Which Operating System and Manager is Right for You?

Your hardware platform can run one of two operating systems. For each operating system, you have a choice of managers. This chapter explains the operating system and manager choices.

Operating Systems

You can use either ASA or Firepower Threat Defense (FTD) operating systems on your hardware platform:

- ASA—The ASA is a traditional, advanced stateful firewall and VPN concentrator.

  You may want to use the ASA if you do not need the advanced capabilities of the FTD, or if you need an ASA-only feature that is not yet available on the FTD. Cisco provides ASA-to-FTD migration tools to help you convert your ASA to an FTD if you start with ASA and later reimage to FTD.

- FTD—FTD, also known as Firepower NGFW, is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS. In other words, the FTD takes the best of ASA functionality and combines it with the best next-generation firewall and IPS functionality.

  We recommend using the FTD over the ASA because it contains most of the major functionality of the ASA, plus additional next generation firewall and IPS functionality.

To reimage between the ASA and the FTD, see Reimage the Cisco ASA or Firepower Threat Defense Device.

Managers

The FTD and ASA support multiple managers.

FTD Managers

Table 1: FTD Managers

Manager	Description
Firepower Device Manager (FDM)	FDM is a web-based, simplified, on-device manager. Because it is simplified, some FTD features are not supported using FDM. You should use FDM if you are only managing a small number of devices and don't need a multi-device manager. **Note** Both FDM and CDO can discover the configuration on the firewall, so you can use FDM and CDO to manage the same firewall. FMC is not compatible with other managers. To get started with FDM, see Firepower Threat Defense Deployment with FDM.
Cisco Defense Orchestrator (CDO)	CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some FTD features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience (similar to FDM). And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as ASAs, so you can use a single manager for all of your security devices. **Note** Both FDM and CDO can discover the configuration on the firewall, so you can use FDM and CDO to manage the same firewall. FMC is not compatible with other managers. CDO is not covered in this guide. To get started with CDO, see the CDO home page.
Firepower Management Center (FMC)	FMC is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use FMC if you want a multi-device manager, and you require all features on the FTD. FMC also provides powerful analysis and monitoring of traffic and events. In 6.7 and later, FMC can manage FTDs from the outside (or other data) interface instead of from the standard Management interface. This feature is useful for remote branch deployments. **Note** FMC is not compatible with other managers because the FMC owns the FTD configuration, and you are not allowed to configure the FTD directly, bypassing the FMC. To get started with FMC, see Firepower Threat Defense Deployment with FMC.
FTD REST API	The FTD REST API lets you automate direct configuration of the FTD. This API is compatible with FDM and CDO use because they can both discover the configuration on the firewall. You cannot use this API if you are managing the FTD using FMC. The FTD REST API is not covered in this guide. For more information, see the FTD REST API guide.

Manager	Description
FMC REST API	The FMC REST API lets you automate configuration of FMC policies that can then be applied to managed FTDs. This API does not manage an FTD directly.
	The FMC REST API is not covered in this guide. For more information, see the FMC REST API guide.

ASA Managers

Table 2: ASA Managers

Manager	Description
Adaptive Security Device Manager (ASDM)	ASDM is a Java-based, on-device manager that provides full ASA functionality. You should use ASDM if you prefer using a GUI over the CLI, and you only need to manage a small number of ASAs. ASDM can discover the configuration on the firewall, so you can also use the CLI, CDO, or CSM with ASDM.
	To get started with ASDM, see ASA and ASA FirePOWER Module Deployment with ASDM.
CLI	You should use the ASA CLI if you prefer CLIs over GUIs.
	The CLI is not covered in this guide. For more information, see the ASA configuration guides.
Cisco Defense Orchestrator (CDO)	CDO is a simplified, cloud-based multi-device manager. Because it is simplified, some ASA features are not supported using CDO. You should use CDO if you want a multi-device manager that offers a simplified management experience. And because CDO is cloud-based, there is no overhead of running CDO on your own servers. CDO also manages other security devices, such as FTDs, so you can use a single manager for all of your security devices. CDO can discover the configuration on the firewall, so you can also use the CLI or ASDM.
	CDO is not covered in this guide. To get started with CDO, see the CDO home page.
Cisco Security Manager (CSM)	CSM is a powerful, multi-device manager that runs on its own server hardware. You should use CSM if you need to manage large numbers of ASAs. CSM can discover the configuration on the firewall, so you can also use the CLI or ASDM. CSM does not support managing FTDs.
	CSM is not covered in this guide. For more information, see the CSM user guide.
ASA REST API	The ASA REST API lets you automate ASA configuration. However, the API does not include all ASA features, and is no longer being enhanced.
	The ASA REST API is not covered in this guide. For more information, see the ASA REST API guide.