Approver	-Kaiden Tan -Marie Ann Cadiz	-Connie Tham -Stephen Tan -Terence Lee
1.9	16-May-2024	Updated: -3.1.3 FMC Clock and NTP - Updated Configuration Reference to include Authentication Settings3.1.4 FMC Syslog - Added ASOC/OIP and removed ELK syslog servers3.3.3 FMC Web Gui - Updated Organization4.1.3 FTD Clock and NTP - Updated Configuration Steps4.1.4 FTD Syslog - Added OIP/CSA and removed ELK/Splunk syslog servers4.2.1 FTD SNMP Settings - Added OIP/CSPC Servers5.1.4 FCM Syslog - Added OIP and removed ELK/Splunk syslog servers5.2.1 FCM SNMP Settings - Added OIP Servers5.3.3 FCM Web Gui - Updated Organization5.3.5 FCM External Authentication - Updated LDAP Servers6 References – Updated HIM-ICT Security Policy Version 1.5.	-Mohamed Refain -Chiu Yih Tah	-Connie Tham -Stephen Tan