Fortinet NSE5

Program Requirements

You must successfully pass a minimum of any two Fortinet NSE 5 certification exams:

FortiManager

FortiAnalyzer

FortiSIEM

FortiClient EMS

FortiEDR

FortiManager

FortiManager 7.0

Exam series: NSE5_FMG-7.0

Number of questions: 35

Exam time: 70 minutes

Language: English and Japanese

Product version: FortiManager 7.0

FortiManager

01: Introduction and Initial Configuration

02: Administration and Management

03: Device Registration

04: Device-Level Configuration and Installation

05: Policy and Objects

06: Global ADOM and Central Management Monitoring

07: Diagnostics and Troubleshooting

08: Additional Configuration

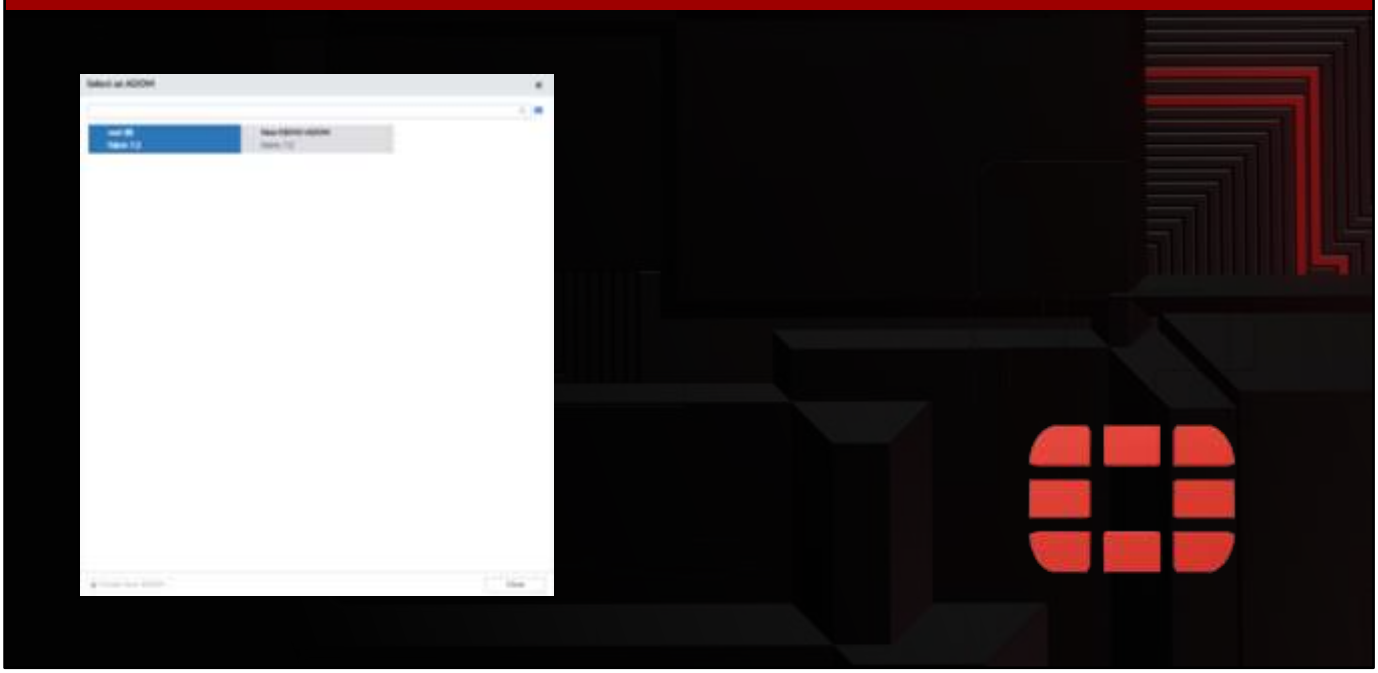
FortiManager
https://fortimanager.fortidemo.com/p/login/
USERNAME:demo PASSWORD:demo

Introduction and Initial Configuration Overview

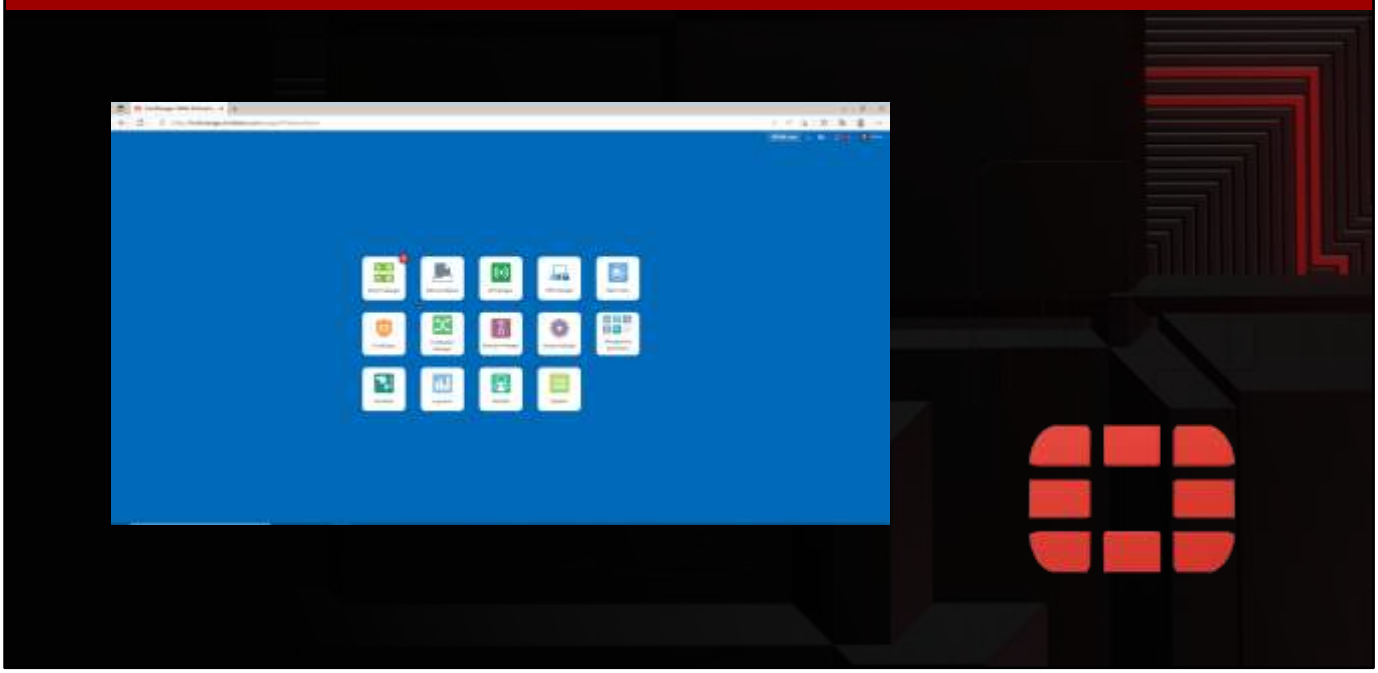
- Initial ADOM
- Fortimanager OverView
- Fortimanager vs FortiAnalyzer
- Management Layers and Modules
- Network Topology
- Connectivity Ports
- Recommendations

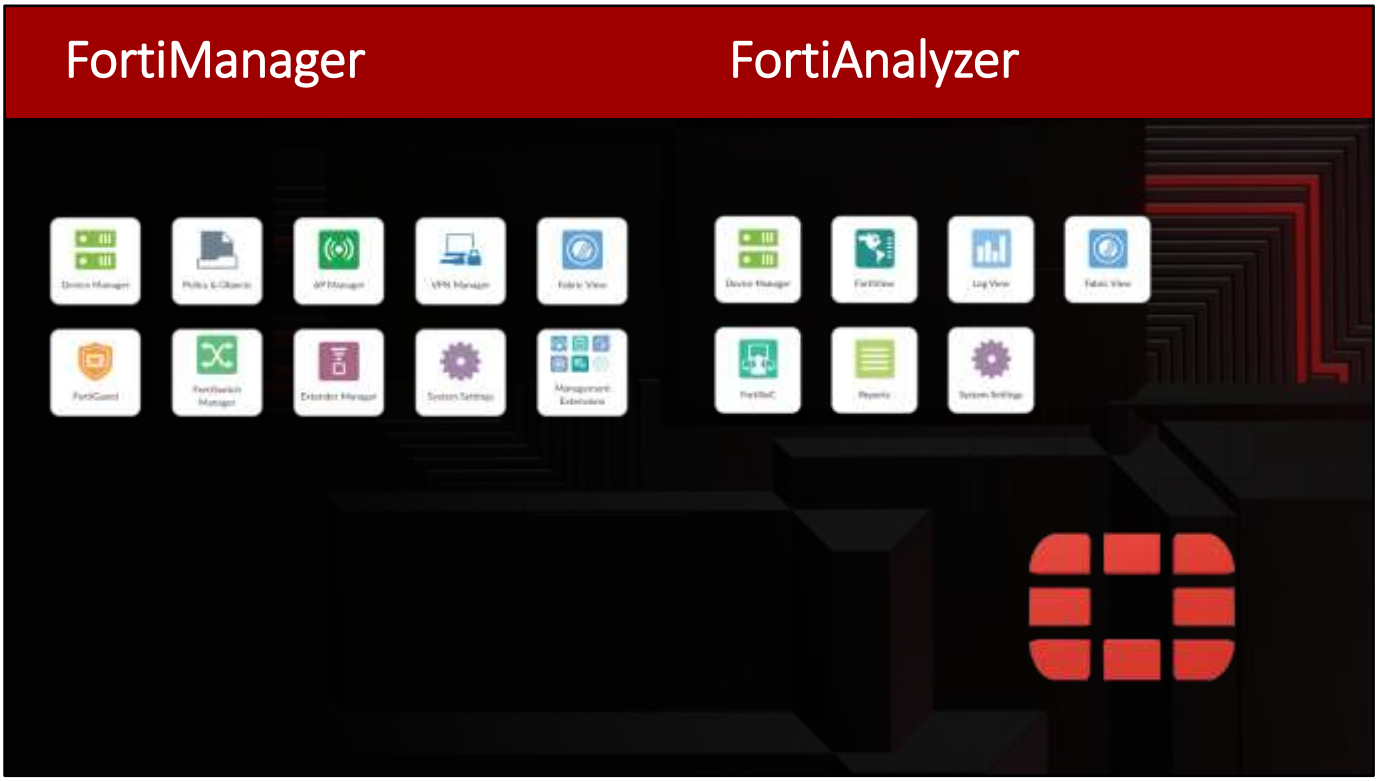
- Factory Default
- Setup Wizard
- Initial Config
- CLI
- System Information
- API

ADOM Overview

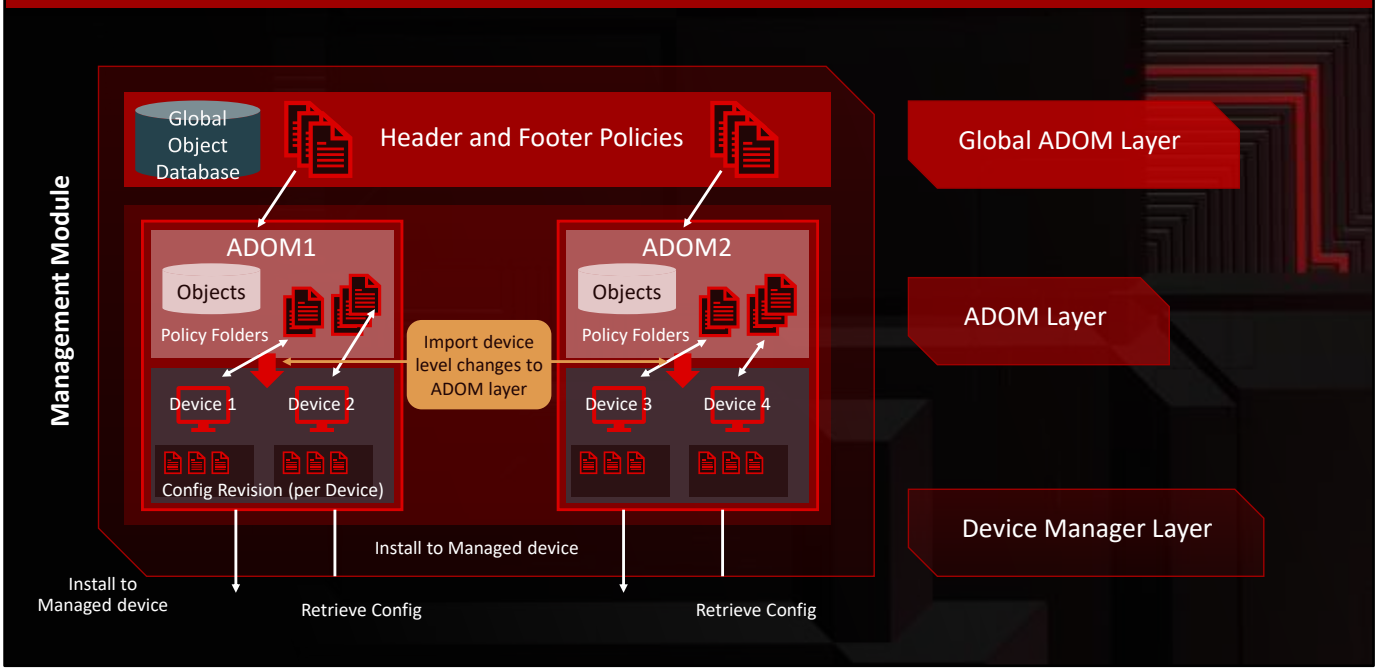


FortiManager Overview and Features

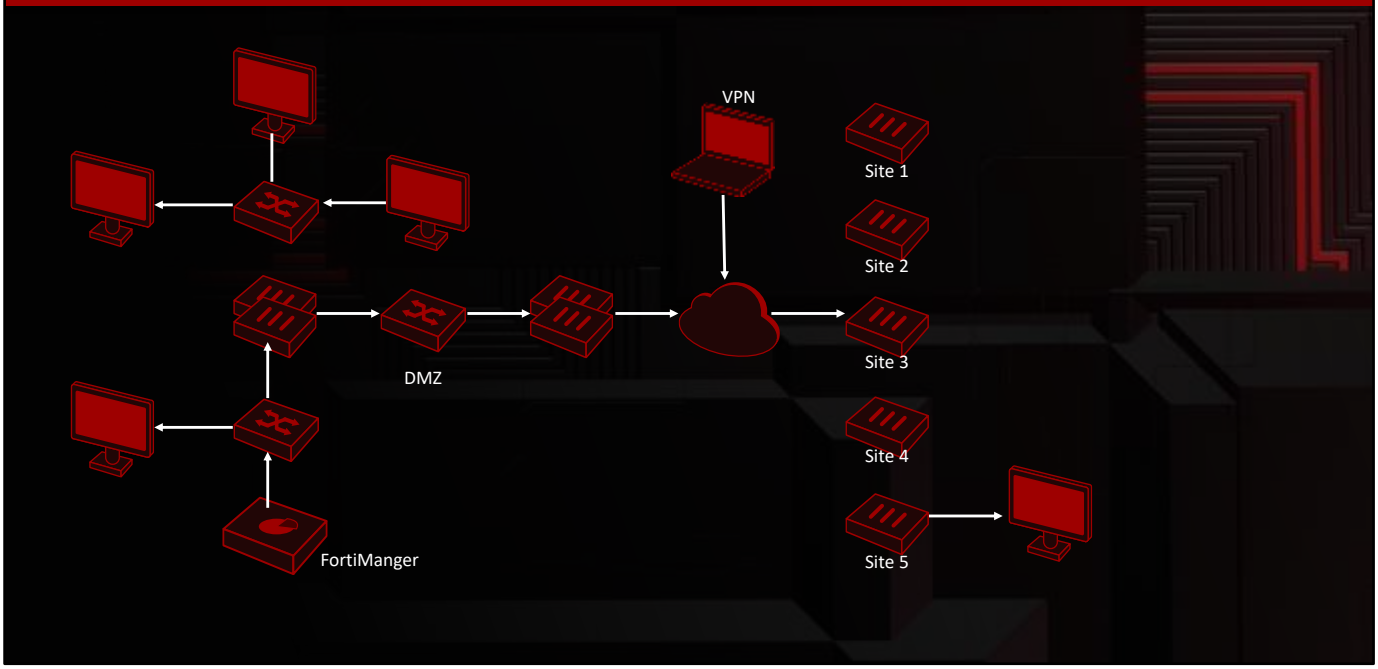




Management Layers and Modules



Network Topology



FortiManager Connectivity Ports

Functionality	Port(s)
Destination Ports	
Remote management of a FortiGate device	TCP 541 (IPv4), TCP 542 (IPv6)
Firmware image download	TCP 443
Antivirus, IPS, web filtering, antispam updates from FortiManager to FND	TCP 443
DNS lookup	UDP 53
Syslog	UDP 514
Listening Ports	
FortiGuard antivirus and IPS update push	UDP 9443
FortiGuard antivirus or IPS update request from a FortiGate device	TCP 8890
FortiGuard antispam or web filtering rating lookup from a FortiClient or FortiGate	UDP 53 or 8888
Web Services (a.k.a XML API)	TCP 8080
Web GUI and JSON API	TCP 443
Antivirus and IPS updates for FortiClient	TCP 80
HA heartbeat or synchronization (FortiManager HA cluster)	TCP 5199
Two FortiManager devices configured in cascade mode	
FortiManager devices in cascade mode both listening and destination ports	TCP 8891,8900 and 8901

Recommendations

- Deploy to a protected and trusted private network
- Use secure communications (HTTPS and SSH)
- Configure trusted hosts
  - Outside access restrict to necessary ports
  - Outside access specific users using HTTPS and SSH
- Secure Password and Policy feature
- Check event logs preferbably using a SIEM
- SAML SSO Authenticaion
  - Must register the FortiManager on the FortiCloud

Factory Default Settings

Default settings are detailed in your FortiManager QuickStart Guide

Initial Connectivity

Port 1 Mgmt Port with a default IP of 192.168.1.99/24

Connectivity ports opened: PING HTTP HTTPS and SSH

UserName admin

Password: blank/none

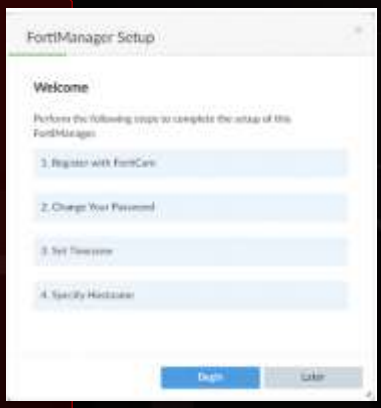
SetUp Wizard

Register with Forticare and some initial settings

Change Password

Set Time Zone

Specify Hostname



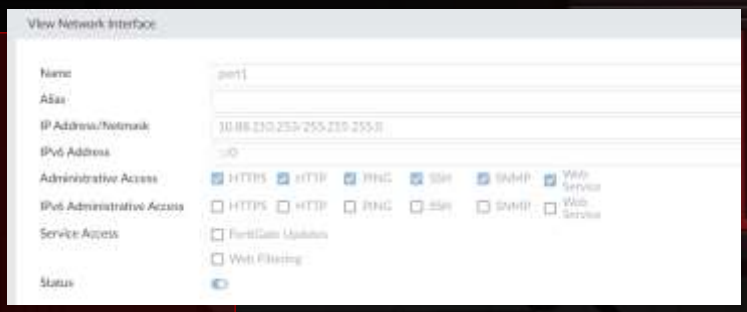
Initial Config

Interfaces

Admin Access

DNS

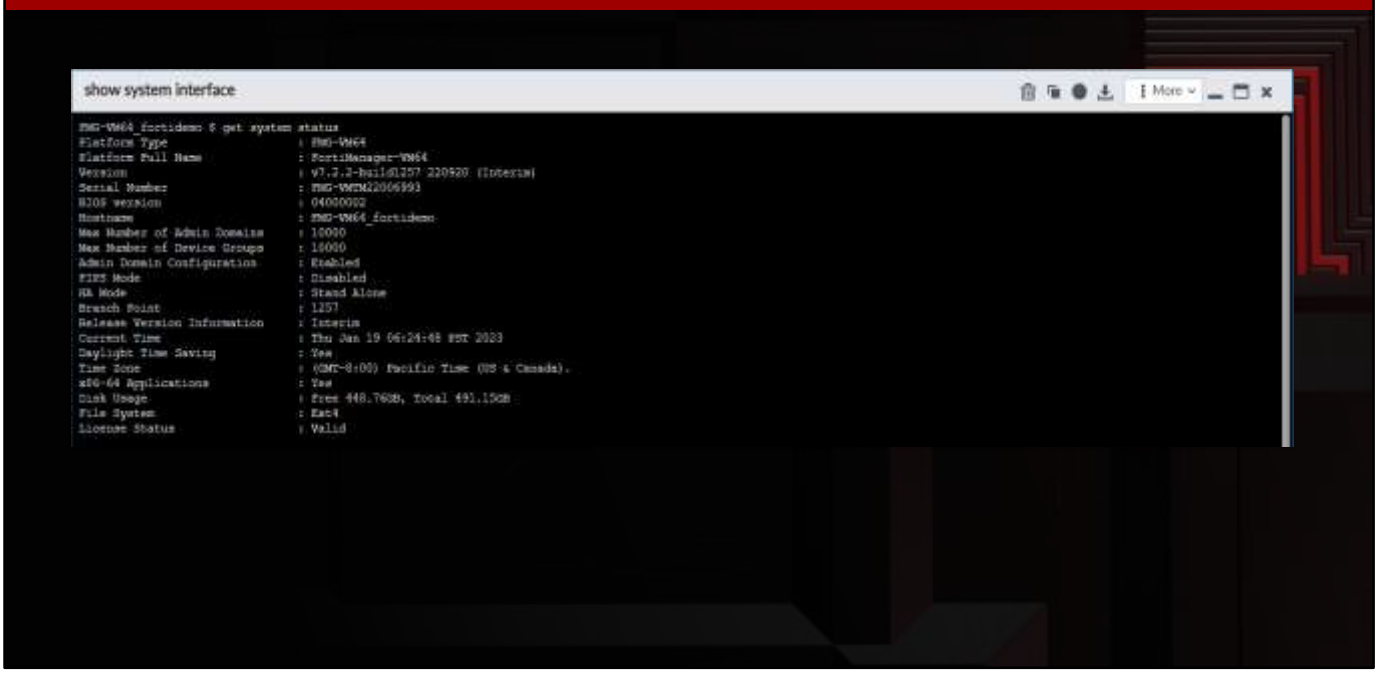
Default Gateway



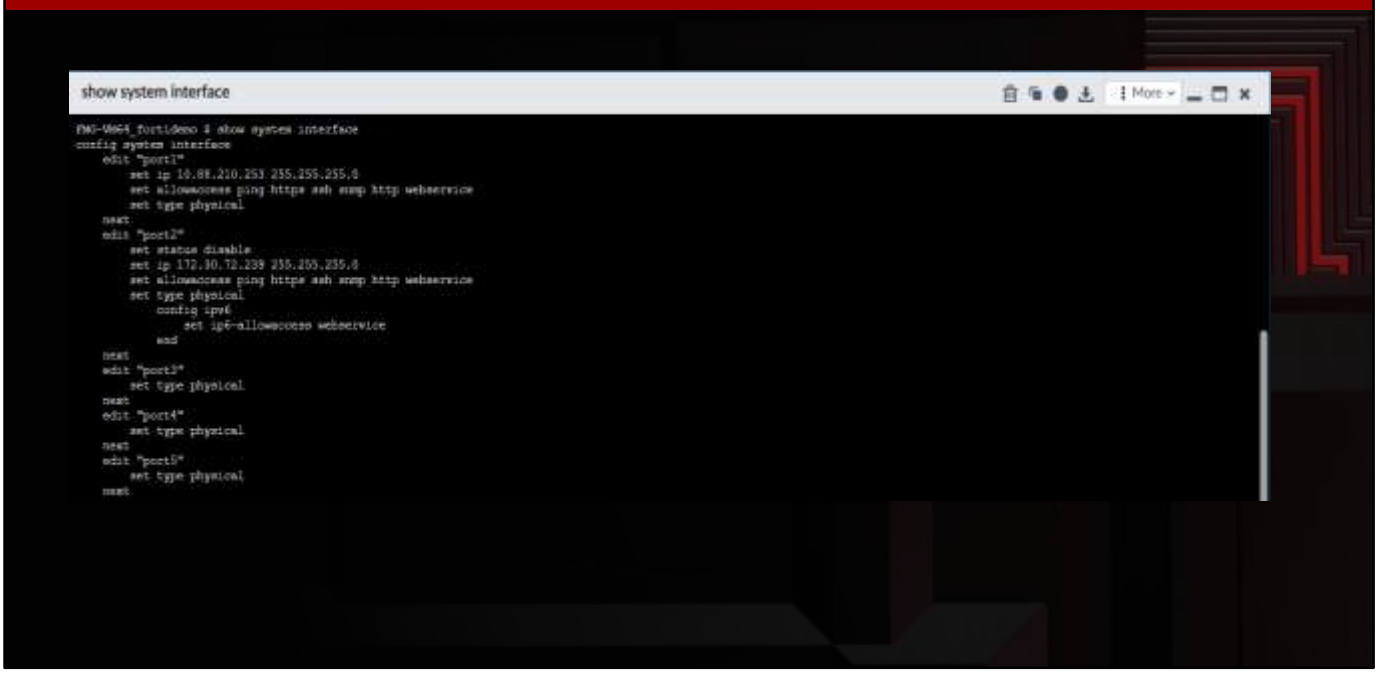
CLI

- Get system status
- Show systems interface
- Show system DNS
- Show system NTP
- Get system NTP
- Show system route

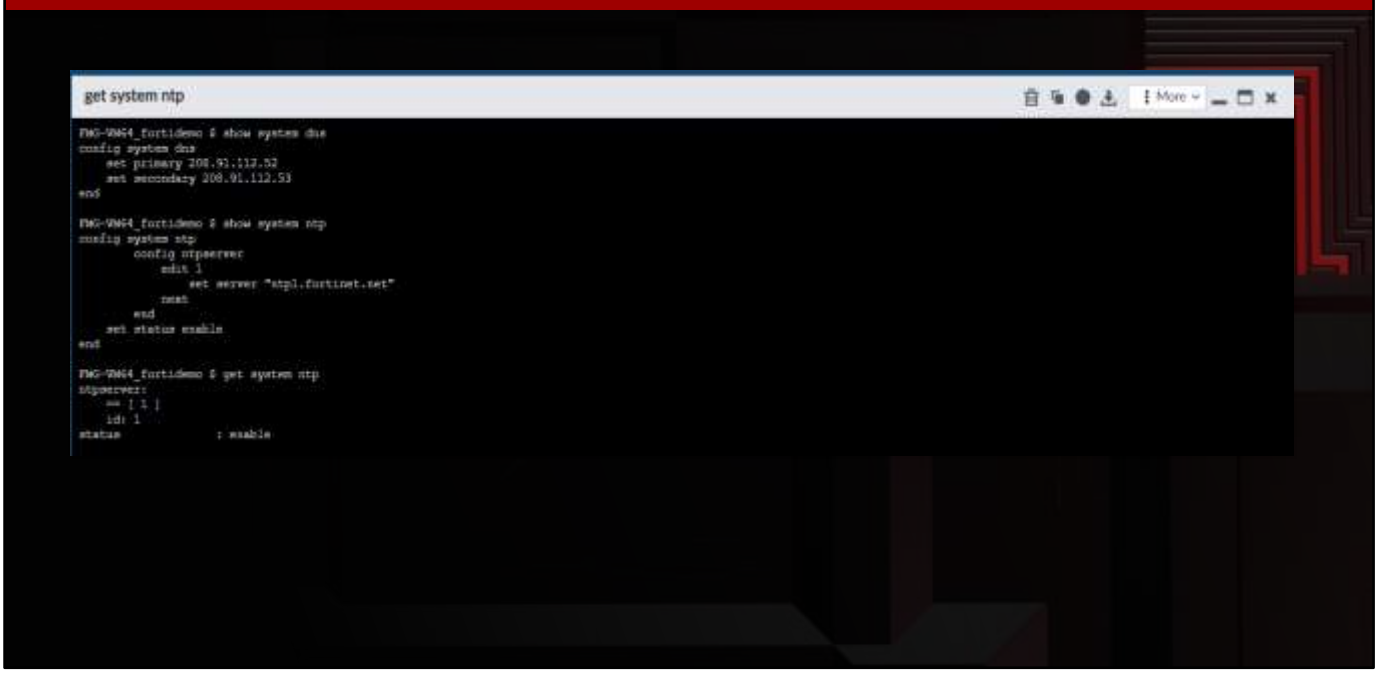
CLI



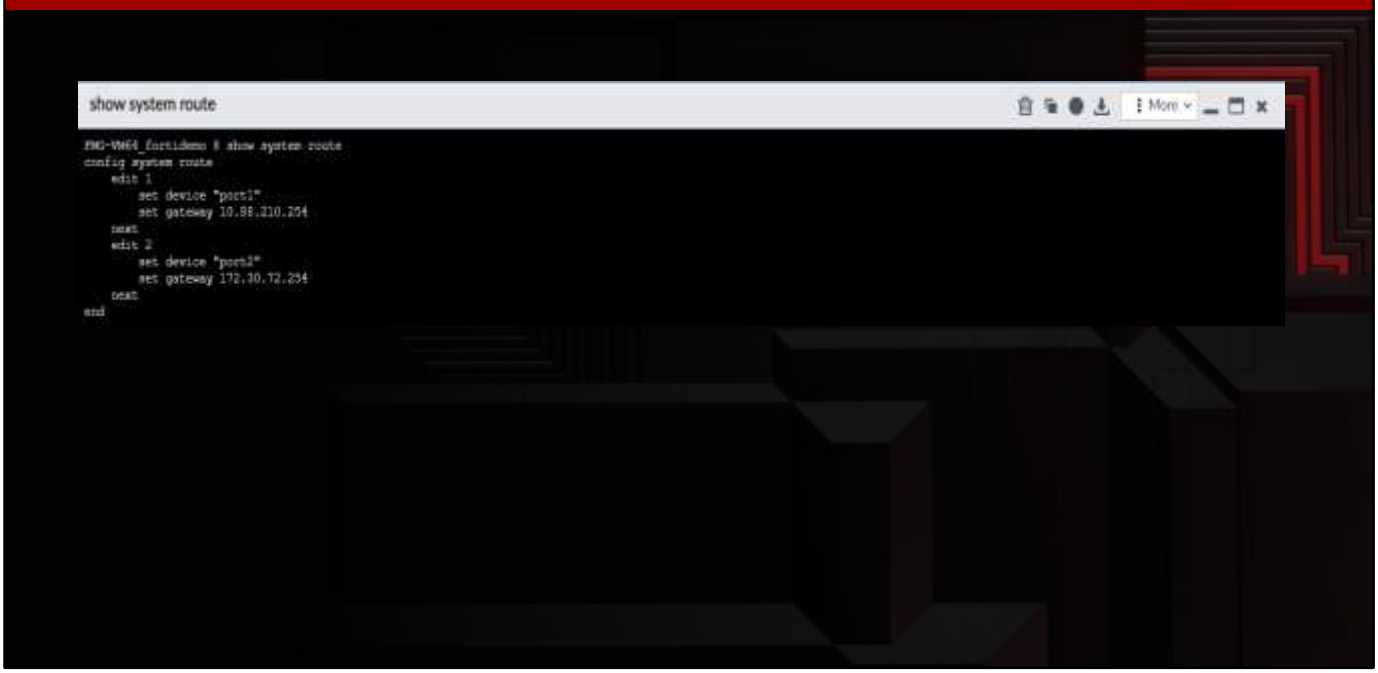
CLI



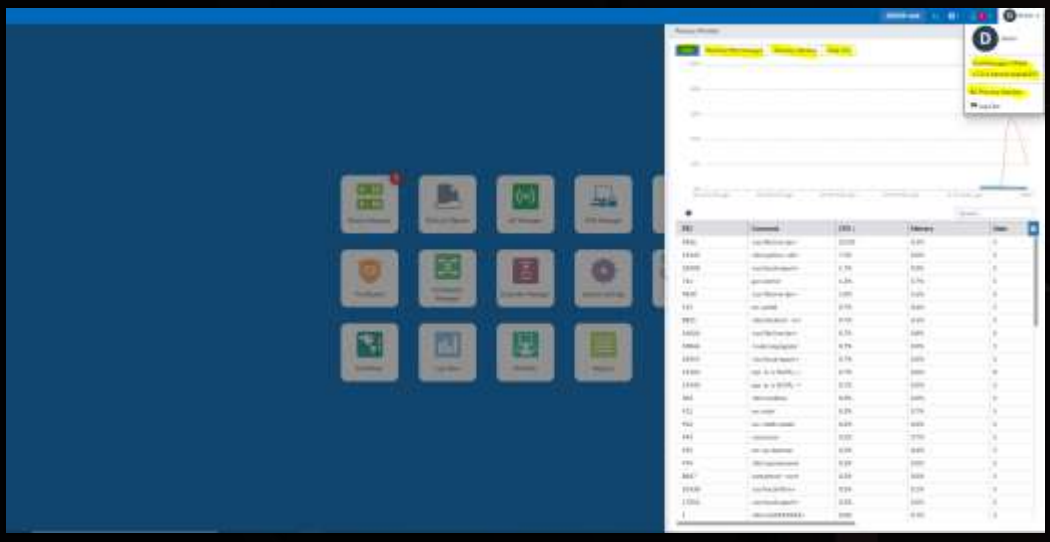
CLI



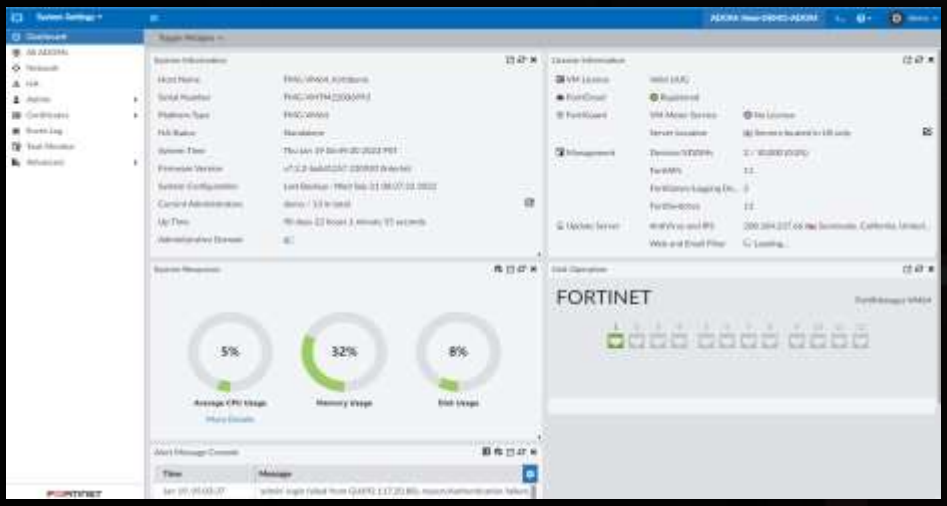
CLI



System Information



System Information



FortiManager API

Application Programming interface allows programs to talk to each other

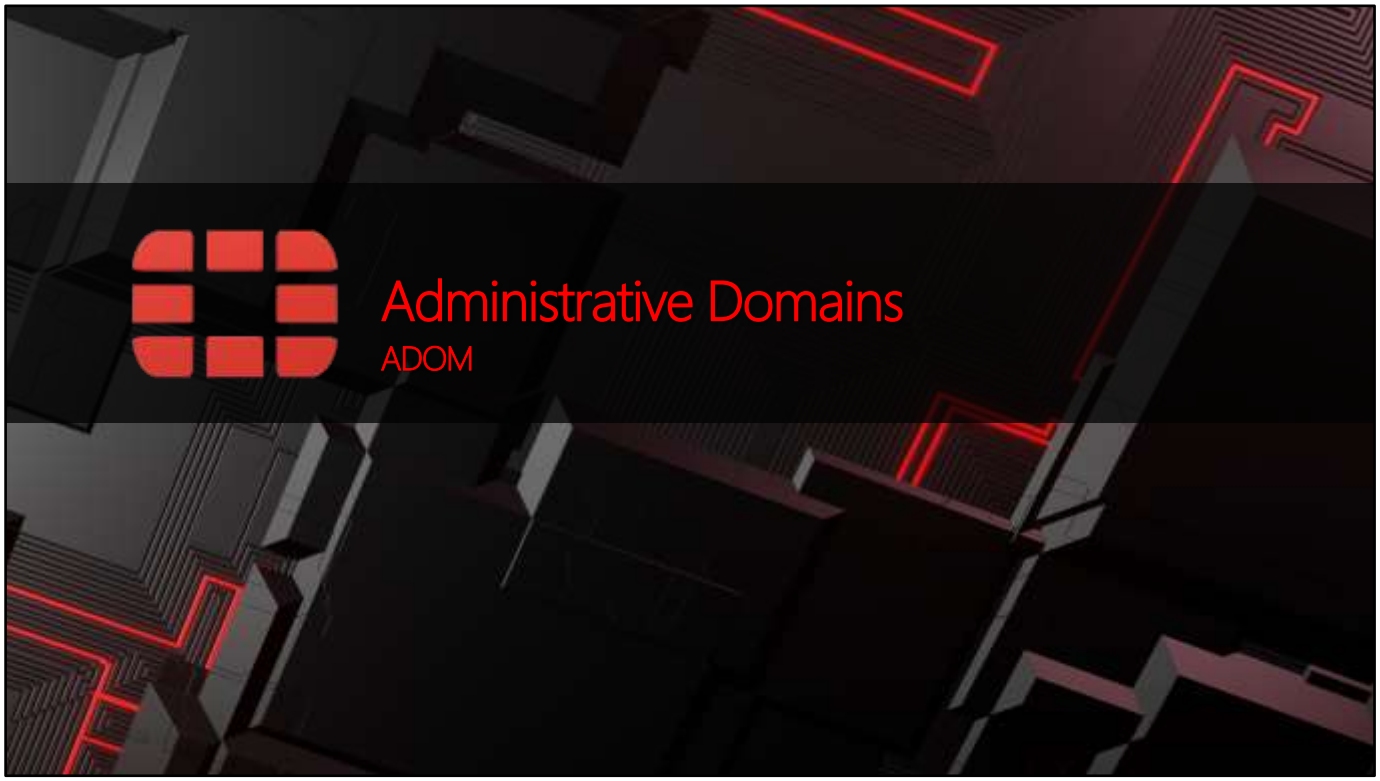
JSON RPC Standard

Detailed documentation in the Fortinet document library

Conclusions

- Initial ADOM
- Fortimanager OverView
- Fortimanager vs FortiAnalyzer
- Management Layers and Modules
- Network Topology
- Connectivity Ports
- Recommendations

- Factory Default
- Setup Wizard
- Initial Config
- CLI
- System Information
- API



Overview

- Identify purpose of ADOMs
- Describe ADOM Modes
- Configure ADOMs
- Create administrator accounts and permissions
- Understand the concurrent access
- Know when and how to use the workspace
- When to upgrade ADOM and troubleshooting
- BackUp and restore
- Offline mode
- Event logs
- Monitoring Tasks

ADOMs Explained

Purpose is to divide device administration by business needs.

- Geographic location
- Business Division
- Compliance standards

ADOMs are not enabled by default

Two types of ADOMs

- **Normal:** Full access to make configuration changes from FortiManager to ADOM and managed services
- **Backup:** Back up configuration changes made directly on managed device

ADOMs Explained

Normal Mode: Read/Write

All Management panes are available

ADOMs Explained

Backup Mode: Read Only

Used when making configuration changes directly on device and fortimanager is used for backups

Device Modes

Normal(Default)

You can add a Fortigate devices to a single ADOM

Advanced (System Settings>Advanced>Advanced Settings)

Allows flexibility on managing ADOMs and VDOMs across multiple platforms

ADOM Organization

- Device Type
- Firmware
- Administration responsibilities
- Geographic
- Customer
- Organizational

*ADOM are limited by models

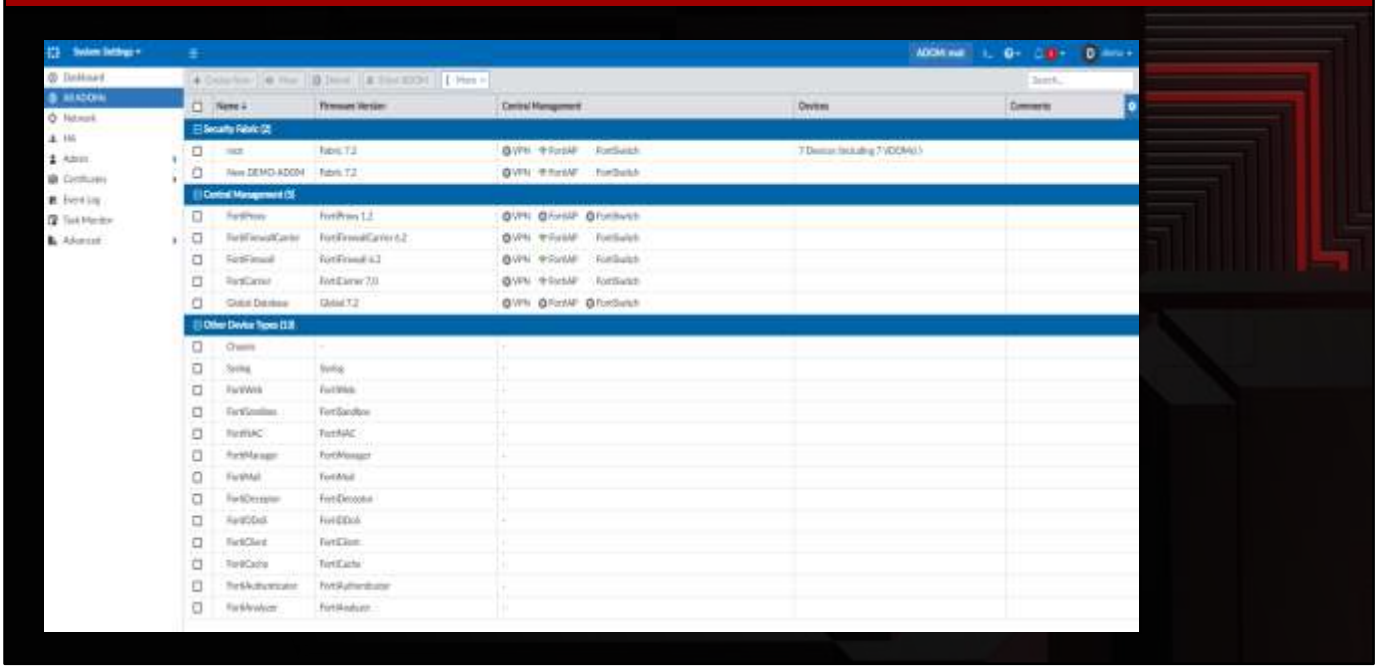
Conclusions

ADOM Overview

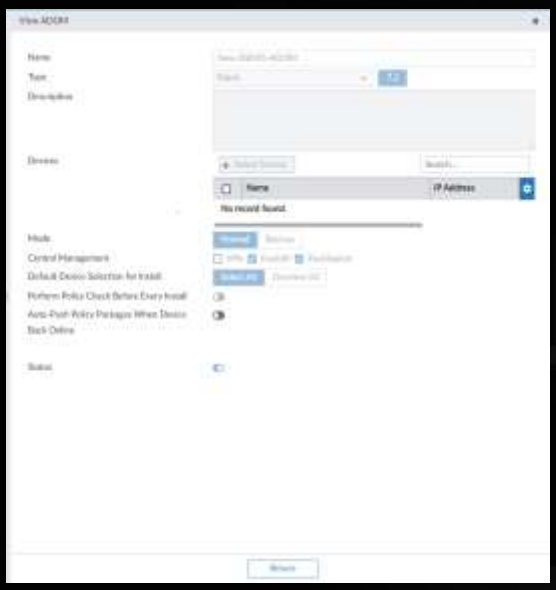
ADOM Modes

Configuring ADOMs

Creating ADOMs

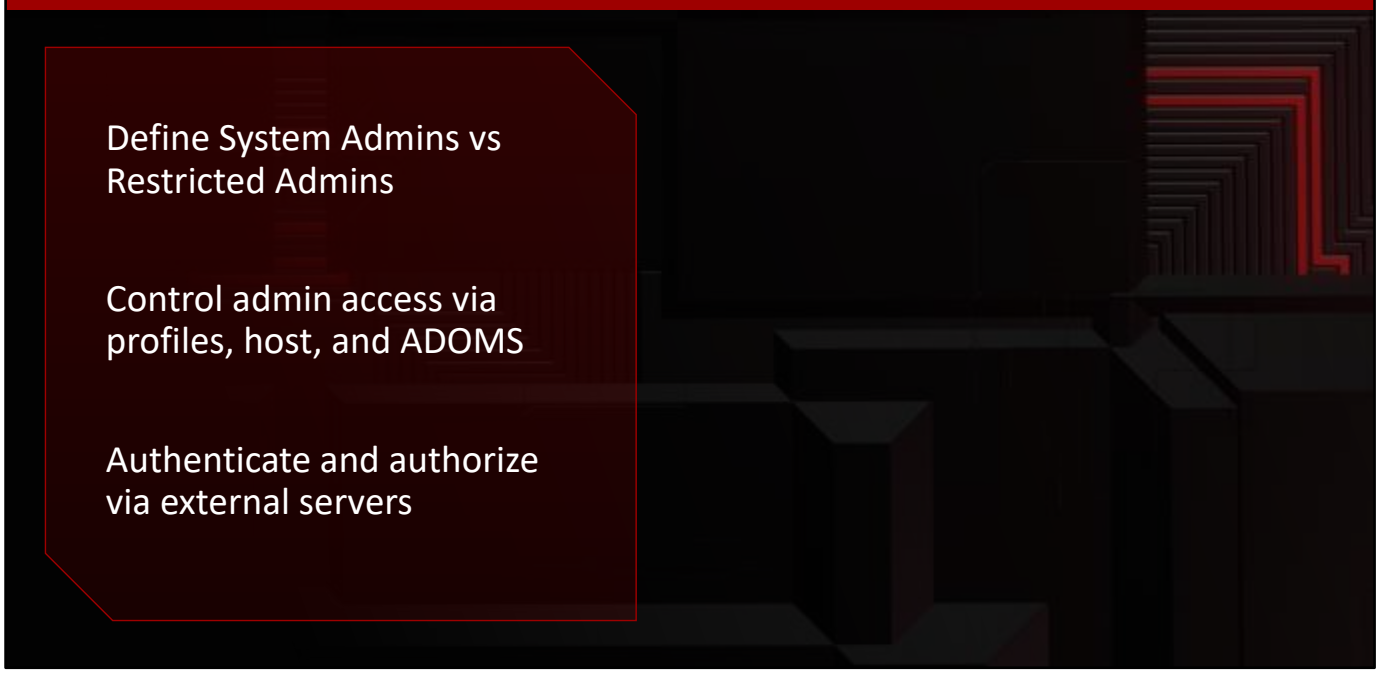


Creating ADOMs



- Firmware
- Type
- Mode
- Management
- Device Selection
- Policy Check
- AutoPush
- Status

Admin Accounts

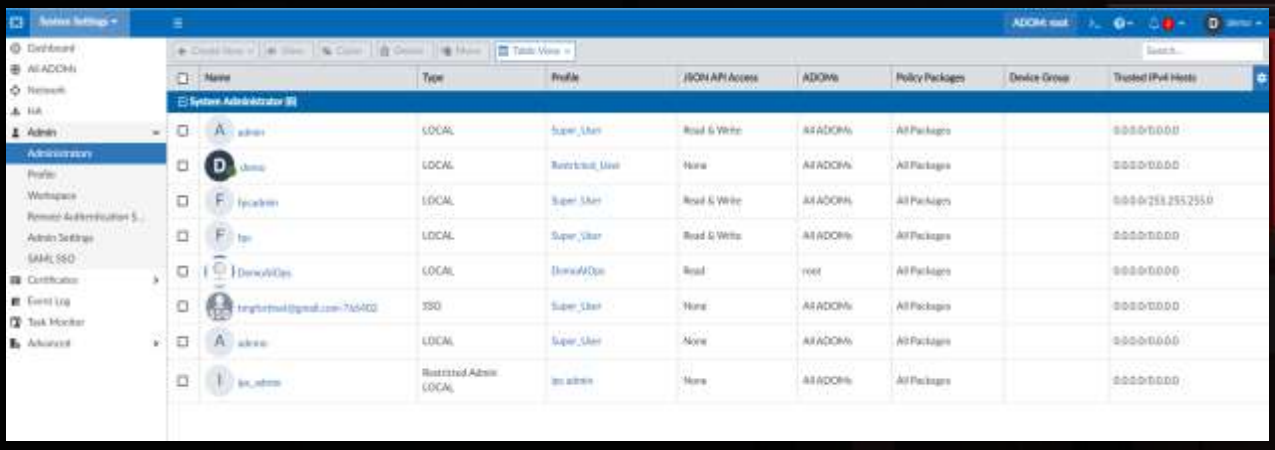


Define System Admins vs Restricted Admins

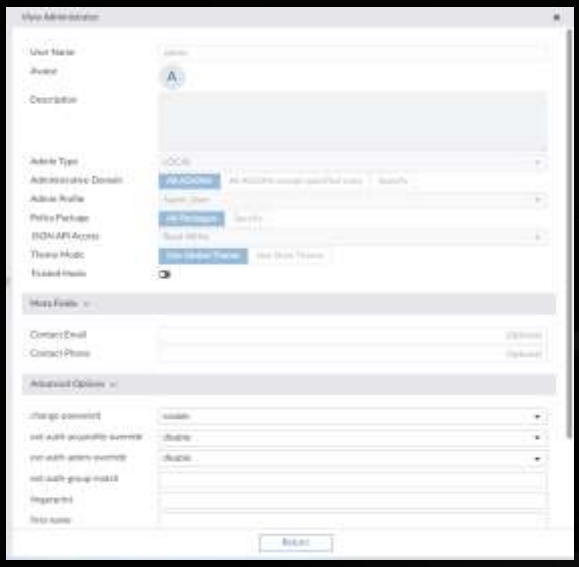
Control admin access via profiles, host, and ADOMS

Authenticate and authorize via external servers

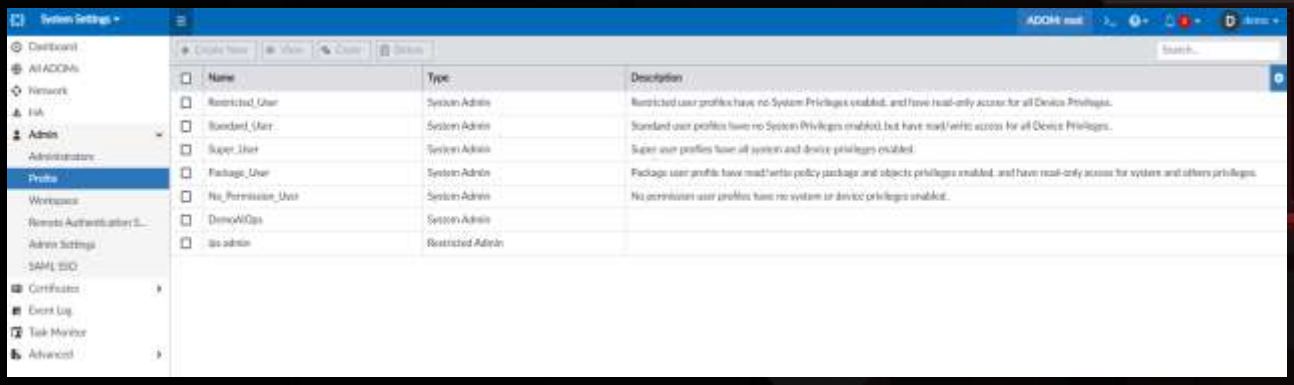
Configuring Admin Accounts



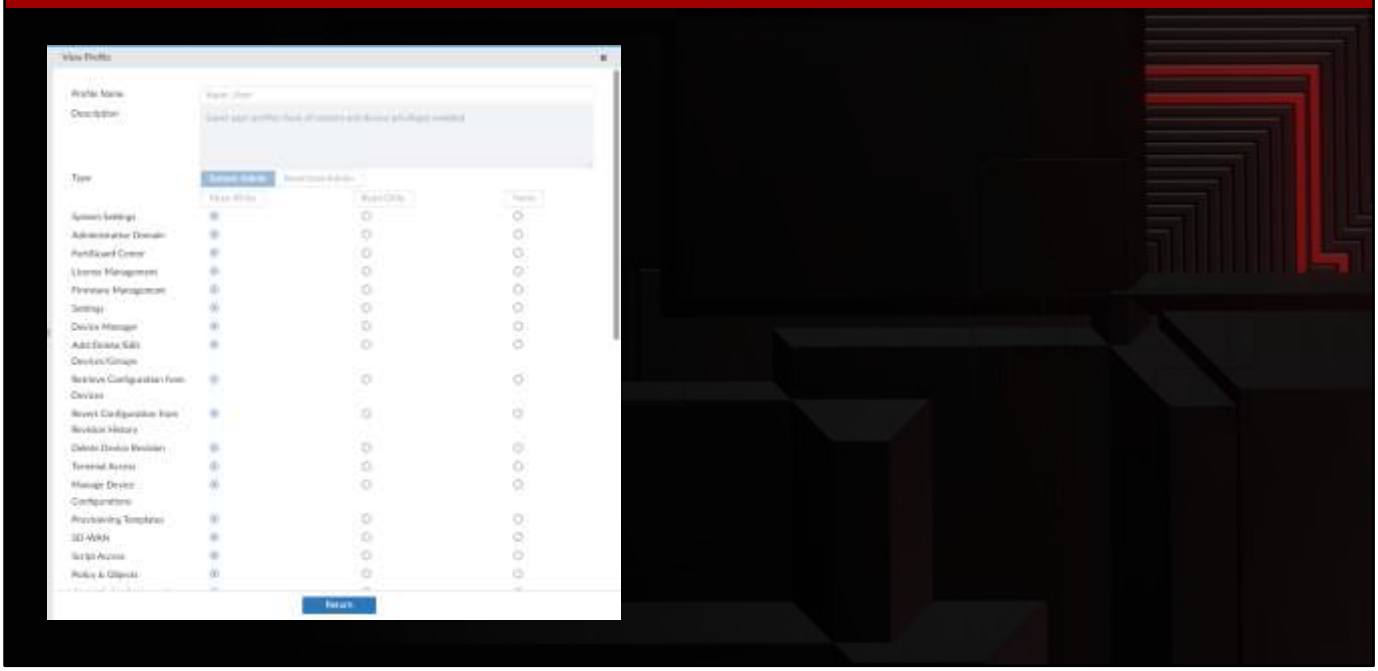
View Administrator



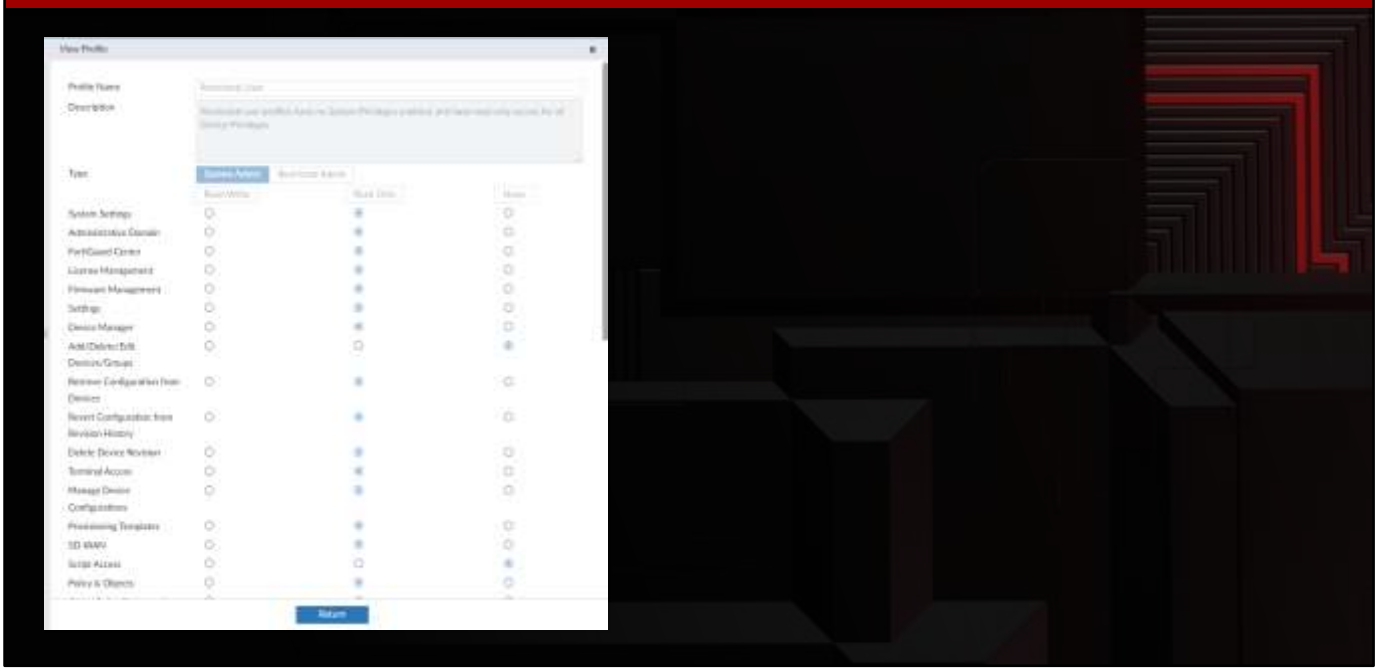
Configuring Admin Profiles



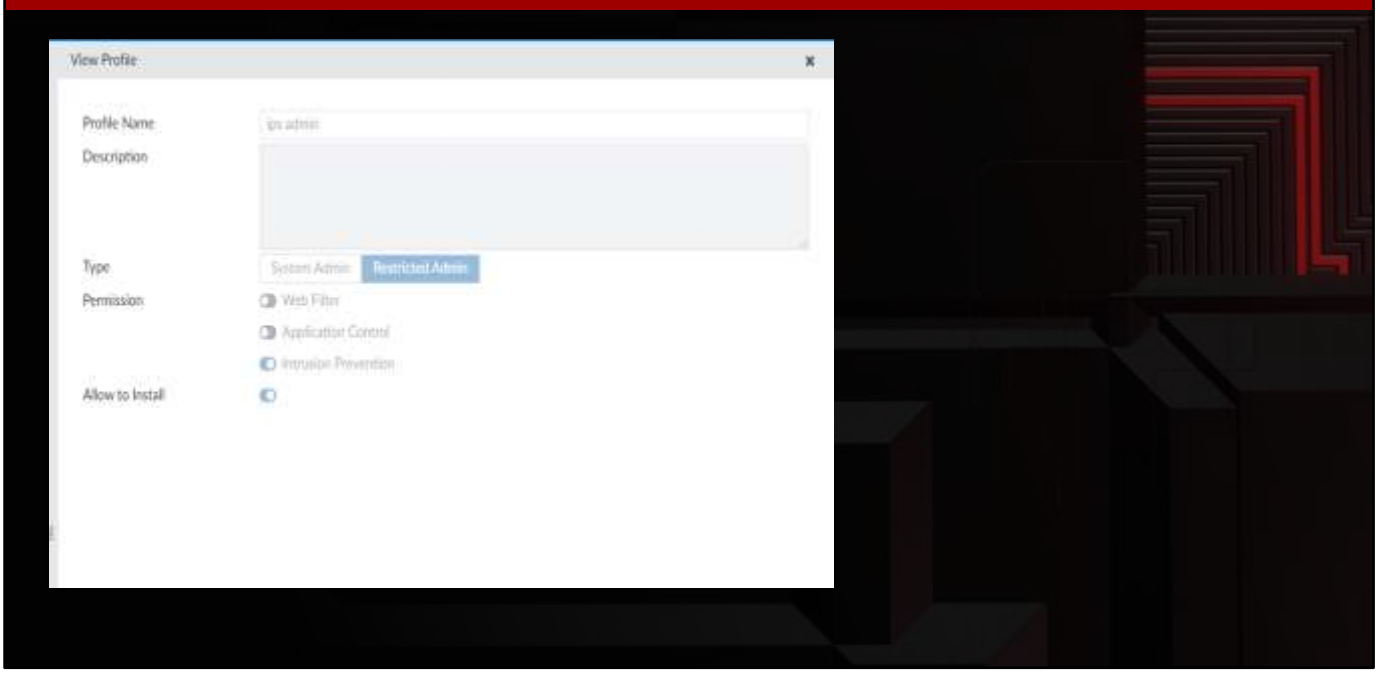
System Admin



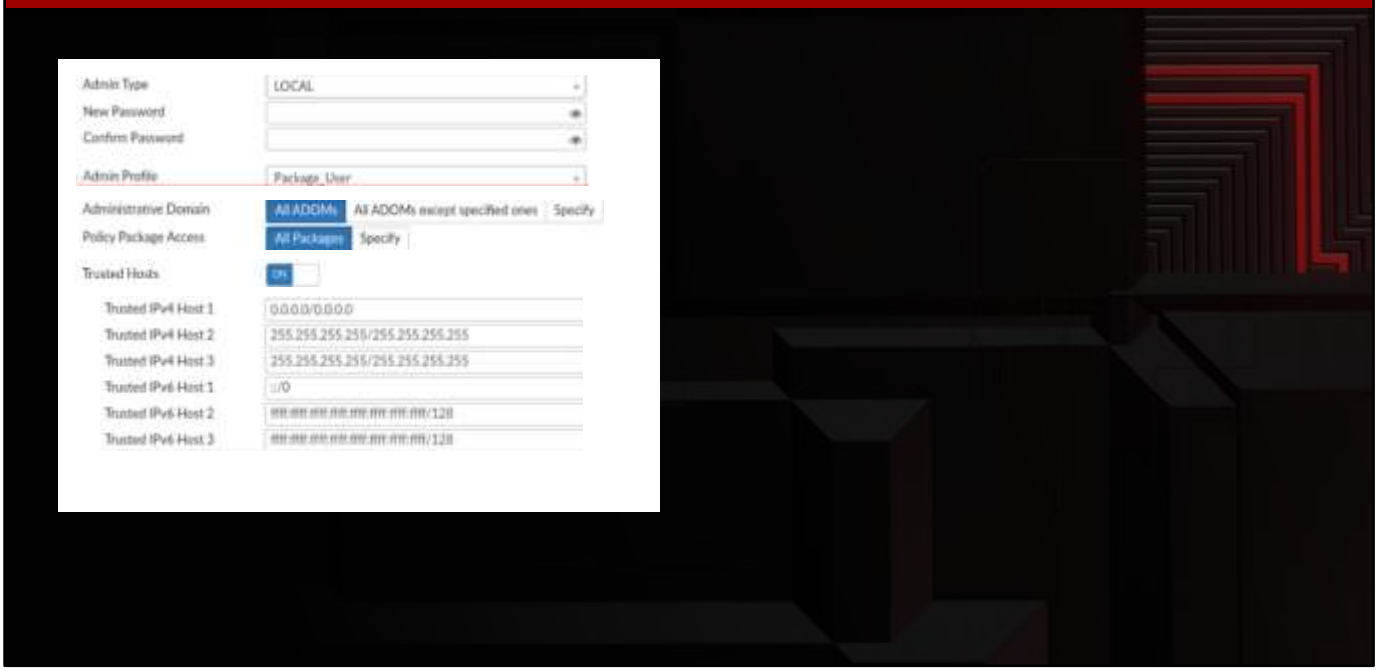
Restricted



Restricted



Multiple Admins and Security



Trusted Hosts for Admin Users

Up to 10 trusted host

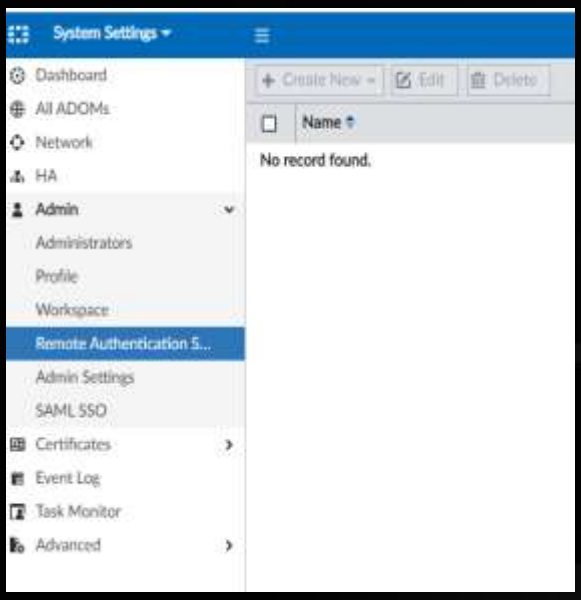
Applies to both GUI and CLI

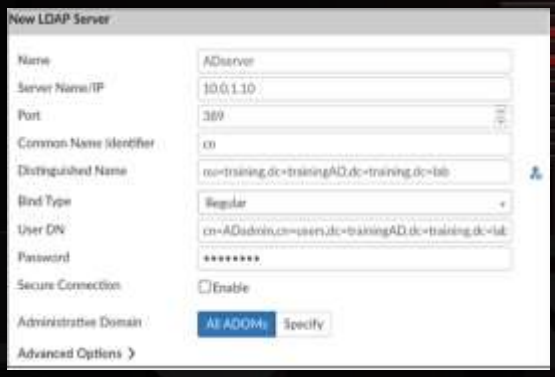
Controlling Access through ADOMs

Monitor and Managed based upon ADOM

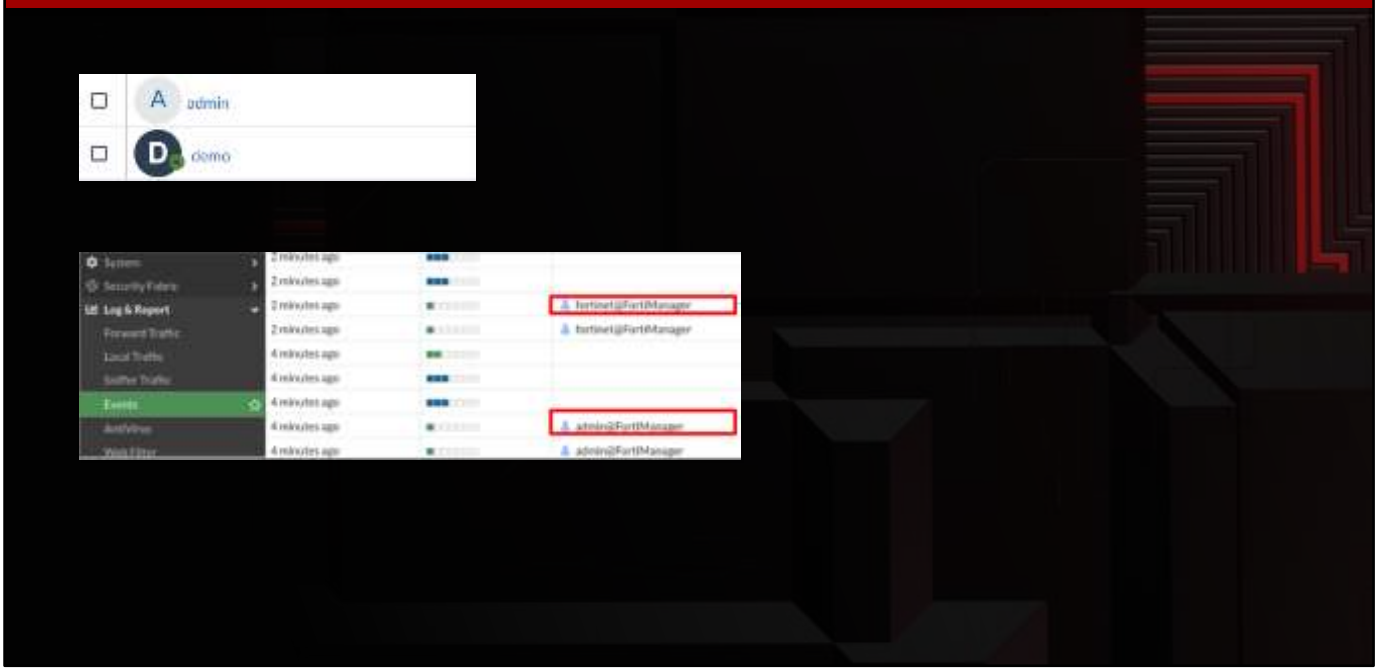
- Increase security and efficiency
- Admins with super_user will have full system access to ADOM

External Validation of Non-Local Admin logins





Monitoring Admin Sessions



Concurrent ADOM Access

By default multiple admins can login to an ADOM at the same time

Can cause conflict with multiple changes to same ADOM at once

```
Config system global
Set workspace-mode disabled
end
```

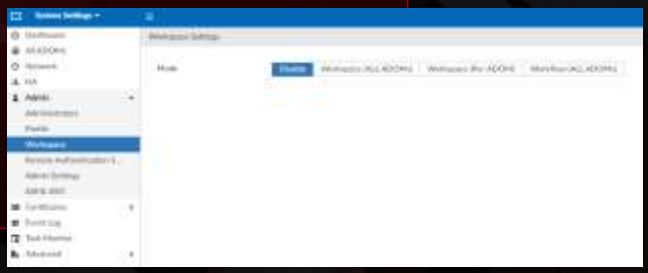
WorkSpace Mode

Disables concurrent ADOM access – ADOM locking

You must lock to perform update

READ/WRITE for active admin all others have read only access

Config system global
Set workspace-mode normal
end



WorkSpace Mode

- Admin will “lock” ADOM
- While ADOM locked
  - Other admins see ADOM with lock symbol
  - Other admins have read only
- Lock Status
  - Grey – ADOM Unlocked
  - Green – ADOM locked by you
  - RED – ADOM locked by another admin

Locking Device or Policy Package (WorkSpace Mode)

Device or Policy package must be locked

1. Select device or policy package to lock
2. Right-click select lock
3. Click unlock

System will remove individual device or policy locks if ADOM is locked

Supported ADOM Versions

Each ADOM is associated with specific firmware

- The same ADOM can manage different versions IF
  - 6.4 and 7
  - Not 5.x with 7

Fortimanager 7.0 supports ADOM 6.2 6.4 7.0

ADOM UpGrade and Debugging

You can upgrade the ADOM after you have upgraded the firmware of all devices contained in it (prior to Fortimanager 7.0)

Starting fortimanager 7.0 can upgrade ADOM 6.2 to 6.4 without updationg all devices in the ADOM from FortiOS 6.2 to 6.4

ADOM UpGrade and Debugging

Before Upgrades

Install any pending devices settings or policy package changes

After Installation, ensure policy packages and device configs are synced

After UpGrade – devices and ADOMS

Check Installation preview to identify any changes caused by the upgrade

Check if the to-be-installed changes are acceptable

Device Migrated

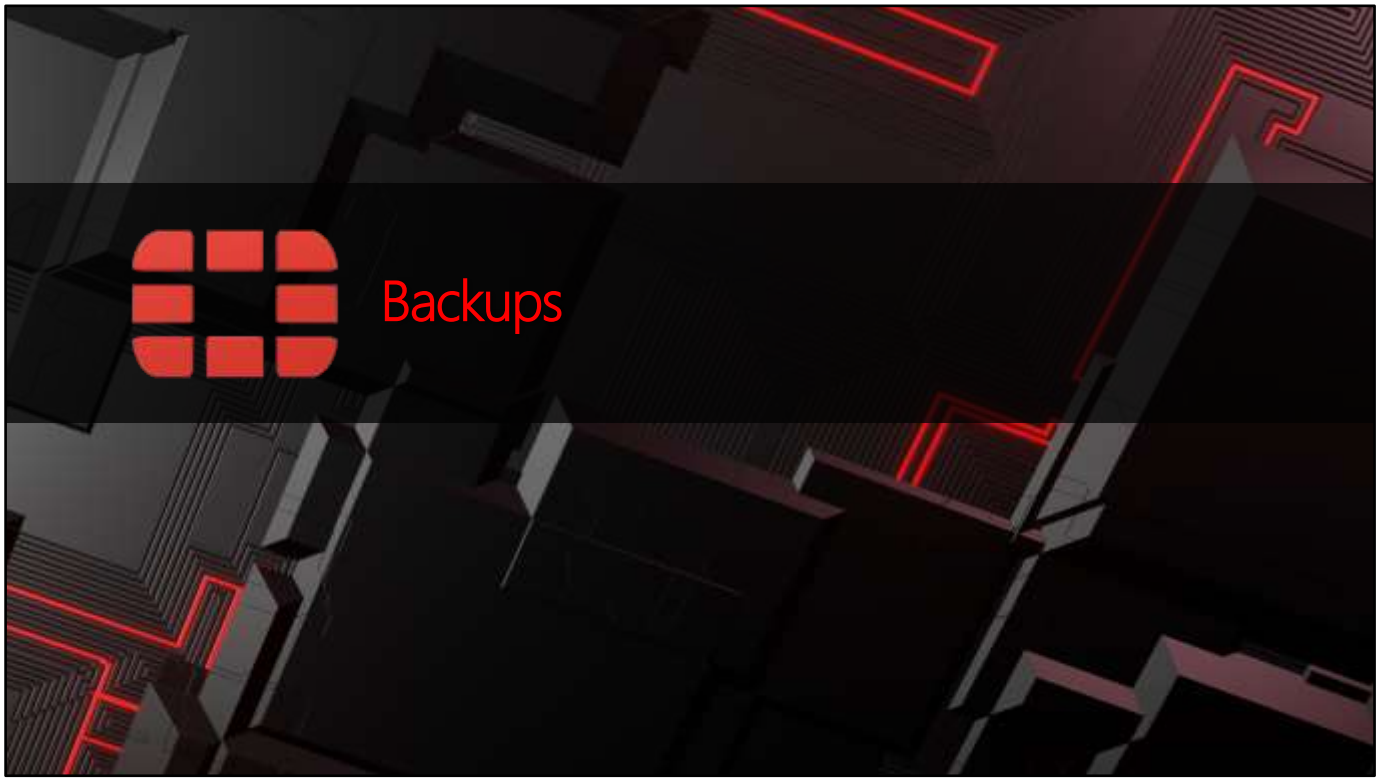
Shared Policy package and objects will not move to the new ADOM

Can perform input policy

Conclusions

Creating ADOMs

- Configuration
- Admin accounts and permissions
- Concurrent access
- Workspace

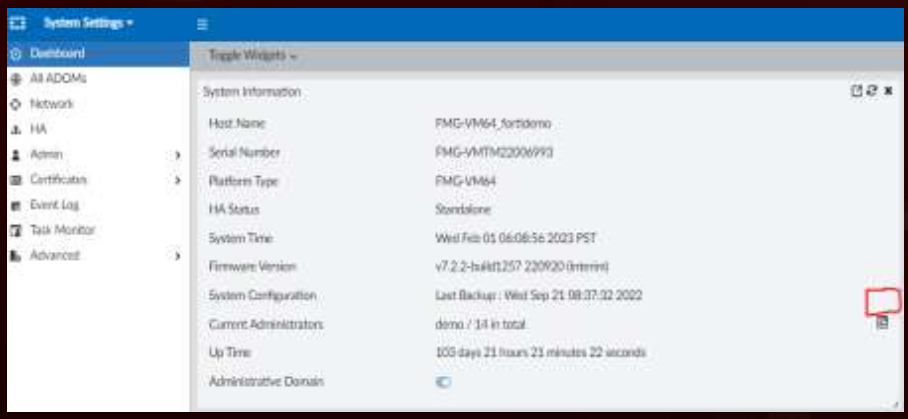


FortiManager Backups

- All Devices
  - Global Database
  - Flash configuration
- Does not backup logs, FortiGuard Objects and firmware
- Scheduled backups from CLI only
  - FTP
  - SCP
  - SFTP

```
config system backup all-settings
set status{enable | disable}
set server {<ipv4 address>|<fqdn str>}
set protocol {ftp | scp | sftp}
```

FortiManager Backups



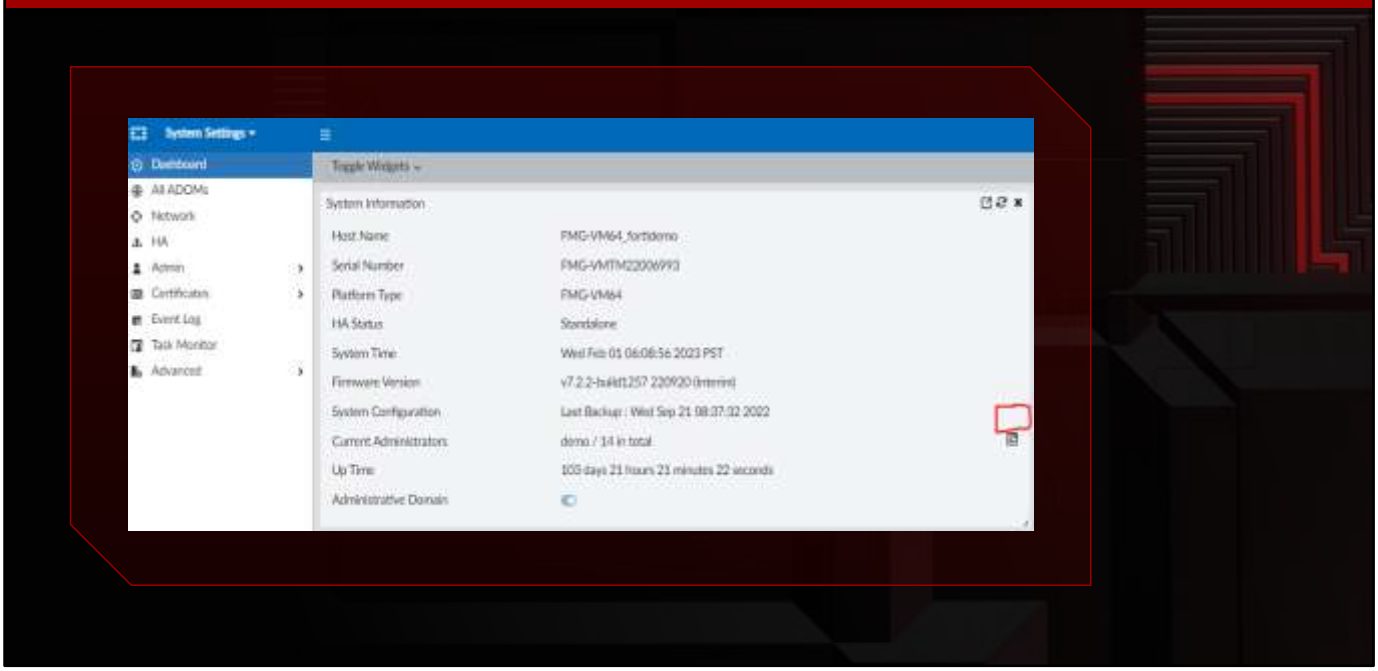
FortiManager Backups – Restoring

Reboots Fortimanager

- Supports restore from GUI and CLI
- Does not support restore of a backup file with mismatching firmware image and mismatch model

```
execute restore all-settings {ftp | scp | sftp}
<ip> <string> <user_name> <password_str> <ssh-
cert> <crpt_password>
```

FortiManager Backups – Restoring



FortiManager Backups – Migrating

BackUp Fortimanager configuration on source FortiManager

On CLI of new device, run the following CLI commands

```
exec migrate all-settings < ftp | scp | sftp > <server> <filepath> <user> <password>
[cryptpasswd]
```

FortiManager Backups – Offline Mode

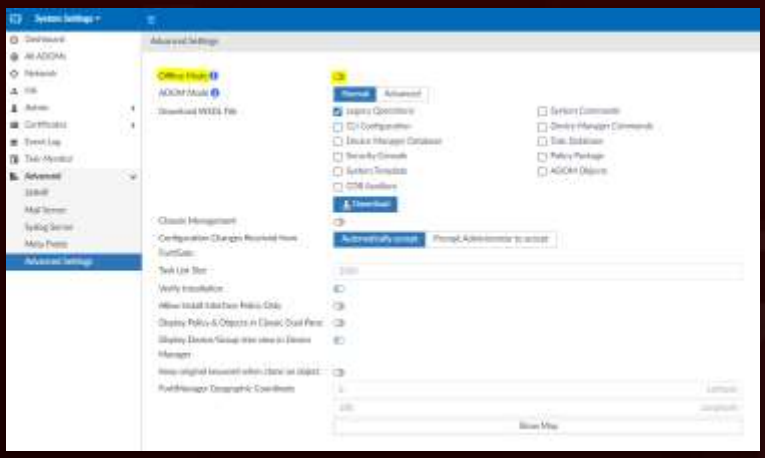
Default Disabled

- Enabling offline mode stope FGFM Management Protocol (TCP 541)
- By Default, offline mode is enabled when a backup is restored
  - You cannot manage devices when offline mode is enabled


```
FMG-VM64 # get sys status
Platform Type      : FMG-VM-64
Platform Full Name : Fortimanager-VM64

Offline Mode       : Enabled
```

FortiManager Backups – Offline Mode



FortiManager Backups – Reset Settings

BackUp, then reset using local console

```
execute reset all-settings
execute reset all-except-ip
```

Reset all configuration except interface and routing configuration

```
execute format {disk | disk-ext3 | disk-ext4} <RAID-level> deep-erase <erase-
count>
```

Reset all settings will

- Reset FortiManager to factory default settings
- Erase the configuration on flash, including IPs and routes
- Disconnect all the sessions and reboot FortiManager

Format command will

- Delete all databases and logs and repartitions hard disk

Conclusions

- Backups
  - Backups overview
  - Restoration
  - Migration
  - Online mode
  - Reset settings

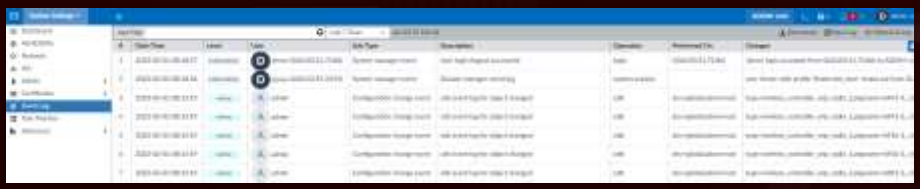
Monitoring Events – Task Monitor

You can Monitor status through System Settings -> Task Monitor

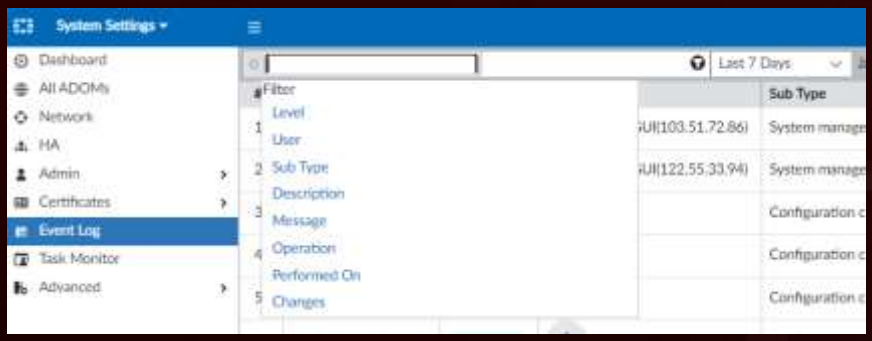
Monitoring Events – Event Log

Monitor Event Logs System Settings -> Event Log

- Default Severity set to information
- Can change from CLI

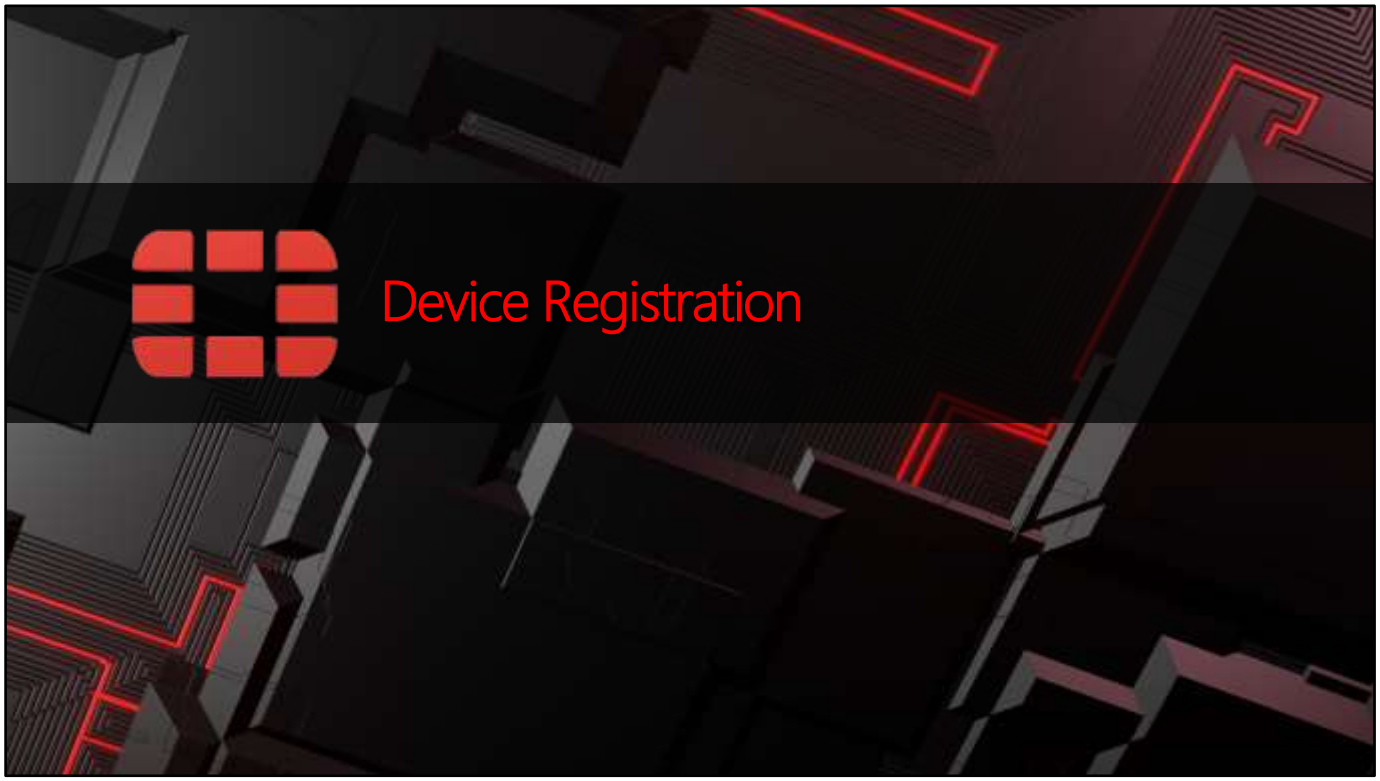


Monitoring Events – Event Log Filters



Conclusions

- Monitoring events
  - Task monitor
  - Event log
    - Filters



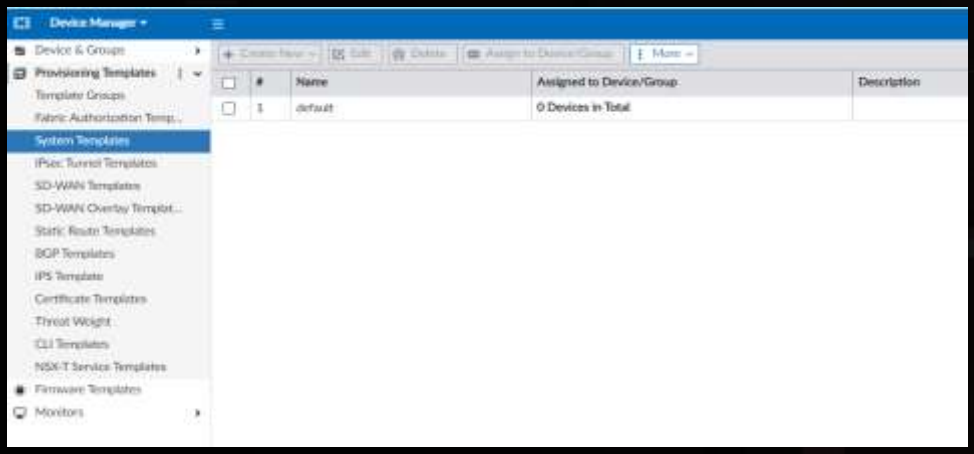
Device Registration – OverView

- Configure and apply provisioning profiles to your managed devices
- Add Fortigate to FortiManager
- Understand the import report
- Add multiple Fortigate devices to FortiManager at same time
- Add chassis to FortiManager
- Manage a FortiGate HA using FortiManager
- TroubleShoot device discovery issues

Apply common device settings to devices

- Modify and reapply settings
- Divide into specific types and modify common
  - System Templates
  - IPSec Tunnel
  - SD-WAN
  - SD-WAN Overlay
  - Static Route
  - Certificate
  - Threat Weight
  - CLI
  - NSX-T Service
  - Firmware

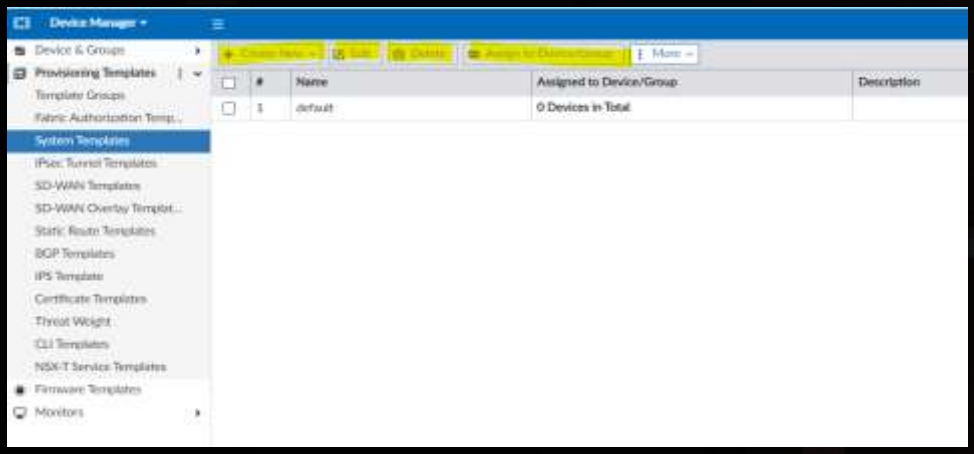
Provisioning Templates



Provisioning Templates

- Subset of Model device configuration – system-level settings
  - Configure of modify common settings
- Create new templates
- Inherit system settings and CLI settings of a managed device using import
- Associate already-managed devices with a profile

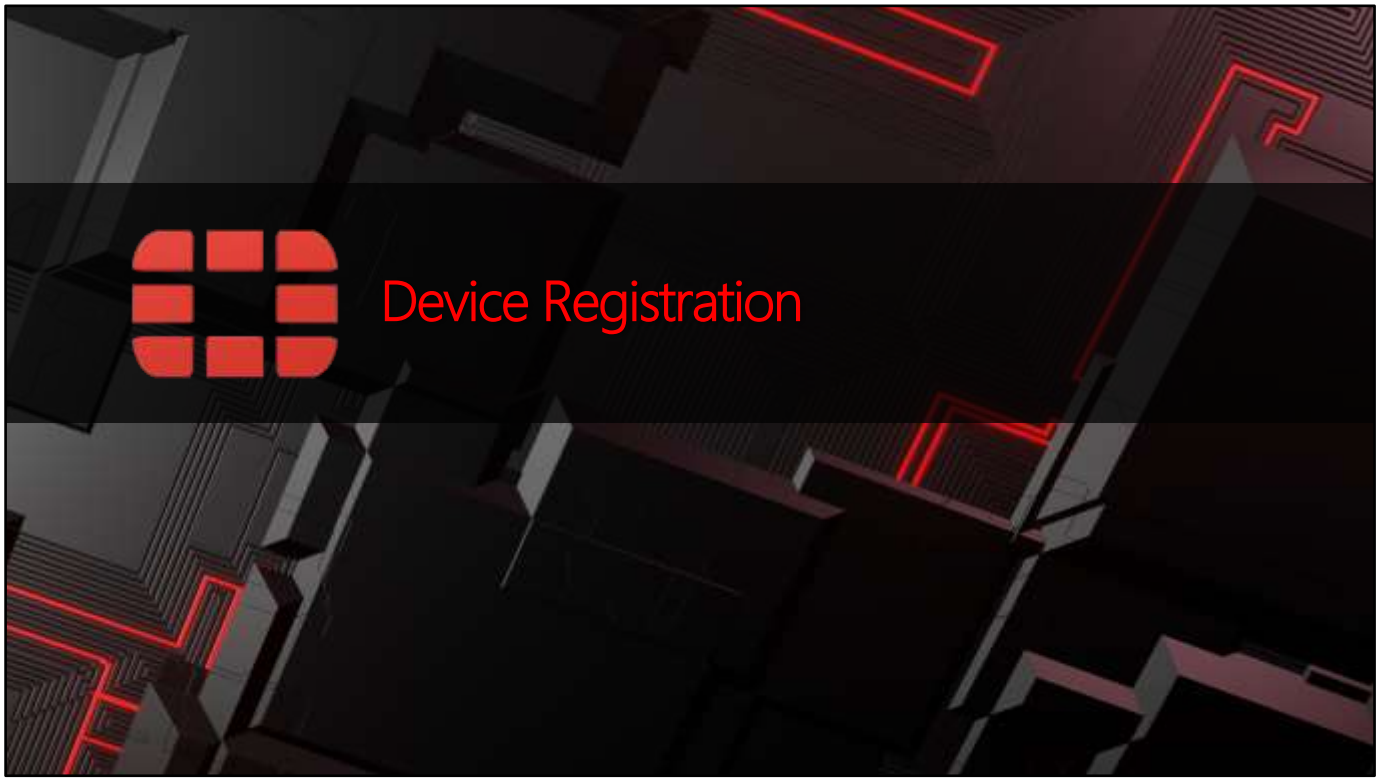
Create, Edit, Delete, Assign



Conclusions

Provisioning Templates

- Applying common device settings to devices
- Provisioning
- Create New, Edit, Delete, Assign



Device Registration

Provisioning Templates

- Each ADOM has its own set of templates
- Can export from one ADOM to another

```
execute fmprofile export-profile <ADOM name> <profile name> <output file name>
```

Export profile from first ADOM to dump to file system

```
execute fmprofile import-profile <ADOM name> <profile name> <full path of exported file>
```

Import profile to new ADOM from file system

Wizards

Assist with various tasks

- Main Wizards
  - Add Device
  - Install
  - Import config
  - Re-Install Policy

Methods Overview

01 Device Registration Wizard

FortiManager Admin uses device registration wizard to register device

If device details are correct, FortiManager registers the device

02 Requests from supported device

Admin from support device request registration

FortiManager admin accepts/denies requests

Add Device Wizard

Adds devices centrally managed by your FortiManager

Import all policies and objects from device into Policy& Objects database

Add devices that are not yet online

Performs multiple checks to ensure potential issues such as duplicate names and conflicts are avoided

Add devices through Device Manager (Device Manager -> Add Device)

Register Fortigate devices only in the root ADOM

If using customer ADOM based on type of device you are registering. Switch to that ADOM before using the wizard

Demo

Add Device Wizard – OAUTH

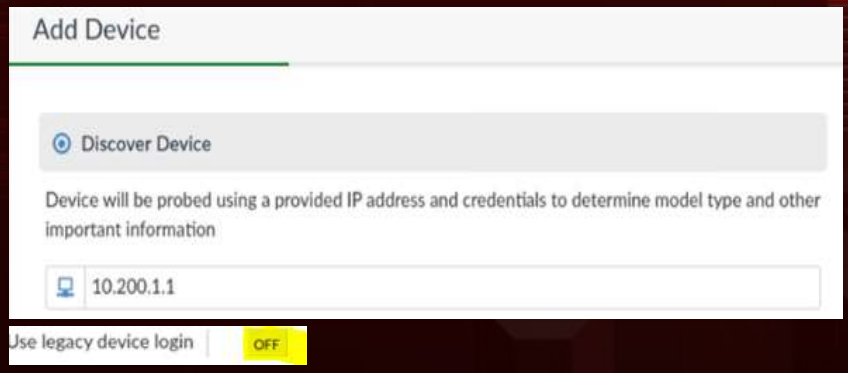
OAuth is an open standard for access delegation, commonly used as a way for internet users to grant websites or applications access to their information on other websites but without giving them the passwords

Add device wizard and Discovery mode can use OAUTH for authorization

- Use legacy device login set to off

Allow pop-ups in your browser

Add Device Wizard – OAUTH

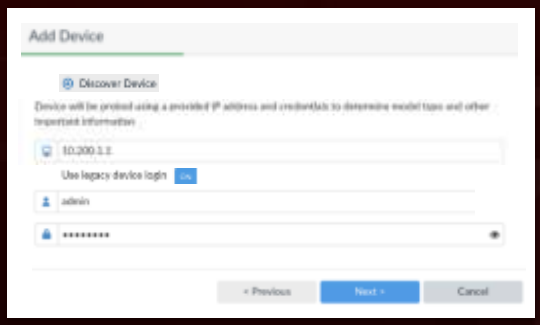


Add Device Wizard – OAUTH

Discover Device – Legacy Login

Provide FortiGate device IP and login credentials

Credentials must be full read/write



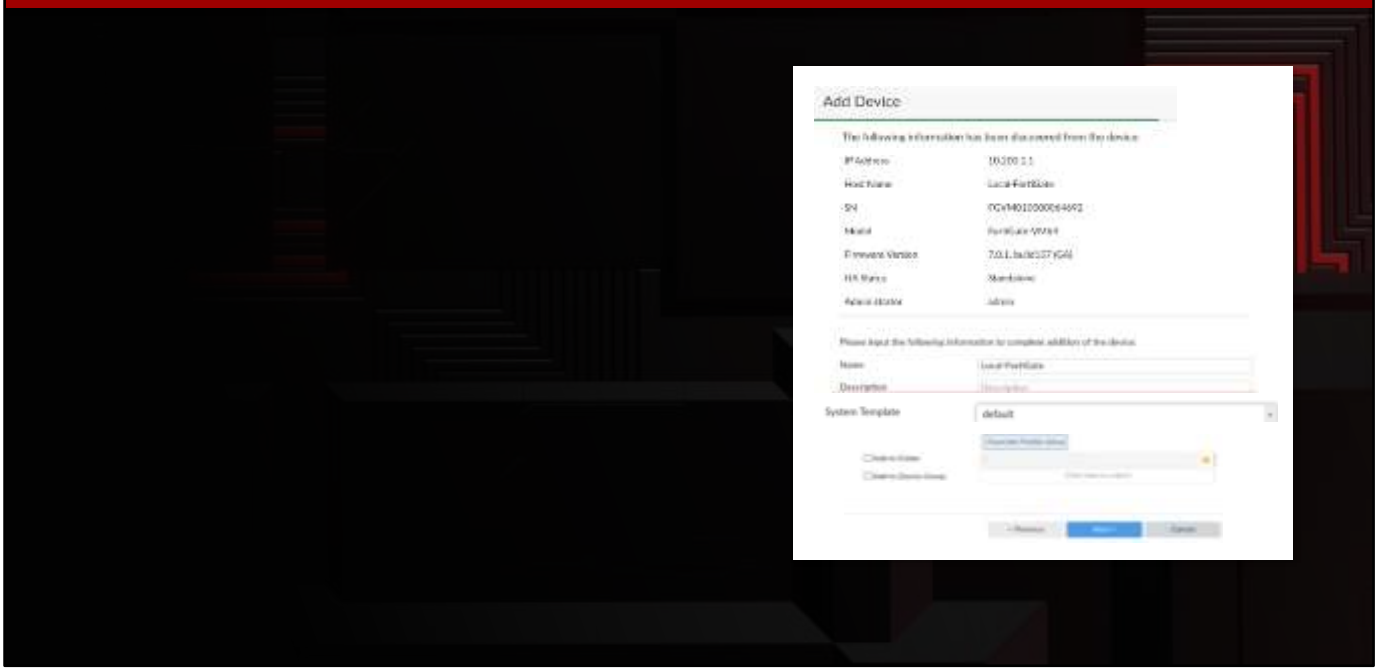
Discover Device – Legacy Login

FortiManager discovers information about the device

- IP ADDRESS
- Host Name
- Serial Number
- Model
- Firmware version
- HA Status
- Admin username

Can apply system templates for specific common device-level settings

Discover Device – Legacy Login



Legacy Login – CLI

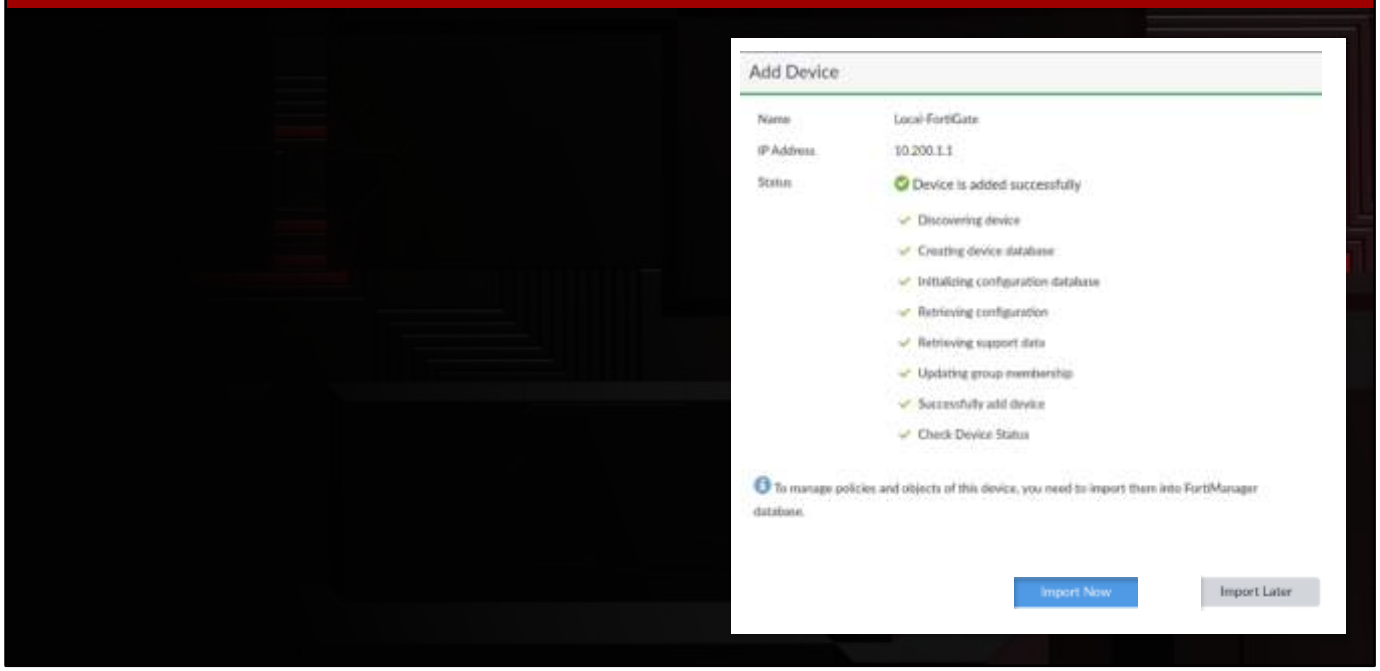
```
# diagnose debug application depmanager 255
# diagnose debug enable

FMG-VM64 # Request:
{ "client": "dvm\/cmd:dvm\/cmd\/discover\/device ...:11174", "id": 2, "method": "
exec", "params": [{ "data": { "host": "10.200.1.1", "passwd": "*******", "usr": "
admin"},
Response:
{ "id": 168, "result": [{ "data": { "branch_pt": 157, "build": 157, "managed_serial": "FMG-VM0A16001583"
"platform_str": "FortiGate-VM64", "serialno": "FGVM010000064692", "version": 700}, "status": {
"code": 0, "message": "ok"}, "url": "start\/probe\/session"}]}.....
```

Device Wizard – Import Options

- Discovers and creates initial config
- Retrieves support contract and IPS signatures
- Choose to import policies and objects
  - Import Now
    - Policy package created
    - Objects added in common ADOM database
  - Import Later
    - No policy package and objects added
    - Can be imported later using the import policy wizard

Device Wizard – Import Options

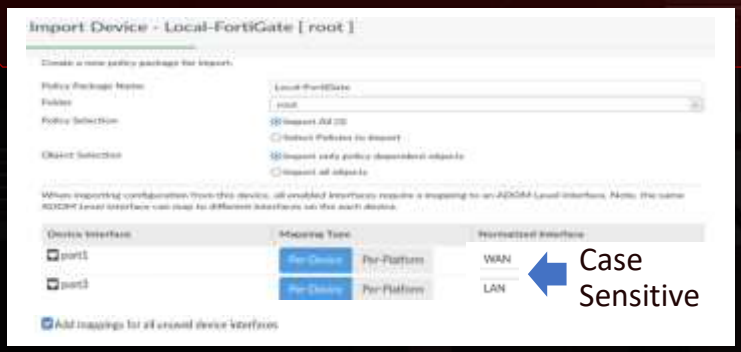


Device Wizard – Policy and Objects

Allows import of policies and objects
Create Policy package under Policy and Object pane

Device Wizard – Interface Mapping

Maps the device interface to the ADOM interface



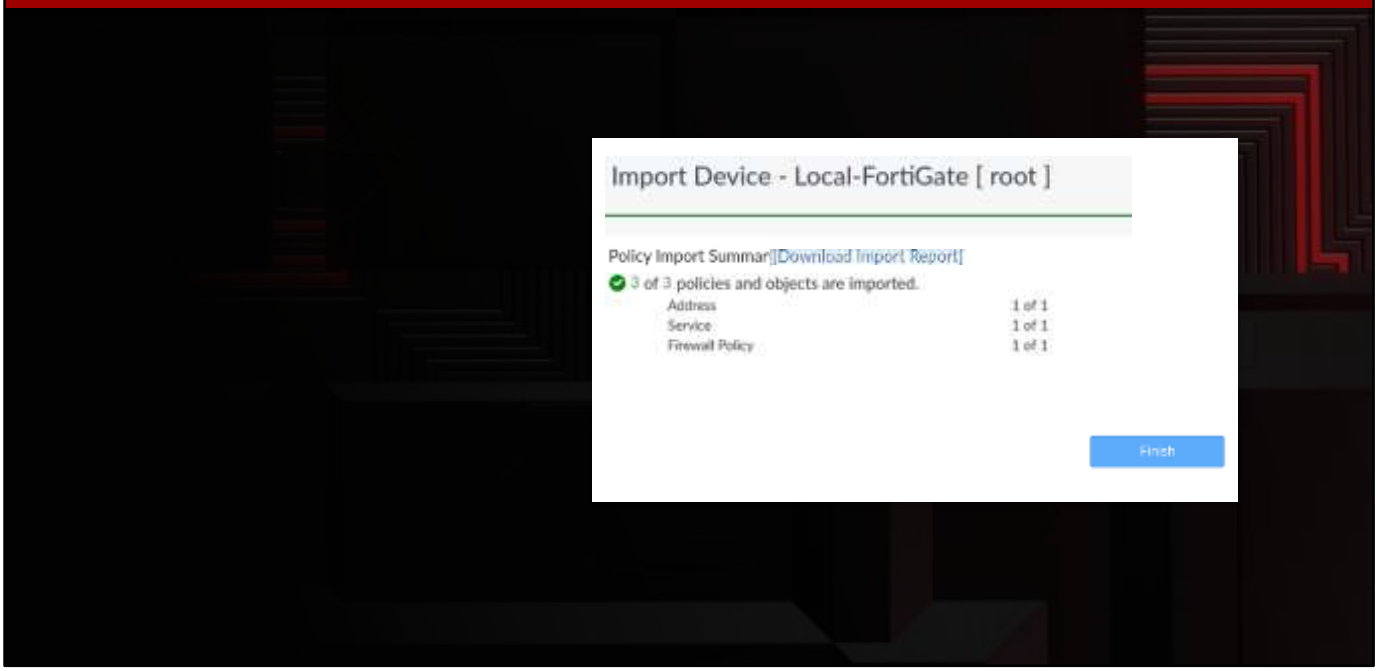
Device Wizard – Object Conflicts

Searches for Objects to be imported and reports conflicts

Device Wizard – Object Import

Displays objects being imported from Fortigate into FortiManager

Device Wizard – Import Summary



Import Report

Start to imp[ort config from device(Local-Firtigate) vdom(root) to adom(new-adom), package(Local-FortiGate-pkg)

"firewall service category",SKIPPED,"(name=General, oid=394,DUPLICATE)

"firewall address".SUCCESS,'(name=SUBNET-LOCAL,oid=525,new object)“

"firewall service custom",SUCCESS,"(name=ALL,oid=44, update previous Object)“

"firewall policy",SUCCESS,"(namew=4, oid=922, new object)"

Device Wizard - Model Device

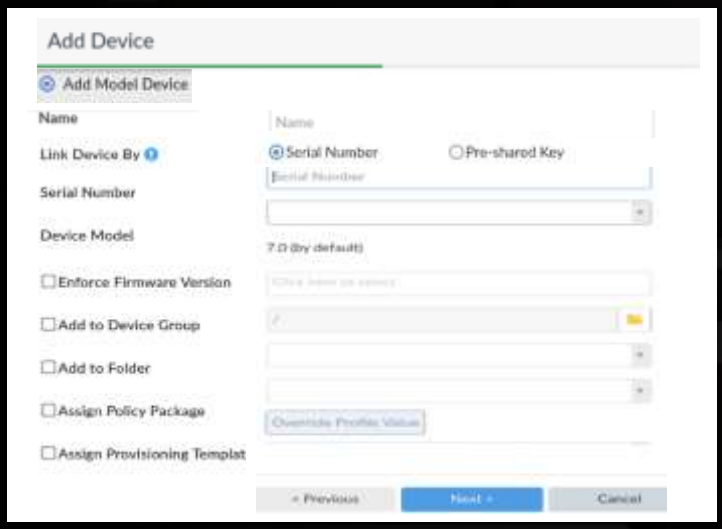
Supports zero-touch, on-site Fortigate deployment by automatically promoting a model device to a managed device

Provisions a device in FortiManager, that is not yet online

Can link device by either:

- Fortigate serial number
- Pre-shared key
  - Must be unique if adding multiple model devices

Device Wizard - Model Device



Device Wizard - FortiGate Configuration

Configuration on FortiGate

If serial number is used

```
config system central-management
set type fortimanager
set fmg <FortiManager IP>
end
config system central-management
set type fortimanager
set fmg <FortiManager IP>
end

execute central-mgmt register-device
<fmg-serial-no> <fmg-register-password>
```

Add Device Wizard - UnAuthorized Device

UnAuthorized devices requesting registration appear under Device Manager

- If ADOMS are enabled, by default unauthorized FortiGate devices appear in the root ADOM

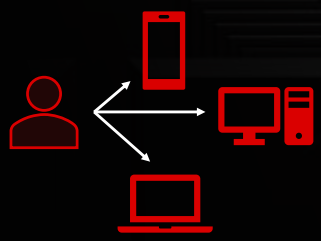
Can enable automatic registration – the default is disabled

Can add Fortigate in different ADOM, if ADOMs enabled

Add Multiple Devices

Can add multiple devices from the Device Manager

Policy package must be imported after devices are added



Viewing Authorized Devices

Device Manager list all authorized and (unauthorized devices)

Chassis Management

Some FortiManager devices support chassis management

- Enable chassis management under advance settings

Added under default chassis ADOM

01. Enter the IP address of the shelf manager running on the chassis
02. You can select Fortigate, FortiCarrier, or FortiSwitch as a slot

Device Count on FortiManager

- Maximum number of managed devices/VMs varies by model
  - Check product matrix for the model limits
- FortiGate Clusters counts as one device
- VDOM count as one device

HA Cluster

- Managed as a single device
- Diagnose dvm device list to see cluster members
- FortiManager is unaware of the FortiGate HA sync status
- HA per device management interface is for SNMP monitoring only for the secondary FortiGate
- Device serial number is automatically updated when there is a new primary FortiGate
- FortiGate HA config is read-only in FortiManager (GUI only)
  - HA failover operations are possible on FortiManager
- Local changes to the Fortigate HA configuration do no cause out-of-sync state

FGFM Management Protocol

- An FGFM daemon runs on both
  - FortiGate – fgfmd
  - FortiManager – fgfmsd
- Secure communication tunnel on port TCP 541 between:
  - FortiManager and all managed FortiGate devices
  - TCP based supports port-based NAT
- Protocol is enabled for each interface on FortiGate (FMG-Access)
- Link-level addresses are used for the management traffic tunnel over secured connections
- Once FortiGate is managed, the FGFM tunnel is authenticated and established using the serial number verification of the FortiGate in the FGFM tunnel

Device Discovery and Add Process

When FortiGate is added to FortiManager, it goes through two steps:

01 Discovery

Secure tunnel established and a get system status is collected to obtain minimal information to start modeling the device

02 Adding

Various other configuration details are obtained through CLI commands and the configuration is retrieved and stored in the device database

The FGFM tunnel is initiated by either of the following:

01 FortiManager, during add and discovery process

02 FortiGate, if a management request is sent by the FortiGate

Device Discovery and Add Process

```
get sys status

get system interface
get system interface physical
get hardware status

get mgmt-data status

config system central-management
set type fortimanager
unset serial-number
set serial-number "FGVM-VM123456"
set fmg "10.200.1.241"
end

get ips rule status
get ips decorder status
get application name status
```

Discovery Failure Check

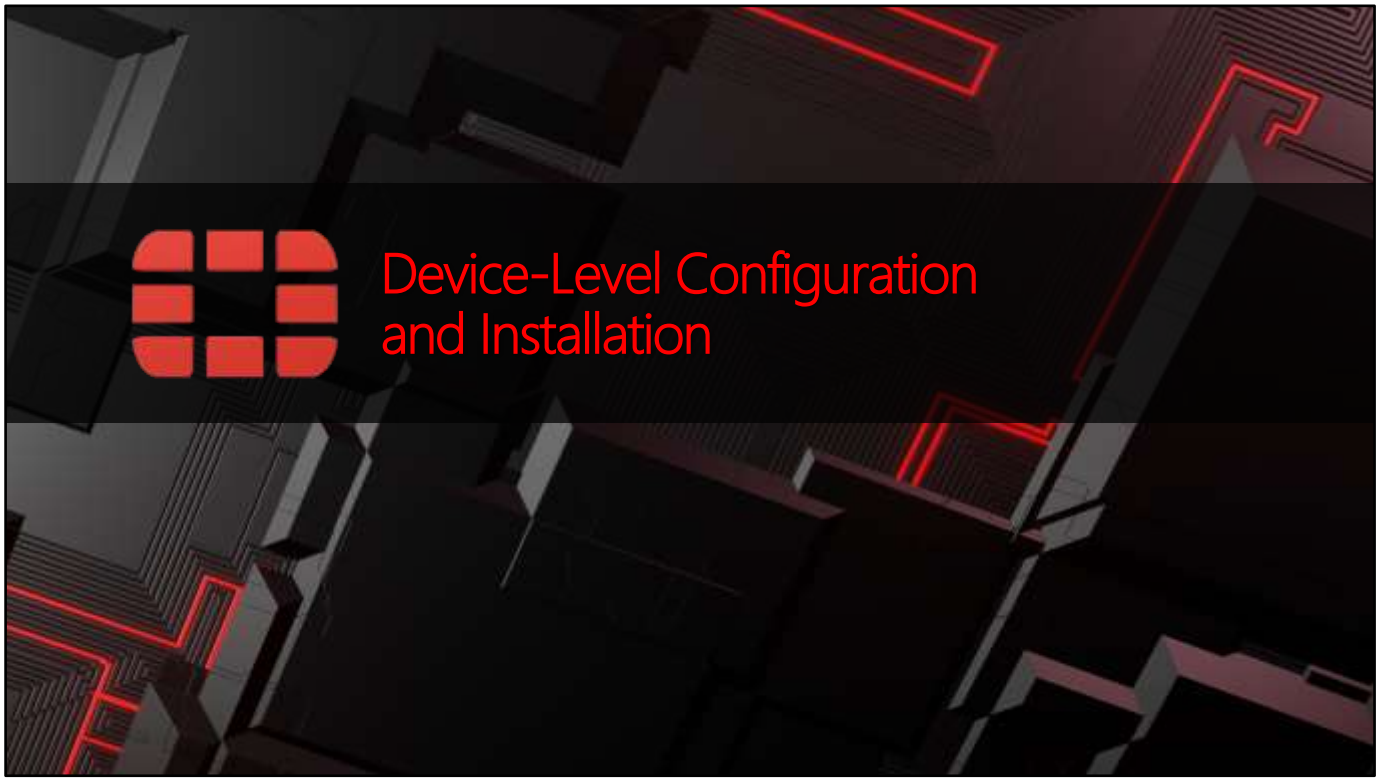
What to Investigate	Common Solutions
Are the devices able to contact each other?	# execute ping
Does the FortiManager administrator have sufficient privileges to add the FortiGate?	Check the FortiManager administrator profile.
Is FortiManager in offline mode? (Can be due to configuration restore.)	Disable offline mode on the **System Settings** pane
Is TCP port 541, between FortiManager and FortiGate, blocked? (Used for communication between FortiGate and FortiManager.)	Use the following command to run packet sniffer on both devices on TCP port 541: # diagnose sniff packet <interface> <filter> <level>
Are the IP address and credentials (super_admin access) of the FortiGate correct in the add device wizard?	Confirm the FortiGate IP address and credentials

Discovery Failure Check

What to Investigate	Common Solutions
Is FGM access on FortiGate interface disabled?	Enable FGFM access on the FortiGate interface facing FortiManager
Is FortiGate already in an unauthorized device list?	Check under the root ADOM or run the CLI `# diagnose dvm device list` If appearing as unauthorized device, add it from root ADOM.
Are the date and time correct on both devices? (Incorrect date or time can result in expired certificates being used in tunnel negotiation between the two devices.)	Check the date and time on both devices
Are incorrect or excessive debug levels set on FortiGate? (May prevent FortiGate from discovery.)	Run the following CLI command on FortiGate to reset the debug level: `diagnose debug reset`

Conclusions

- Configure and apply provisioning profiles to your managed devices
- Add Fortigate to FortiManager
- Understand the import report
- Add multiple Fortigate devices to FortiManager at same time
- Add chassis to FortiManager
- Manage a FortiGate HA using FortiManager
- Troubleshoot device discovery issues



Overview

- Configure device-level settings
- Understand FortiGate configuration status and synchronization behavior
- Push config changes to FortiGate
- Use revision history for diagnosing and troubleshooting
- Configure and install scripts and managed devices
- Use device groups for simplifying management of FortiGate devices

Device-Level Settings

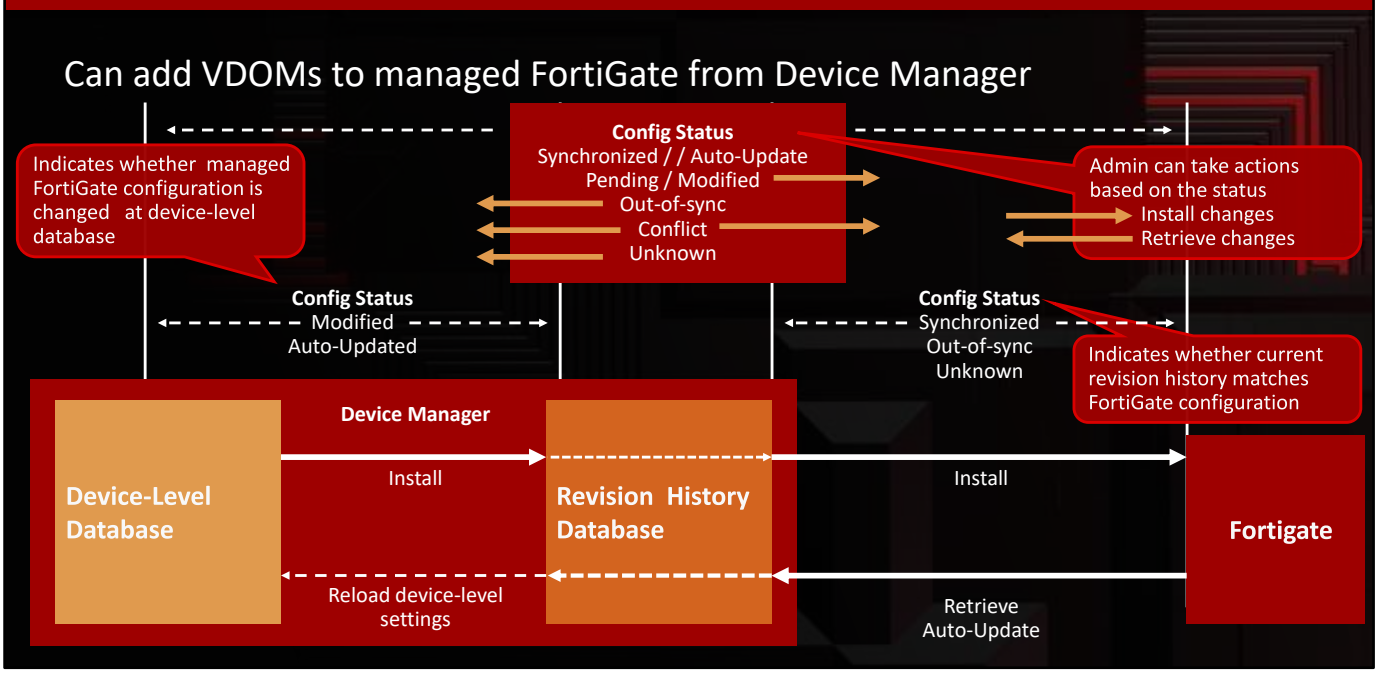
Device-Level settings can be viewed or configured for individual managed devices

CLI-Only Objects

Can be configured through the FortiManager GUI

- Disabled by default
- Can enable under display options

VDOMs



Managed Device Status

Indicate whether FortiGate configuration matches the current revision history

MAIN STATUS

Synchronized

Out-of-Sync

Unknown

Conflict

Installation failed

Configurations are modified on both FortiManager and the managed device, and are not automatically synchronized with FortiManager

Managed Device Status

Indicate whether the FortiGate configuration in the device-level database matches current revision history

MAIN STATUS

Auto-updated

FortiGate configuration at device-level database

Revision History

Modified

FortiGate configuration at device-level database

Revision History

Modified
auto-updated)

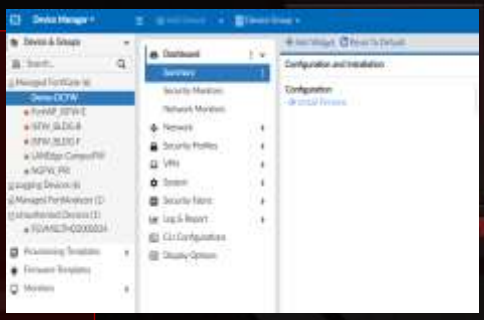
(re-sent

FortiGate configuration at device-level database

Revision History

Installation Preview

- Displays device-level changed applied to FortiManager
  - Does not display ADOM-level changes
    - Changes made to firewall policies
- Changes are yet to be installed



Install Preview of Local-FortiGate

```
config router static
    edit 2
        set gateway 10.200.2.254
        set priority 5
        set device "port2"
    next
end
```

FGFM Session List

Lists the status of the FGFM tunnels for all managed devices

- IP Address
- UpTime
- Link-Level address

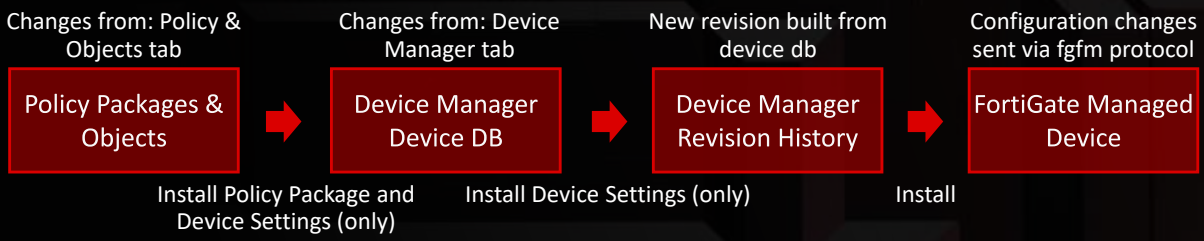
```
# diagnose fgfm sess-list
Session count = 1
Local-Fortigate(270) sn(FGFM1234567890) ip(10.10.10.10)
state(3)tunnel(169.254.0.2) UpTime: Mon Feb 6 15:15:15 202
```

Installation Process

Changes made from the Device Manager Pane are made to the device database

A new revision is generated and changes installed

Changes made from the Policy and Object Pan are made to the device database



Install Policy Package and Device Settings (only)

Install Device Settings (only)

Install

Install Wizard

Installs settings on FortiGate device(s)

Two Install Wizard Options

Device Settings Only

- Only device settings for a select set of devices
- Policy and Objects are not installed

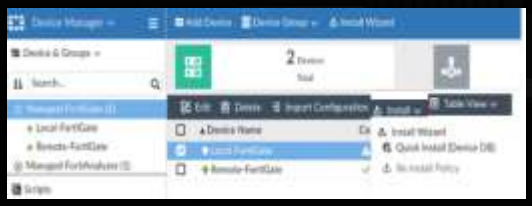
Policy Package and Device Settings

- Selected policy package
- Any device-specific settings for devices associated with the package

Install Wizard

Launch Install Wizard from device manager

Select Install Device Settings (only) to install device-level changes



Install Wizard – Cont

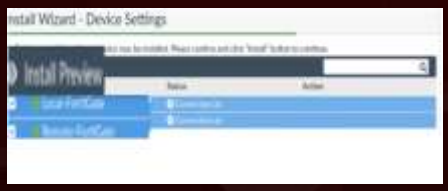
Device and Selection and Validation

- Indicate where to install changes
- Can select multiple device, if changes are mde to multiple
- Verify device settings that will be installed
- Prepares a preview

Install Wizard – Cont

Multiple Device Selection and Preview

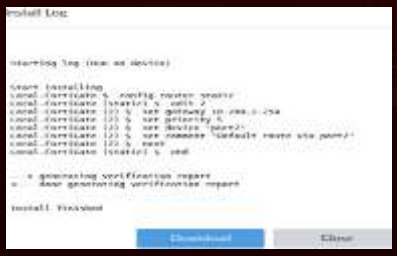
- Can select multiple devices if needed
- Consolidated preview for up to 10 devices



Install Wizard – Cont

Install

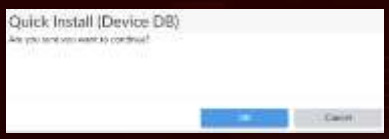
- Indicate where changes were installed
- Installation status
- Provides Install Log



Quick Install

Install device-level changes to FortiGate without wizard

Does not provide preview



Revision History

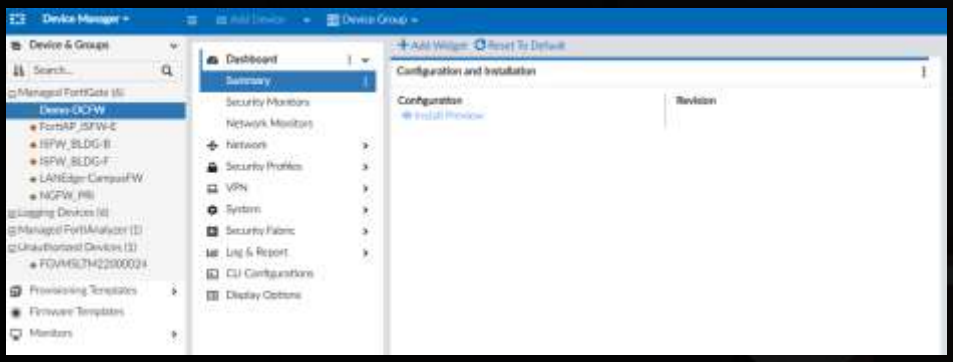
The repository stores all configuration revisions for devices

- Tags each revision with an ID number
- Identifies which admin or process created the revisions

Allows

- View version history
- Download Configuration
- Compare different versions
- View Installation logs

Revision History Cont.



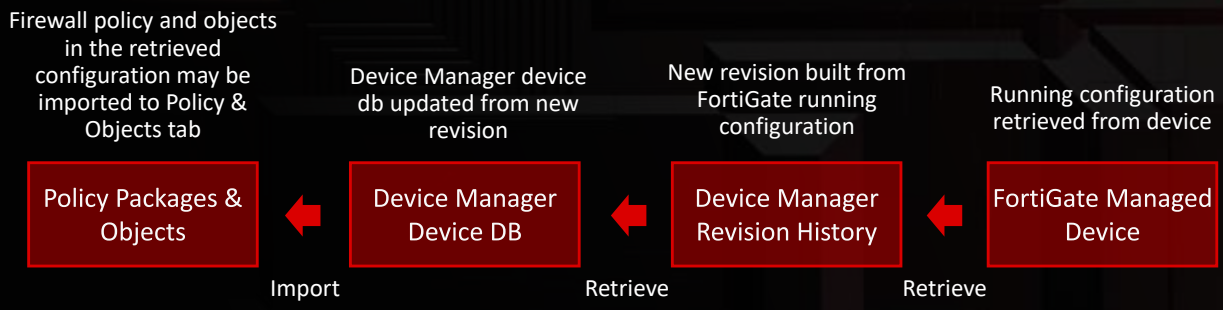
Configuration Issues

- Retrieve the configuration of a managed device
- Automatic update
- Install configuration changes to FortiGate after modifying on FortiManager
- Revert to previous working config
- Import configuration from a local computer
  - Can import files that are downloaded from a FortiManager, otherwise import will fail

Retrieve

Checks current configuration on the device

UpDates FortiManager revision repository



Automatic UpDate

Modifying configuration directly on a managed device automatically creates a new revision

Can disable auto update from FortiManager CLI

- Default Enabled
- If disabled can accept or reject changes

Config status is updated automatically under device manager

```
config system admin settings
set auto-update disable
end
```

Revert

Usually the top reversion entry corresponds to the device manager database, which is the synced config

Can revert to previous revision history

- Will revert only database to previous revisions
- Revert does not revert policy and objects, must import policies and objects

Must install these reverted changes on FortiGate

Scripts

- Can make multiple changes to multiple managed devices
  - Provision FortiGate devices
  - Automate config changes
- Bulk config changes to maintain consistency
- CLI – Command line interface (enabled by default)
- TCL – Tool Command Line
- TCP can be enabled on the FortiManager CLI

```
config system admin setting
set show_tcl_script enable
end
```

```
TCL scripts are not run through the FGFM tunnel like CLI.
Use SSH to authenticate and implement
```

Scripts (Cont.)

Best Practice

Use complete command syntax

```
config router static  VS  con rou stat
```

A comment line starts with the # symbol

```
# This line is for commenting and documentation
```

Ensure console output on the FortiGate CLI is set to standard, otherwise scripts and other output longer that screen length will not execute or display properly

```
config system console
set output standard
end
```

Scripts (Cont.)

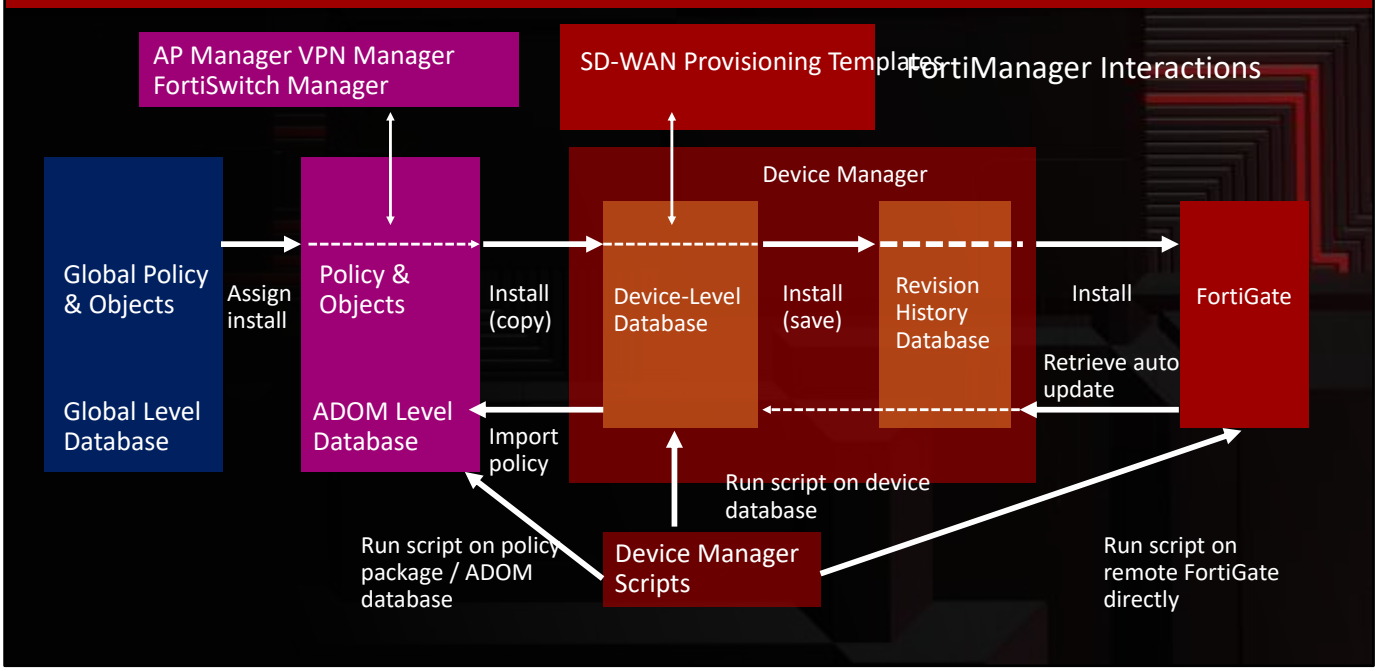
Can be run on

- Device Database
- Policy package, ADOM database

By default, scripts can run on the device database

Can select advance filters to restrict the script to be executed on devices

FortiGate



Running and Scheduling

Execute Scripts

- Run Script Now
- Schedule Scripts

Install must be performed if a script run on the device database, policy package, or ADOM database

Can clone, export, or import scripts from a local computer

Schedules cannot be used on scripts with the target policy package or ADOM database

```
config system admin setting
set show_schedule_script enable
end
```

Troubleshooting

Diagnose debug application depmanager 255

Diagnose debug enable

Common errors	Common causes	Common solution
Command parse error	Misspelled keyword or incorrect command format*	Check the script output
Unknown action	Previous line of the script was not executed	Check the script output
Device <name> filed-1	Problem with the end of the script. Usually script has no end statement FortiGate not in sync with FortiManager	Check the script output Add an end statement Resync FortiGate by retrieving configuration

Troubleshooting (Cont.)

There should be no punctuation at start or end of lines

Can view the details from script history

Task Monitor

From events logs – if debug level set to debug

Useful Commands

CLI Command	Used for
clean-sched	Unable to delete scheduled scripts if an associated device has been deleted Cleans script schedule table for all non-existent devices
copy	Copy scripts between ADOMs
Import	Import a script to FortiManager
List <adom name>	List scripts in ADOMs
Showlog <devicename>	Show a run script log for a device

Conclusions

Configure device-level settings

Understand FortiGate configuration status and synchronization behavior

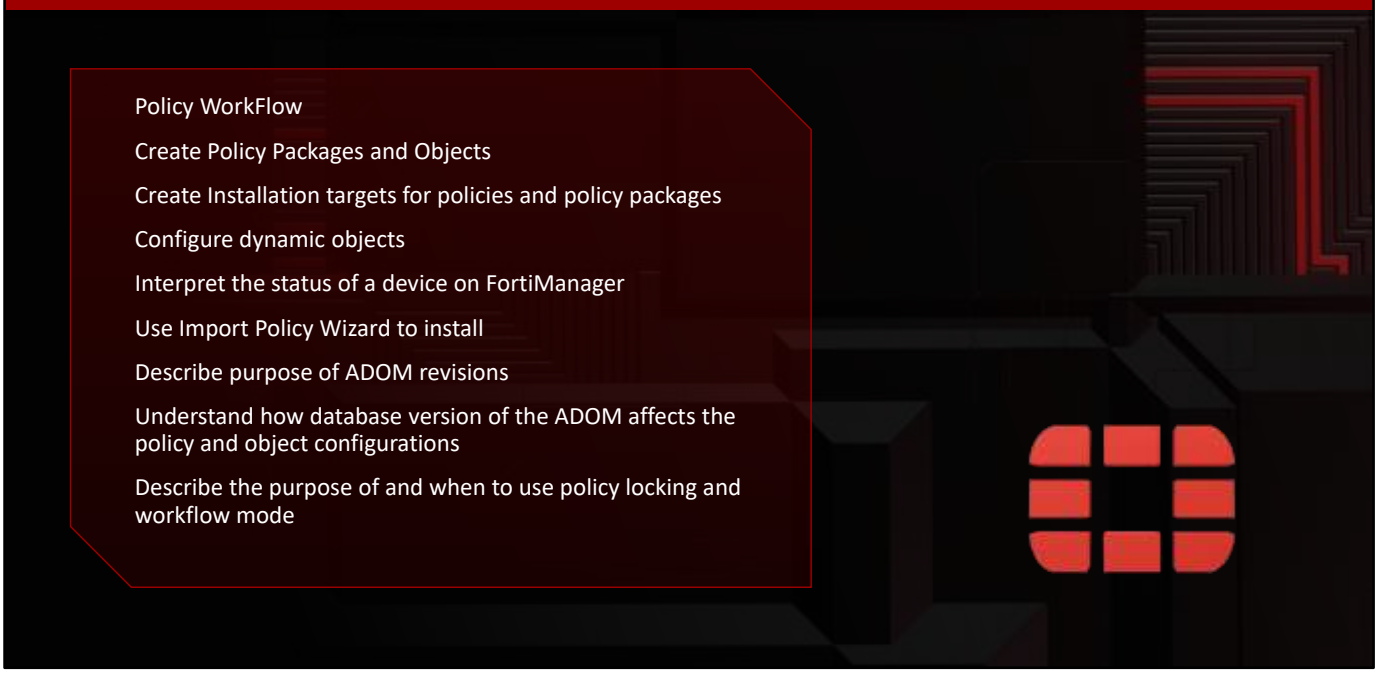
Push config changes to FortiGate

Use revision history for diagnosing and troubleshooting

Configure and install scripts and managed devices

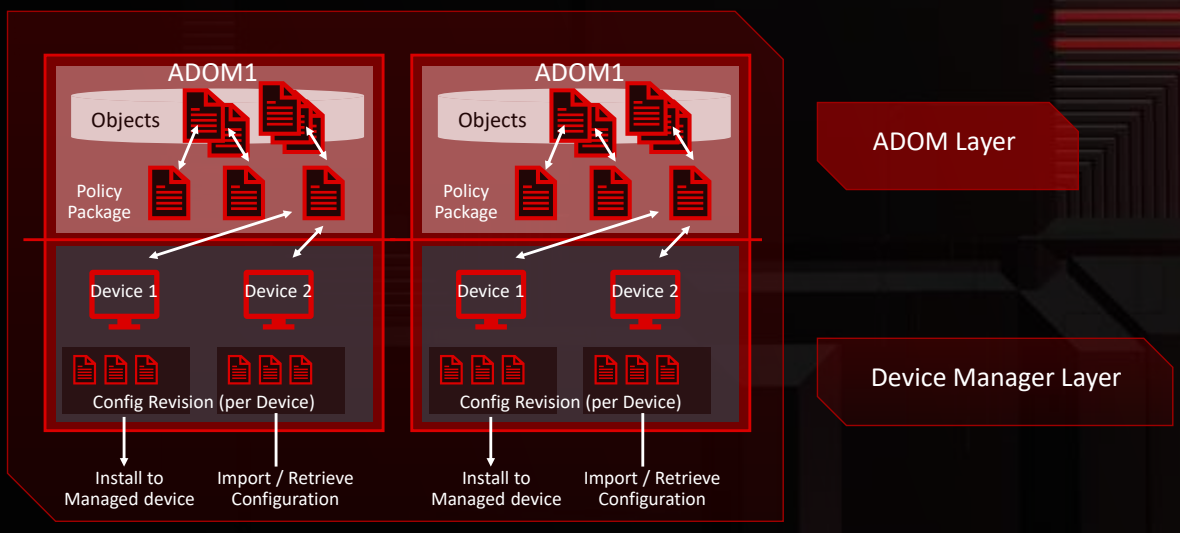
Use device groups for simplifying management of FortiGate devices

Overview



- Policy WorkFlow
- Create Policy Packages and Objects
- Create Installation targets for policies and policy packages
- Configure dynamic objects
- Interpret the status of a device on FortiManager
- Use Import Policy Wizard to install
- Describe purpose of ADOM revisions
- Understand how database version of the ADOM affects the policy and object configurations
- Describe the purpose of and when to use policy locking and workflow mode

Policy WorkFlow



Policy Packages

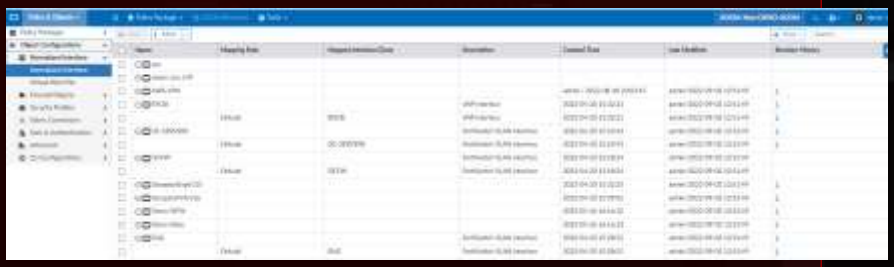
ADOM -> Policy & Objects -> Policy Package

- Create firewall policy in policy packages
- Displays all the policy packages for the adom

Object Configurations

ADOM -> Policy & Objects -> Object Configuration

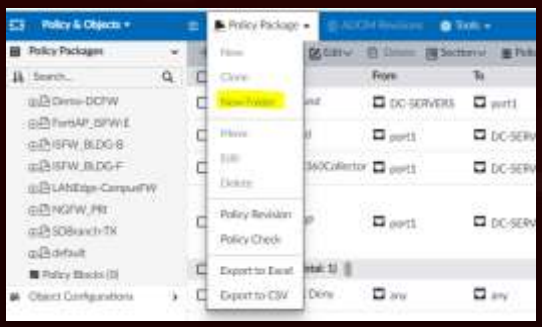
Firewall Policies in policy packages refer to objects define in ADOM database



Policy Folders

Manage and Organize your policy packages

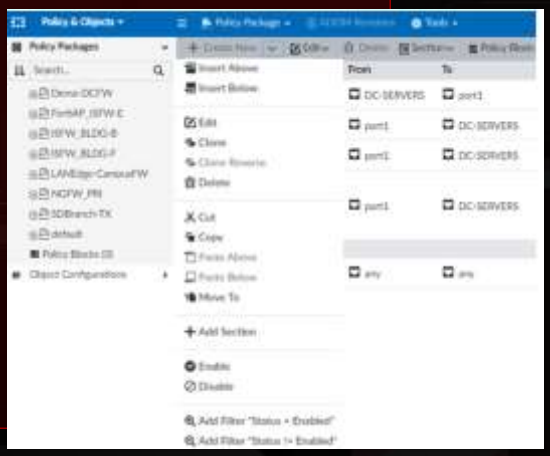
Allows nesting of policy folders



Creating and Modifying Firewall Policies

Policy Packages -> Firewall Policy

- Create new
- Insert Policy
- Clone – cut – copy – paste
- Move policy
- Enable and disable
- delete

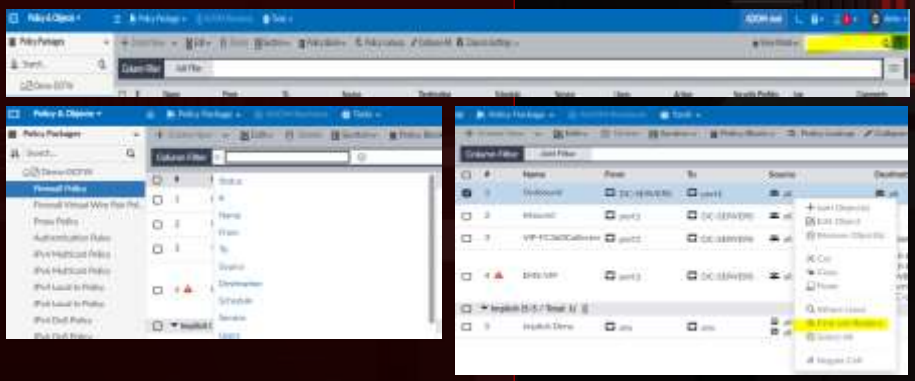


Adding and Removing Objects

Policy Search and Filter

Use search field to search or filter for matching rules or objects

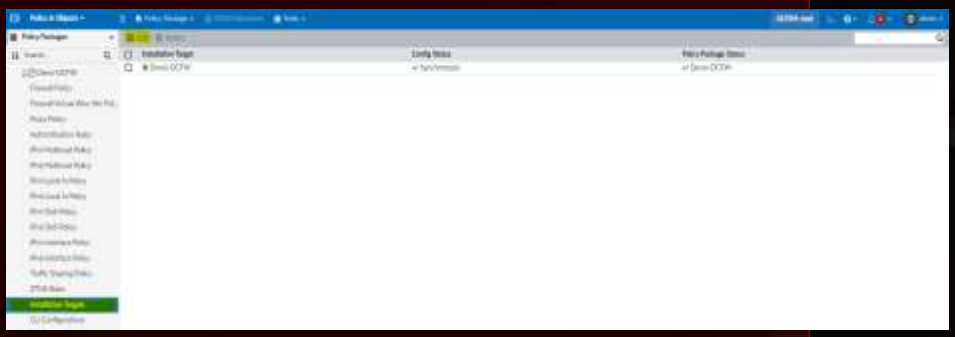
- Simple Search
- Column Filter
- Find and Replace



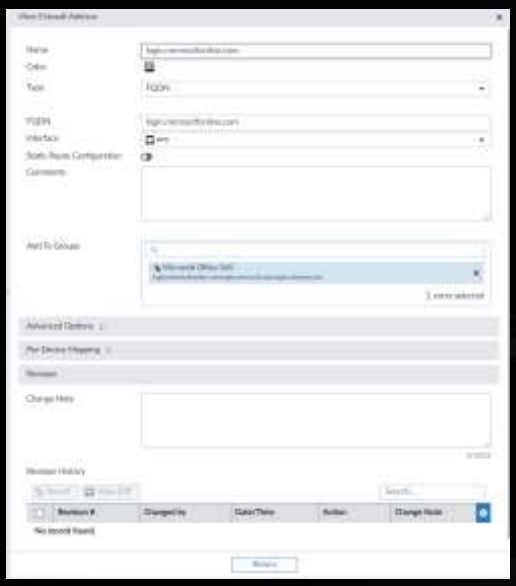
Installation Target

Policy Package -> Installation Targets

Target one or more devices or VDOMs

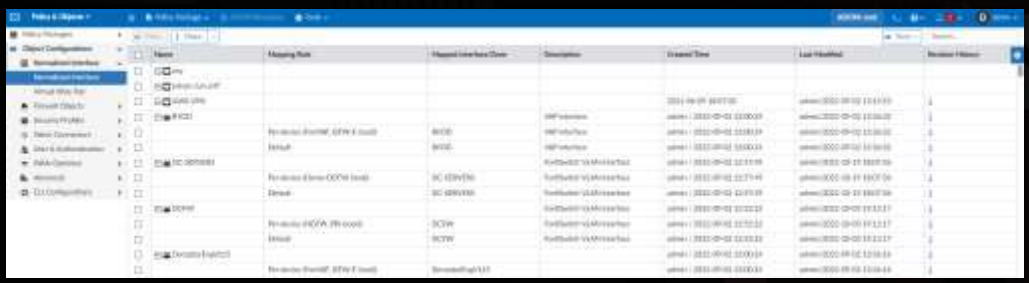


Dynamic Objects



Interface Mappings

- Defines mapping rules for interfaces
- When normalized interface is used in Policy, the per-devices mappings have higher priority than per-platform mappings



Firewall Policy

FortiManager

Used Objects

- You can delete a used Object
  - View where the Object is used in the Policy

- If you delete a used object it will be replaced with a none object
  - This none object will result in that policy resulting in a block

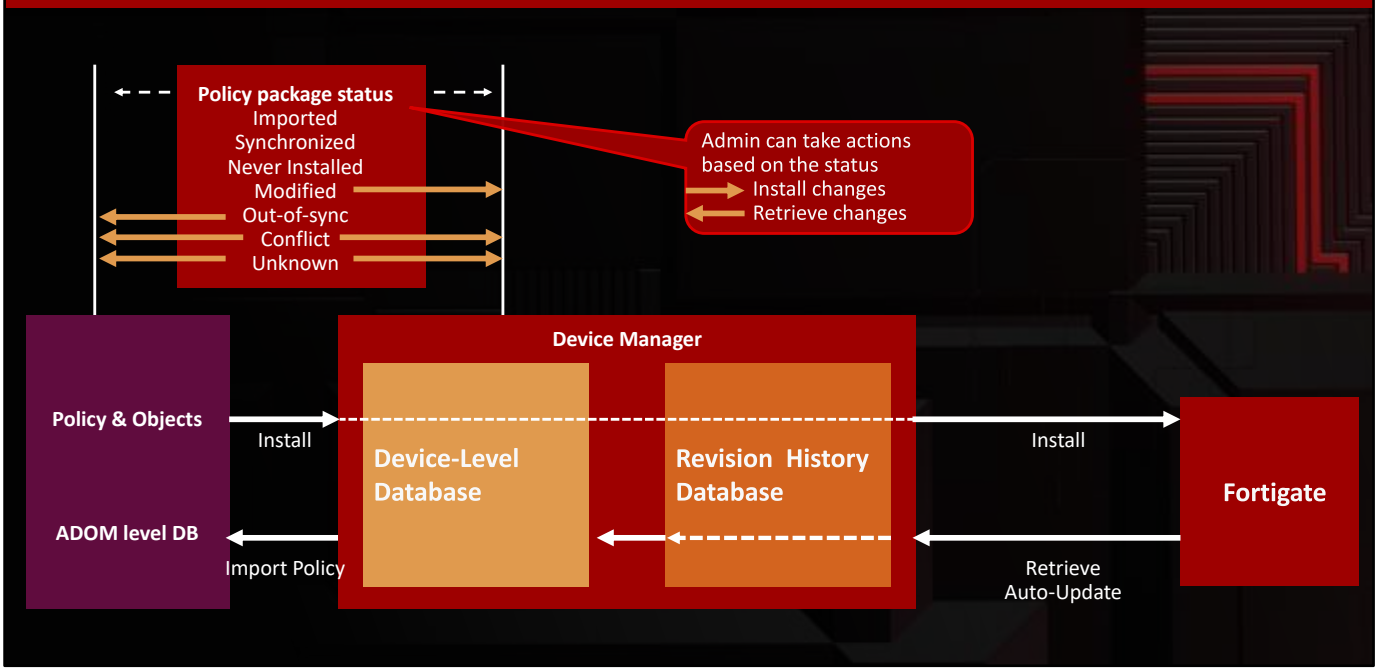
UnUsed/Duplicate Objects

- GUI tool can help identify unused objects
- Tool displays all object that are currently ununsed
- You can merge duplicate objects

Policy Check

- Looks for consistency and conflicts in policy package
- Optimize rules to assist in reducing size of policy database

Per-Policy Lock – Policy Package Status



ADOM Revisions

- Policy Objects -> ADOM Revisions
- Create a snapshot of all policy and object configurations for the ADOM

- Settings provides access to auto-delete settings
- Lock revisions to prevent auto-deletions

Per-Policy Lock – ADOM versions

Database versions refer to valid syntax for that FortiOS version

Moving FortiGate to another ADOM

Considerations before moving devices:

- Policies and objects don't move to the new ADOM
  - If using a shared policy package, it is not moved
- UnUsed objects don't move
- When FortiGate devices are upgraded, it is best to keep them in the same ADOM and use ADOM upgrade
- After moving devices
  - Import Policy Package
    - Can use CLI to import unused objects if needed

```
execute fmpolicy copy adom object
```

WorkSpace Mode Normal

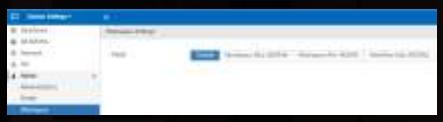
- Lock a single policy package instead of entire ADOM
- Works with workspace-mode normal
- Locks only policy package, not entire object database
- Edit locked policy in private workspace
- Multiple Admins can lock and work on separate policies at the same time
- Allows admins to lock single policy in policy package
- Lock is released automatically when admin times-out, session is closed gracefully without unlocking the policy

```
config system global
set workspace-mode normal
end
```

WorkFlow Mode

- Sessions can be created only in the Policy & Objects pane
- Another global mode that works together with ADOM locking
- Controls creation, config and installations of policies and objects
- Approval is required before changes are installed
- Mods made during a workflow session must be discarded or submitted for approval at the end of the session
- Rejected sessions can be repaired and resubmitted as a new session for approval
- Panes are initially read-only until ADOM is locked

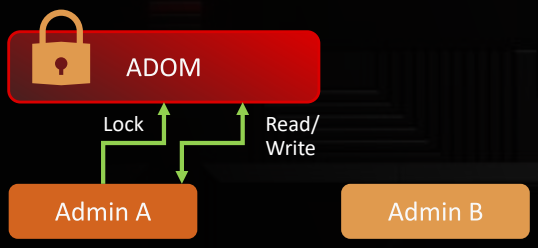
```
config system global
set workspace-mode workflow
end
```



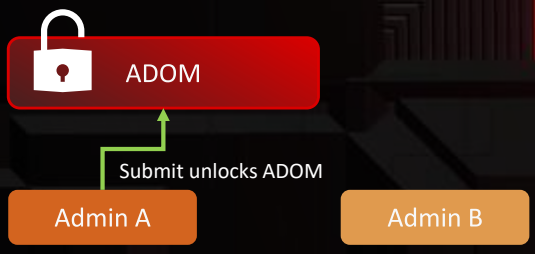
WorkFlow Mode (Cont.)

Sessions can be created only in the Policy & Admin A locks ADOM and gains read-write access.

Creates new session, changes policy and objects



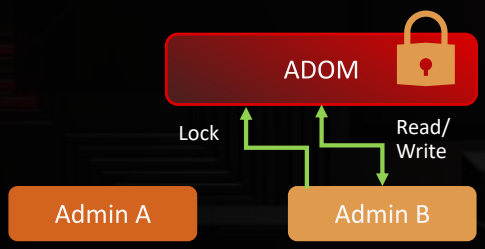
Admin A changes configuration and submits request for approval to Admin B, which unlocks the ADOM.



WorkFlow Mode (Cont.)

Admin B now locks the ADOM and has read-write access.
Admin B opens the session list and can:

- Approve
- Reject
- Discard
- View Diff

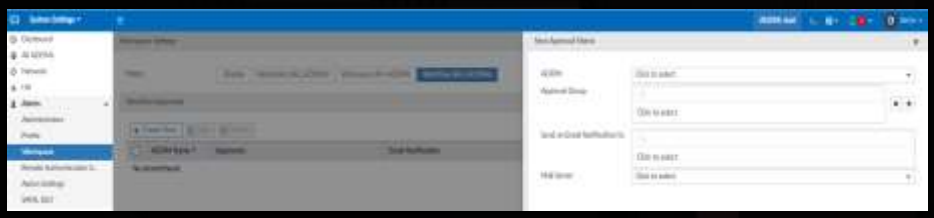


WorkFlow Permissions

Admins must be part of an approval group before the can approve

- Regardless of which admin profile an account is part of
- Also requires access to the ADOM in which the session is created

On the GUI the approval matrix must be configured before the workflow sessions are allowed



Creating a new WorkFlow Session

Start workflow session

- Select and lock ADOM
- Open session list in Policy & Objects
- Create a new session

Submitting a WorkFlow Session

- Save session then submit
  - Session changes are discarded if admin logs out without saving
  - Saved session can be updated
- Session drop down has 3 options
  - View Diff
  - Submit
  - Discard
- After submitting changes for approval ADOM is unlocked

Approving, Rejecting, or Repairing Sessions

To Approve

Admin must have assigned rights

Must lock the ADOM in which changes are made

Open session list

Approval options

- Approve
- Reject
- Discard
- View Diff

Rejected session can be resubmitted with updated changes

Locked ADOMs

- If a session is not closed gracefully (PC crashed, closed browser window, etc) FortiManager will not close the session
- Sessions will have to manually deleted CLI or GUI

Conclusions

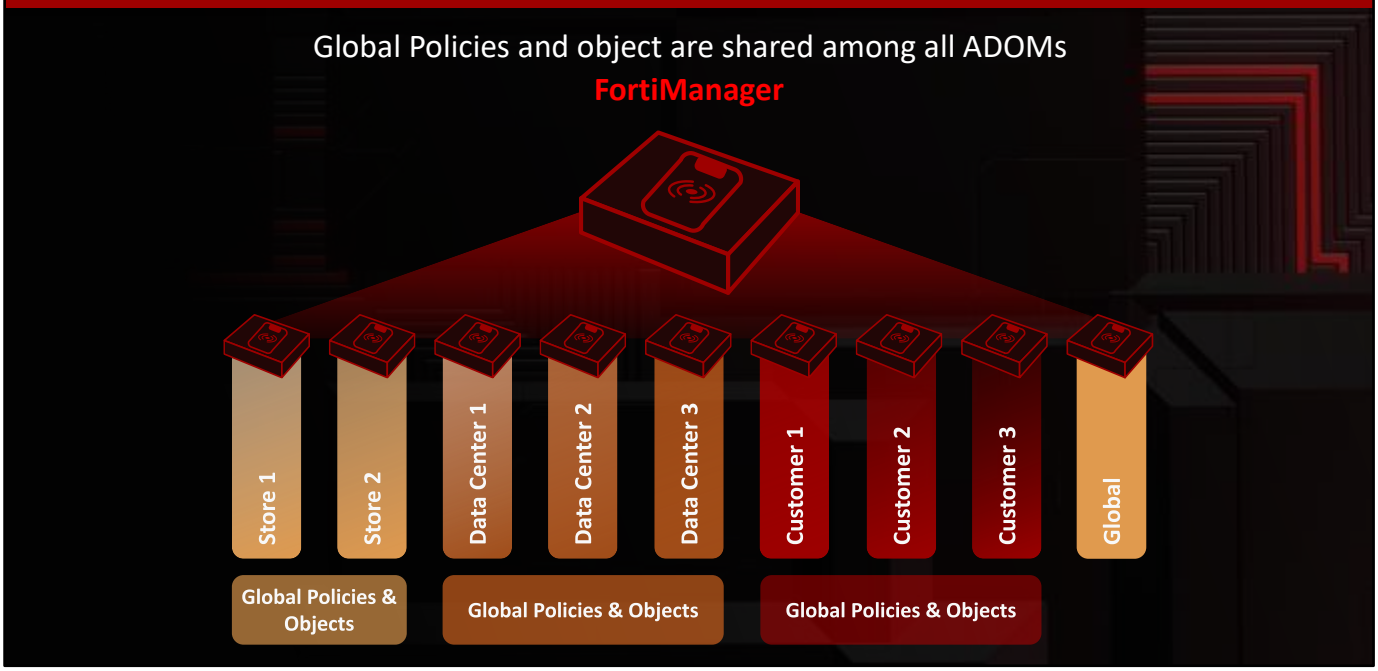
- Policy WorkFlow
- Create Policy Packages and Objects
- Create Installation targets for policies and policy packages
- Configure dynamic objects
- Interpret the status of a device on FortiManager

- Use Import Policy Wizard to install
- Describe purpose of ADOM revisions
- Understand how database version of the ADOM affects the policy and object configurations
- Describe the purpose of and when to use policy locking and workflow mode

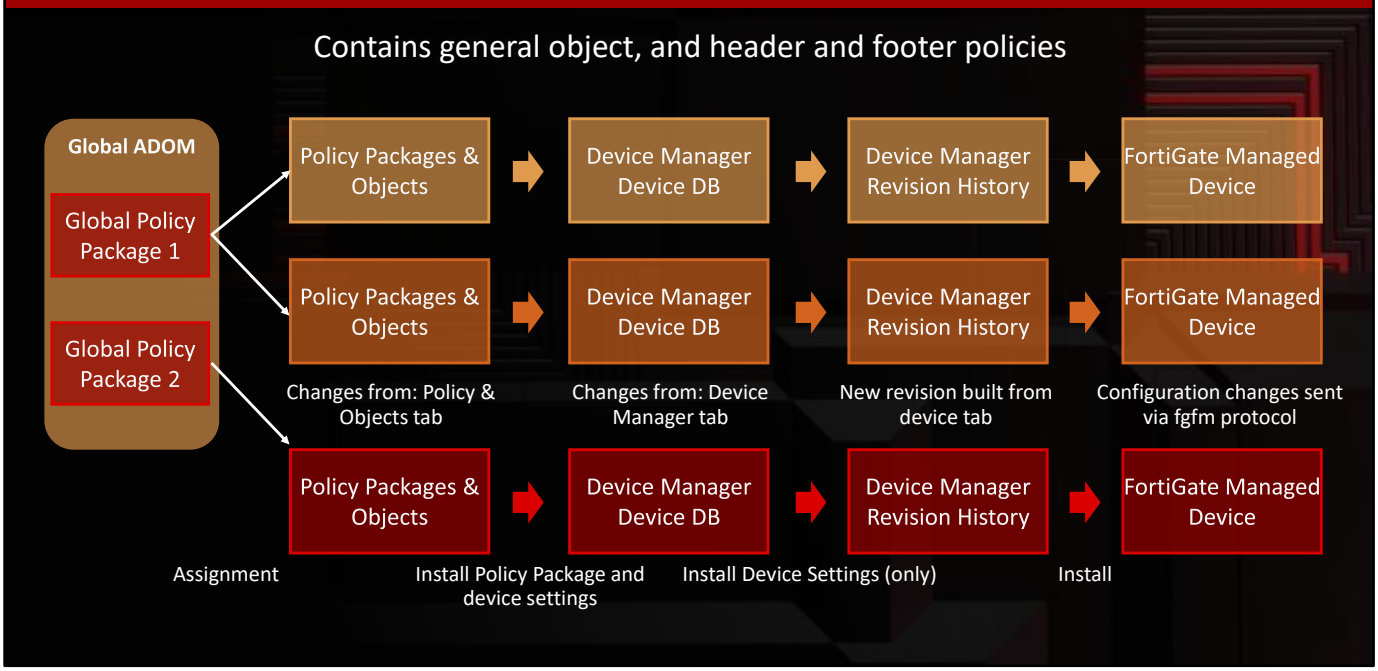
Overview

- Global ADOM
- FortiManager Panes
- SecurityFabric View with FortiManager
- Security Fabric Technology
- FortiManager MEAs
- FortiManager MEAs requirements

Shared Global Policies and Objects



Global ADOM

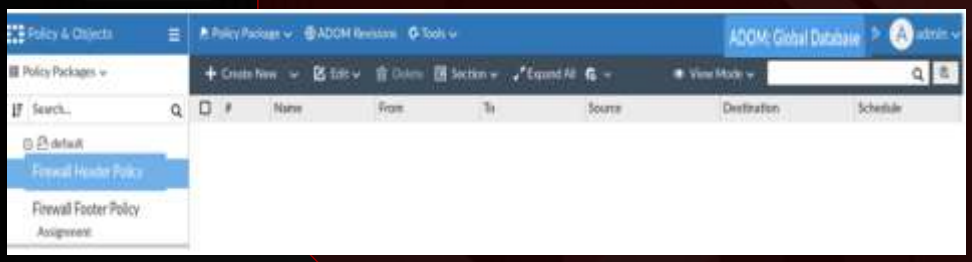


Policy Types

Switch to Global Database ADOM

Two types of Policies

- Header – placed at the top of the policy package in the individual ADOM
- Footer – placed at the bottom of the policy package in the individual ADOM



Manager Panes

VPN Manager

- Simplifies the administration of multiple IPSec VPNs

AP Manager

- Centrally manage FortiAP devices

FortiSwitch Manager

- FortiSwitch templates and VLANs and monitor FortiSwitch devices that are connected to FortiGate devices

Extended Manager

- Managed FortiExtender

Fabric View

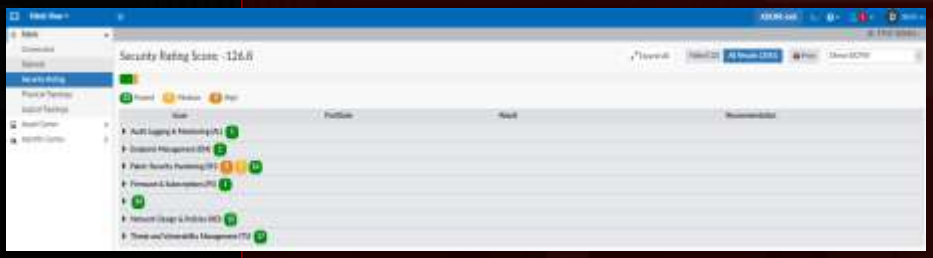
FabricView (Security Fabric)

- View security fabric ratings of configurations for Security Groups (must generate rating using FortiOS first)
- You can view ratings for multiple groups

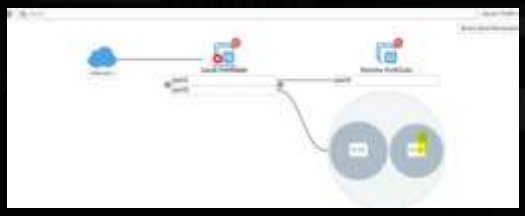
Security Fabric Rating

Three Major Scorecards: security posture, fabric coverage and optimization

Provides executive summary of the security focus



Fabric Topology



Management Extensions Application (MEA)

MEAs all you to enable

- SD-WAN
- FortiWLM
- FortiPortal
- FortiSigConverter
- FortiAuthenticator
- FortiSOAR
- FortiAIOps
- Universal Connector

MEA Requirements

- Require a minimum memory and/or CPUs
- FortiManager uses TCP 443 or 4443 to connect to Fortinet registry and download MEAs
- Ensure port is open to upstream device
- Admin with superuser profile can enable MEAs
- Some MEAs require read/write JSON API access
- RAM and CPU are capped at 50% for MEAs

Conclusions

Global ADOM

FortiManager Panes

SecurityFabric View with FortiManager

Security Fabric Technology

FortiManager MEAs

FortiManager MEAs requirements

Overview

- Describe various deployment scenarios
- Understand FGFM keepalives
- Replacer standalone managed device
- CLI troubleshoot connectivity and resource issues
- Verify FortiManager database integrity
- Diagnose and troubleshoot device and ADOM database issues
- Issues related to import and installation

FortiManager Behind a NAT Device

- Only FortiManager can discover device
- During discovery NATed IP is not set on the FortiGate
- Only FortiManager tries to reestablish the FGFM tunnel if torn down

```
Config system central-management
set fmg <FMG_NATed IP address>
```

- Configuring the NAT on the FortiManager allows
  - FortiGate to announce itself to FortiManager
  - Both can reestablish FGFM tunnel if town down

```
Config system admin setting
set mgmt-addr <FMG_NATed IP address
```

FortiGate Behind a NAT Device

- FortiManager can discover FortiGate through FortiGate NAT IP
- FortiManager does not auto attempt to reestablish FGFM tunnel if torn down

  Click refresh icon in the connection summary widget forces one-time attempt

```
Config system central-management
set fmg <FMG IP address>
```

- FortiGate can announce itself to FortiManager
- Only FortiGate tries to reconnect FGFM tunnel if torn down

Both Devices Behind a NAT Device

- FortiManager can discover FortiGate through FortiGate NAT IP
- Click refresh icon in the connection summary widget forces one-time attempt

```
Config system central-management
set fmg <FMG_NATed IP address>
```

- If a FortiManager NAT IP is configured on the FortiGate then
  - FortiGate can announce itself to the FortiManager
  - Only FortiGate reconnects automatically if connection torn down

FGFM KeepAlives

- Configured on the FortiManager

```
Config system dm
set fgfm-sock-timeout 360
set fgfm_keepalive_itvl 120
```

- Only FortiGate sends a keepalive to FortiManager
- FortiGate sends checksum to confirm sync as part of keep alive

FortiGate **# diagnose debug application fgfmd 255**
FortiGate **# diagnose debug enable**
FGFMs: client:send:
keepalive
checksum=56 06 ae ab ea 15 72 …
ipsversion=18.00132(2021-07-31 01:29)

FortiGate **# diagnose debug application fgfmd 255**
FortiGate **# diagnose debug enable**
FGFMs:(FGVM…-10.0.1.254): server:
keepalive
checksum=56 06 ae ab ea 15 72 …
ipsversion=18.00132(2021-07-31 01:29)

- Timeout is configured on the FortiManager

#FGFMs: Timeout[360] for sock.
FGFMs(FGVM..-10.0.1.254): Cleanup devid=307
Tunnel_ip from DVM (ret=0)

Recovery Logic

- To make configuration changes to FortiGate, FortiManager sends set and unset CLI commands
- FortiGate devices
  - Apply set commands
  - Test FGFM connections to FortiManager
- If the connection fails, FortiGate applies the unset command after 15 minutes

```
Config system dm
set rollback-allow-reboot enable
end
```

Replace a Managed StandAlone Device

- When a management connection request is made, the FortiGate serial number is verified
- When replacing Stand-Alone device, you must change the serial number and redeploy the configuration
- When replacing a FortiGate cluster member, FortiManager learns the new serial number through the FGFM tunnel

Replace a Managed StandAlone Device

Steps to replace

1. Note Original FortiGate Device name

```
diagnose dvm device list
```

2. Update the serial number of the replace FortiGate

```
execute device replace sn <devname> <New serialnum>
```

3. Verify the FortiManager updated the serial number

```
diagnose dvm device list
```

4. Send a registration request from the replaced FortiGate

5. If connectivity is down after updating the serial number, potentially need to reclaim the management tunnel

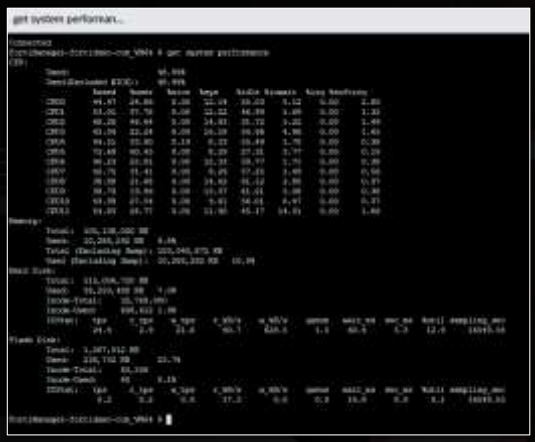
```
execute fgfm reclaim-dev-tunnel <optional device name>
```

Basic Commands

Command	Information
# get system status	Current status — serial number, firmware version, ADOM status, HA Status
# get system performance	Overall resource utilization — CPU, memory, disk
# execute top (lists processes with high CPU or memory usage) # execute iotop (lists processes with high i/o usage)	Top processes
# diagnose debug crashlog read	Crash logs
# diagnose sniffer packet <interface> <filter> <verbose> <count> <timestamp>	Packet sniffer
# execute ping <FortiGate IP> # execute ssh <FortiGate IP> # execute ssh <FortiGate FGFM IP> (link level IP address from session-list or dvm device list command) # diagnose fgfm session-list # diagnose dvm device list	Testing device reachability from FortiManager Confirming FGFM tunnel is up
# diagnose system print df # diagnose system print partitions	Disk partition layout and status

System Resource Usage

- Get system performance displays information about system resources, such as CPU, memory, hard disk, and disk usage



High CPU and Memory Troubleshooting

- Execute top displays realtime system monitoring

```
FMG-VM64 # execute top
top - 13:08:23 up 1 day, 1:01, 0 users, load average: 2.40, 3.19, 3.34
Tasks: 188 total, 2 running, 186 sleeping, 0 stopped, 0 zombie
%Cpu(s): 15.4 us, 7.7 sy, 0.0 ni, 76.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mere : 2010.164 total, 41.250 free, 974.086 used, 994.828 buff/cache
MiB Swap: 2027.867 total, 1361.922 free, 665.945 used. 855.359 avail Mem
```

High Disk Usage Troubleshooting

- Execute iotop displays the process that are responsible for high I/O usage

```
FMG-VM64 # execute iotop
Total DISK READ : 0.00 B/s I Total DISK WRITE : 0.00 B/s
Actual DISK READ: 0.00 B/s I Actual DISK WRITE: 0.00 B/s
TID PRIO USER       DISK READ   DISK WRITE   SWAPIN    IO>    COMMAND
512 rt/4 root       0.00 B/s    0.00 B/s     0.00 %  0.00 %  fortilogd
[fortilogd.wrtr2]
      1 be/4 root   0.00 B/s    0.00 B/s     0.00 %  0.00 % initXXXXXXXXXX
      2 be/4 root   0.00 B/s    0.00 B/s     0.00 %  0.00 % [kthreadd]
      3 be/4 root   0.00 B/s    0.00 B/s     0.00 %  0.00 % [ksoftirqd/O]
    516 rt/4 root   0.00 B/s    0.00 B/s     0.00 %  0.00 % fortilogd
[fortilogd.stat]
      5 be/0 root   0.00 B/s    0.00 B/s     0.00 %  0.00 % [kworker/0:0H]
```

Packet Sniffer

- Packet sniffer is useful for troubleshooting connectivity issues
- FortiManager supports verbose options 1, 2, and 3

Diagnose sniffer packet <interface> <filter> <verbose> <count> <timestamp>

```
2021-10-08 09:09:35.339199 192.168.1.69.541 -> 192.168.1.99.14288: psh 3363626479 ack
1008803733
2021-10-08 09:09:35.340822 192.168.1.99.14288 -> 192.168.1.69.541: psh 1008803733 ack
3363626713
2021-10-08 09:09:35.340840 192.168.1.69.541 -> 192.168.1.99.14288: ack 1008803903
2021-10-08 09:09:35.340912 192.168.1.69.541 -> 192.168.1.99.14288: psh 3363626713 ack
1008803903
2021-10-08 09:09:35.379884 192.168.1.99.14288 -> 192.168.1.69.541: ack 3363626819
```

Process Status

- Check for unexpected lock processes

```
# diagnose dvm lock
Global database pending read: unlocked
Global database pending write: unlocked
Global database reserved read: unlocked
Global database reserved write: unlocked
Global database shared read: unlocked
Global database shared write: unlocked
```

Debug Commands

Command	Information
# diagnose debug enable # diagnose debug timestamp enable	Enable debug output on SSH/Telnet session Enable timestamp in the debug output
# diagnose debug application dmapi 255 # diagnose dvm debug enable all	Debug device-level operations: registering, deleting, refresh, auto-updates, resync process
# diagnose debug application securityconsole 255	Debug ADOM to device database copy process and import policy packages
# diagnose debug application depmanager 255 # diagnose debug dpm conf-trace enable	Debug the registration process and install process, including CLI scripts run directly on devices, retrieves, and revision history

File System Integrity

- An abnormal shutdown can cause database corruption
- Check logs for related messages


```
.....
.....
.....
.....ready.

Serial number: FMG-VM0A16001583

The disk was not unmounted properly.
You should run 'diag sys fsck harddisk'.

FMG-VM64 login: _
```

```
FMG-VM64 # diagnose system fsck harddisk
This operation will check and repair the file
system, then reboot the system.
Do you want to continue? (y/n)y

The system is going down NOW!!
Fsck /dev/mdvg/mdlv…
 Done, no error.
Please stand by while rebooting the system.
```

Best Practices - DataBase Integrity

- Always shutdown gracefully -> execute shutdown
- Follow proper upgrade path
- Recommendations
  - Enable ADOM locking
  - Log all admins off and integrity checks on database before firmware upgrade
  - Backup FortiManager

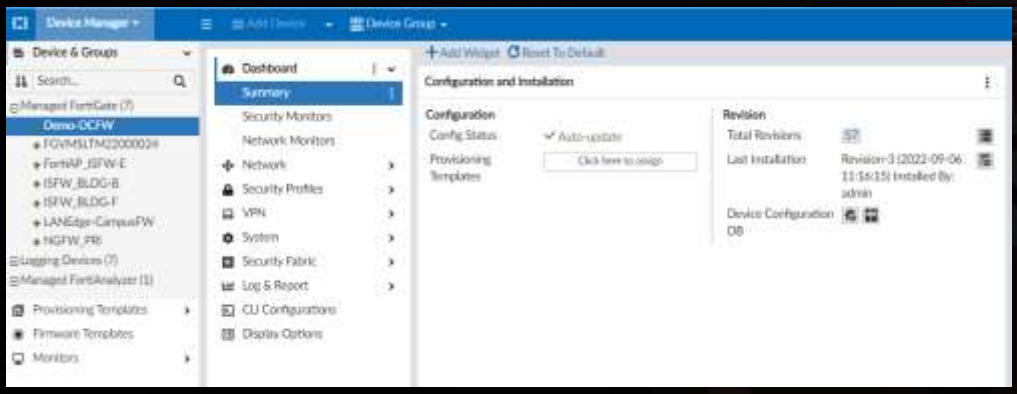
```
diagnose dvm check-integrity
diagnose cdb check adom-integrity
diagnose cdb check adom-revision
diagnose cdb check policy-packages
diagnose cdb check update-devinfo
```

Troubleshooting Device and ADOM Databases

Command	Information
# diagnose dvm check-integrity	Verify and correct parts of the device manager databases, including: Inconsistent device-to-group and group-to ADOM memberships Unregistered, registered, and deleted device states Device lock statuses Duplicate VDOM entries
# diagnose cdb upgrade check objcfg-integrity	Object config database integrity—Perform a check to see if upgrade and repair is necessary
# diagnose cdb upgrade check reference-integrity	Perform a check to see if upgrade and repair is necessary for reference table.
# diagnose cdb check update-devinfo	Update device info by directly changing the database
# diagnose cdb check adorn-integrity	Internally upgrades existing ADOMs to the same ADOM version in order to clean up and correct the ADOM syntax
# diagnose cdb check policy-packages	Verifies and checks dynamic mappings and removes invalid dynamic mappings

Provisioning Templates

- Multiple way to verify which template is assigned to which device



Provisioning Templates

- Shows the exact FortiOS CLI that will be installed to the manage device

```
execute fmpolicy print-adorn-package <adom> <policy package/template name>
<package> <category> lall[<key>lallIlist]
```

Device Database

- Display the whole device configuration or individual object configuration
  - Execute fmpolicy print-device-database Displays device-level changes made from FortiManager
    - Does not display changes from applied system templates
  - Execute fmpolicy print-device-object Does not display any ADOM-level (firewall policy and related objects) changes made from the FortiManager
  - Execute fmpolicy print-device-object <adom-name> <device-name> <vdom-name> <category-name>
    - Displays individual object configuration

```
FMG-VM64 # execute fmpolicy print-device-object root Local-FortiGate root 15 Dump all
objects for category [system dns] in device [Local-FortiGate]
vdom[root]:
config system dns
set primary 208.91.112.53
set secondary 4.2.2.2 end
```

ADOM Databases

- Displays
  - Entire ADOM database with a policy package and objects
    - Execute fmpolicy print-adom-database
  - Firewall policies contained in a specific package in the ADOM
    - Execute fmpolicy print-adom-package
  - Individual objects in an ADOM
    - Execute fmpolicy print-adom-object

Failed Reload

- An operation that fails to update the device-level database from the revision history database
- Inconsistent or corrupt FortiGate configuration
  - Can be due to not following upgrade path
- Troubleshoot reload failure

```
Diagnose test deploymanager reloadconf <devid>
```

- Shows the stage at which the configuration is failing to update the device-level database
- If successful, the device-level database is updated with the FortiGate configuration
  - No new revision history is created

Import Issues - Failed Import

- Verify that policies or object have been imported (not failed)
- Check download report for reason of failure
- If logging local set to debug, events logs include failed import logs

Failed Import - Impact and Resolution

- Impact
  - On subsequent policy package installs from FortiManager the failed objects and policies are deleted
- Two ways to fix the issue
  - Remove interface binding
    - Run script from FortiManager using the option Remote FortiGate Directly (via cli)
    - Remove the interface binding by locally logging into the fortigate
  - Rename address object
    - Run script from FortiManager using the option Remote FortiGate Directly (via cli)
    - Remove the interface binding by locally logging into the fortigate
- Must reimport the policy package after fixing the address object

Copy Failed Issues

- Internal operation part of policy package installation
  - First thing that is performed before the installation
- An operation that fails between ADOM database and device database
- Usually due to missing or incorrect object dependency when copied from ADOM database to device database
- When performing the installation, View progress report shows the failing message

Conclusions

- Describe various deployment scenarios
- Understand FGFM keepalives
- Replacer standalone managed device
- CLI troubleshoot connectivity and resource issues
- Verify FortiManager database integrity
- Diagnose and troubleshoot device and ADOM database issues
- Issues related to import and installation

Overview

Deploy FortiManager in HA cluster

Understand what is synchronized between HA cluster member

Recover a failed device

Configure FortiGuard setting on FortiManager

Understand the purpose and use of server override mode and override server address

Configure FortiGate devices to use FortiManager as a local FortiGuard server

Troubleshoot FortiGuard issues

High Availability

- All FortiManager devices in cluster must be same model and firmware
- Designed for 1 Primary multiple secondary(Up to 4 – 5 devices total)
- Support geographical redundancy
  - HA sync is TLS1.0 over TCP 5199
- Each HA member operates independently
  - Unique IP for each FortiManager
- Upgrading Primary also upgrade secondaries at same time
  - Upgrade process similar to standalone upgrade
  - FortiManager operations are temporarily interrupted during upgrade
  - Reboots Devices

High Availability - Sync

- Make change on primary and sync to secondary
  - Replicate primary device database
  - Promote secondary in the event of primary failure
- Sync'd
  - All device configurations – including global Databases
  - All configuration revisions
- NOT Sync'd
  - Config settings
    - Interface – routes – HA – SNMP – Logs – Faz
  - FortiGuard
    - AntiVirus/IPS - WebFliter – AntiSpam
  - Local logs and alerts
  - FortiGate logs sent to FortiManager

High Availability - Failure Behavior

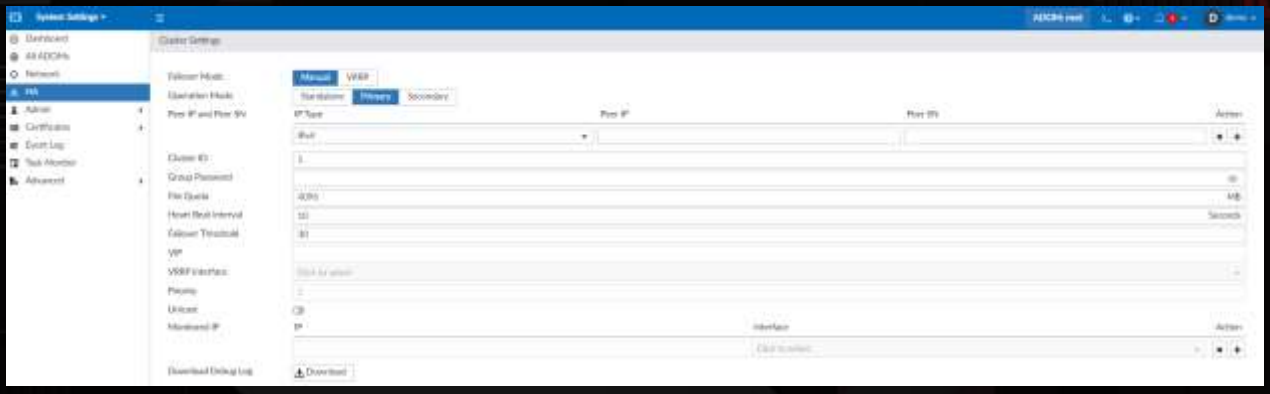
Primary Fails

- Must manually reconfigure a secondary to primary
- Reconfigure all secondary to new primary
- Reboot not necessary

Secondary Fails

- On Primary remove peer of failed secondary
- Can leave configs so when secondary comes online it can resync

High Availability - Configuring



High Availability - FortiManager HA Status

High Availability - HA Sync Failure Checklist

What to Investigate	Where to Check
Verify TCP port 5199 connectivity	diagnose sniffer packet <port> 'port 5199' <level>
Check Alert Message console Check Event logs	Under System Settings > Dashboard Under System Settings > Event Logs
Debug on HA daemon	diagnose debug application ha 255 diagnose debug enable
Check if there is pending synced data (bytes)	diagnose ha stats

Resolving

Force Resync: diagnose ha force-resync

Execute on Primary force full sync to all secondary

Execute on secondary only resyncs that secondary

Local FortiGuard

Downloads all AntiVirus IPS Packages WebFilter EmailFilter databases on FortiManager

Reduces internet connection load

- Local FortiManager provides faster response
- Can redistribute packages to multiple devices
  - In some high-security devices internet access for internal FortiGate is restricted

FortiManager as a local FortiGuard

- Connects to FortiGuard servers
  - Downloads License status for managed devices
  - Syncs FortiGuard packages
  - Unless configured for closed network operation
- Can cache available firmware updates on managed devices
- Can act as downstream FortiGuard providing
  - AntiVirus and IPS signatures
  - WebFiltering and AntiSpam rating databases and lookups
- In HA, each FortiManager acts as an individual FortiGuard Server
  - Each HA member independently downloads and provides these services

Terminology

Terminology Used		Service Type
FortiGate	FDS	Antivirus and IPS
	FGD	Web filter and email filter
FortiClient	FCT	Antivirus and IPS
	FGC	Web filter and email filter
	FDN	Public FortiGuard Distribution Network

FortiManager Port and Protocol Usage

Uses TCP 443 to obtain updates from public FDN

Used to replicate public FDN

FortiGuard Service		Process	Initial Connectivity to Public FDN (TCP 443)
FortiGate	FDS	fdslinkd	fds1.fortinet.com usfds1.fortinet.com – For US servers only
	FGD	fgdlinkd	guard.fortinet.net and qsvr.fortinet.net
FortiClient	FCT	fctlinkd	forticlient.fortinet.net
	FGC	fgclinkd	fgd1. fortigate.com

Enabling Built-In FDS (FortiGuard)

Two Steps

1. Enable Service access settings on interface
2. Enable FortiGuard Services

Enable services access settings for each interface

- Used by FortiManager to communicate with FortiGate devices

Can enable the following services

- AntiVirus and IPS
- WebFilter
- Email Filter

By default, communication with public FDN is enabled on FortiManager

Can change FortiGuard communication between Global or US based servers

AntiVirus and IPS Services

- AntiVirus and IPS update services are enabled together
  - Must enable supported FortiManager firmware versions
- Updates available for
  - FortiGate
  - FortiClient
  - FortiAnalyzer
  - FortiMail

Schedule Updates for Antivirus and IPS

By default FortiManager performs updates every 10 minutes

Push Updates

- By default FortiManager contacts public FDS on a schedule
- Push Updates allow urgent updates to be pushed directly by FortiManager when they become available on the FDN
  - FortiManager immediately downloads these updates
- Push update fail if FortiManager behind NAT due to sending it's IP

Package Management - Receive Status

Package Management - Service Status

Antivirus and IPS update services are enabled together

Configuring Web Filter and Email Filter

First time can potentially take several hours to download databases

Three main process

1. Fgdlinkd

   Downloading web filter and email database

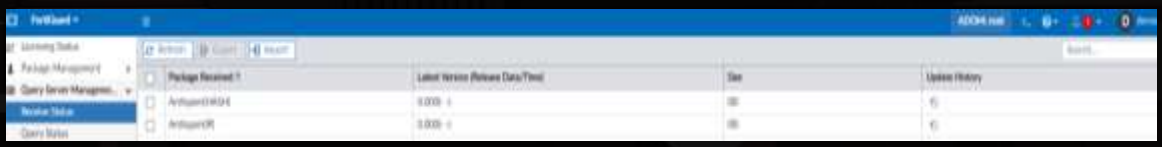
2. Fgdups

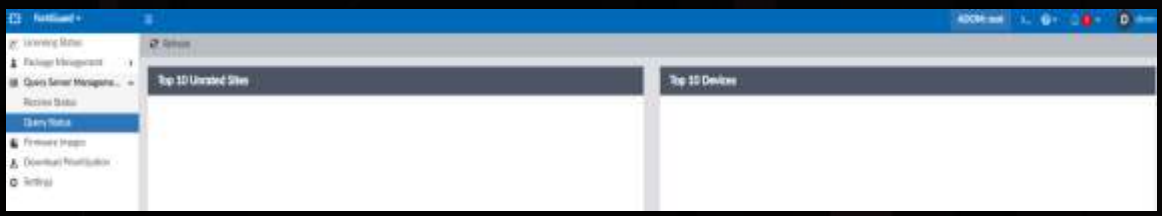
   Database merging and consolidating smaller delta files into larger files

3. Fgdsrv

   Serves FortiGate and FortiClient for web filter and email filter requests

Query Server Management

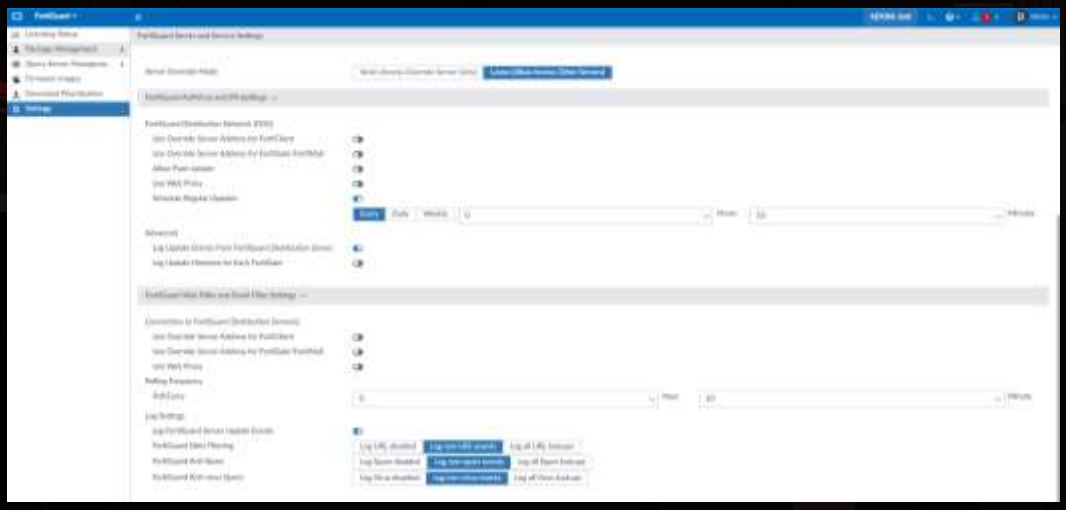




Server Override Mode

- Addresses of FDS servers for FortiManager to connect to and get updates
- Options used:
  - When necessary to connect FortiManager to specific FDN server on the internet
  - To connect downstream FortiManager to another upstream FortiManager to download updates
- Can override server addresses for
  - AntiVirus, IPS
  - WebFilter and EmailFilter

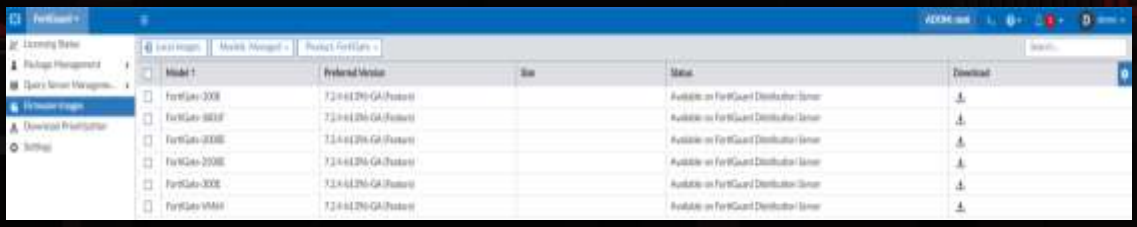
Server Override Mode



FortiGuard License Status

View License information for FortiGate Devices

Firmware Cache



FortiGate Firmware Update from FortiManager

- Upgrading Firmware
  - For Individual devices
    - From System Information Widget
  - For Multiple devices in ADOM
    - From the device manager pane
    - Can upgrade firmware on group
- Can schedule firmware upgrades
  - Firmware Templates
    - DeviceManager -> Firmware Templates

Verifying Configuration to Troubleshoot FortiGuard Connectivity

FortiGuard server on FortiManager is resolved

```
executive ping <FortiGuard domain address>
```

Communication to public network is enabled

```
# get fmupdate publicnetwork
Status                :enable
```

Service is enabled

```
# config fmupdate service
get
avips                 :enable
Query-antispam        :enable
Query-webfilter       :enable
```

Troubleshooting FortiGuard Connectivity

Diagnose fmupdate view-serverlist [fds|fct|fgd|fgc|ftmr]

List all upstream FDN servers FortiManager is communicating for Updates

Diagnose fmupdate update-status [fds|fct|fgd|fgc|ftmr]

Check UpullStat for current status

Diagnose fmupdate dbcontract [fds|fgd] [device serial-number]

List contract information for all the devices

FortiGate Troubleshooting

Shows version, last update, contract expiration date

```
 # get system fortiguard-service status
NAME                VERSION LAST UPDATE          METHOD    EXPIRE
AV Engine            6.262  2021-05-06 01:46:00  manual    2023-01-20 23:59:59
Virus Definitions    89.5851  2021-10-11 20:04:46  scheduled 2023-01-20 23:59:59
Extended set         89.5851  2021-10-11 20:04:46  scheduled 2023-01-20 23:59:59
```

Real-time Update

Shows FortiGuard serve from which FortiGate is trying to download updates

```
# diagnose debug application update -1
# diagnose debug enable
# execute update-now

Local-FortiGate # upd_daemon[1794]-Received update now request
upd_daemon[1613]-Found cached action=00000002
do_update[606]-Starting now UPDATE (final try)
upd_comm_connect_fds[455]-Trying FMG 10.0.1.241:8888
[752] ssl_new: SSL object is created pack_obj[183]-Packing pack_obj[196]-Packing
obj=Protocol=3.2|Command=Update|Firmware=FGVM64-FW-7.00-0157|SerialNumber=FGVM010000064692|
UpdateMethod=0|AcceptDelta=1|Uid=42384969a5650d78bcc75b5c921fda4e|DataItem=07000000AVDB00201-
00089.05851-211011624* ....
] ssl_disconnect: Shutdown
do_update[636]-UPDATE successful
```

Conclusions

- Deploy FortiManager in HA cluster
- Understand what is synchronized between HA cluster member
- Recover a failed device
- Configure FortiGuard setting on FortiManager
- Understand the purpose and use of server override mode and override server address
- Configure FortiGate devices to use FortiManager as a local FortiGuard server
- Troubleshoot FortiGuard issues