

Securing Networks with
Cisco FTD

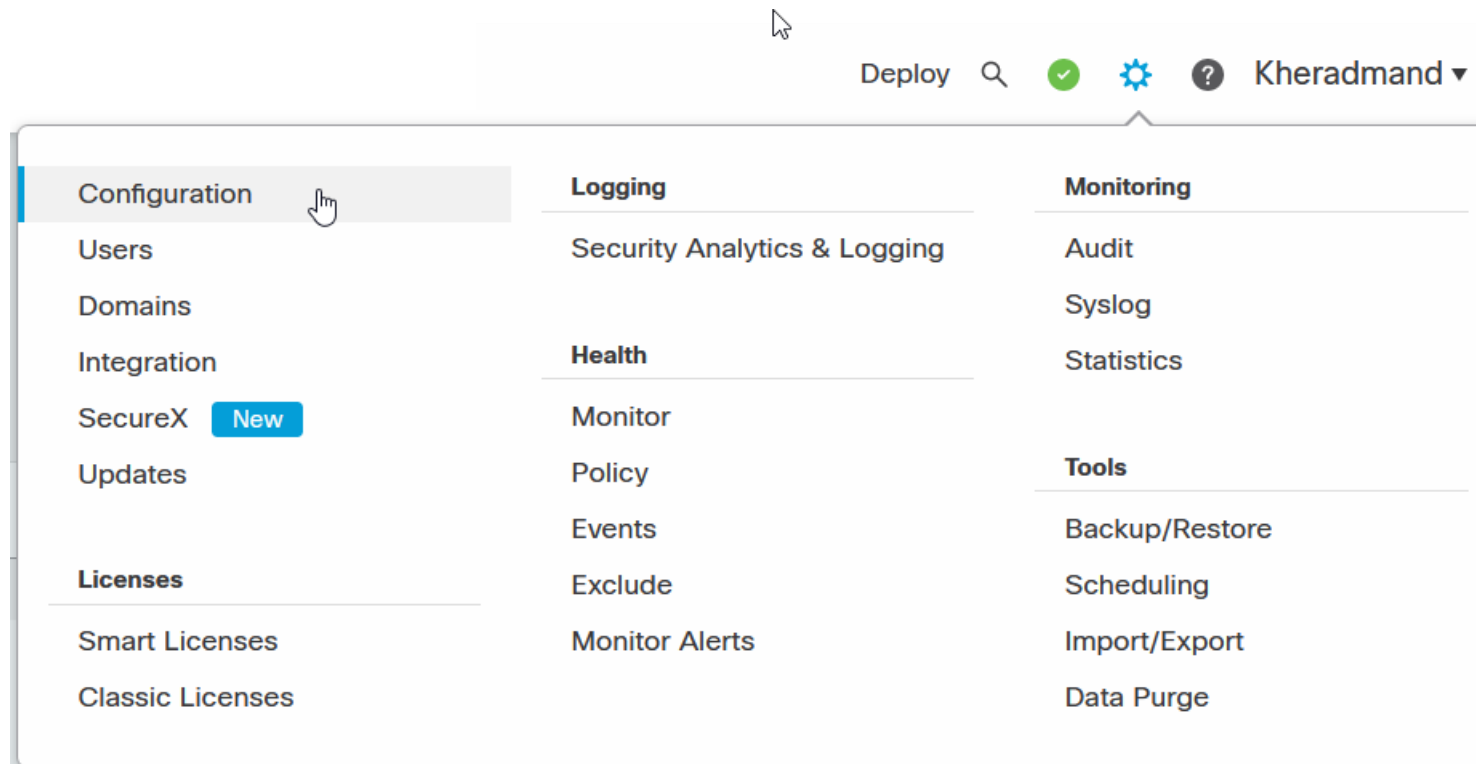
Chapter 2

FMC/FTD basic system setting

Mohsen Kheradmand

Firepower System Configuration

- On the top menu click System 
- Then click Configuration



Information

Here ,You can change the FMC name.

Access List
Access Control Preferences
Audit Log
Audit Log Certificate
Change Reconciliation
DNS Cache
Dashboard
Database
Email Notification
External Database Access
HTTPS Certificate
Information
Intrusion Policy Preferences
Language
Login Banner
Management Interfaces
Network Analysis Policy Preferences
Process
REST API Preferences
Remote Storage Device
SNMP
Session Timeout

Name	FMC
Product Model	Cisco Firepower Management Center for VMware
Serial Number	None
Software Version	7.0.1
Operating System	Cisco Firepower Extensible Operating System (FX-OS)
Operating System Version	2.10.1
IPv4 Address	192.168.1.250
IPv6 Address	Disabled
Current Policies	Health Policy Initial_Health_Policy 2024-10-10 09:47:32
Model Number	66
RefreshSave	

Access List

Acceptable addresses to connect to FMC via :
SSH , HTTPS or SNMP

Click Add Rules (to add IP address)

- Enter new IP/Subnet
- Click any port you want to allow this via this address
- Then delete *ANY* rules

- ✓ Note: type NMS station IP address (if you want to send traps from the FMC to the NMS station)
- However, you must set the SNMP configuration further down before you can configure the NMS station IP address

Access List

Access Control Preferences

Audit Log

Audit Log Certificate

Change Reconciliation

DNS Cache

Dashboard

Database

Email Notification

External Database Access

+ Add Rules

Host	Port	
192.168.1.142	22	
192.168.1.142	443	
192.168.1.52	22	
192.168.2.0/29	22	
192.168.2.0/29	443	

IP Address 192.168.2.0/29

Port ☒ SSH ☒ HTTPS ☐ SNMP

Cancel Add

Management interface

- ✓ You can edit MGMT interface setting
- ✓ Edit IPv4/v6 gateway
- ✓ Hostname , Domain , DNS & remote port
- ✓ Enable / disable ICMPv6 echo options
- ✓ Enable or disable Proxy and address/port/auth

- Access List
- Access Control Preferences
- Audit Log
- Audit Log Certificate
- Change Reconciliation
- DNS Cache
- Dashboard
- Database
- Email Notification
- External Database Access
- HTTPS Certificate
- Information
- Intrusion Policy Preferences
- Language
- Login Banner
- Management Interfaces**
- Network Analysis Policy Preferences
- Process
- REST API Preferences
- Remote Storage Device
- SNMP
- Session Timeout
- Time
- Time Synchronization
- UCAPL/CC Compliance
- User Configuration
- VMware Tools

▼ Interfaces

Link	Name	Channels	MAC Address	IP Address	
✓	eth0	Management Traffic Event Traffic	00:0C:29:B7:D0:32	192.168.1.250	

▼ Routes

IPv4 Routes +

Destination	Netmask	Interface	Gateway	
*			192.168.1.1	

IPv6 Routes +

Destination	Prefix Length	Interface	Gateway	
-------------	---------------	-----------	---------	--

▼ Shared Settings

Hostname

FMC

Domains

Dena.local

Primary DNS Server

192.168.10.10

Secondary DNS Server

192.168.10.20

Tertiary DNS Server

Remote Management Port

8305

▼ ICMPv6

Allow Sending Echo Reply Packets

☒

Allow Sending Destination
Unreachable Packets

☒

▼ Proxy

Enabled

☐

Cancel

Save

Management interface

Management interface Edit

The *eth0* is the default and must be used for MGMT

However, eth1-3 can be used on hardware FMC

For large number of FTDs , Adding more management interfaces can improve throughput and performance.

▼ Interfaces					
Link	Name	Channels	MAC Address	IP Address	
✓	eth0	Management Traffic Event Traffic	00:0C:29:B7:D0:32	192.168.1.250	

Edit Interface

Enabled:

☒

Channels:

☒ Management Traffic

☒ Event Traffic

Mode:

Autonegotiation

MDI/MDIX:

Auto-MDIX

MTU:

1500

IPv4 Configuration:

Static

IPv4 Management IP:

192.168.1.250

IPv4 Netmask:

255.255.255.0

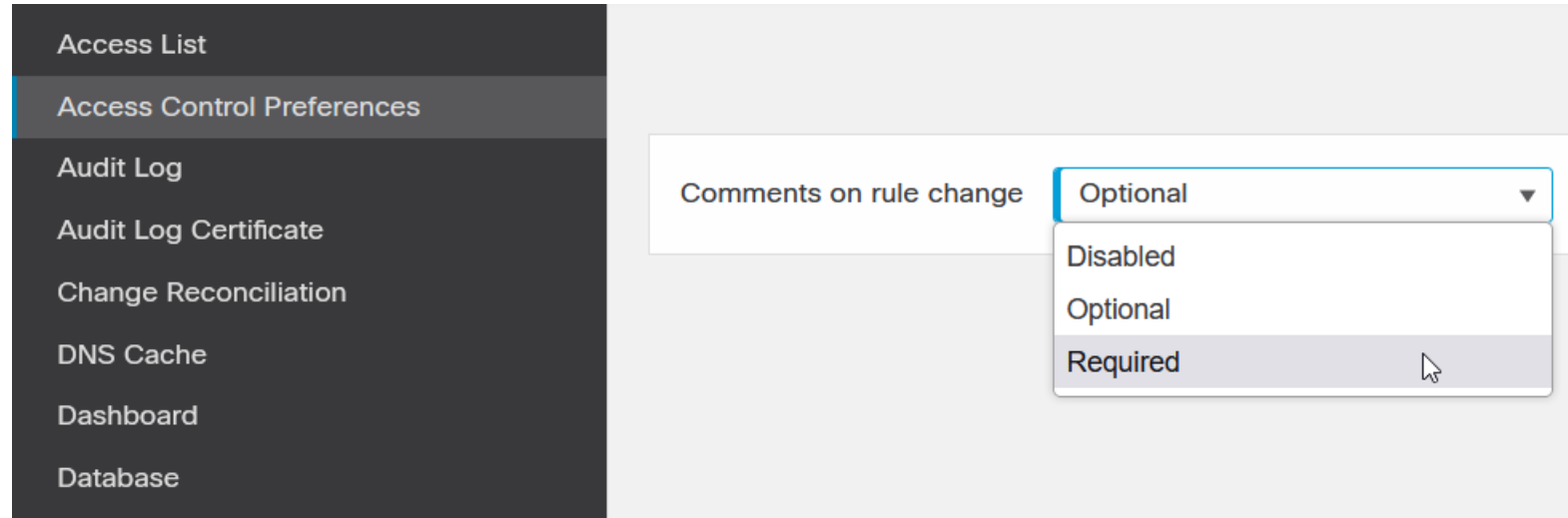
IPv6 Configuration:

Disabled

Cancel

OK

Access Control Preferences



Disabled : When you edit an access control rule, nothing happens upon saving the rule

Optional : When you save an access control rule, the comment dialog appears, and you can add a comment or Cancel

Required: When you save an access control rule, the comment dialog appears, and you must enter a comment

Audit Log

Configure Syslog server to send logs

Host : IP or FQDN of syslog server

Facility : the type of message

Severity : level of the message

The screenshot displays the FMC configuration interface for the Audit Log. The left sidebar contains a list of configuration options: Access List, Access Control Preferences, Audit Log (selected), Audit Log Certificate, Change Reconciliation, DNS Cache, Dashboard, Database, Email Notification, External Database Access, HTTPS Certificate, Information, and Intrusion Policy Preferences. The main configuration area is divided into two sections. The first section, 'Send Audit Log to Syslog', includes a dropdown menu set to 'Enabled', a text input for 'Hosts (Up to 5)' containing '191.168.1.25', a dropdown for 'Facility' set to 'SYSLOG', a dropdown for 'Severity' set to 'NOTICE', and an empty text input for 'Tag (optional)'. The second section, 'Send Audit Log to HTTP Server', includes a dropdown menu set to 'Enabled' and a text input for 'URL to Post Audit' containing 'http://192.168.1.30'. A blue button labeled 'Test Syslog Server' is located at the bottom right of the configuration area.

You can send your audit via syslog (UDP/514) or HTTP.

User activity is recorded in the audit log, including each page visited, policy changes, and user account activity.

Logs are saved in the FMC database automatically. This setting allows you to send logs to an external system as well

Audit Log certificate

Access List

Access Control Preferences

Audit Log

Audit Log Certificate

Change Reconciliation

DNS Cache

Dashboard

Database

Generate New CSR

Import Audit Client Certificate

No Audit Client Certificate Loaded

Audit Server Certificate Settings

Enable TLS ☒

Enable Mutual Authentication ☐

Save

Generate Certificate Signing Request

Subject

Country Name (two-letter code)

State or Province

Locality or City

Organization

Organizational Unit (Department)

Common Name

Close

Generate

You can use (TLS) certificates to secure communications between the FMC and a trusted audit log server.

- Generate a (CSR) to be signed by your CA for
- Export CSR and issue it by CA
- Then import issued certificate via Import Audit Client Certificate

Login banner

The screenshot displays the FMC system configuration interface. On the left is a dark sidebar menu with the following items: Access List, Access Control Preferences, Audit Log, Audit Log Certificate, Change Reconciliation, DNS Cache, Dashboard, Database, Email Notification, External Database Access, HTTPS Certificate, Information, Intrusion Policy Preferences, Language, and Login Banner (which is highlighted). The main content area is titled 'Custom Login Banner' and contains a text box with the message: 'This is a banner from Mohsen Kheradmand Every action is logging and recording in AAA server'. Overlaid on this is a 'Login Banner' modal dialog box. The dialog has a title bar with a close button (X). Inside, there is a text area containing the same message as the background, but with the first line in red: 'This is a banner from Mohsen Kheradmand'. At the bottom right of the dialog are 'Cancel' and 'Accept' buttons. Below the dialog, a 'Username' label is partially visible.

Time Synchronization

Set date/Clock via NTP servers
Or set manually in time setting

External Database Access

HTTPS Certificate

Information

Intrusion Policy Preferences

Language

Login Banner

Management Interfaces

Network Analysis Policy Preferences

Process

REST API Preferences

Remote Storage Device

SNMP

Session Timeout

Time

Time Synchronization

Serve Time via NTP

Enabled

Set My Clock

Manually in Local Configuration

Via NTP

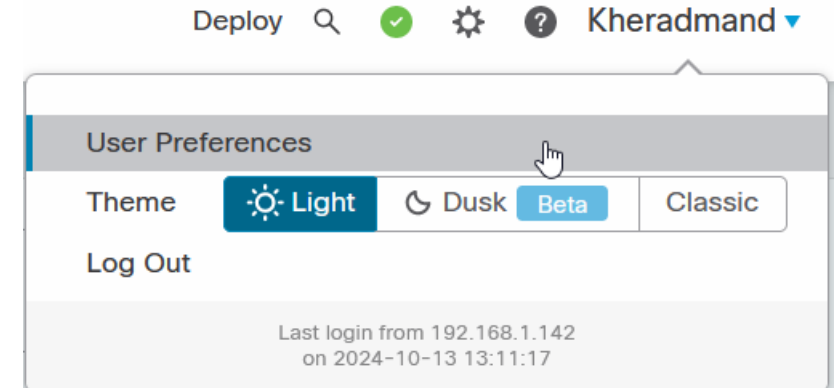
☐ Use the authenticated NTP server only

+ Add

NTP Server	Authentication	Action
0.sourcefire.pool.ntp.org	N/A	
1.sourcefire.pool.ntp.org	N/A	

Time Synchronization

- To adjust time zone:
 - Click user preferences under username
 - Select your time zone



UI Theme

Light

Please provide any Light theme feedback to fmc-light-theme@cisco.com

Time Zone

toro

America/Toronto

Change Password

Change Password

Session timeout

- GUI timeout in minutes
- CLI timeout in minutes

Audit Log	
Audit Log Certificate	
Change Reconciliation	
DNS Cache	
Dashboard	
Database	
Email Notification	
External Database Access	
HTTPS Certificate	
Information	
Intrusion Policy Preferences	
Language	
Login Banner	
Management Interfaces	
Network Analysis Policy Preferences	
Process	
REST API Preferences	
Remote Storage Device	
SNMP	
Session Timeout	

Browser Session Timeout (Minutes)

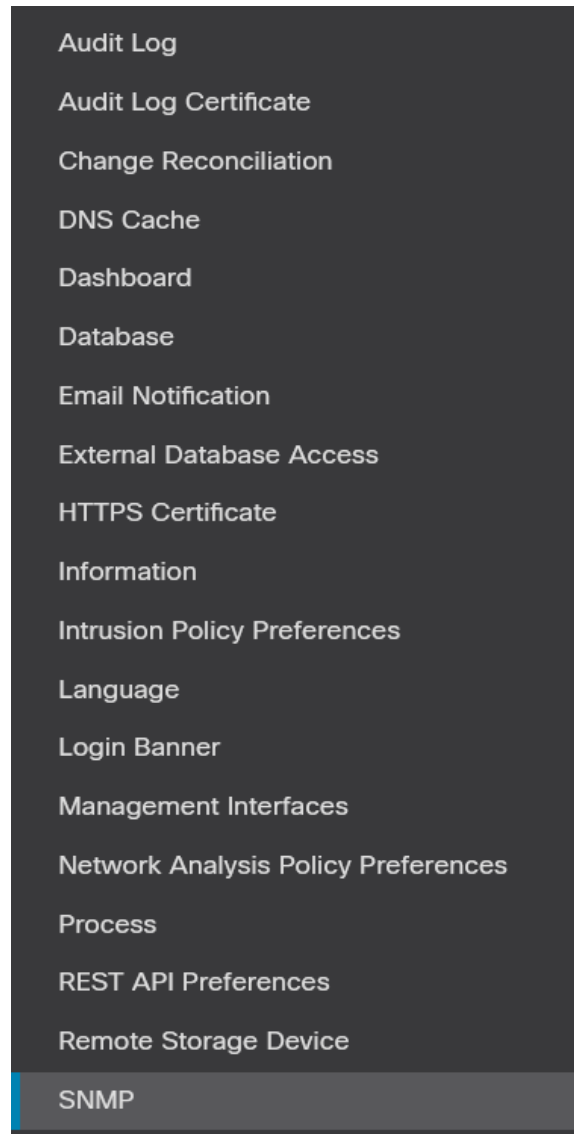
60

CLI Timeout (Minutes)

30

SNMP setting

- Configure SNMP to monitoring software and simple configurations
- You can use SNMP **V1** , **V2** or V3
- In V1-2 , just need community string
- In V3 specify:
 - A username
 - Authentication protocol
 - Authentication password
 - Encryption protocol
 - Encryption key

A configuration form for SNMP Version 2. It contains two fields: 'SNMP Version' with a dropdown menu set to 'Version 2', and 'Community String' with a text input field containing 'Denaman'.A configuration form for SNMP Version 3, labeled 'Version 3' in orange text. It contains several fields: 'Username' (text input with 'kheradmand'), 'Authentication Protocol' (dropdown menu with 'SHA'), 'Authentication Password' (password input with 8 dots and an eye icon), 'Verify Password' (password input with 8 dots and an eye icon), 'Privacy Protocol' (dropdown menu with 'AES128'), 'Privacy Password' (password input with 8 dots and an eye icon), and 'Verify Password' (password input with 8 dots and an eye icon). An 'Add' button is at the bottom right.

User configuration

External Database Access

HTTPS Certificate

Information

Intrusion Policy Preferences

Language

Login Banner

Management Interfaces

Network Analysis Policy Preferences

Process

REST API Preferences

Remote Storage Device

SNMP

Session Timeout

Time

Time Synchronization

UCAPL/CC Compliance

User Configuration

VMware Tools

Password Reuse Limit

Limit (0 = no limit)

Users can not use previous password (in time)

Track Successful Logins

Days (0 = no tracking, 365 = max value)

Log successful logging in days

Max Number of Login Failures

Maximum number of failures before temporary lockout (0 = no lockout, 999 = max value)

After max try system will be locked

Set Time in Minutes to Temporarily Lockout Users

Minutes (0 = no wait time, 1440 = max value, 1 day)

Lockout timer after login failure

Max Concurrent Sessions Allowed

Maximum sessions for users with Read Only privileges (0 = no limit, 1024 = max value)

Maximum concurrent session for R/O users

Maximum sessions for users with Read/Write privileges/CLI users (0 = no limit, 1024 = max value)

Or R/W users

Info

This user has successfully logged in 1 times over the past 30 days.

Change Reconciliation

Send a daily Change Reconciliation report with any configuration changes to the FMC in the previous 24 hours

Access List

Access Control Preferences

Audit Log

Audit Log Certificate

Change Reconciliation

DNS Cache

Dashboard

Enable ☒

Time to Run 16 : 00

Email to service@Dena.local [Resend Last Report](#)

Include Policy Configuration ☒

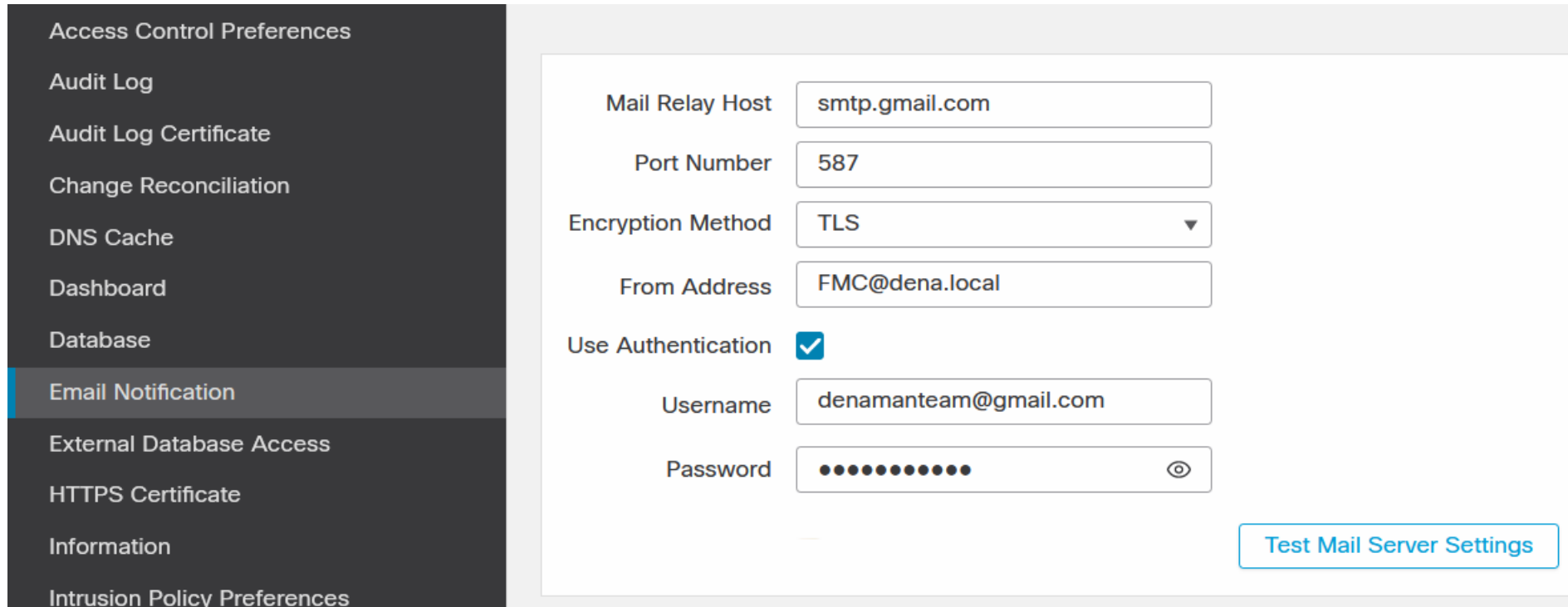
Show Full Change History ☐

Save

Note that to use this, you must first configure a mail relay

Email Notification

If you want your FMC to send email notifications (and everyone does), configure an SMTP mail relay



The screenshot displays the FMC system configuration interface. On the left is a dark sidebar with a list of menu items: Access Control Preferences, Audit Log, Audit Log Certificate, Change Reconciliation, DNS Cache, Dashboard, Database, Email Notification (highlighted with a blue bar), External Database Access, HTTPS Certificate, Information, and Intrusion Policy Preferences. The main content area is light gray and contains the 'Email Notification' configuration form. This form includes several fields: 'Mail Relay Host' with the value 'smtp.gmail.com', 'Port Number' with '587', 'Encryption Method' with a dropdown menu set to 'TLS', 'From Address' with 'FMC@dena.local', and 'Use Authentication' which is checked with a blue checkbox. Below these are 'Username' and 'Password' fields; the username is 'denamanteam@gmail.com' and the password is masked with dots. A 'Test Mail Server Settings' button is located at the bottom right of the form.

Mail Relay Host	smtp.gmail.com
Port Number	587
Encryption Method	TLS ▼
From Address	FMC@dena.local
Use Authentication	☒
Username	denamanteam@gmail.com
Password	••••••••••

Test Mail Server Settings

DNS Cache

The length of time hostnames will be cached within the UI

Access List

Access Control Preferences

Audit Log

Audit Log Certificate

Change Reconciliation

DNS Cache

Save

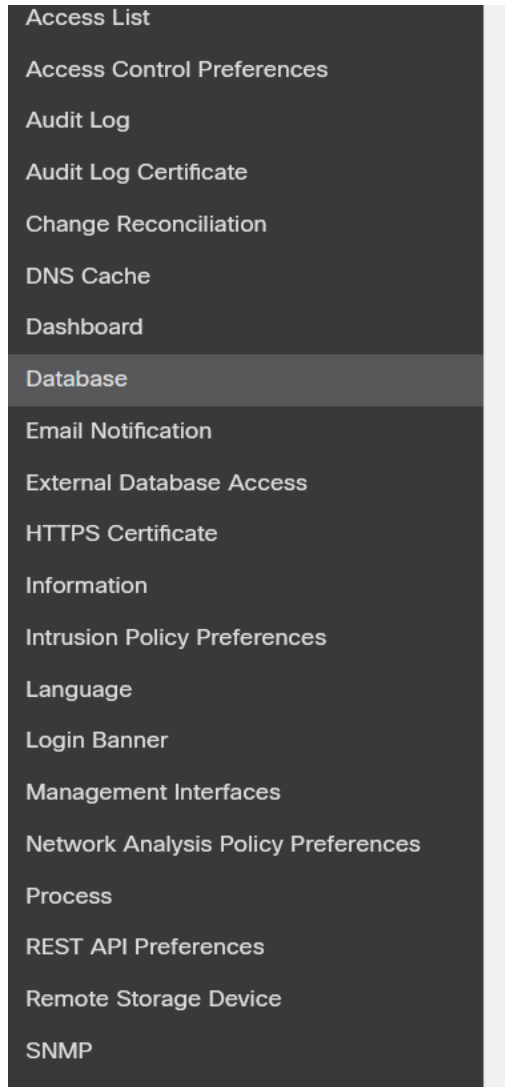
DNS Resolution Caching Enabled ▼

DNS Cache Timeout (in minutes) 300

This prevents the FMC from constantly performing DNS lookups every time you load an event view page

Database

Configure the maximum size of the various databases within the FMC



Intrusion Event Database

Supported Platforms Firepower Management Center

Maximum Intrusion Events 1000000

Discovery Event Database

Supported Platforms Firepower Management Center

Maximum Discovery Events (0 = do not store) 1000000

Connection Database

Supported Platforms Firepower Management Center

Maximum Connection Events (0 = do not store) 1000000

Maximum Security Intelligence Events 1000000

Connection Summary Database

Supported Platforms Firepower Management Center

Maximum Connection Summaries (0 = do not store) 2000000

Correlation & Allow List Event Database

Supported Platforms Firepower Management Center

Maximum Correlation & Allow List Events 1000000

Malware Event Database

Supported Platforms Firepower Management Center

Maximum Malware Events 1000000

File Event Database

Supported Platforms Firepower Management Center

HTTPS Certificate

- Generate a new CSR to CA server , export it , Issue CSR to Cert and then import HTTPS Cert into FMC

Access List

Access Control Preferences

Audit Log

Audit Log Certificate

Change Reconciliation

DNS Cache

Dashboard

Database

Email Notification

External Database Access

HTTPS Certificate

Information

Intrusion Policy Preferences

Language

Login Banner

Management Interfaces

Network Analysis Policy Preferences

Generate New CSR

Import HTTPS Server Certificate

Current HTTPS Server Certificate

Subject	commonName FMC	countryName US	organizationName Cisco Systems, Inc	organizationalUnitName Intrusion Management System
Issuer	commonName FMC	countryName US	organizationName Cisco Systems, Inc	organizationalUnitName Intrusion Management System
Validity	Not Before Oct 11 10:45:28 2024 GMT	Not After Dec 21 10:45:28 2026 GMT		
Version	3			
Serial Number	2F5D5951657608B2278CA7D5212405F1233C7F0F			
Signature Algorithm	sha256WithRSAEncryption			

Renew HTTPS Certificate

HTTPS Client Certificate Settings

Enable Client Certificates ☐

Save

Remote Storage Device

- Remote storage can be configured to store **backups** and **reports**

The screenshot displays the 'Remote Storage Device' configuration interface. On the left is a dark sidebar with a menu containing the following items: 'Intrusion Policy Preferences', 'Language', 'Login Banner', 'Management Interfaces', 'Network Analysis Policy Preferences', 'Process', 'REST API Preferences', 'Remote Storage Device' (which is highlighted), 'SNMP', 'Session Timeout', 'Time', and 'Time Synchronization'. The main configuration area on the right is titled 'Remote Storage Device' and contains the following sections:

- Storage Type:** A dropdown menu set to 'NFS'.
- Connection:**
 - Host:** A text input field containing '192.168.10.10', with the label 'IP or hostname' to its right.
 - Directory:** A text input field containing '/FMCbackup'.
- Advanced:**
 - Use Advanced Options:** An unchecked checkbox.
- System Usage:**
 - Use for Backups:** A checked checkbox.
 - Use for Reports:** A checked checkbox.
 - Disk Space Threshold:** A text input field containing '90', followed by a '%' symbol.

At the bottom right of the configuration area are two buttons: 'Test' and 'Save'.

FDM Management Access

Firepower Device Manager

Monitoring

Policies

Objects

Device: FTD

>

admin Administrator

Model
Cisco Firepower Threat Defense for VMwa...

Software
7.0.1-84

VDB
338.0

Intrusion Rule Update
20210503-2107

Cloud Services
 Not Registered | [Register](#)

High Availability ?
Not Configured

CONFIGURE

Inside Network

0/1

Cisco Firepower Threat Defense for VMware

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT

CONSOLE

0/0

Internet

DNS Server

NTP Server

Smart License

ISP/WAN/Gateway

Interfaces
Connected

Routing
There are no static routes yet

Updates
Geolocation, Rule, VDB, System Upgrade,

System Settings
[Management Access](#)

MohsenKheradmand

FDM Management Access

Management interface

Configure IPv4 and IPV6 address

System Settings ←

Management Access

Logging Settings

DHCP Server

DNS Server

Management Interface

Hostname

Time Services

SSL Settings

HTTP Proxy

Cloud Services

Web Analytics

Reboot/Shutdown

Traffic Settings

URL Filtering Preferences

⚠ Changes are deployed immediately, and deployment can take a few minutes to complete. You will lose access to Firepower Device Manager if you change the address to which you are connected.

CONFIGURE IPV4

Type

Static ▾

IP Address

192.168.1.200

e.g. 192.168.5.15

Network Mask

255.255.255.0

e.g. 255.255.255.0 or 24

Gateway

192.168.1.1

CONFIGURE IPV6

Type

Static ▾

IP Address

2001:ABCD:1234:1::200

e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Prefix

64

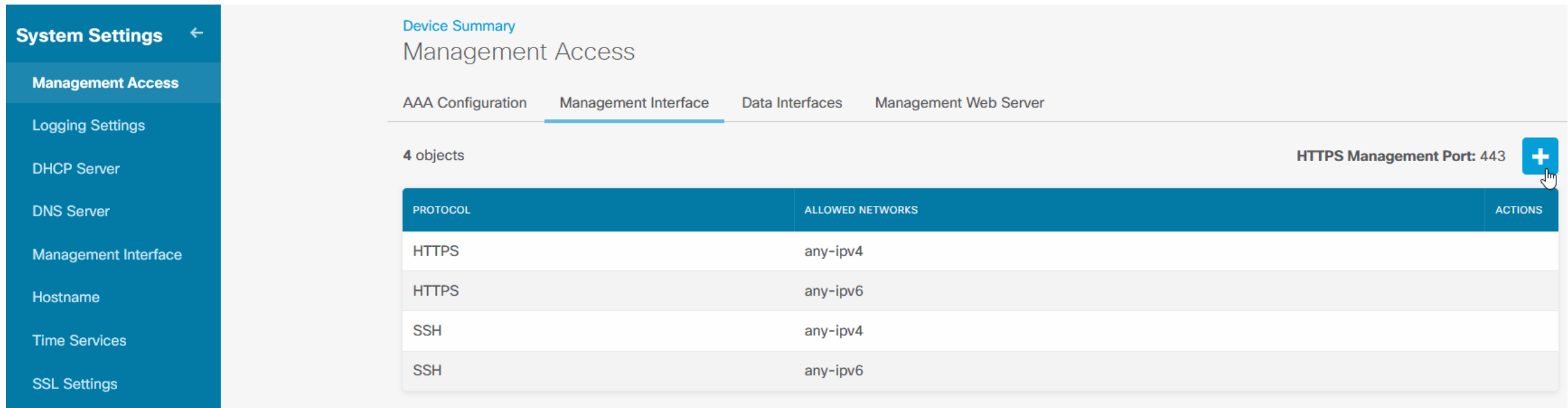
Gateway

2001:ABCD:1234:1::1

FDM Management Access

Management Access

- 1) Click management interface
- 2) Click + to add new IP address that can access to FDM



System Settings ←

- Management Access
- Logging Settings
- DHCP Server
- DNS Server
- Management Interface
- Hostname
- Time Services
- SSL Settings

Device Summary

Management Access

AAA Configuration Management Interface Data Interfaces Management Web Server

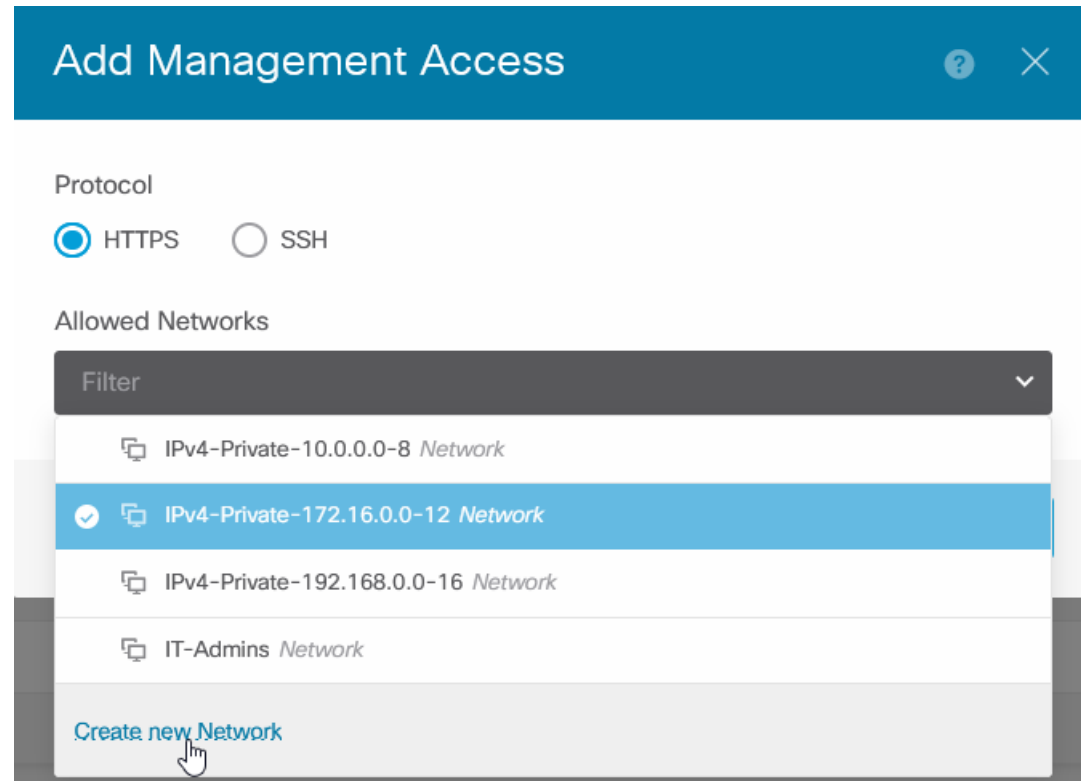
4 objects **HTTPS Management Port: 443** 

PROTOCOL	ALLOWED NETWORKS	ACTIONS
HTTPS	any-ipv4	
HTTPS	any-ipv6	
SSH	any-ipv4	
SSH	any-ipv6	

FDM Management Access

Management Access

- 3) Select protocol type to connect to FDM
- 4) Then click “ Create new Network ”



The screenshot shows a dialog box titled "Add Management Access" with a blue header bar. Below the header, there is a "Protocol" section with two radio buttons: "HTTPS" (selected) and "SSH". Underneath is the "Allowed Networks" section, which contains a list of network ranges. A "Filter" input field is at the top of the list. The list items are: "IPv4-Private-10.0.0.0-8 Network", "IPv4-Private-172.16.0.0-12 Network" (highlighted with a blue background and a checkmark icon), "IPv4-Private-192.168.0.0-16 Network", and "IT-Admins Network". At the bottom of the dialog, there is a link that says "Create new Network" with a hand cursor pointing at it.

Protocol

☒ HTTPS ☐ SSH

Allowed Networks

Filter

- IPv4-Private-10.0.0.0-8 Network
- ☒ IPv4-Private-172.16.0.0-12 Network
- IPv4-Private-192.168.0.0-16 Network
- IT-Admins Network

[Create new Network](#)

FDM Management Access

Management Access

- Type a name for new group/client
- Description (optional)
- Type : network address or single host
- Network : IPv4 or IPv6 address of client/group

Add Network Object

Name

IT-Admins

Description

IT admin department can connect to FDM

Type

☒ Network ☐ Host

Network

192.168.1.0/26

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL OK

FDM Management Access

Time service

- Configure NTP servers

The screenshot displays the 'System Settings' interface with a sidebar on the left and a main content area on the right. The sidebar lists various settings: Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, Time Services (highlighted), SSL Settings, HTTP Proxy, and Cloud Services. The main content area is titled 'Device Summary' and 'Time Services'. Under 'Time Services', there is a section for 'NTP' configuration. It includes a dropdown menu for 'NTP Time Server' with options 'Default NTP Servers' (selected) and 'User-Defined NTP Servers'. Below the dropdown, two NTP servers are listed: '1.sourcefire.pool.ntp.org' and '2.sourcefire.pool.ntp.org'. A 'SAVE' button is located at the bottom of the configuration section.

System Settings ←

- Management Access
- Logging Settings
- DHCP Server
- DNS Server
- Management Interface
- Hostname
- Time Services**
- SSL Settings
- HTTP Proxy
- Cloud Services

Device Summary

Time Services

NTP

NTP Time Server

Default NTP Servers ▼ ⓘ

Default NTP Servers

User-Defined NTP Servers

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

SAVE

FDM Management Access

Logging setting

- Enable DATA LOGGING
- Click + to add Syslog server
- Select severity of events to send logs

System Settings ←

Management Access

Logging Settings

DHCP Server

DNS Server

Management Interface

Hostname

Time Services

SSL Settings

HTTP Proxy

Cloud Services

Web Analytics

Reboot/Shutdown

Traffic Settings

URL Filtering Preferences

Logging Settings

Remote Servers

DATA LOGGING ☒

Syslog Servers

+

172.16.21.1

Message Filtering for Firepower Threat Defense

☒ Severity level for filtering all events

Warning

☐ Custom Logging Filter

Please select an Event List Filter

FILE/MALWARE LOGGING ☒

i

To generate file/malware syslog messages, you must also configure file policies on at least one access control rule, and enable the File Events > Log Files option on the rule.

Syslog Server

172.16.21.1

Log at Severity Level

FDM Management Access

Logging setting

- Enter Syslog server address
- Select protocol type
- Enter the port number of syslog server
- Select source interface of FTD to send events to Syslog server

Add Syslog Server

IP Address

172.16.21.1

Protocol Type

☒ UDP ☐ TCP

Port Number

1721

514, 1025 - 65535

Interface for Device Logs

Select the interface for sending diagnostic syslog messages.

Note: The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

☐ Data Interface

Please select an interface

☒ Management Interface

CANCEL

OK

FDM Management Access

Logging setting

- Select severity for saving logs to internal buffer
- Enter buffer size in Bytes
- Select severity for showing logs to Console

Internal Buffer

Message Filtering for Firepower Threat Defense

☒ Severity level for filtering all events

Error

☐ Custom Logging Filter

Please select an Event List Filter

Buffer Size

4096 - 52428800

Console Filter

Severity

Critical