



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå os her

Email: training.ecs.dk@arrow.com
Phone: +45 7025 4500

CODE:	LENGTH:	PRICE:
FNT_FMGT	16 Hours (2 dage)	Request Price

Description

FortiManager Centralized Device Management (FMGT)

In this 2-day class, you will learn the fundamentals of using FortiManager for centralized network administration of many FortiGate devices. Example use cases include large enterprise and carrier networks. You will explore various deployment strategies which include single or multiple ADOMs, policy packages, shared objects, & provisioning FortiManager as a local FortiGuard Distribution Server for your managed firewalls.

This course is part of preparation for the NSE 5 certification exam.

Training material: English

Language spoken: Dutch (English and other languages upon request)

Objectives

Upon completion of this course, students will be able to:

- Describe capabilities of FortiManager
- Add FortiGate devices to Device Manager and import their running configuration
- Use provisioning templates and scripts for device-level changes across many devices
- Identify the synchronization states
- Manage the revision history of managed devices
- Offer a local FortiGuard Distribution Server to your Fortinet devices
- Deploy administrative domains (ADOMs) to support multiple customers on a single FortiManager
- Manage firewall policies across multiple FortiGate devices using policy packages with shared and dynamic objects
- Deploy policies and objects from the global ADOM to multiple ADOMs
- Explain high availability, backup, and recovery options for FortiManager
- Compare methods for centrally managing IPsec VPNs
- Explain the restricted "admin" profile and API high-level usage
- Use workspaces and workflow mode
- Identify steps to replace a managed FortiGate device
- Manage FortiGate devices' firmware centrally

Audience

This course is intended for networking and security professionals involved in providing installation, management, administration, and troubleshooting functions for centrally managed FortiGate deployment(s) using FortiManager appliances.

Prerequisites

- Knowledge of firewalling concepts in an IPv4 network
- Familiarity with all topics in FortiGate I and FortiGate II
- Basic understanding of network management systems

Programme

Module 1 Introduction to FortiManager

The learning goal for this module is to understand the centralized management approach for managing FortiGate devices using FortiManager and to identify common use cases.

A Student Should Be Able To:

- » Identify the key features of FortiManager
- » Identify licensing differences between the physical and virtual appliances
- » Describe the device life cycle management tasks
- » Identify the different management tabs and the functionality of each
- » Identify the commonalities between FortiManager and FortiAnalyzer
- » Describe the management module framework for FortiManager
- » Identify two use cases and usage examples of the FortiManager product
- » Identify the three APIs available on FortiManager and the purpose of the Fortinet Developer Network service

Module 2 System Settings

The learning goals for this module are to familiarize the student with the FortiManager system settings in order to perform the initial configuration prior to deploying the first devices, review common maintenance tasks, configure ADOMs and configure system administrators.

Objectives

A Student Should Be Able To:

- » Describe at a high-level the configuration settings available on the System Settings tab
- » Identify system network configuration settings
- » Describe the concept of ADOMs, ADOM locking, common usage scenarios and the basic steps to perform an ADOM configuration
- » Describe the granularity achievable with different admin profile settings
- » Describe the correct procedure to backup and restore the FortiManager system
- » Identify the purpose of offline mode, when it is active and how to deactivate it
- » Identify the procedure to factory reset a FortiManager device
- » Identify the purpose of meta fields
- » Read the alert message console and event log
- » Identify how to track the status of tasks resulting from management actions using the Task Monitor

Module 3 Device Manager

The learning goals for this module are to familiarize the student with adding FortiGate devices to FortiManager and how configuration changes made in Device Manager are installed on a managed device, as well as reading both the revision and installation history to understand the changes made to a device.

Objectives

A Student Should Be Able To:

- » Identify the key features of Device Manager
- » Describe the steps to add a FortiGate device to the FortiManager system and the stages of the add device wizard
- » Identify the import process for firewall policy and objects
- » Make device changes from Device Manager and install them on a managed device
- » Describe Provisioning Profiles and their usage
- » Describe the FortiManager and FortiGate configuration status and synchronization behavior and the Install, Restore and Retrieve tasks
- » Describe the purpose of Revision History and how to identify which action created a revision
- » Describe the capabilities of scripts in Device Manager
- » Identify the steps to replace a managed FortiGate device
- » Identify the usage of Device Groups
- » Describe what action the refresh command performs
- » Identify the capabilities of chassis management in FortiManager
- » Describe how to manage a FortiGate HA device with FortiManager

Module 4, Policy & Objects

The learning goals for this module are to familiarize the student with tasks involved when working in the Policy & Objects tab in order to centrally manage firewall policies and install policies on multiple devices.

Objectives

A Student Should Be Able To:

- » Describe the functionality of Policy & Objects at an ADOM level and how they are used to manage firewall policies on managed FortiGate devices
- » Identify how folders help you manage your policy packages
- » Describe the purpose of ADOM revisions and describe how to create and restore ADOM revisions
- » Identify the database version of an ADOM and how this affects Policy & Objects tab configurations
- » Describe how objects can be shared between multiple devices and the purpose of dynamic objects
- » Describe the usage of installation targets for policy packages and individual policies
- » Describe the purpose of zones defined in the Policy & Objects tab and their usage in policy packages
- » Describe the Import Policy wizard stages and common considerations when importing FortiGate configurations
- » Identify the stages when performing an Install Policy Package and Device Settings and the purpose of the re-install command
- » Identify how cut & paste, cloning and exporting help you to manage your firewall policies
- » Describe the VPN Management mode and use both Policy & Device VPNs and VPN Console to configure an IPSec VPN
- » Describe the functionality of Policy & Objects and a Global ADOM level

Module 5 Additional System Operations

The learning goals for this module are to familiarize the student with additional system features that are common to many deployments. In particular the student will work with Web Portals, FGFM management protocol, HA and FortiGuard.

Objectives

A Student Should Be Able To:

- » Describe the Web Portal feature and its configuration requirements to provide customers access to their managed devices
- » Describe the FGFM management protocol and tasks that administrators may need to perform to test correct operation
- » Identify the configuration requirements of an High Availability deployment
- » Describe the FortiGuard services available with FortiManager and how to configure FortiGate devices to work with a local FortiGuard server
- » Describe the private network configuration where the FortiManager is not connected to the public Internet
- » Describe the firmware image management available on FortiManager FortiGuard server
- » Identify the options for deploying new firmware at a device level and a group level

Session Dates

På anmodning. [Kontakt os venligst](#)

Yderligere Information

Denne træning er også tilgængelig som træning på stedet. [Kontakt os for at finde ud af mere.](#)