Securing Networks with

Cisco FTD

Chapter 19

System Logging (Syslog)

Mohsen Kheradmand

Syslog

- You can use logging for real-time alerting as well as for auditing purposes
- The Internet Engineering Task Force (IETF) standardizes system logging (syslog) in RFC 5424
- Secure Firewall supports sending syslog messages to third-party syslog servers and SIEM tools
- The FMC or the FTD can send logs to the syslog server separately , but it’s better to choose one of these
- Syslog messages can be sent over TCP or UDP (TCP is more reliable but has more overhead due to the multiple connections)

RFC	Description
RFC 5424	The Syslog Protocol
RFC 5426	Transmission of Syslog Messages over UDP
RFC 6587	Transmission of Syslog Messages over TCP
RFC 5425	Transport Layer Security (TLS) Transport Mapping for Syslog

Syslog Security Levels

- Each syslog message is associated with a severity level
- A severity level indicates the significance of a message.

Severity Level (0–7)	Messages That Describe…
EMERG	An emergency condition where the system is unusable
ALERT	A condition where an action must be taken immediately to fix the issue
CRIT	A critical condition that indicates a failure in the primary system
ERR	An error condition
WARNING NOTICE	A warning condition
INFO	A condition that does not indicate an error but may require special attention
DEBUG	Debug-level information to help the developers of an application or system

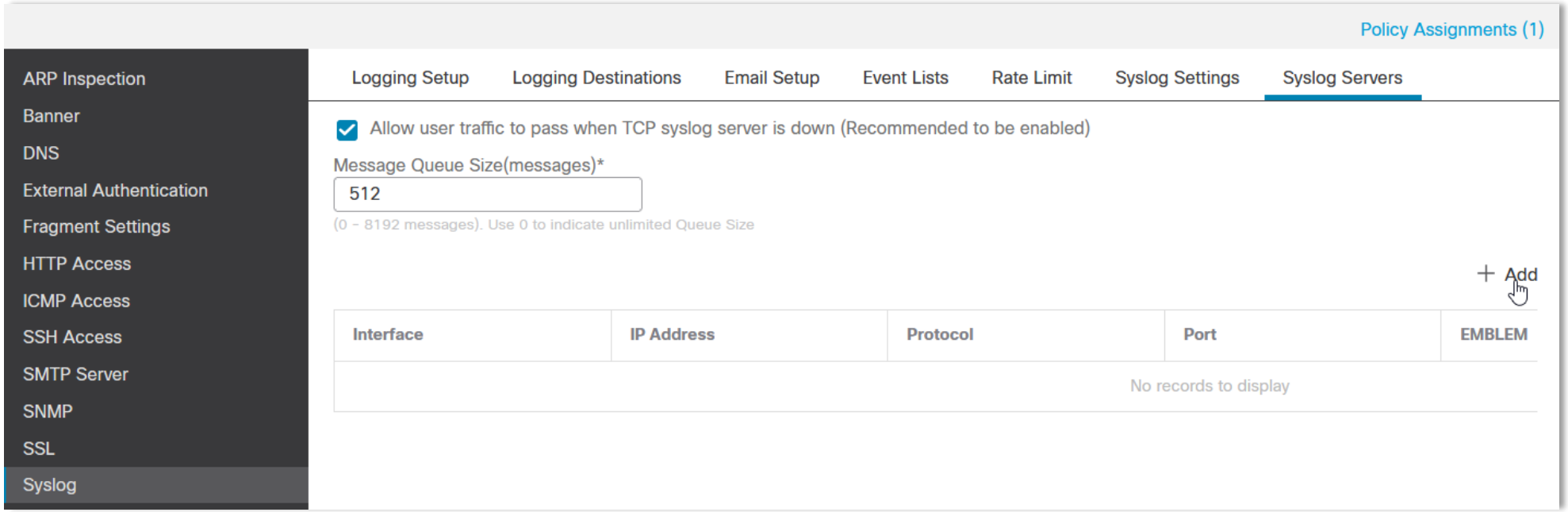
Facility of Syslog message

- The IETF uses the term facility to refer to various subsystems

KERN : Kernel
USER : User-level process
MAIL : Mail system
DAEMON : System daemon
AUTH : Security/authentication subsystem
SYSLOG : System logging daemon (syslogd)
LPR : Line printer subsystem
NEWS : Network news subsystem
UUCP : Unix-to-Unix copy subsystem
CRON : Clock/scheduling daemon (Used by Syslog server running on a Linux OS)
AUTHPRIV : Security/authentication system
FTP : FTP daemon
NTP : NTP subsystem
AUDIT : Audit subsystem (Security log audit)
ALERT : Alerting subsystem (Console)
CLOCK : Clock/scheduling daemon (Used by Syslog server running on Windows OS)
LOCAL0–LOCAL7 : Locally defined facilities

Best Practices for Logging

- If your syslog server uses TCP, enable the **Allow User Traffic to Pass When TCP Syslog Server Is Down** option.
- It enables the traffic flow to continue in case of any issues with the syslog server

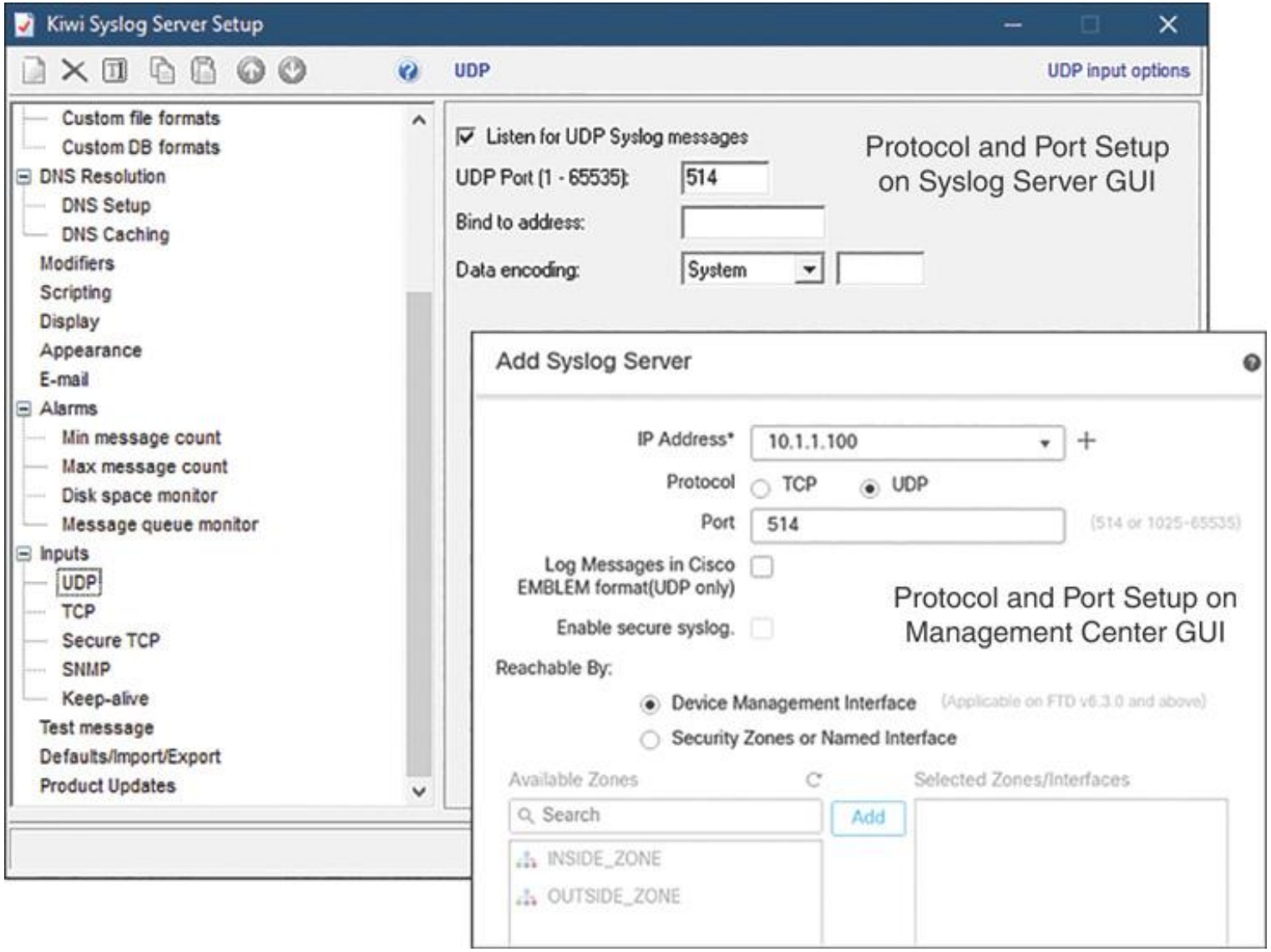


- To prevent a syslog server from crashing, you can enable rate limiting for certain types of syslog messages
- Syslog over TCP can introduce overhead in a large deployment. In this case , syslog over UDP can improve performance.

Syslog configuration

- You can configure a Syslog server like Kiwi and configure address and port on it

- The default port for syslog servers is UDP port **514** or TCP port **1470**



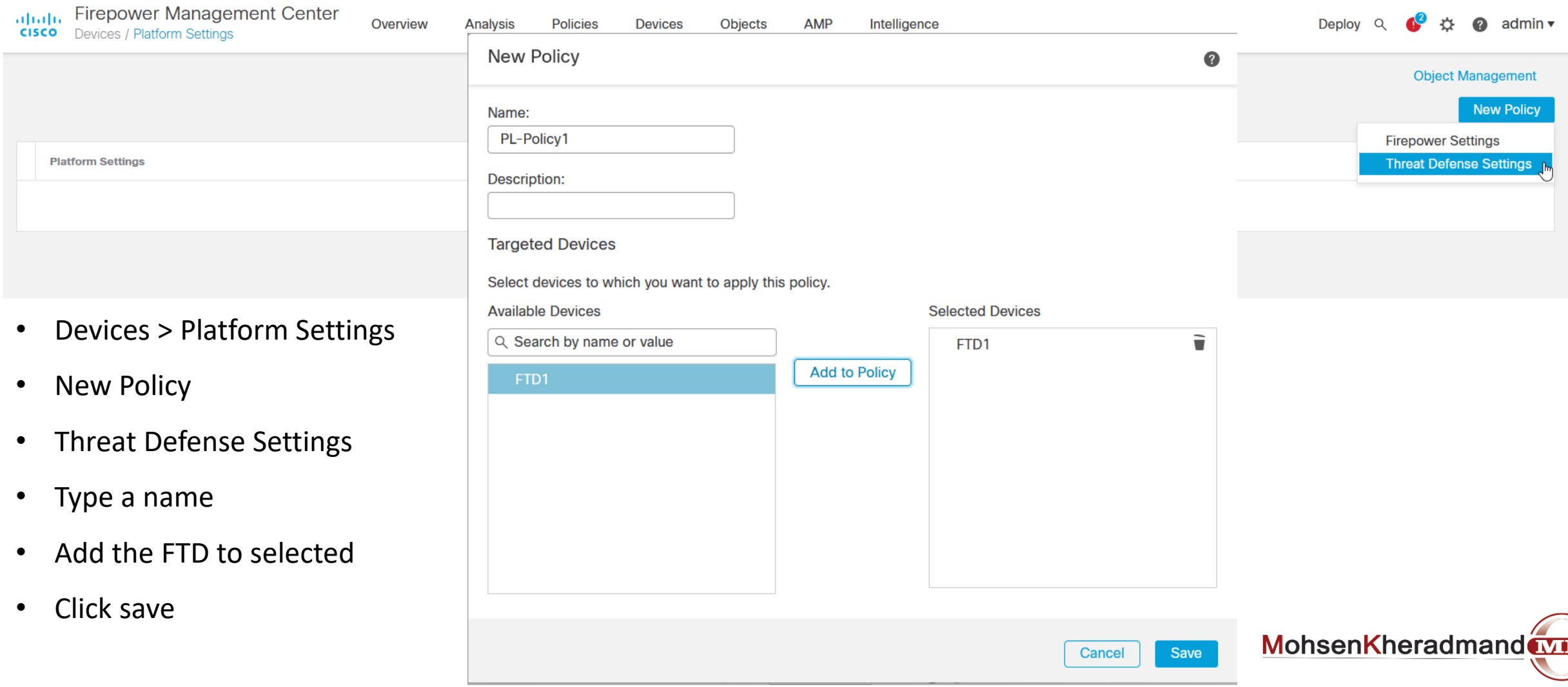
Sending Syslog from Threat Defense

Platform settings

- By using the platform settings policy, you can deploy different logging configurations to different threat defense devices
- The platform settings policy allows you to configure many device-specific options in one place and then deploy them to one or more threat defense devices as needed.
  - ❑ For example:
    - You can add a custom banner to appear during a threat defense login
    - Allow the hosts that can communicate with a threat defense over SSH, HTTPS, and ICMP protocols
    - Define how the threat defense device will synchronize time with its management center or an NTP server
    - Provide health monitoring status over the simple network management protocol (SNMP)
    - Send security events and system messages to an external syslog server
    - And other configurations and settings

Sending Syslog from Threat Defense

Platform settings

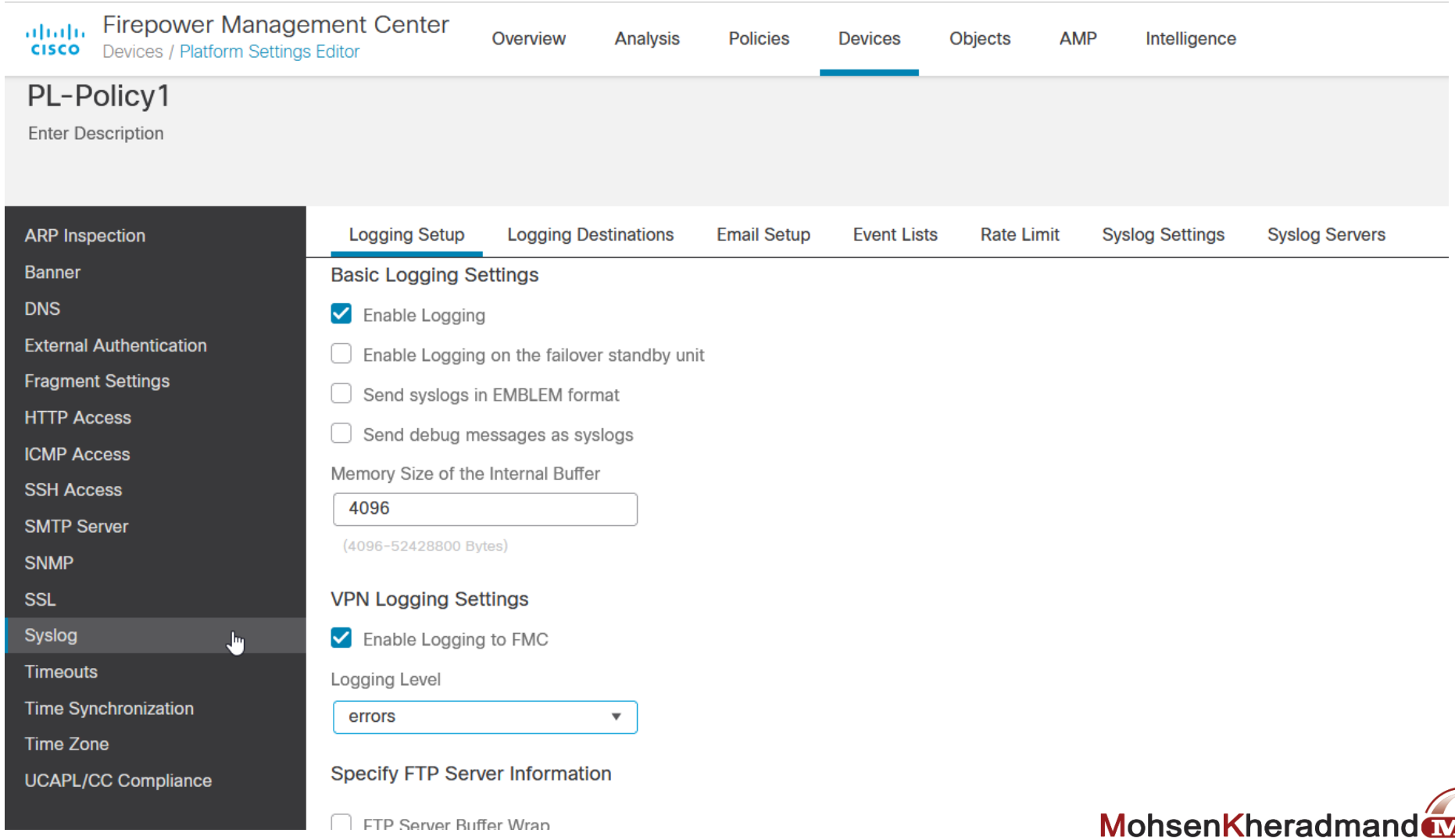


- Devices > Platform Settings
- New Policy
- Threat Defense Settings
- Type a name
- Add the FTD to selected
- Click save

MohsenKheradmand MK

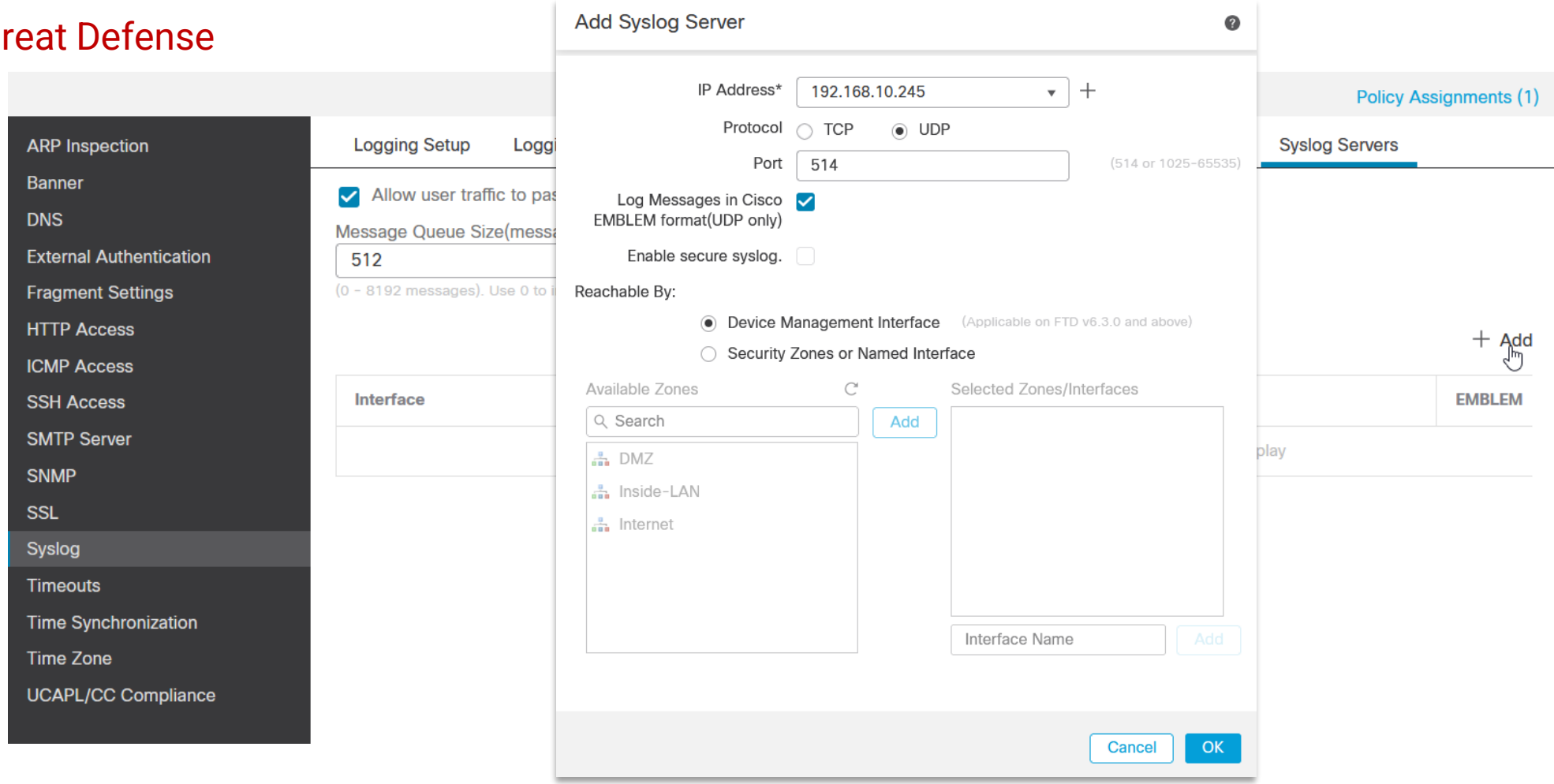
Sending Syslog from Threat Defense

- Click syslog
- Enable logging



Sending Syslog from Threat Defense

- Click Syslog Servers tab
- Click Add



- Enter the syslog server IP address, transport protocol, and port number.
- If syslog server is in management network select Device Management Interface
- If not , select other source interface to send logs through that
- Click Ok

Enable Logging on Access Control Policy

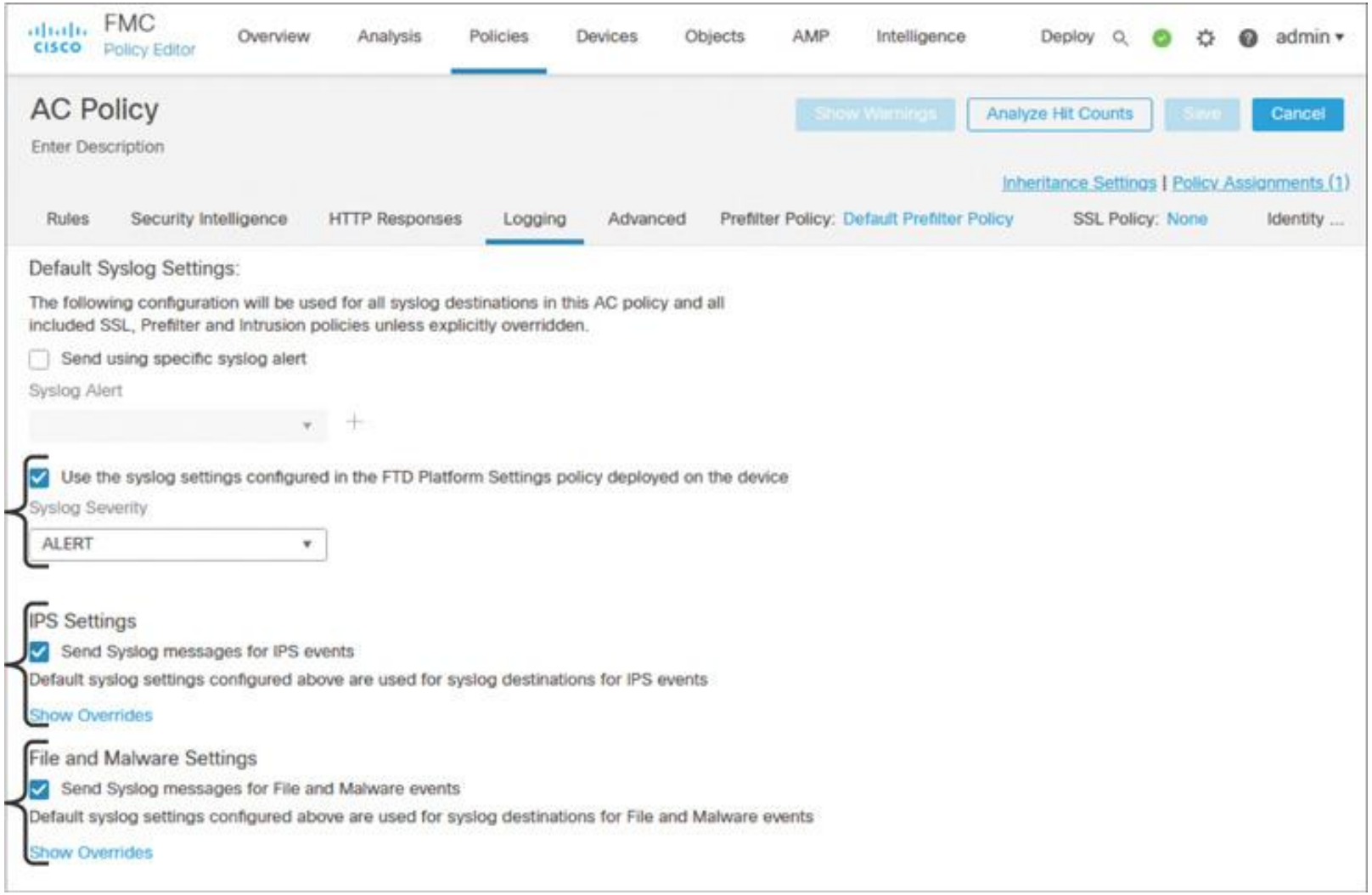
Policies

Access Control Policy

Select the policy

Click Logging tab

Select these items as you see :



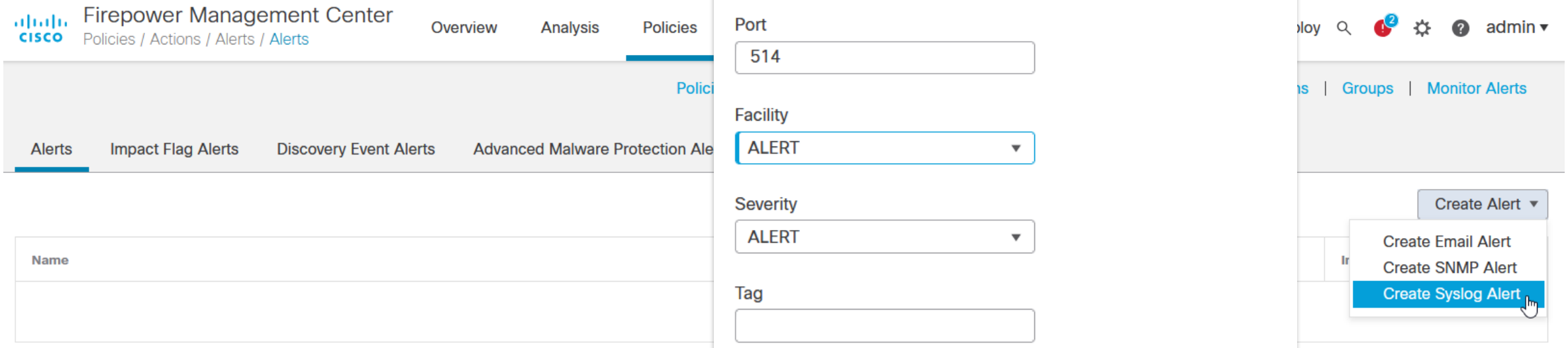
Sending Syslog from Management Center

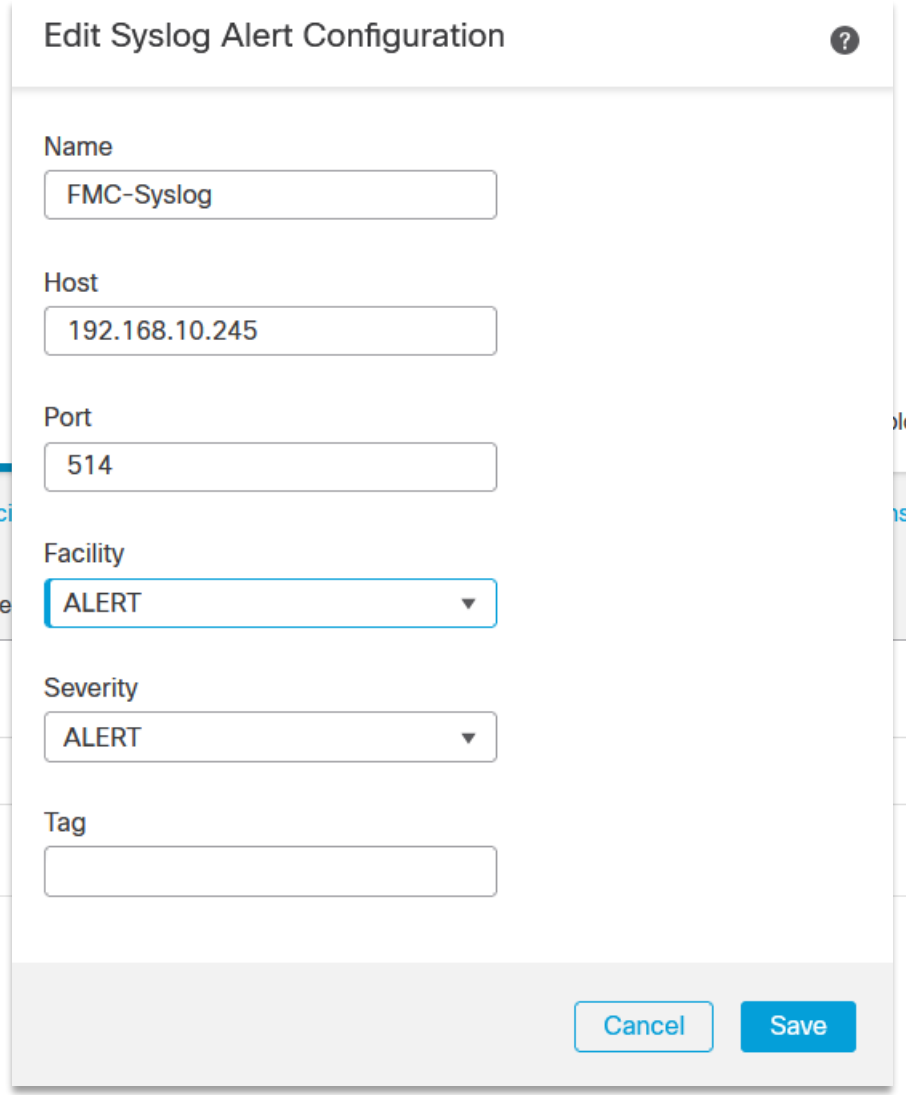
Create Syslog Alerts

Policies > Actions > Alert

Create Alert

Create Syslog Alert





Enter a name for this Alert

Enter Syslog server Address

Select Port , Facility and Severity and the click Ok

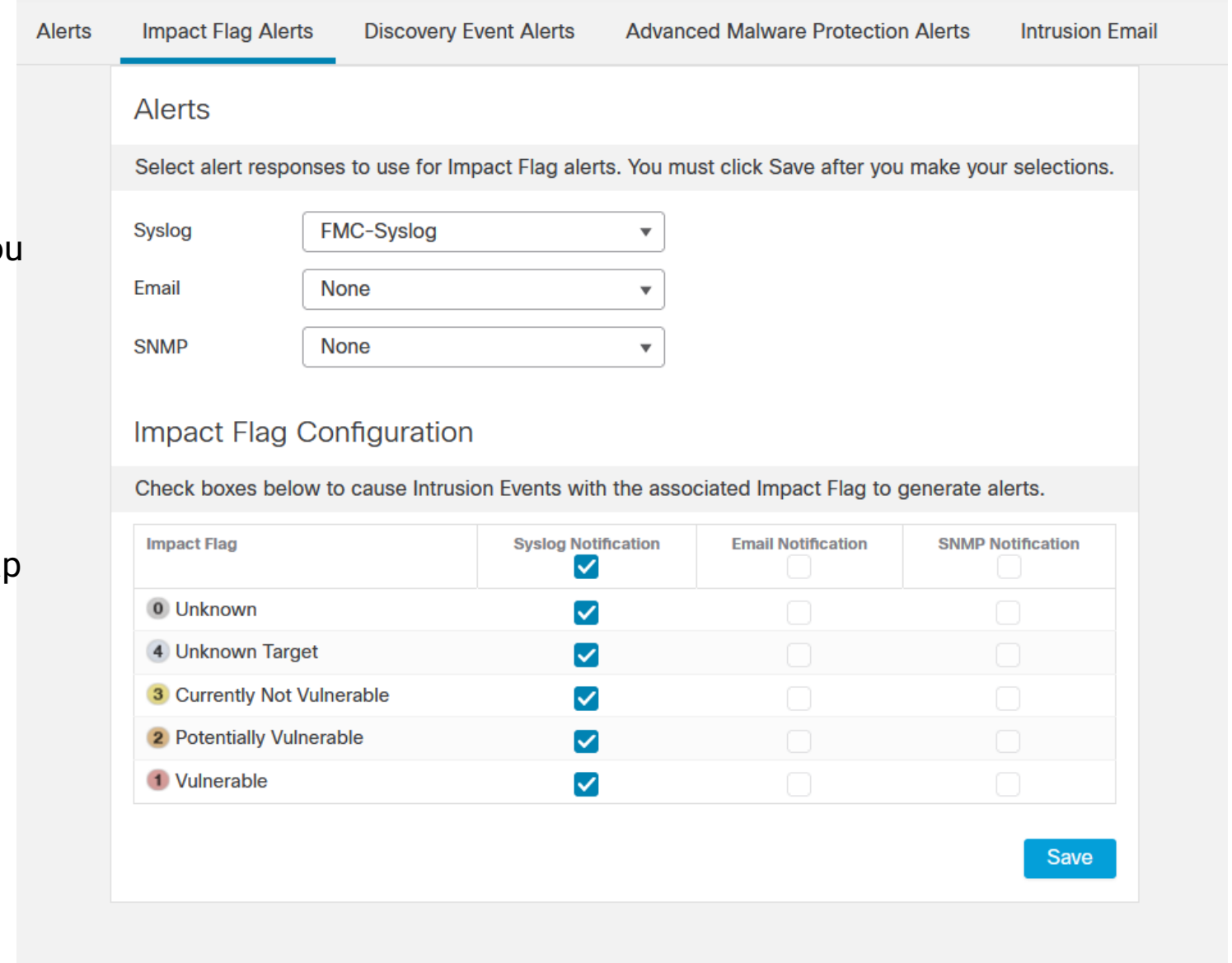
MohsenKheradmand

Sending Syslog from Management Center

Impact Flag Alerts

- You can choose the types of events for which you want to receive alerts on the syslog server

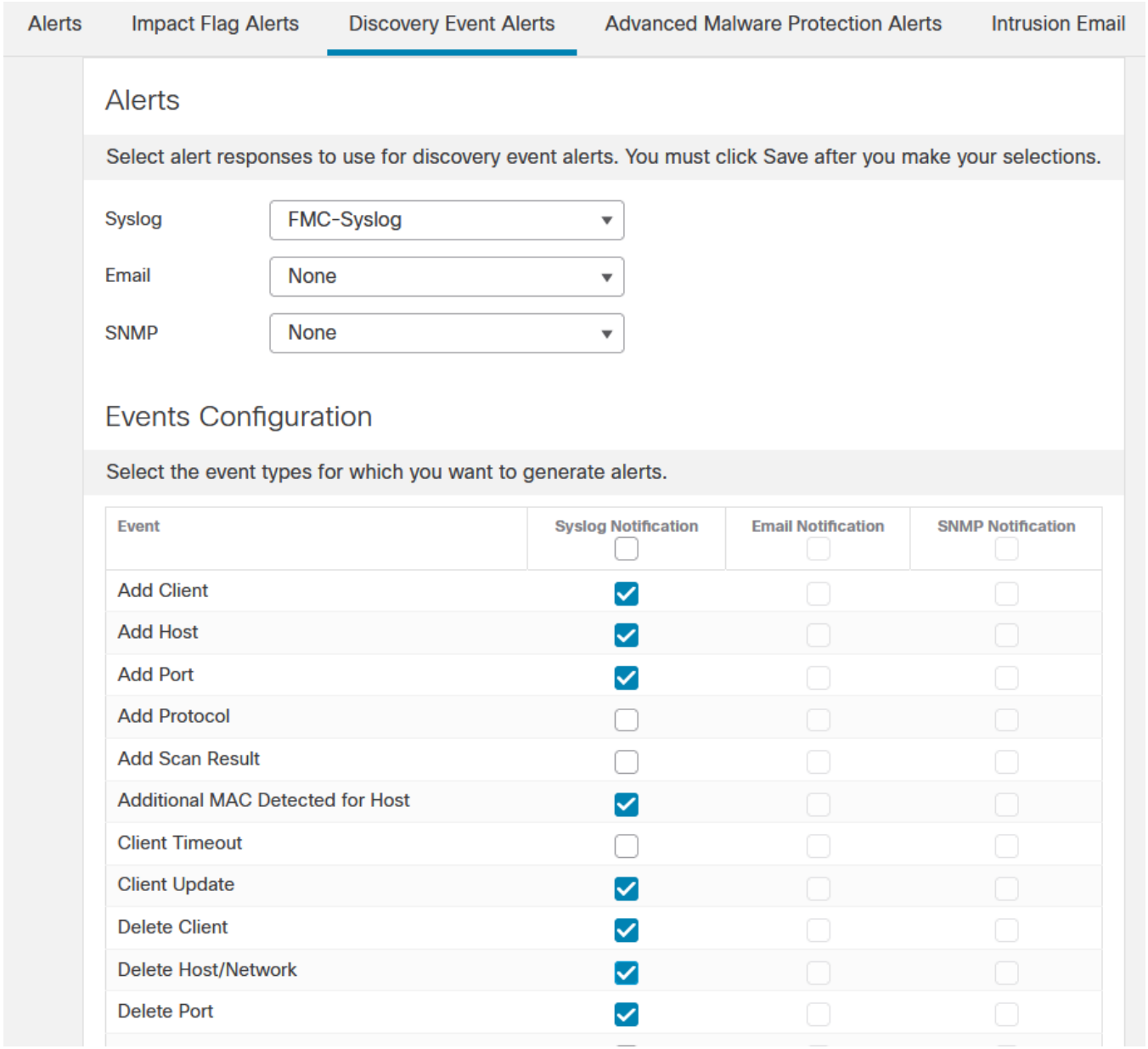
- Select Syslog Server
- Optional : select Email address to send Alerts
- Optional : configure SNMP to sent alerts as a Trap
- Select Impact Level to send Logs
- Click Save



Sending Syslog from Management Center

Discovery Event Alerts

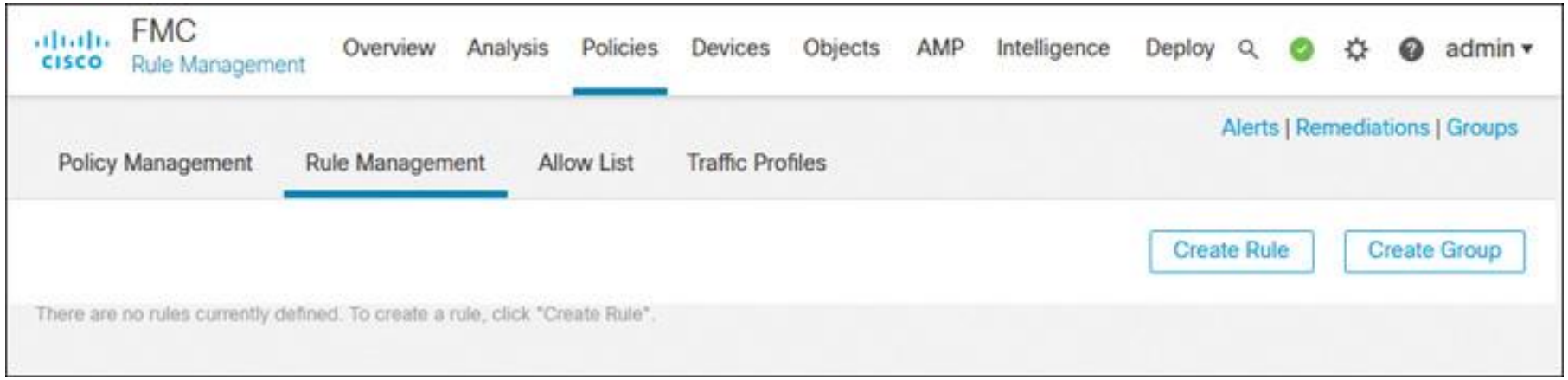
- To trigger these alerts, the FMC requires an active Network Discovery policy
- Select Syslog server , (Email or SNMP)
- Select event type for which to generate alerts
- Click Save



Correlate Events to Send Syslog Alerts

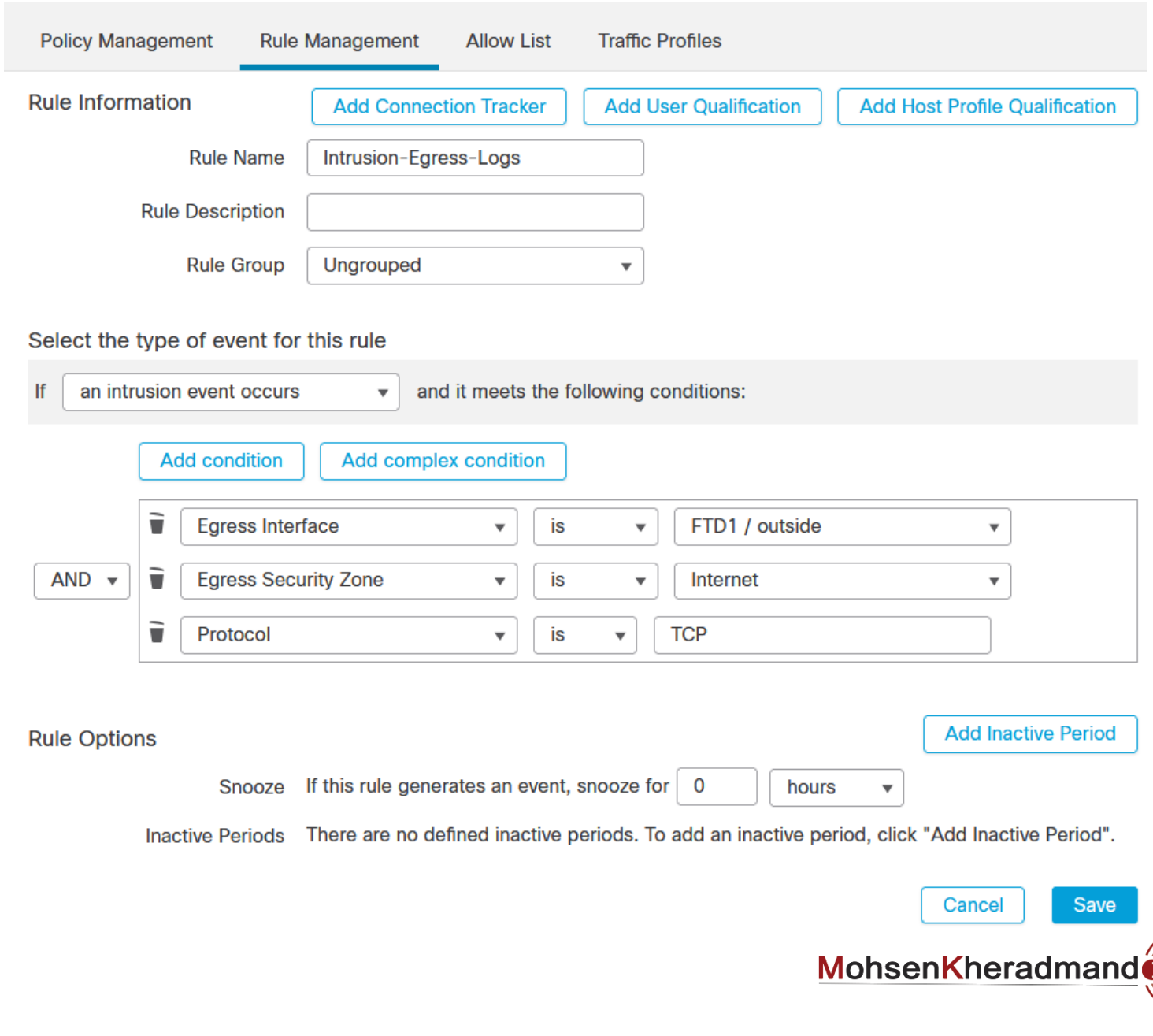
- Correlation policy: produce syslog events under the specific set of conditions in logging
- You can create correlation rules based on discovery events, intrusion events, file events, connection events, and a variety of other conditions

1) Create a rule :
   - ➢ Policies > Correlation
   - ➢ Rule Management tab
   - ➢ Create Rule



Correlate Events to Send Syslog Alerts

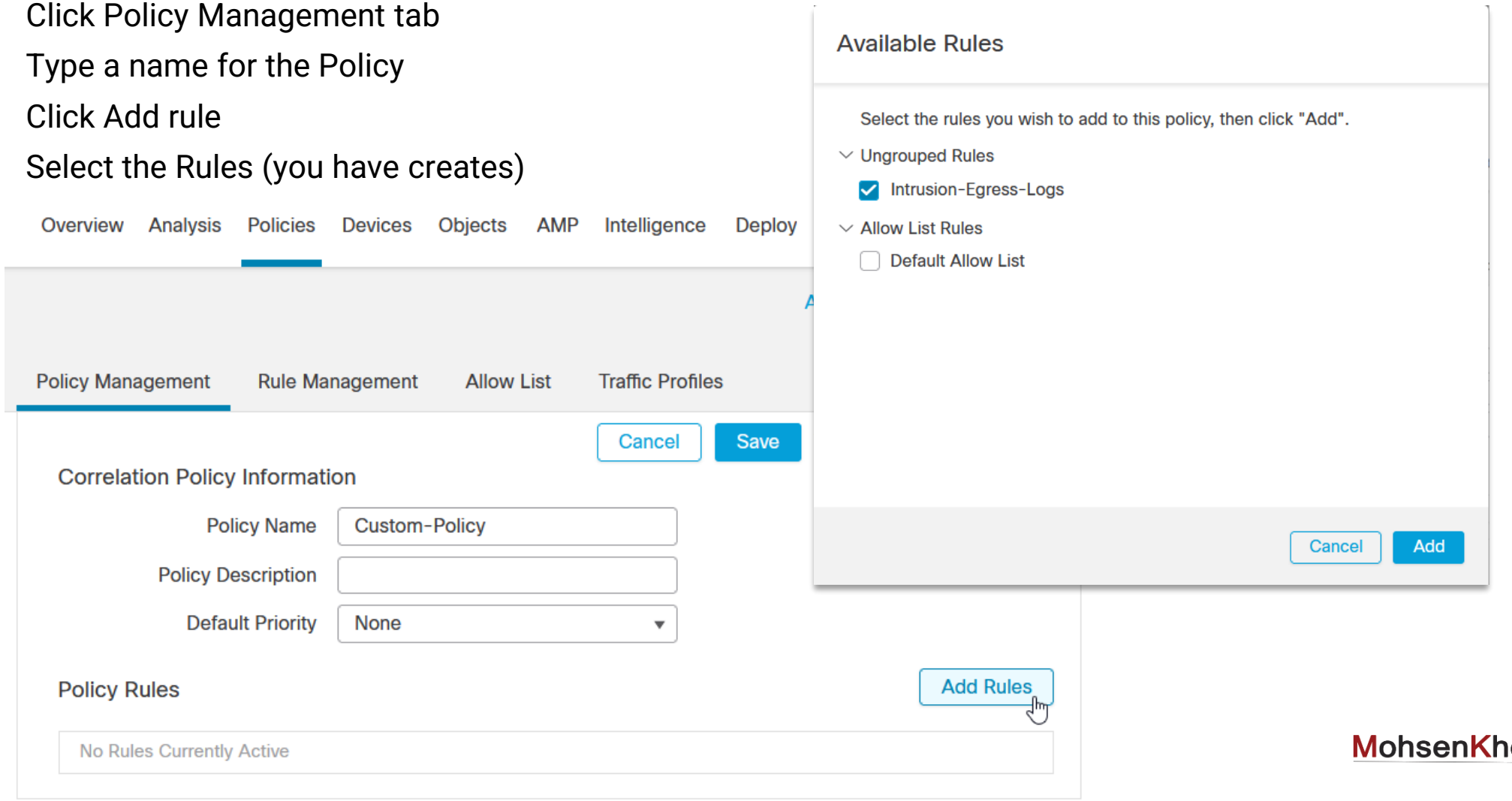
- Enter a name for rule
- Optional : description
- Optional : Rule group
- Select the type of event
- Click Add Condition
- Add your conditions to take effect
- Click Save



MohsenKheradmand MK

Correlate Events to Send Syslog Alerts

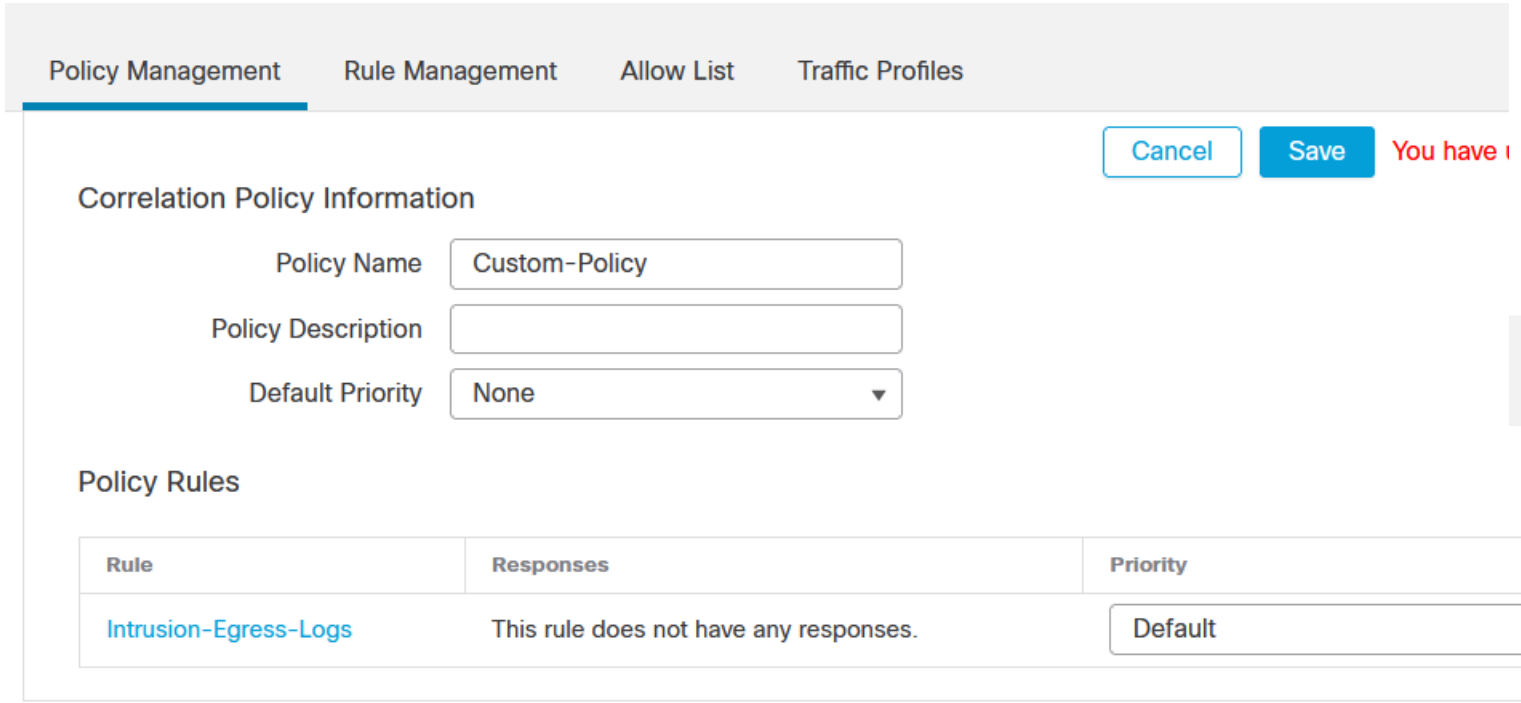
2) Create a Policy
   - Click Policy Management tab
   - Type a name for the Policy
   - Click Add rule
   - Select the Rules (you have creates)

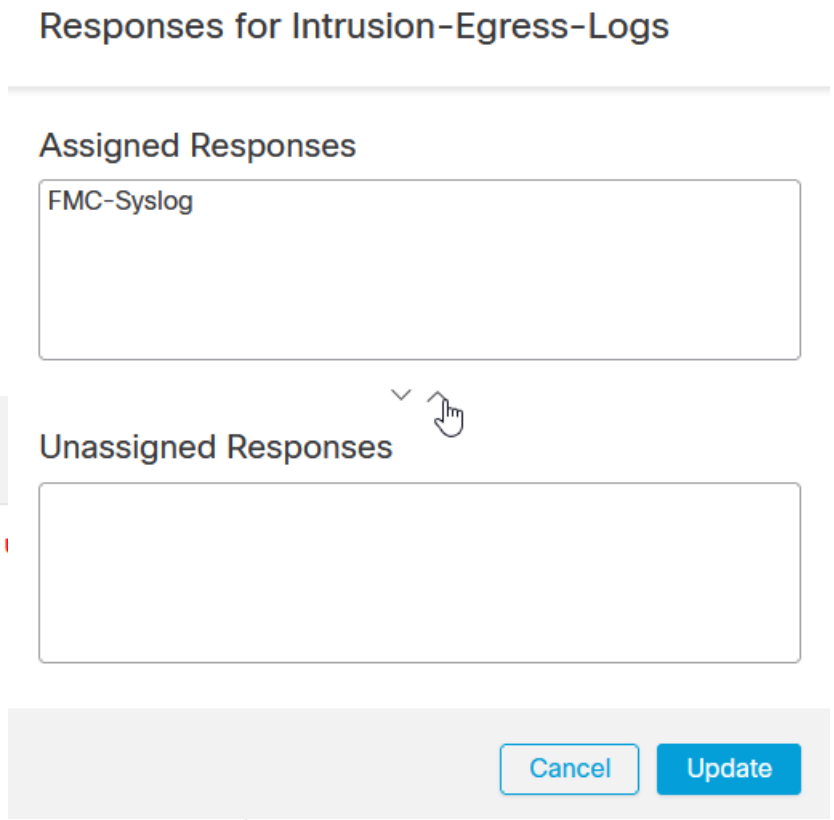


Correlate Events to Send Syslog Alerts

3) Assign policy to Syslog server

- Click Responses (next to the policy name)
- Move the preconfigured syslog alert to the Assigned Responses creates)
- Click update and then click Save

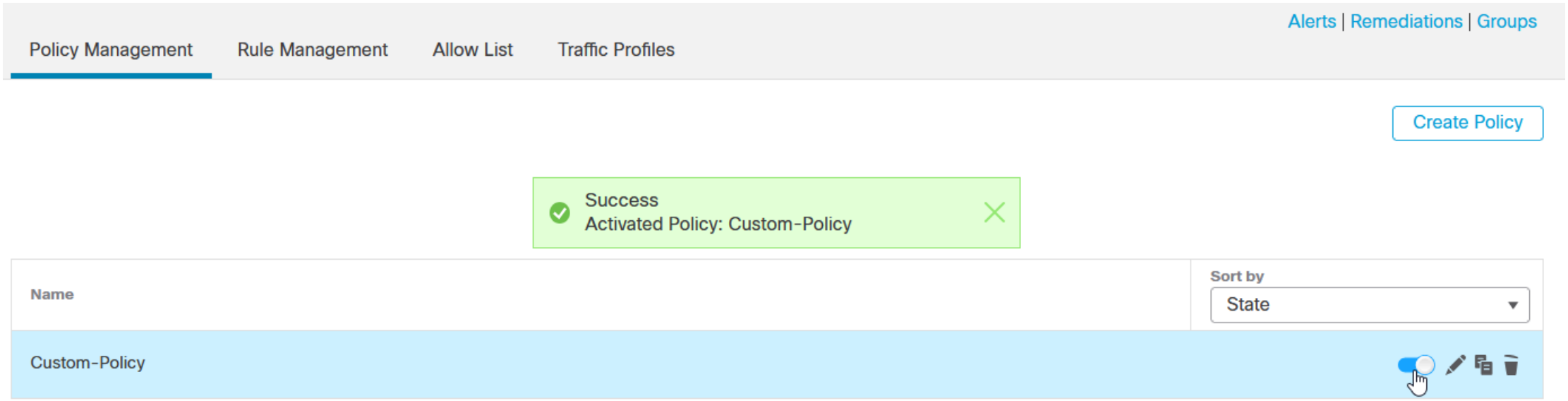




Correlate Events to Send Syslog Alerts

4) Activate the Policy

- Make sure to activate it



Monitoring

To View the syslog messages of the FMC

- Monitoring > Syslog