Securing Networks with

Cisco FTD

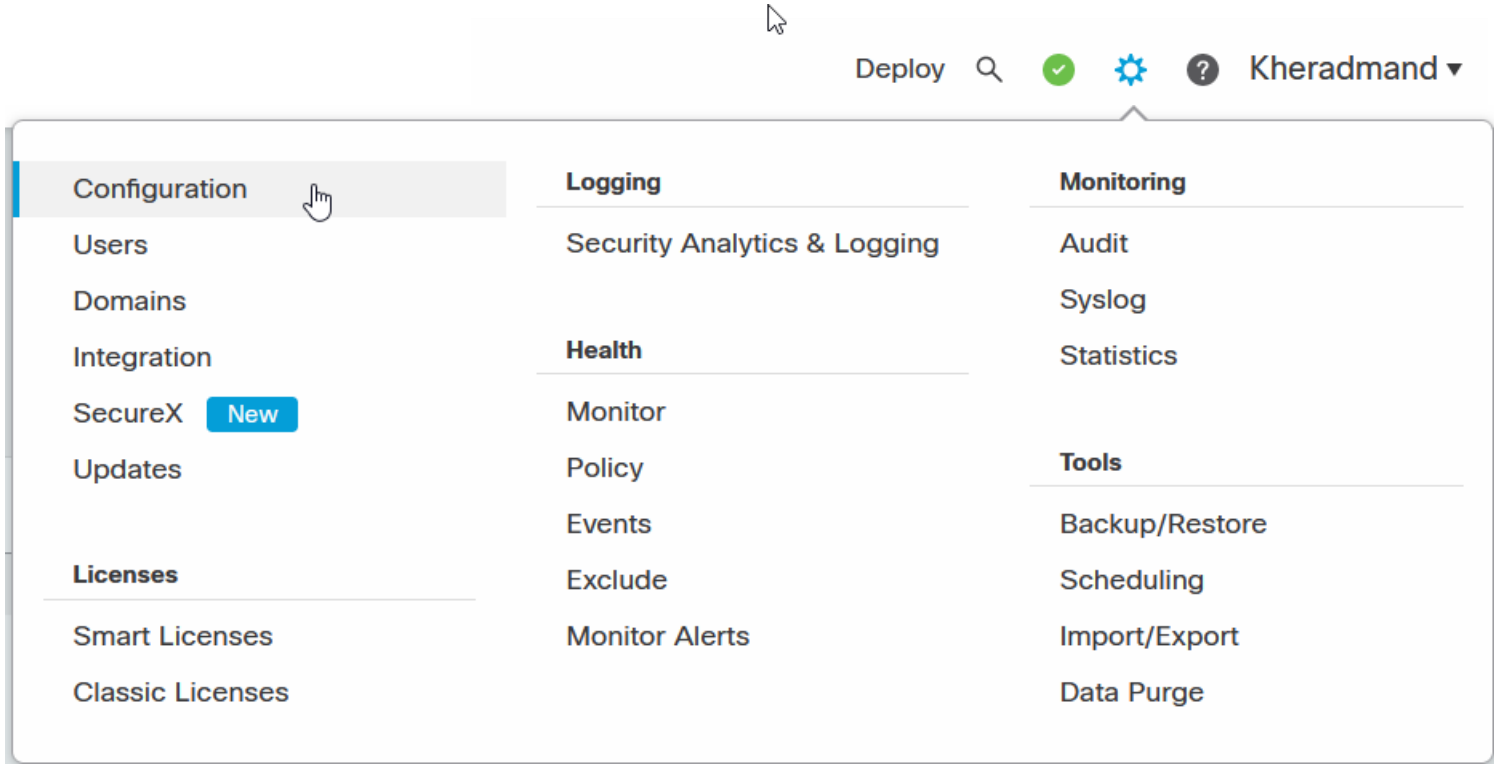
Chapter 2

FMC/FTD basic system setting

Mohsen Kheradmand

Firepower System Configuration

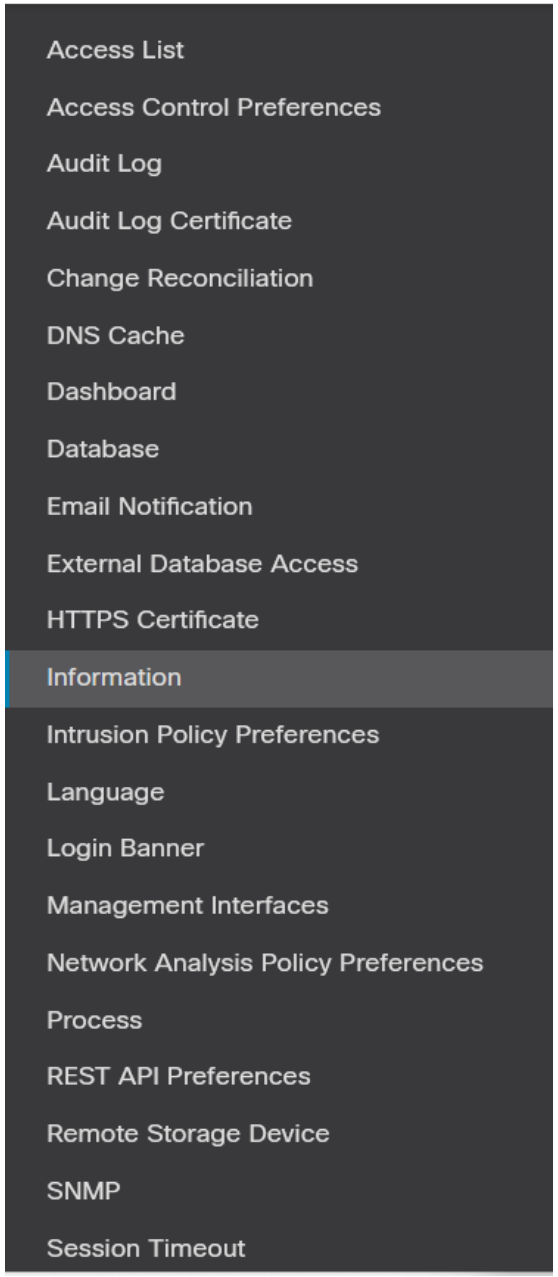
- On the top menu click System
- Then click Configuration

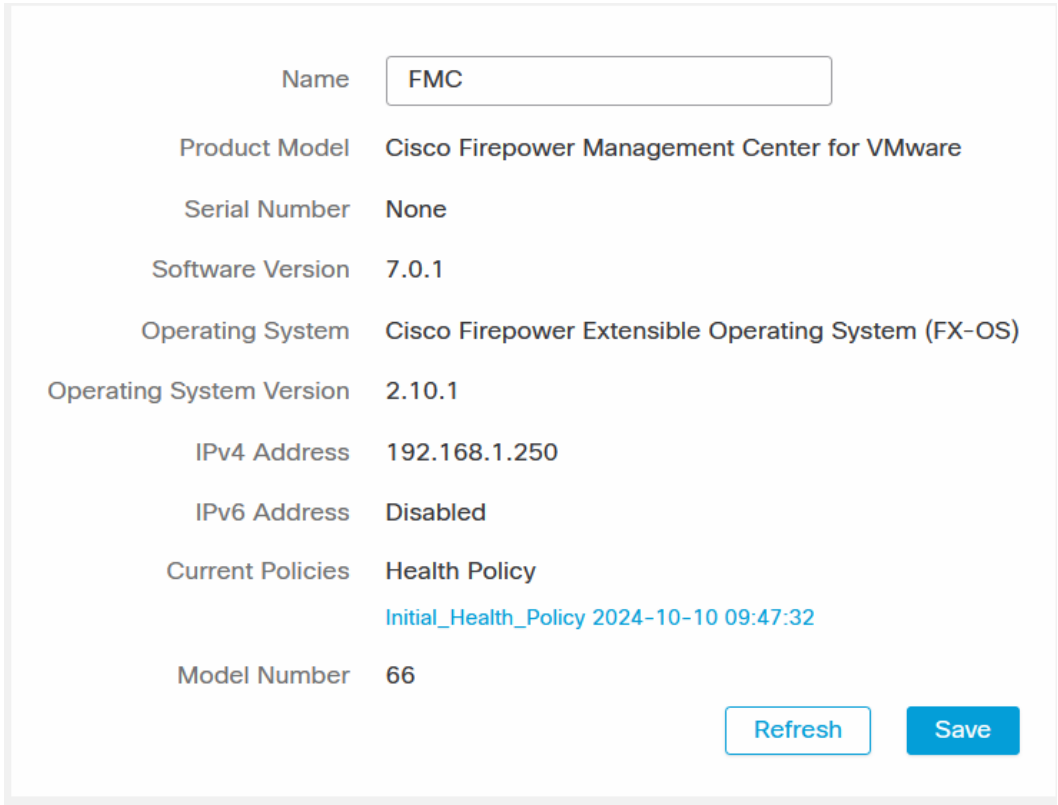


FMC system configuration

Information

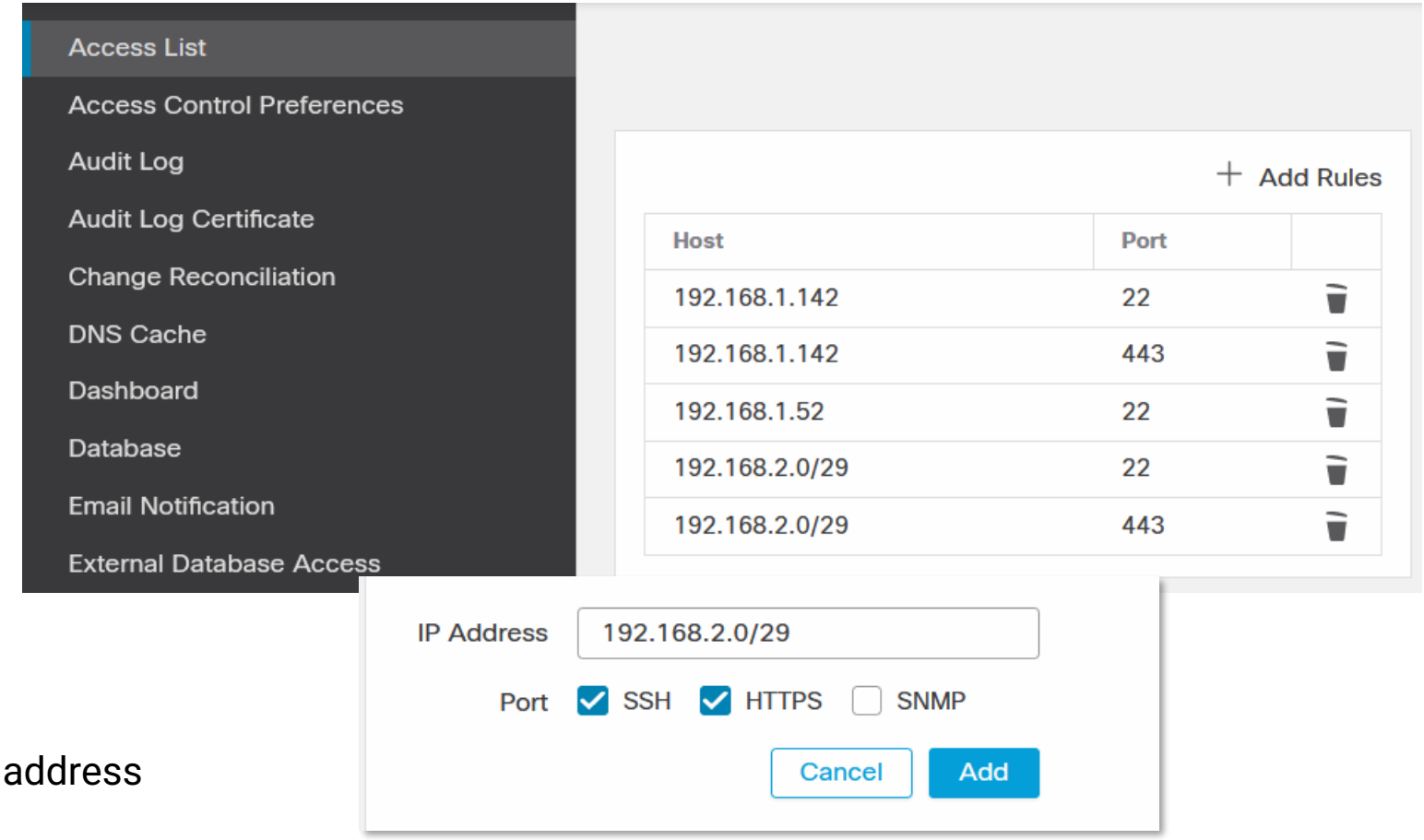
Here ,You can change the FMC name.





MohsenKheradmand MK

Access List



Acceptable addresses to connect to FMC via :

SSH , HTTPS or SNMP

Click Add Rules (to add IP address)

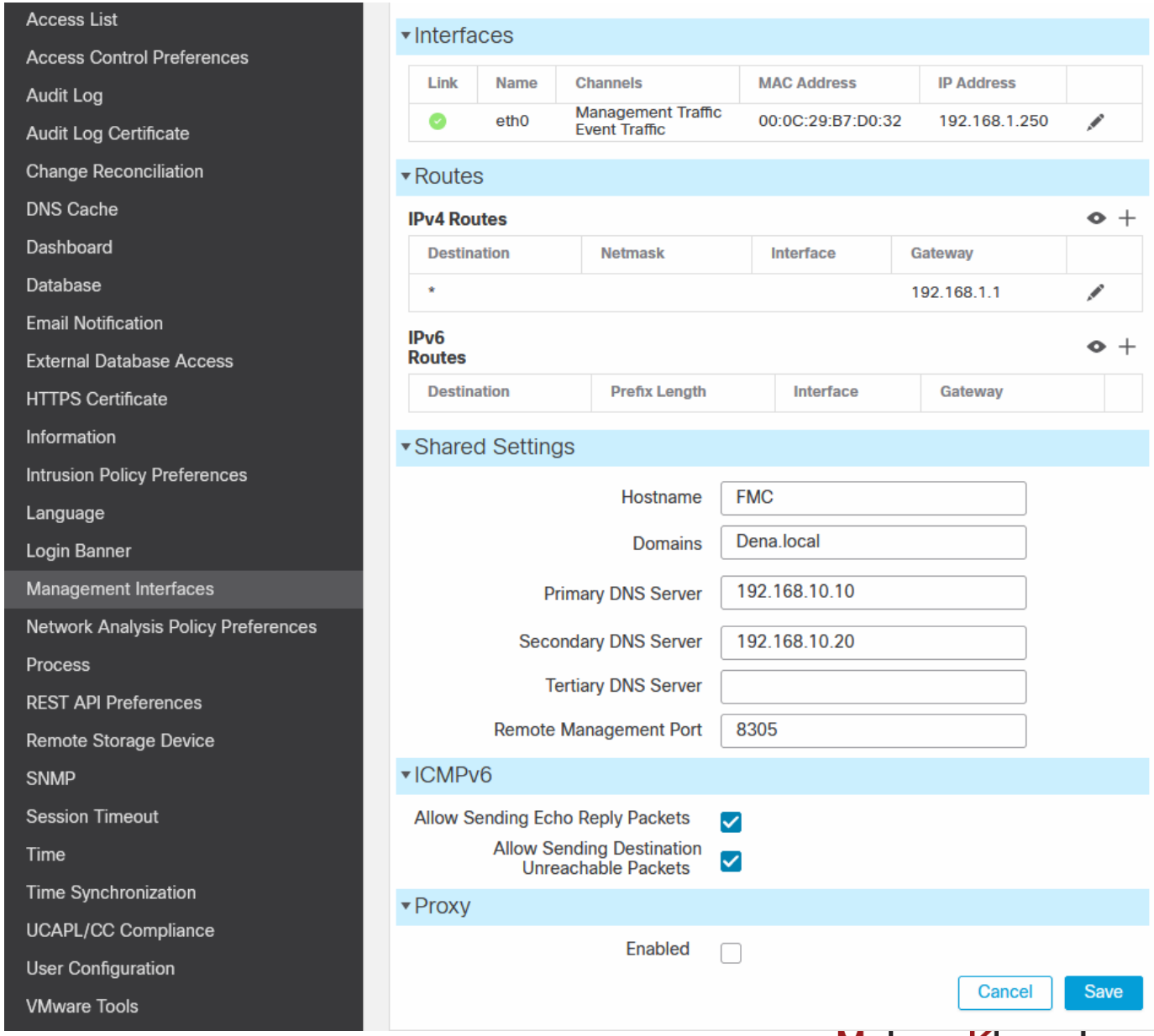
- Enter new IP/Subnet
- Click any port you want to allow this via this address
- Then delete *ANY* rules

✓ Note: type NMS station IP address (if you want to send traps from the FMC to the NMS station)

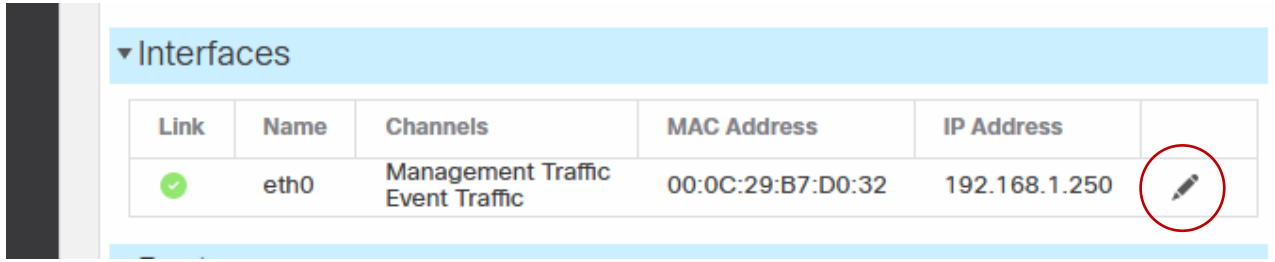
- However, you must set the SNMP configuration further down before you can configure the NMS station IP address

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



Management interface

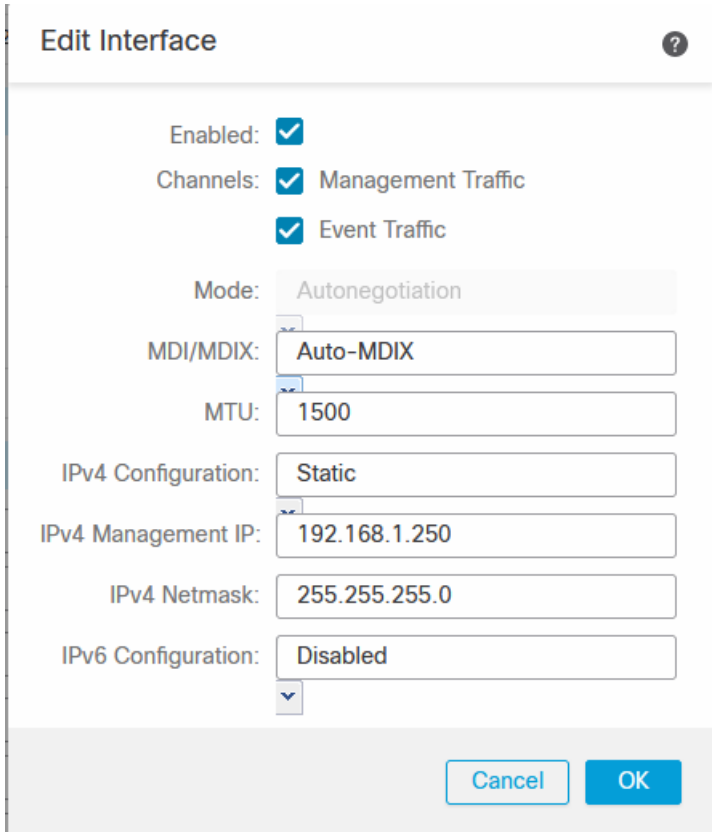


Management interface Edit

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

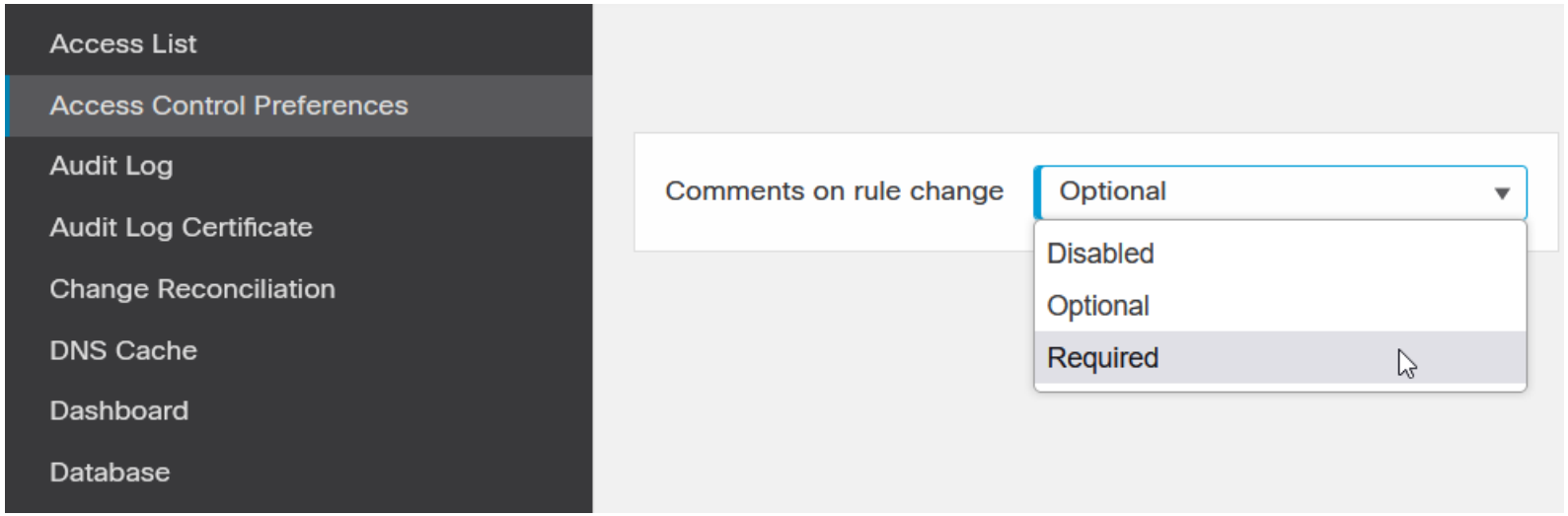
However, eth1-3 can be used on hardware FMC

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



MohsenKheradmand

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

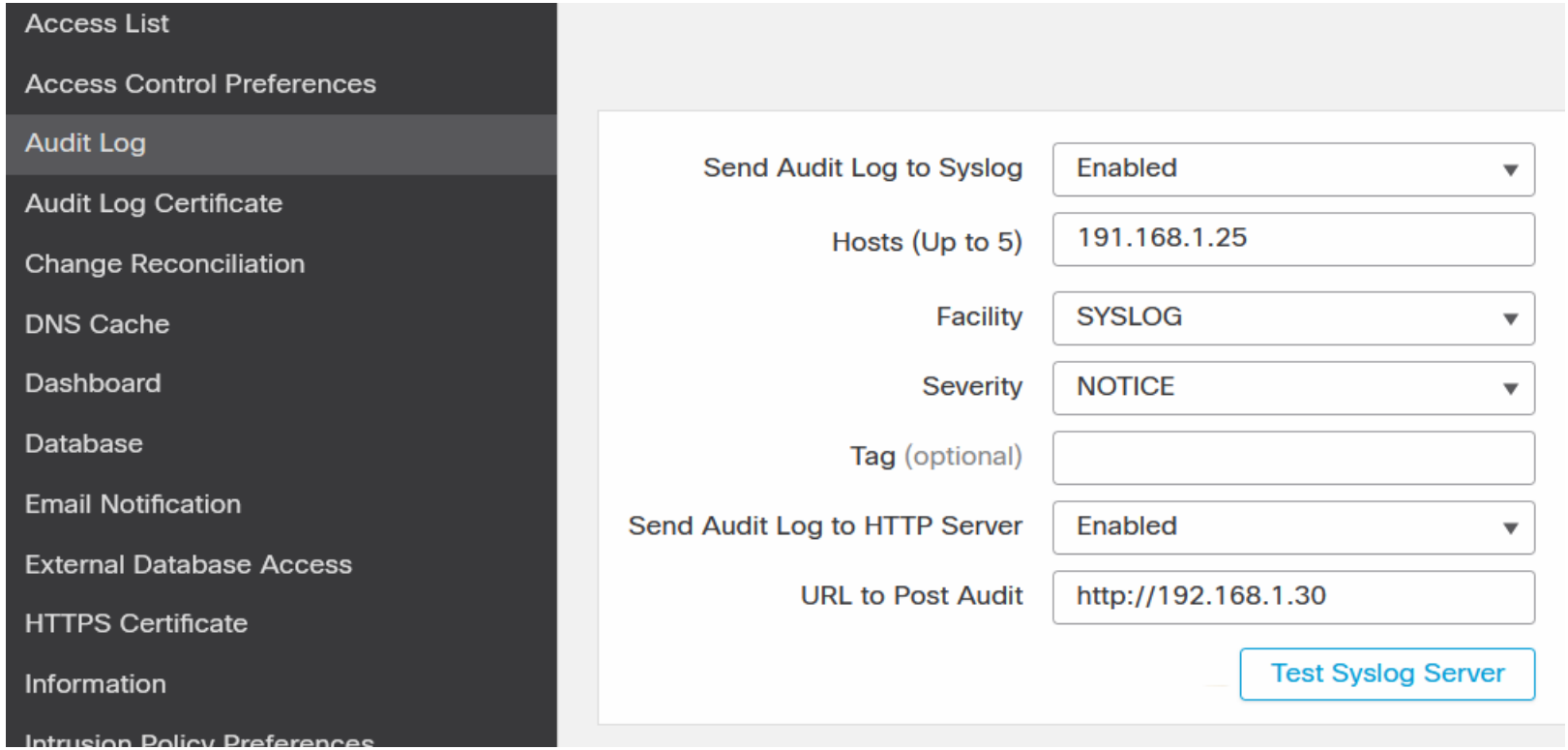
Audit Log

Configure Syslog server to send logs

Host : IP or FQDN of syslog server

Facility : the type of message

Severity : level of the message

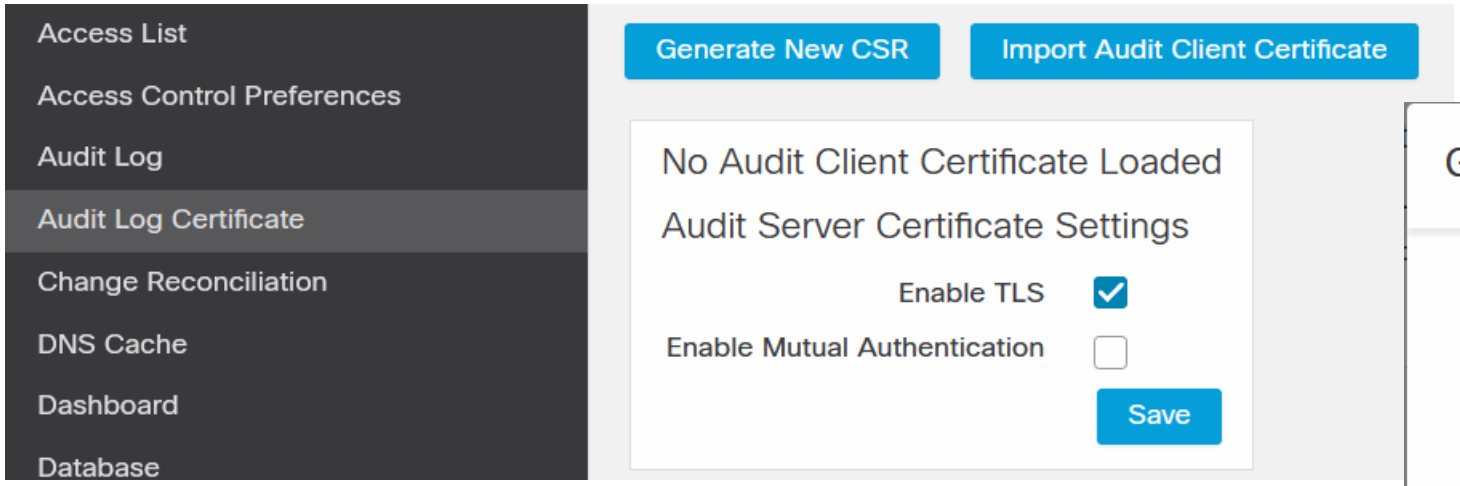


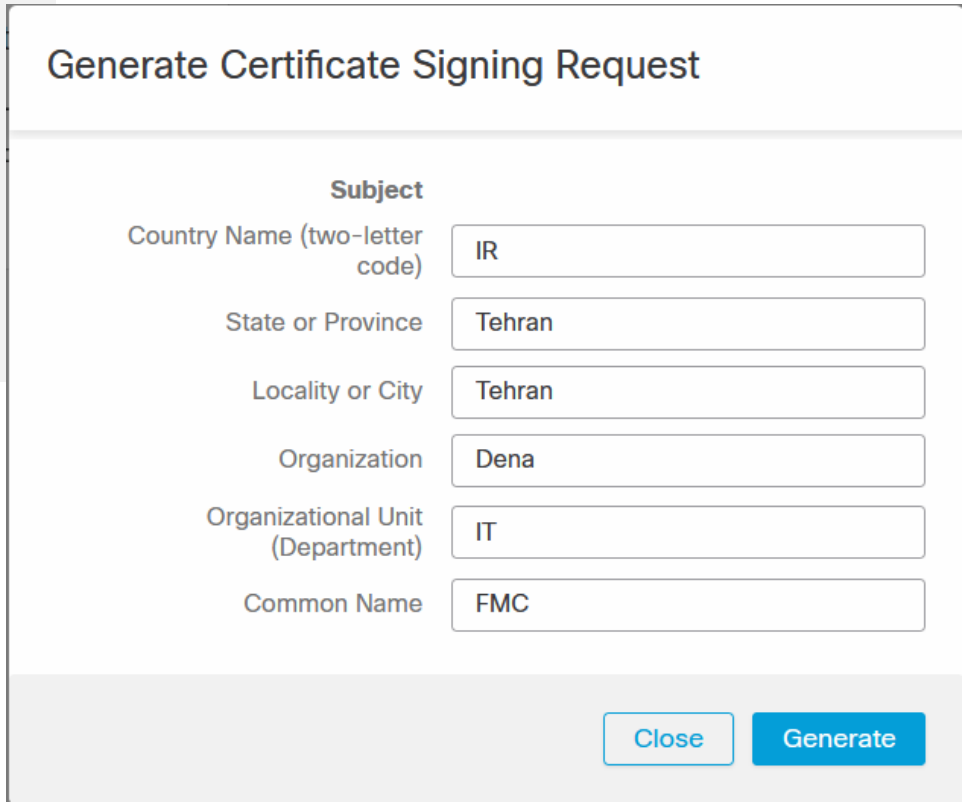
You can send your audit via syslog (UDP/514) or HTTP.

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



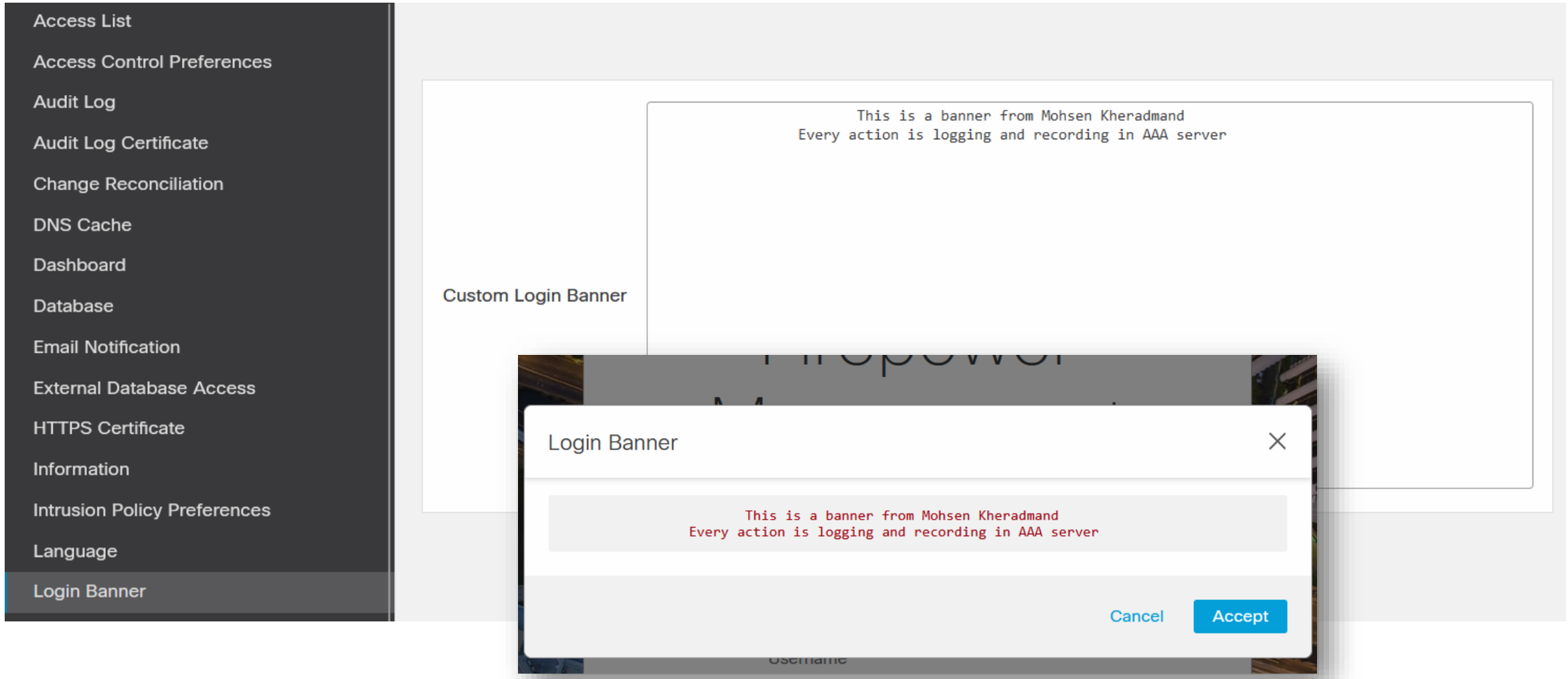


You can use (TLS) certificates to secure communications between the FMC and a trusted audit log server.

- 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

MohsenKheradmand MK

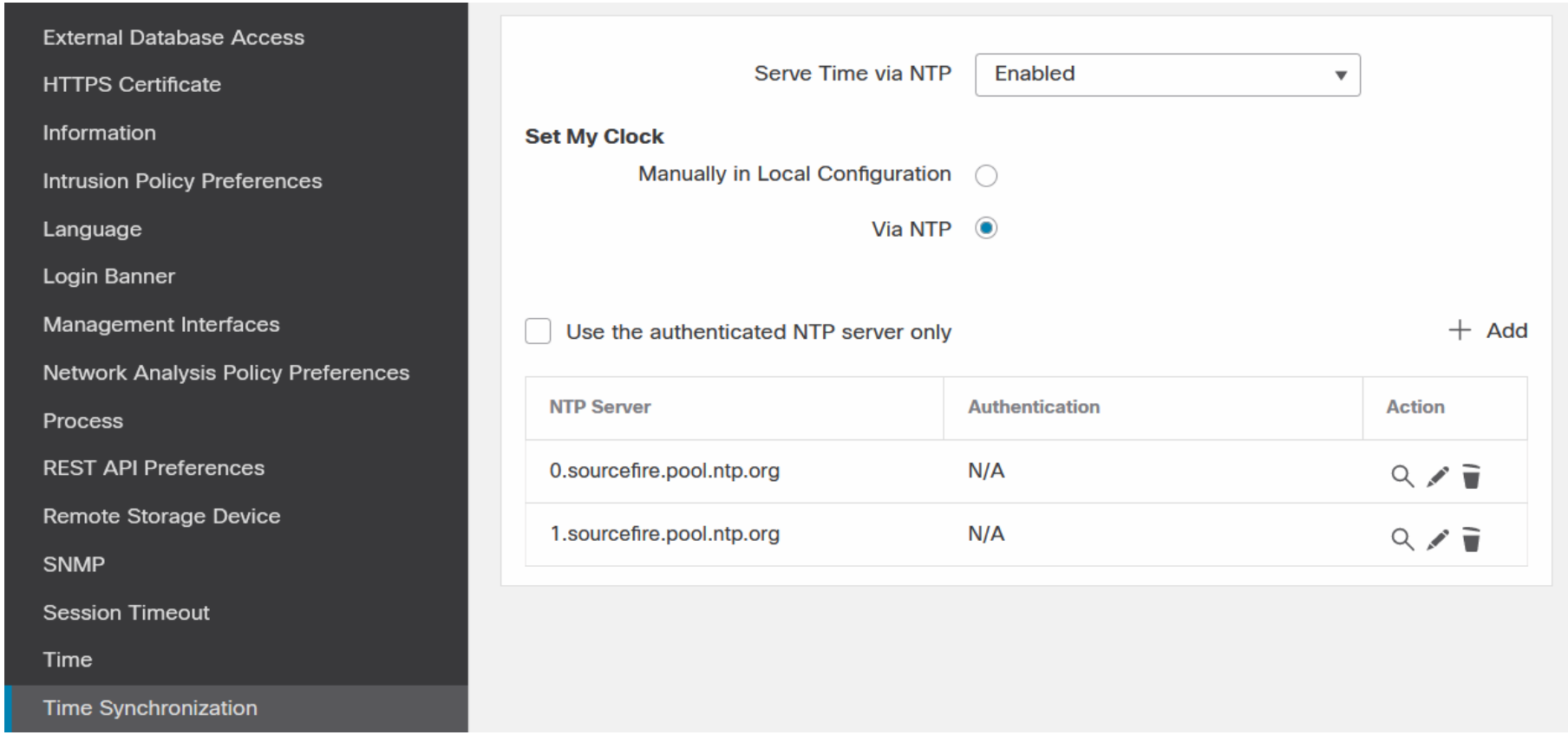
Login banner



Time Synchronization

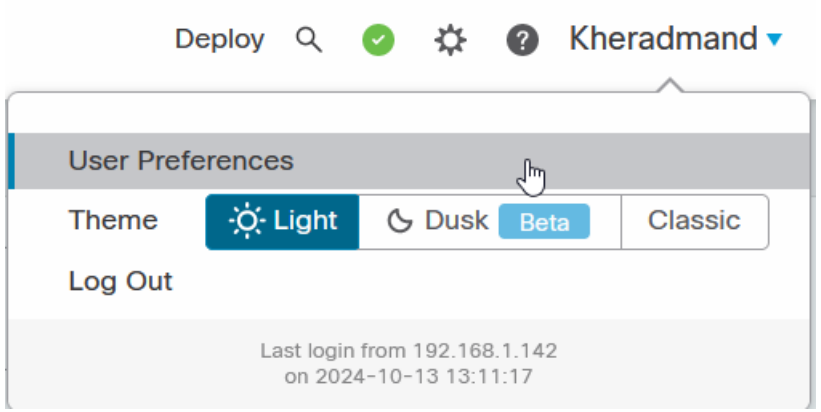
Set date/Clock via NTP servers

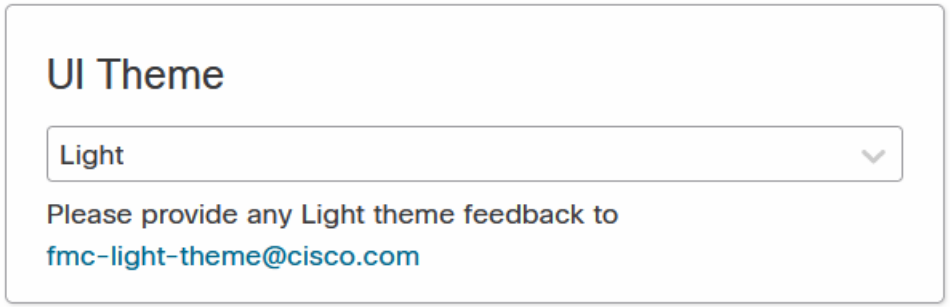
Or set manually in time setting

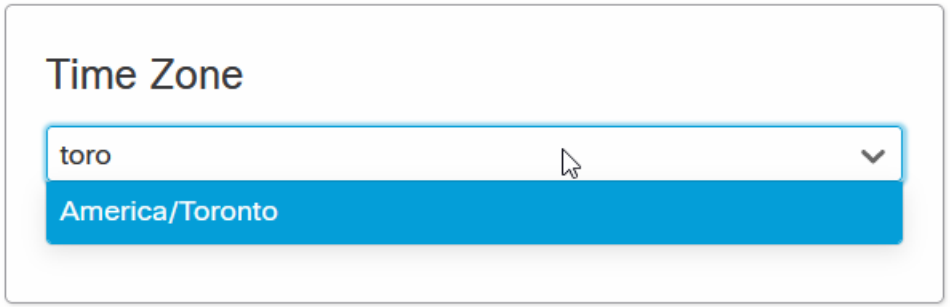


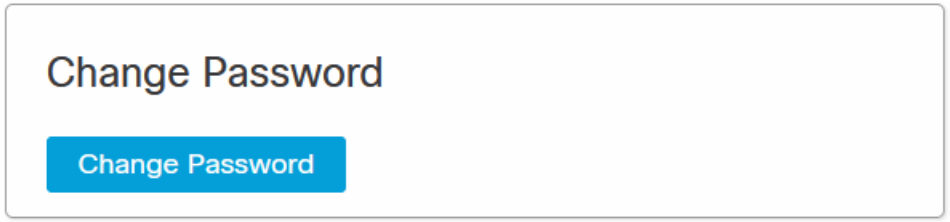
Time Synchronization

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



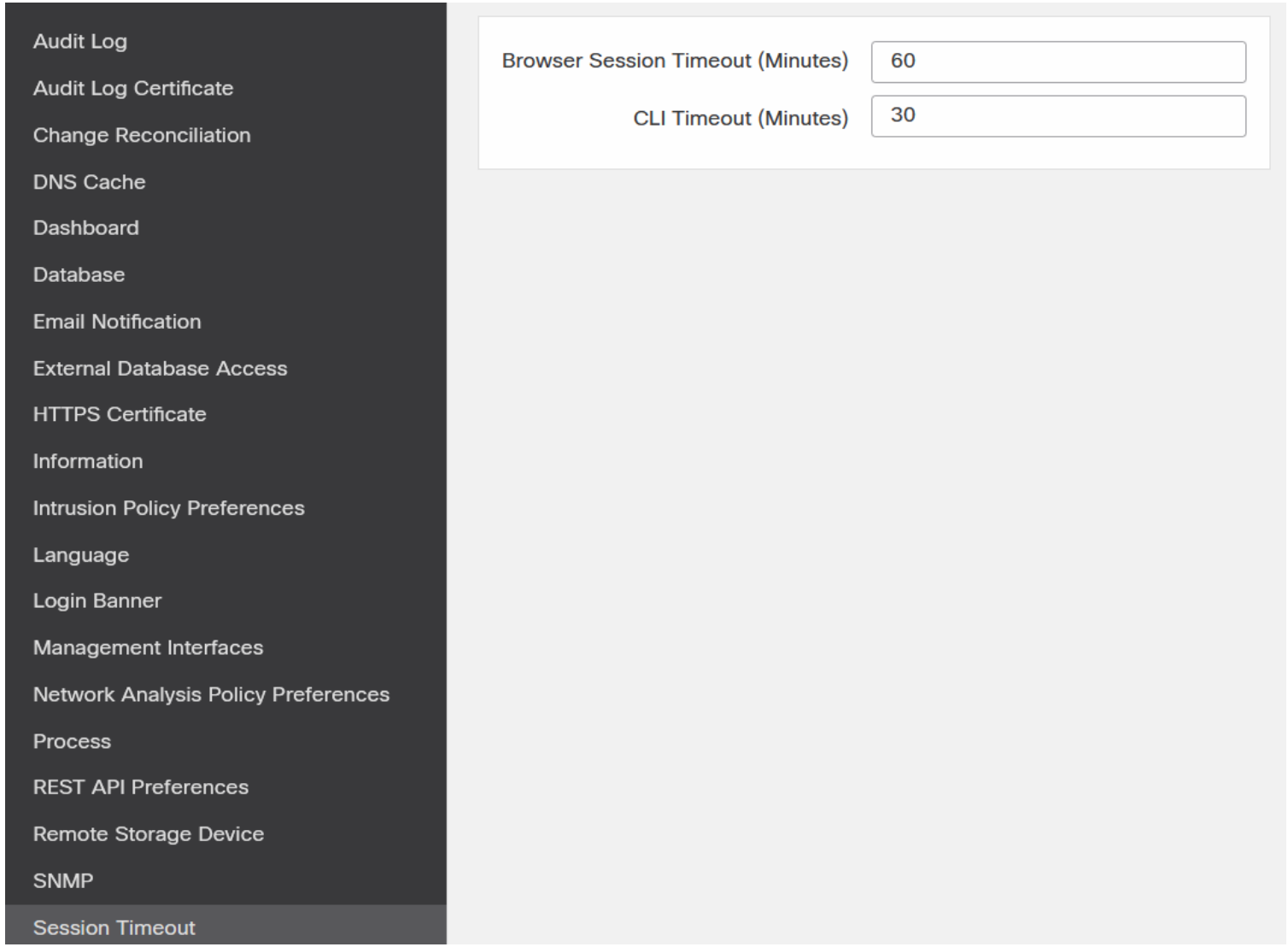






Session timeout

- GUI timeout in minutes
- CLI timeout in minutes



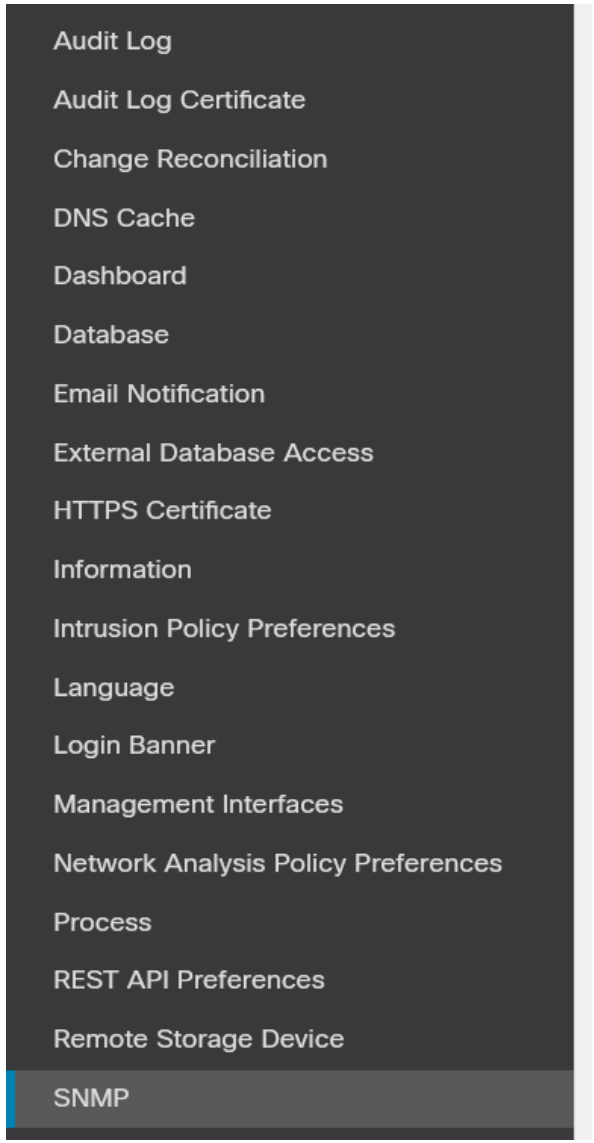
SNMP setting

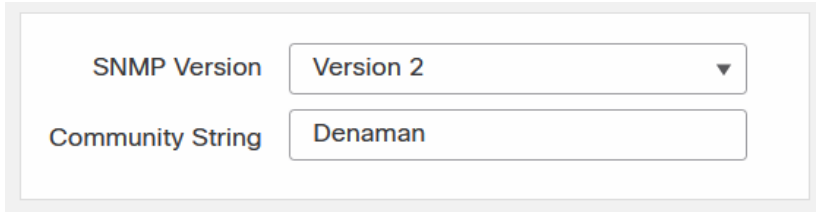
- Configure SNMP to monitoring software and simple configurations

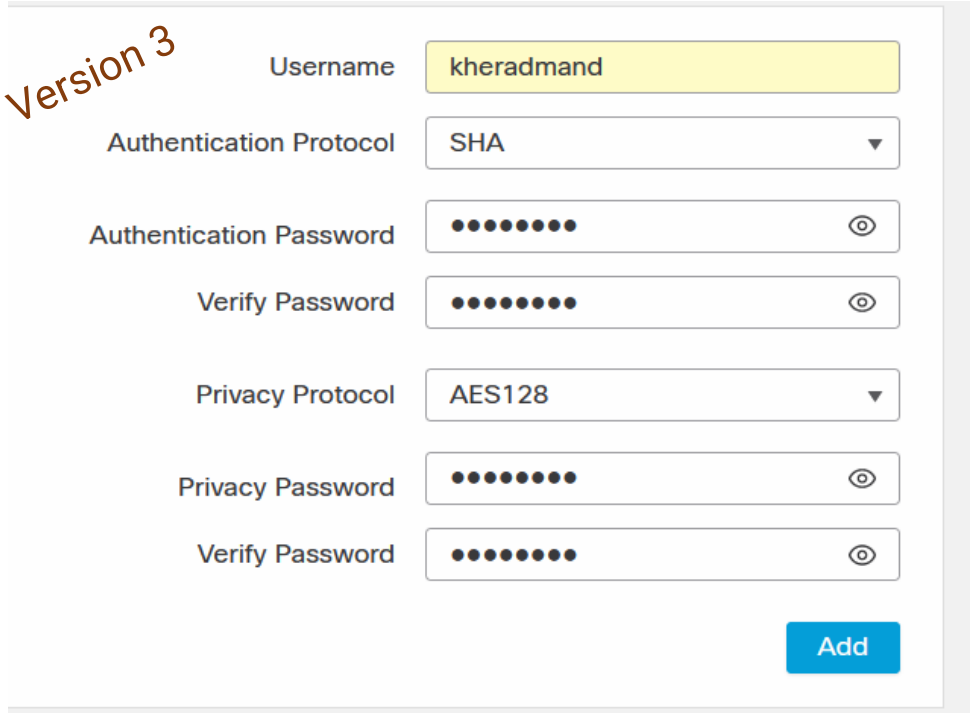
- You can use SNMP V1 , V2 or V3

- In V1-2 , just need community string

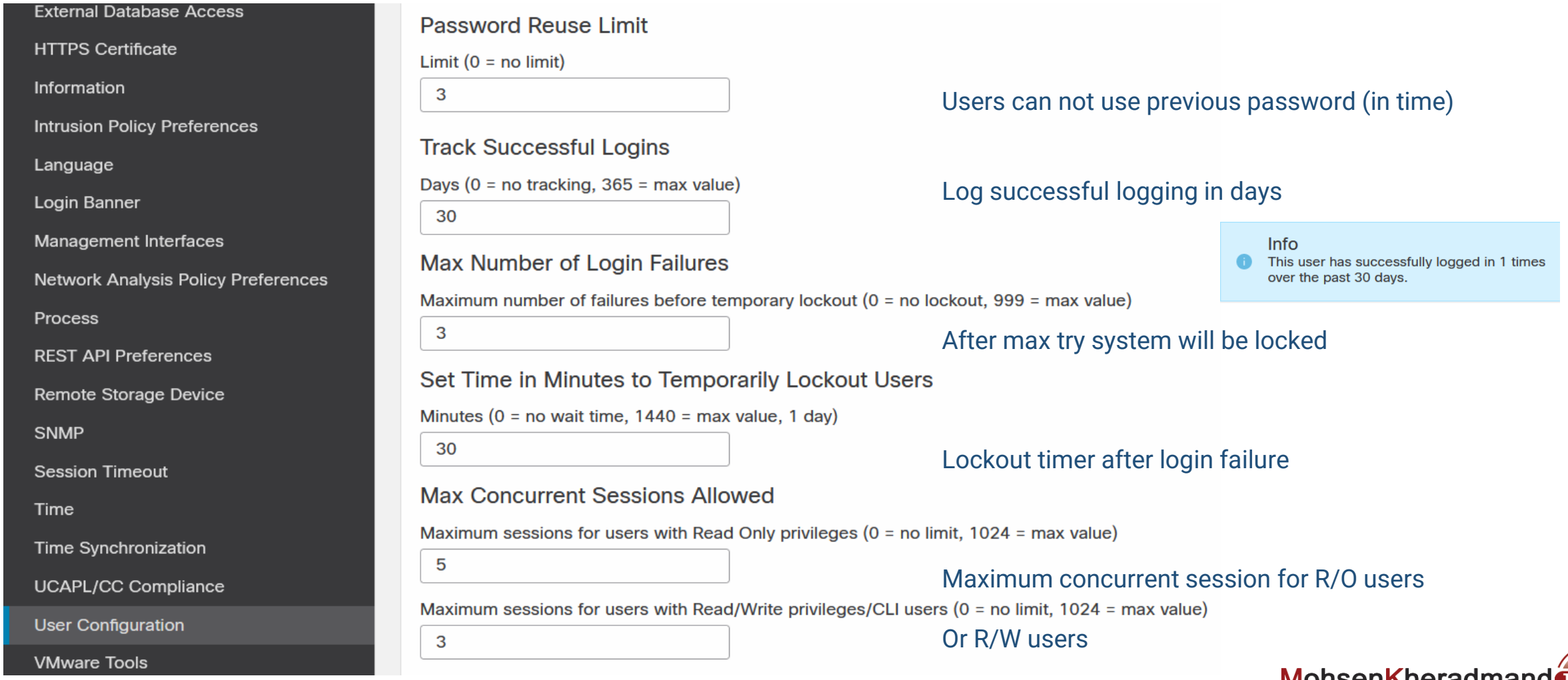
- In V3 specify:
  - A username
  - Authentication protocol
  - Authentication password
  - Encryption protocol
  - Encryption key







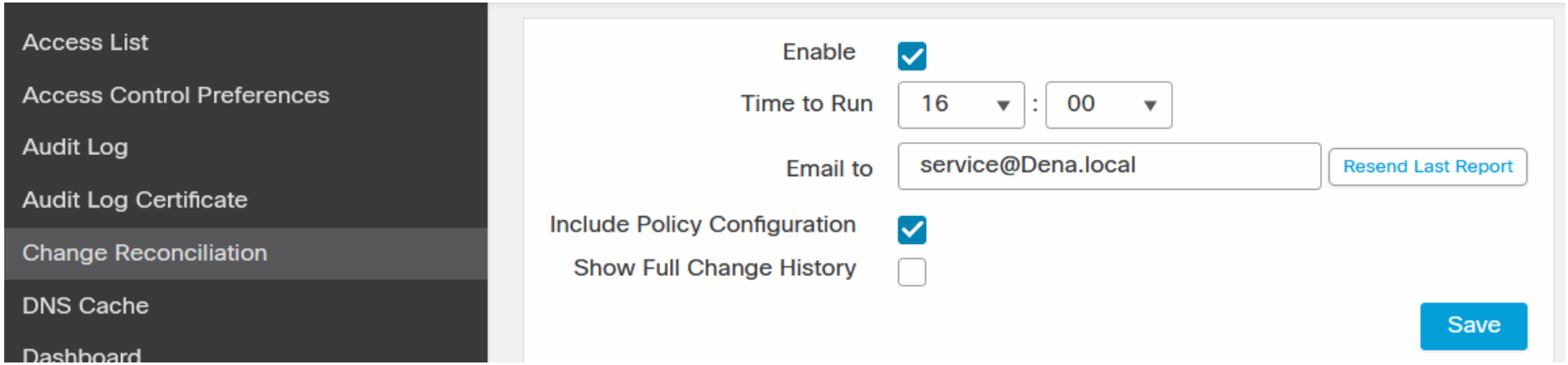
User configuration



MohsenKheradmand MK

Change Reconciliation

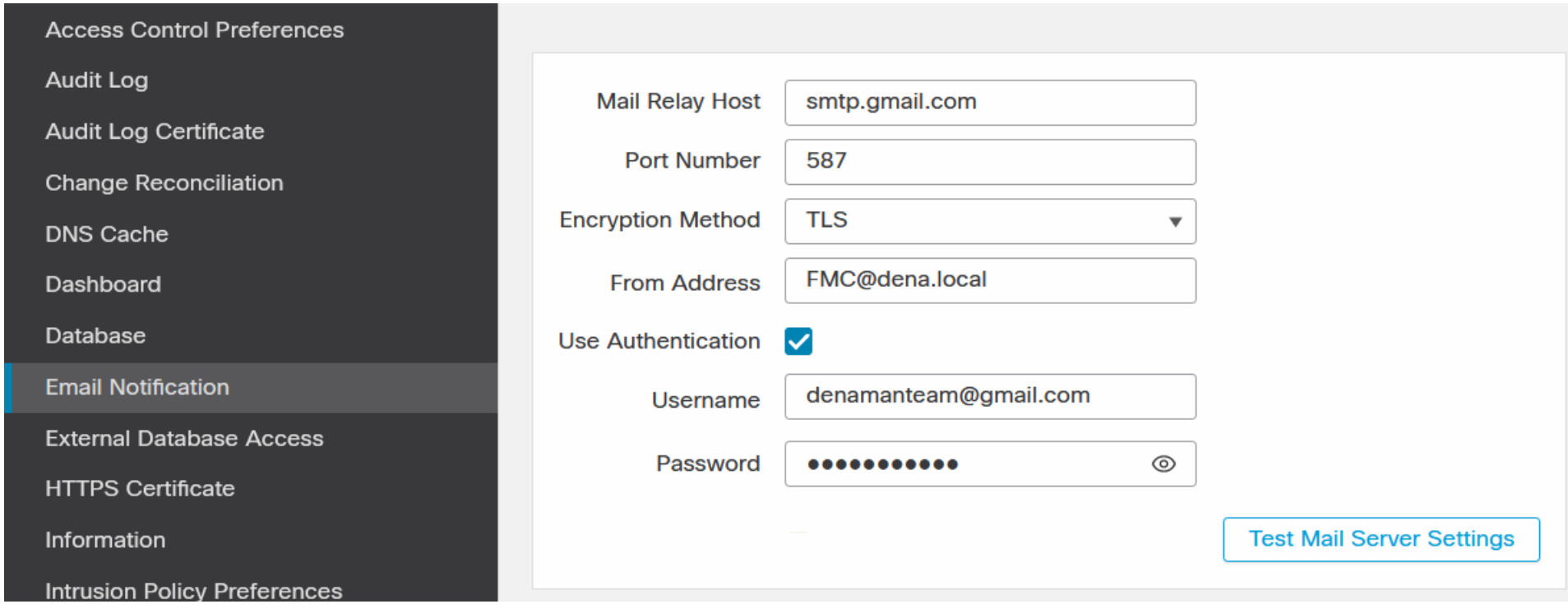
Send a daily Change Reconciliation report with any configuration changes to the FMC in the previous 24 hours



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

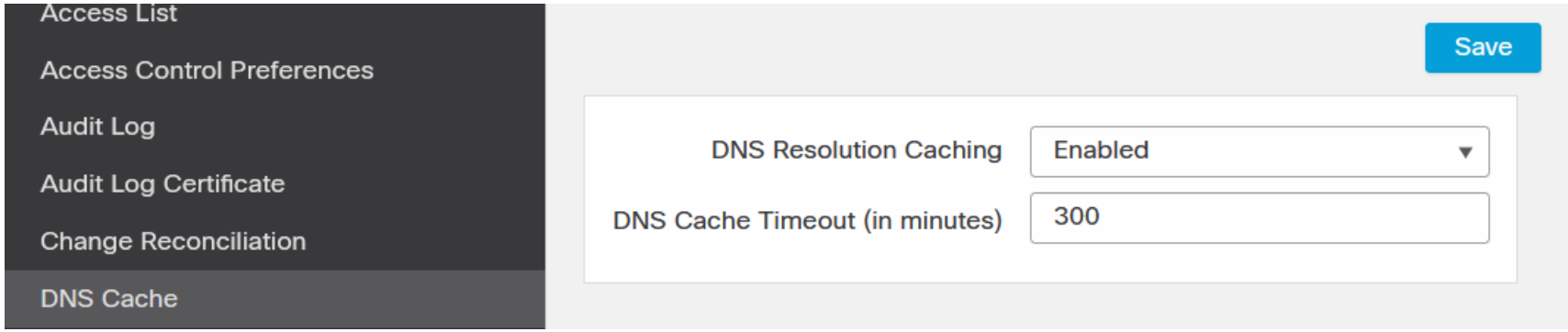
Email Notification

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



DNS Cache

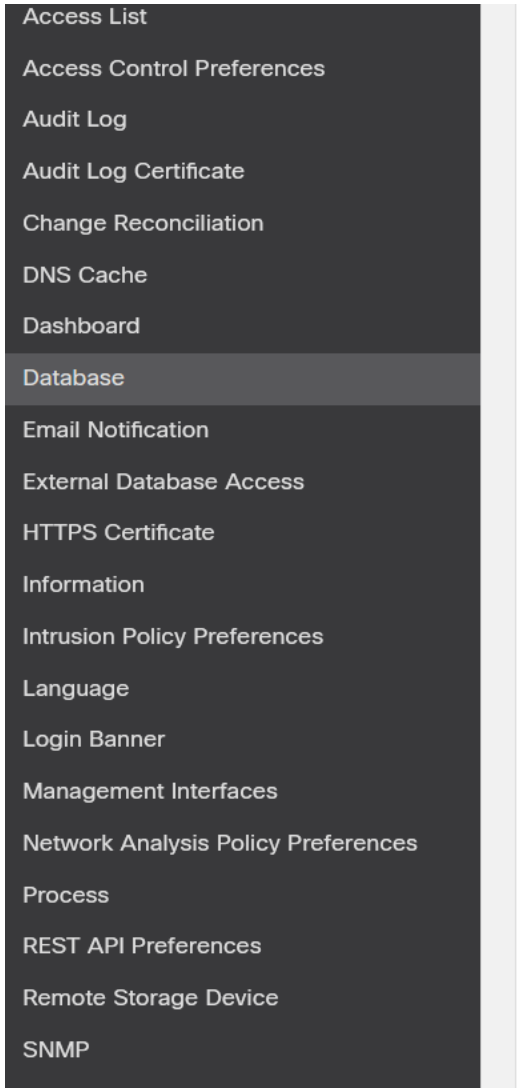
The length of time hostnames will be cached within the UI

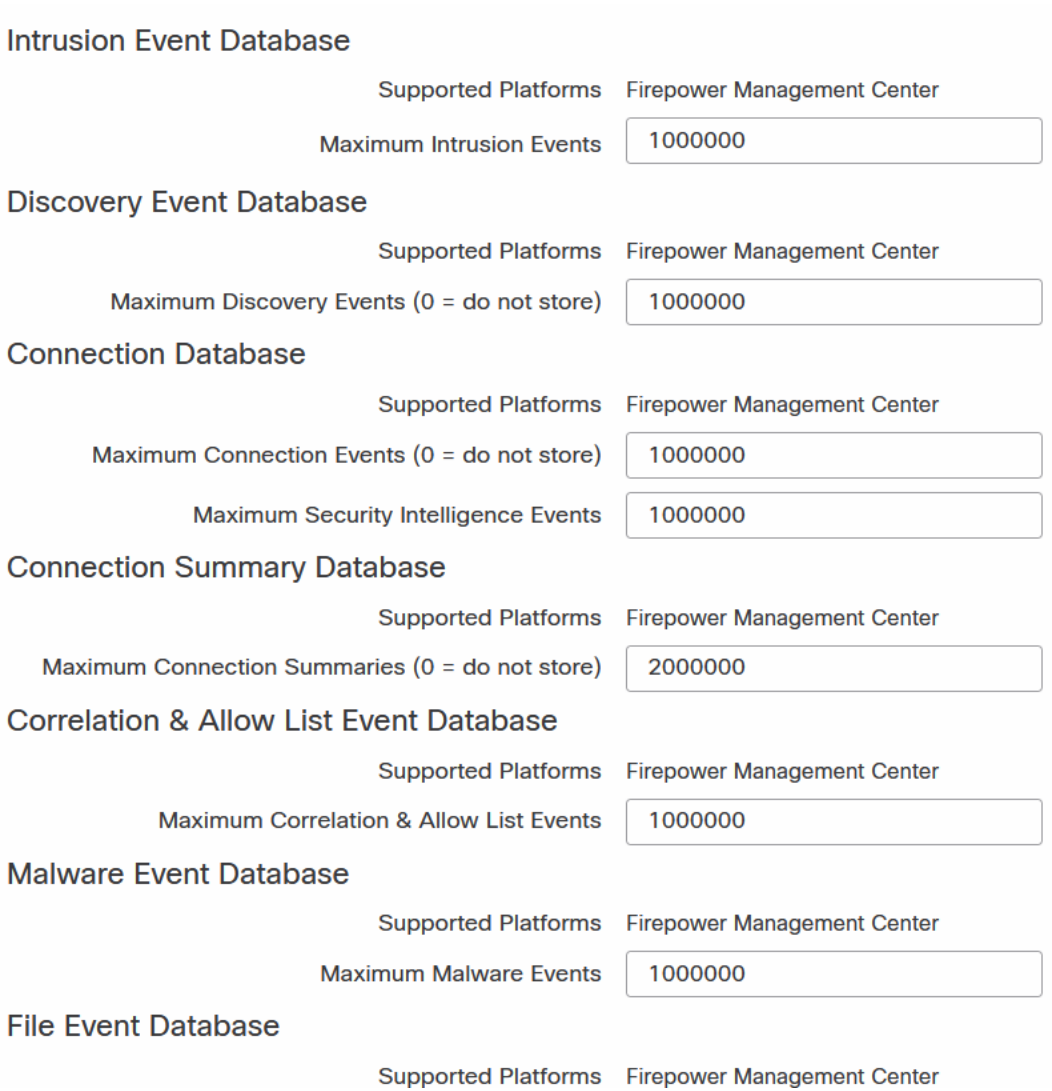


This prevents the FMC from constantly performing DNS lookups every time you load an event view page

Database

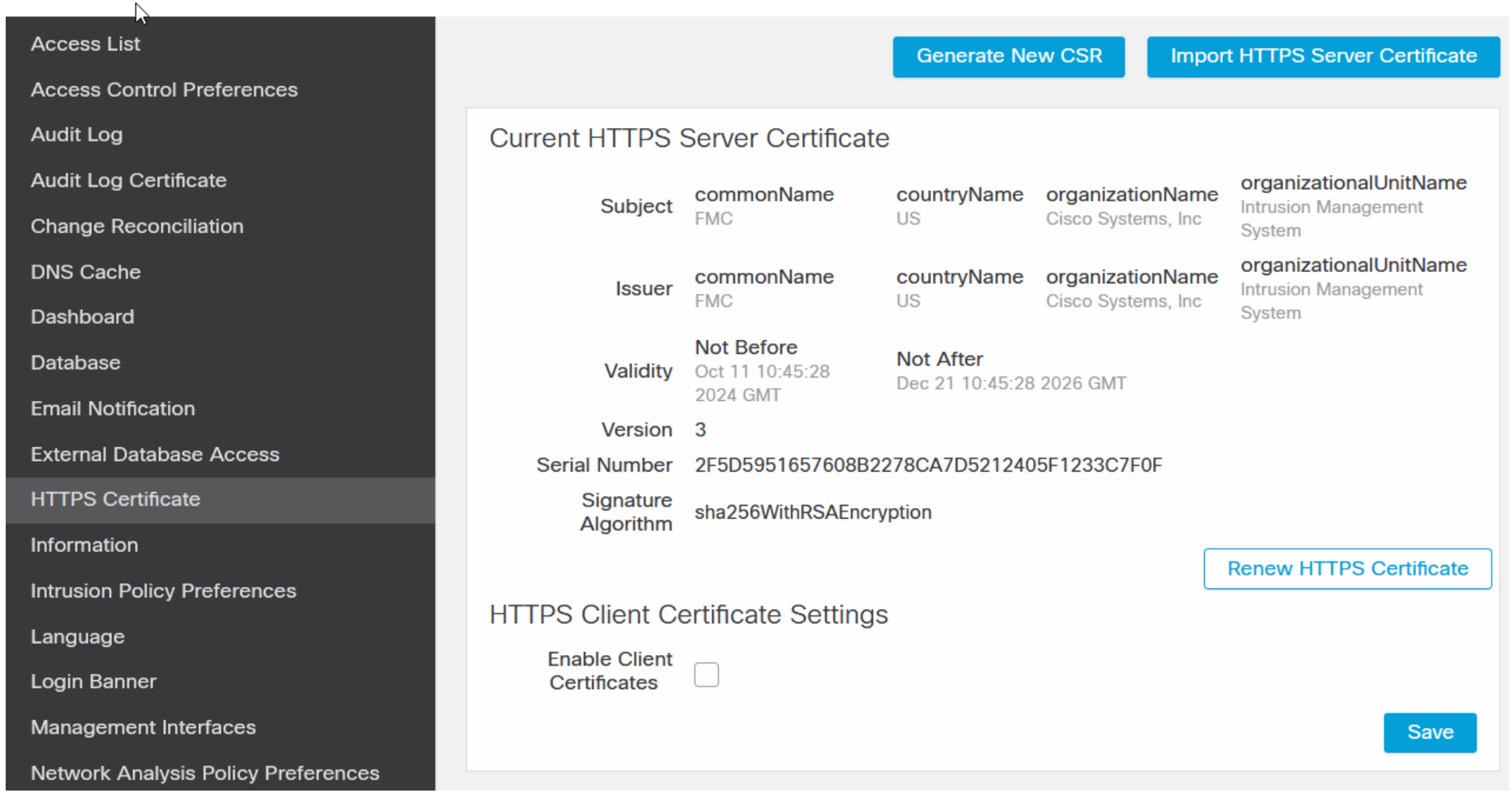
Configure the maximum size of the various databases within the FMC





HTTPS Certificate

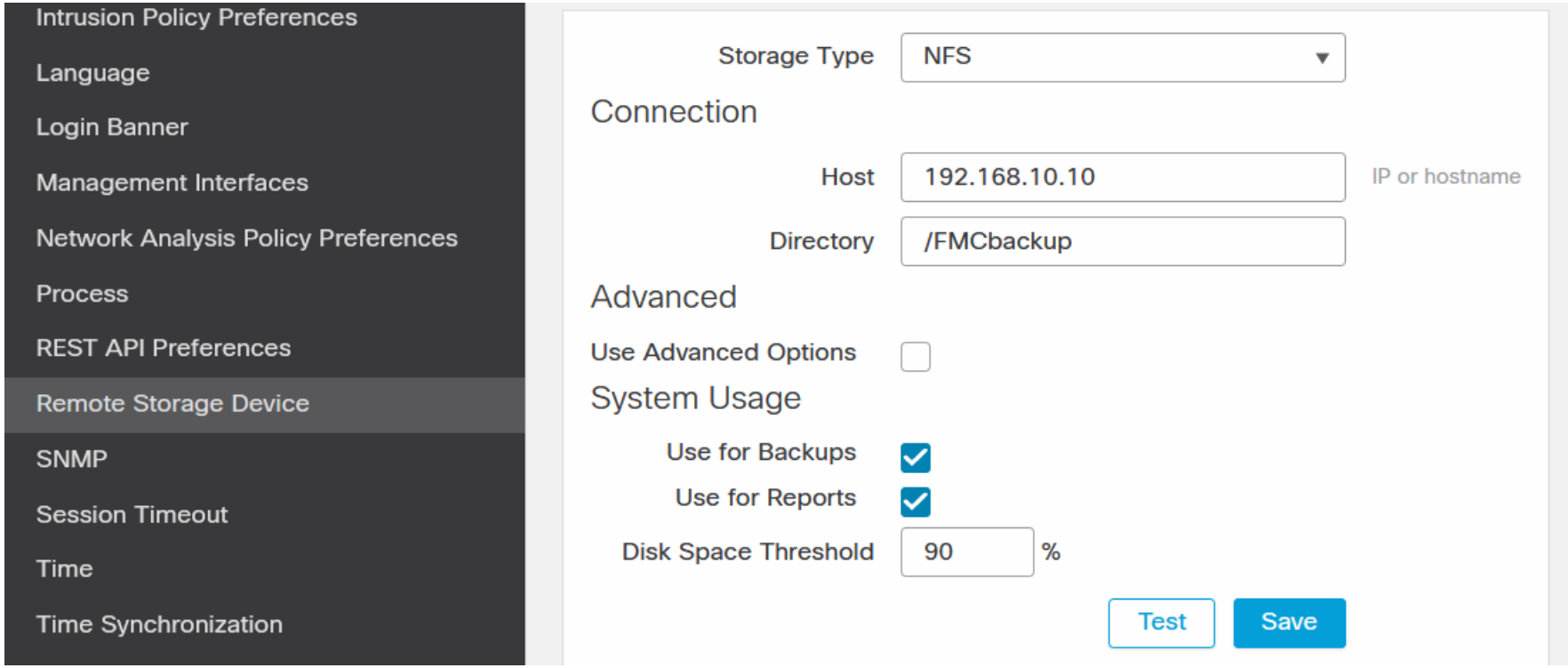
- Generate a new CSR to CA server , export it , Issue CSR to Cert and then import HTTPS Cert into FMC



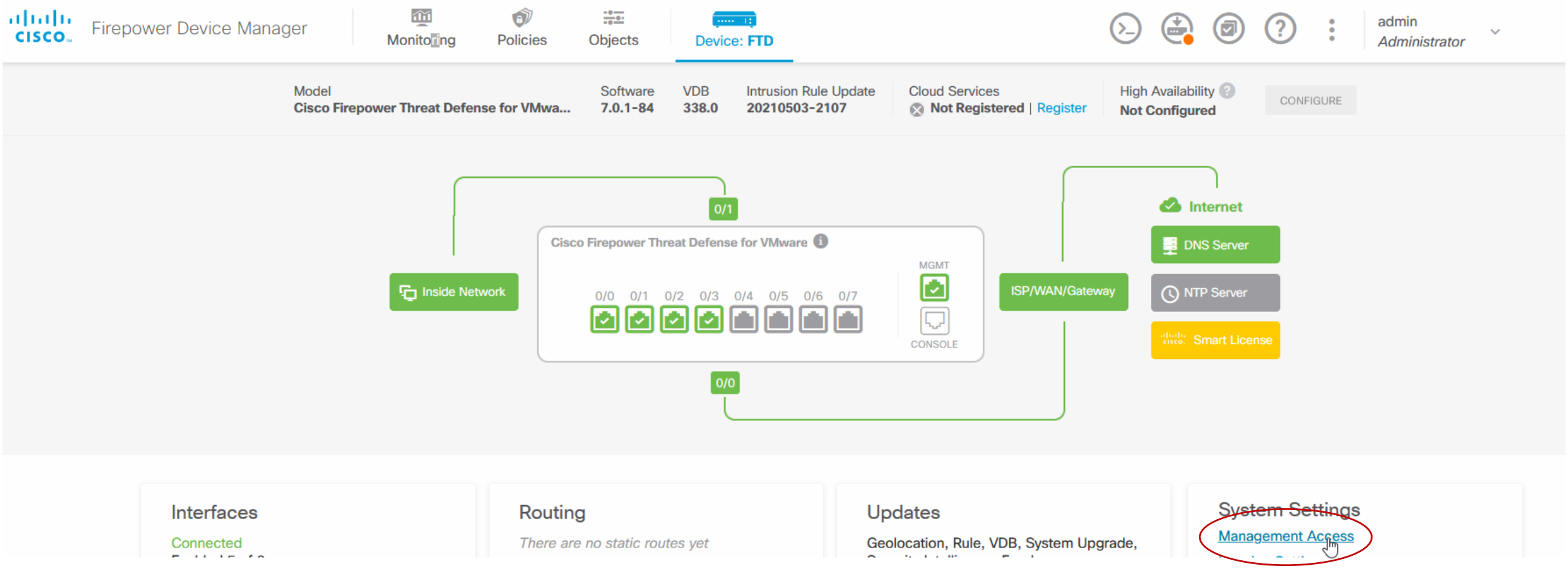
MohsenKheradmand MK

Remote Storage Device

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



FDM Management Access

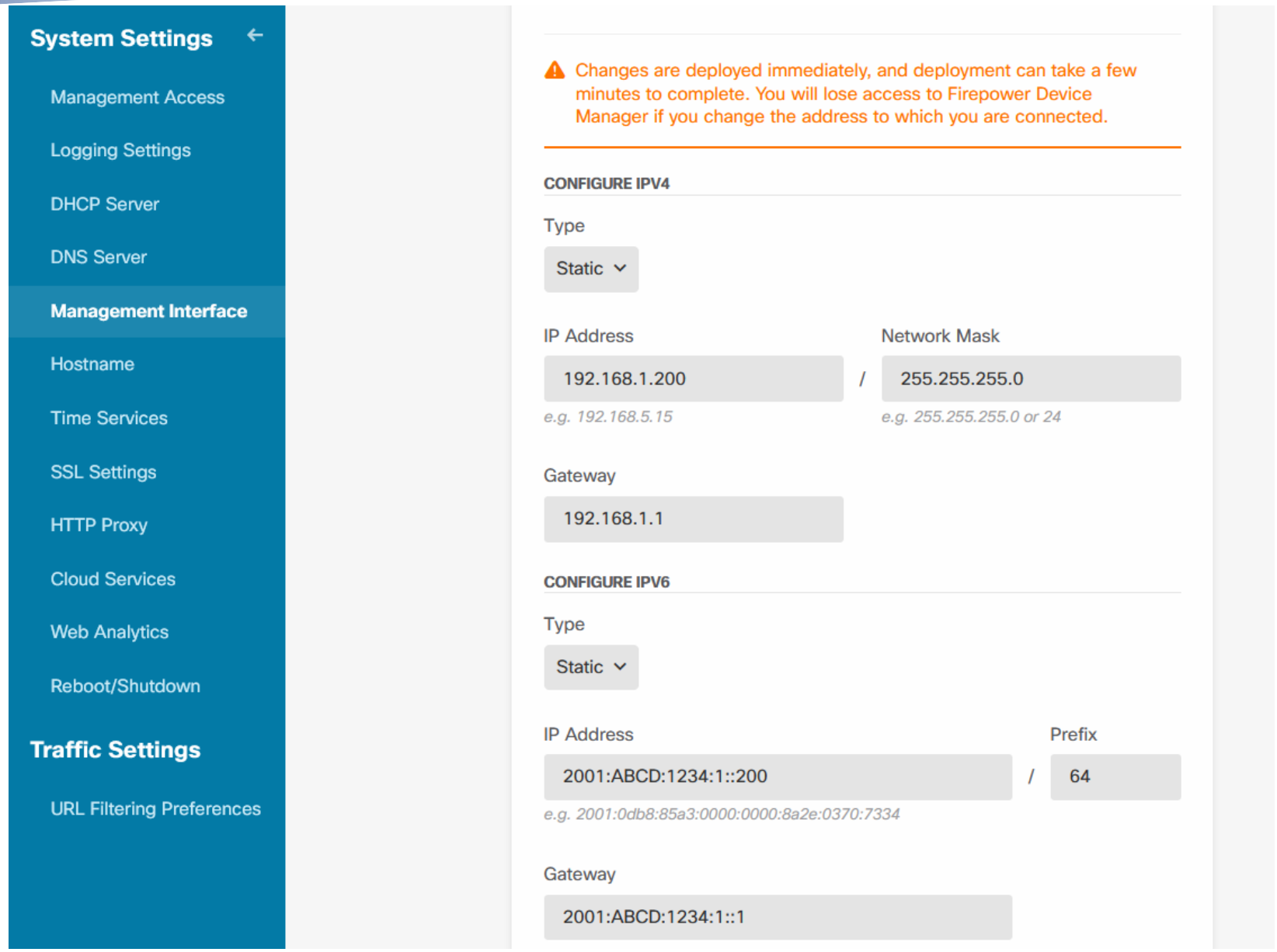


FDM system configuration

FDM Management Access

Management interface

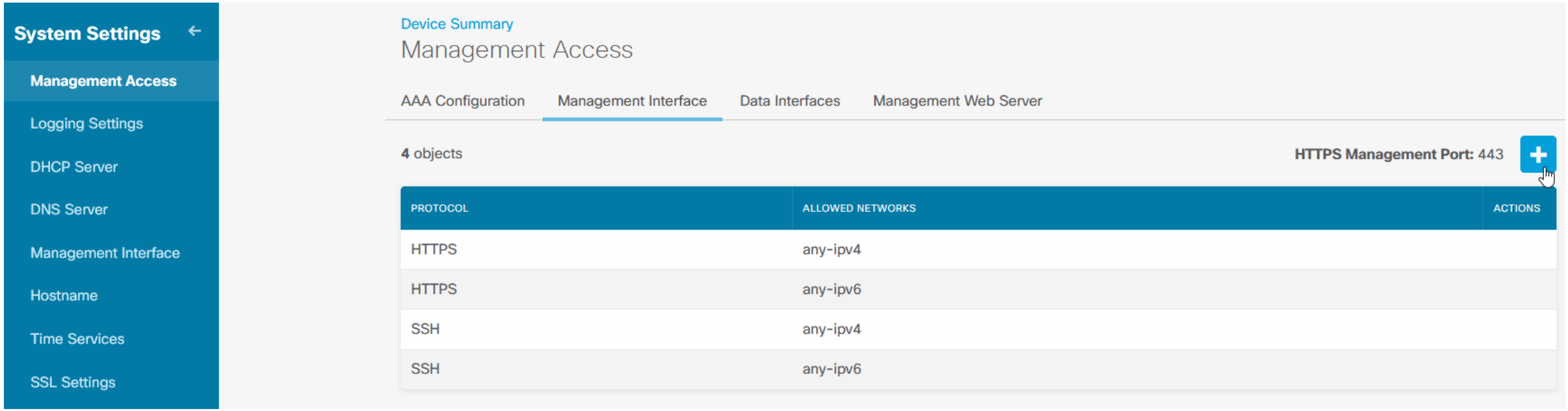
Configure IPv4 and IPV6 address



FDM Management Access

Management Access

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

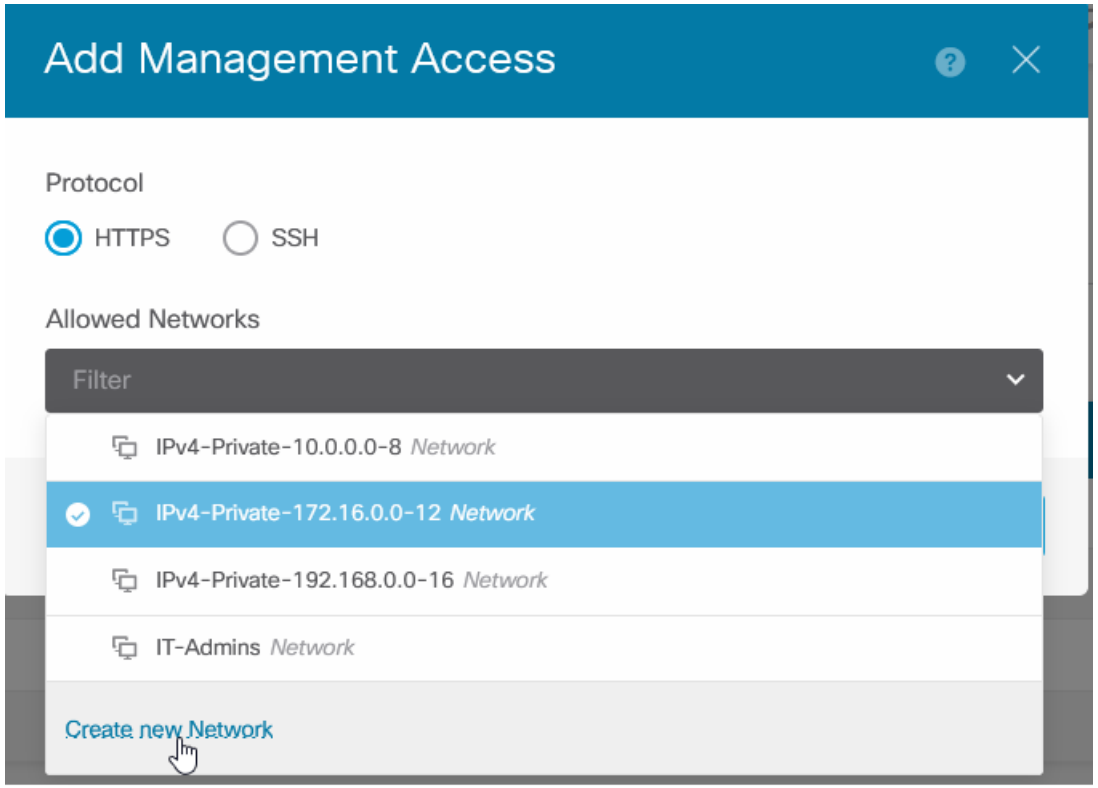


FDM Management Access

Management Access

3) Select protocol type to connect to FDM

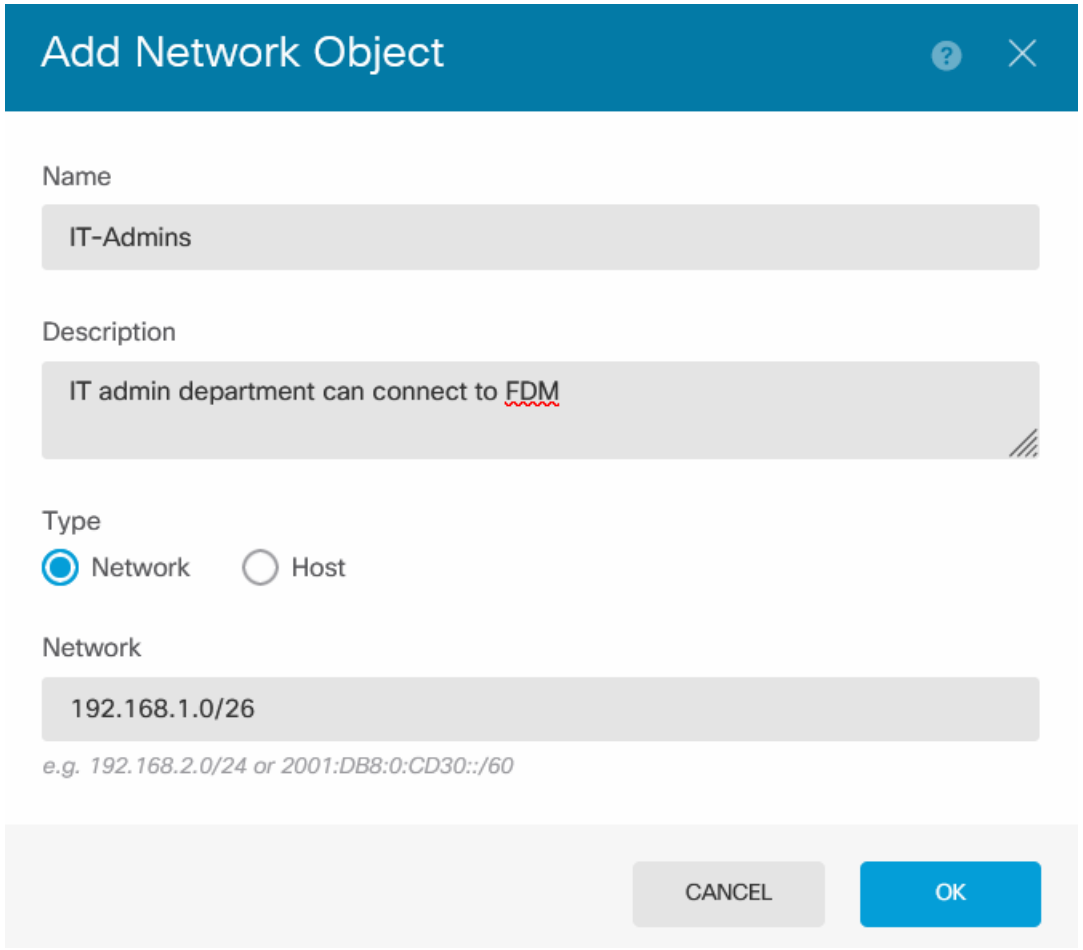
4) Then click “ Create new Network ”



FDM Management Access

Management Access

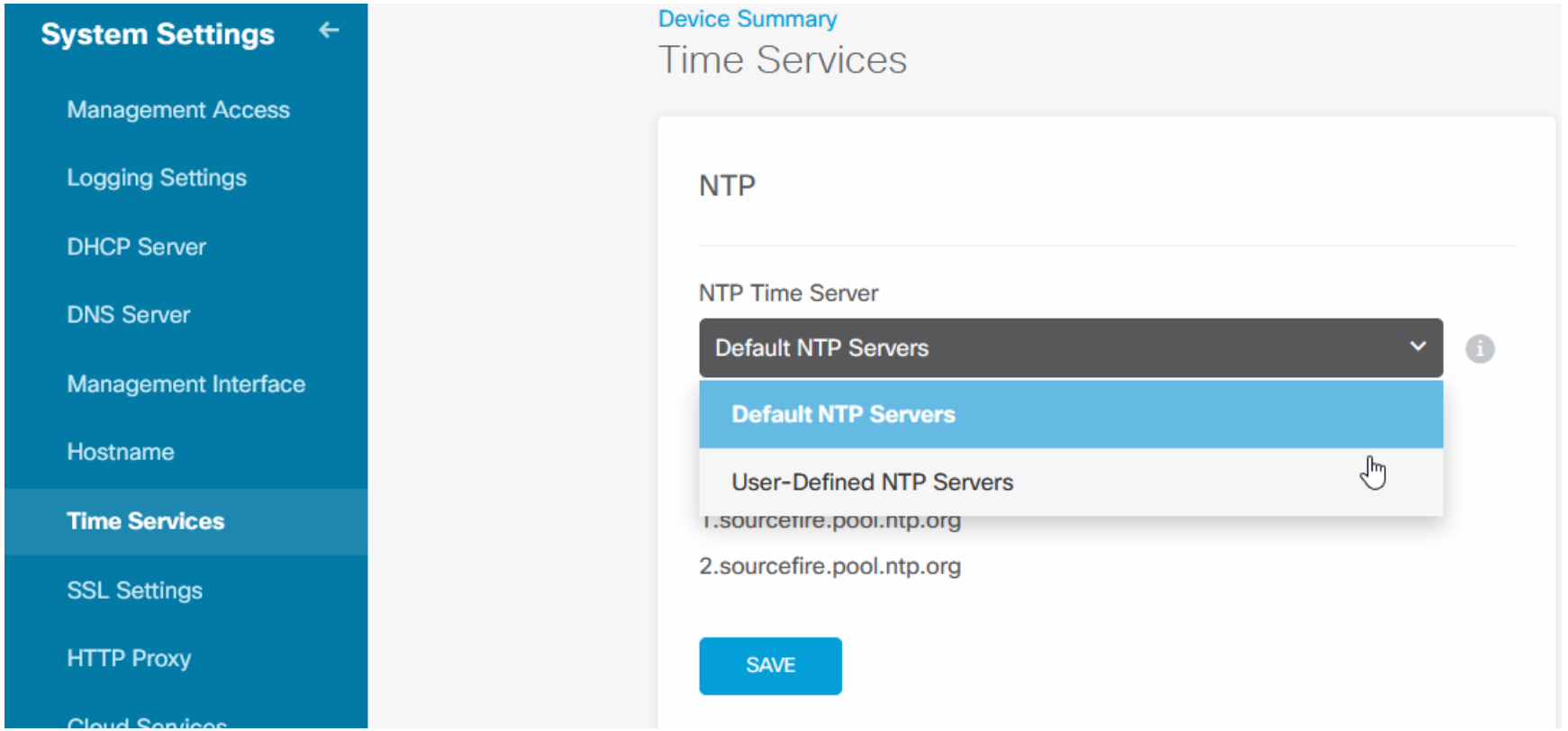
- Type a name for new group/client
- Description (optional)
- Type : network address or single host
- Network : IPv4 or IPv6 address of client/group



FDM Management Access

Time service

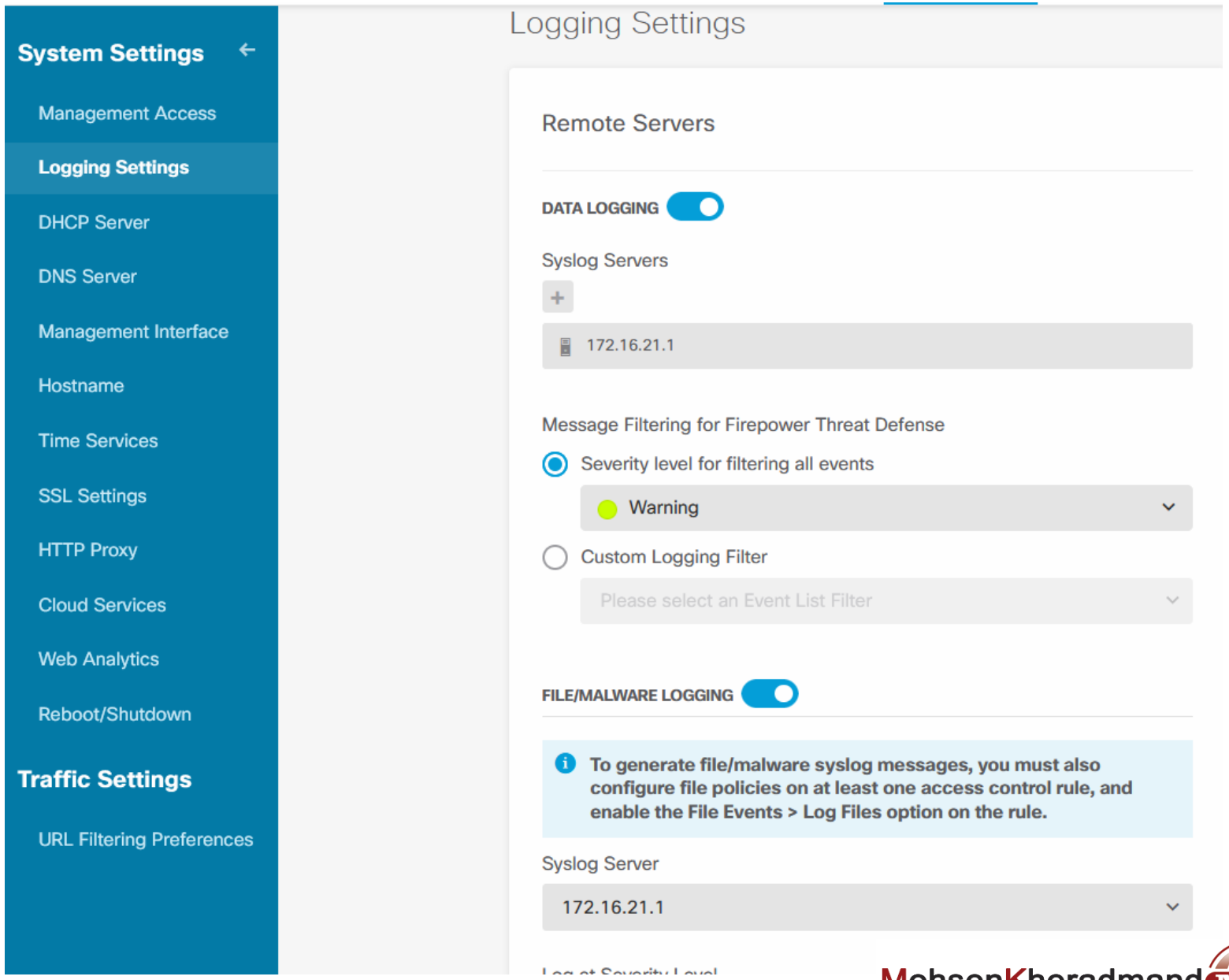
- Configure NTP servers



FDM Management Access

Logging setting

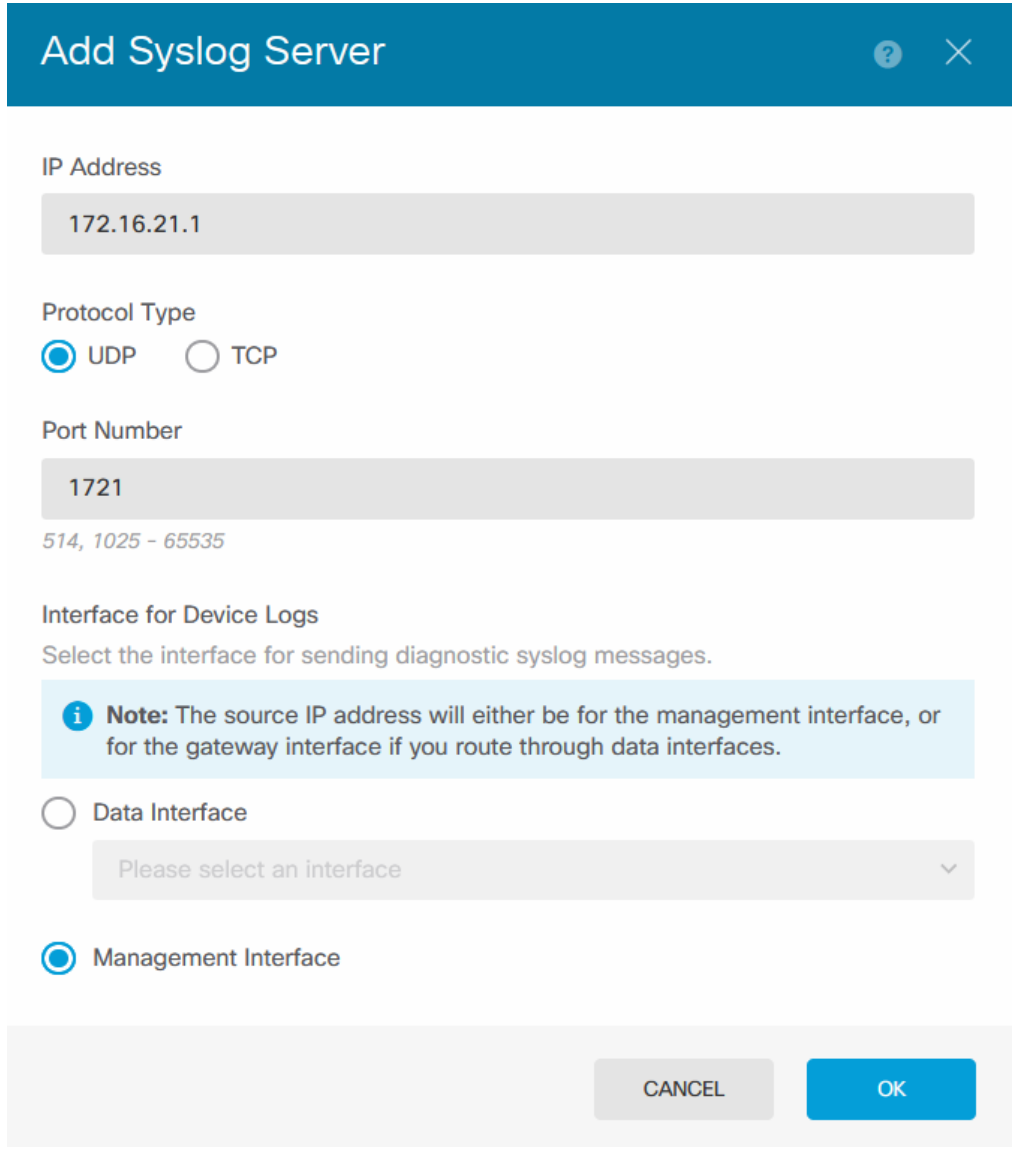
- Enable DATA LOGGING
- Click + to add Syslog server
- Select severity of events to send logs



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



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