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 the Secure Firewall ASA or the Secure Firewall Threat Defense (formerly Firepower Threat Defense) operating system 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 threat defense, or if you need an ASA-only feature that is not yet available on the threat defense. Cisco provides ASA-to-threat defense migration tools to help you convert your ASA to the threat defense if you start with ASA and later reimage to threat defense.

- Threat Defense—The threat defense is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS. In other words, the threat defense takes the best of ASA functionality and combines it with the best next-generation firewall and IPS functionality.

  We recommend using the threat defense 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 threat defense, see the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Managers

The threat defense and ASA support multiple managers.

Threat Defense Managers

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	The management center 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 the management center if you want a multi-device manager, and you require all features on the threat defense. The management center also provides powerful analysis and monitoring of traffic and events. In 6.7 and later, the management center can manage the threat defenses from the outside (or other data) interface instead of from the standard Management interface. This feature is useful for remote branch deployments. **Note** The management center is not compatible with other managers because the management center owns the threat defense configuration, and you are not allowed to configure the threat defense directly, bypassing the management center. To get started with the management center, see Threat Defense Deployment with the Management Center.
Secure Firewall Device Manager (formerly Firepower Device Manager)	The device manager is a web-based, simplified, on-device manager. Because it is simplified, some threat defense features are not supported using the device manager. You should use the device manager if you are only managing a small number of devices and don't need a multi-device manager. **Note** Both the device manager and CDO in FDM mode can discover the configuration on the firewall, so you can use the device manager and CDO to manage the same firewall. The management center is not compatible with other managers. To get started with the device manager, see Threat Defense Deployment with the Device Manager.
Cisco Defense Orchestrator (CDO)	CDO offers two management modes: • (7.2 and later) Cloud-delivered management center mode with all of the configuration functionality of an on-premises management center. For the analytics functionality, you can use either Secure Cloud Analytics in the cloud or an on-prem management center. • (Existing CDO users only) Device manager mode with a simplified user experience. This mode is only available to users who are already using CDO to manage threat defenses in device manager mode. This mode is not covered in this guide. 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. CDO is not covered in this guide. To get started with CDO, see the CDO home page.

Manager	Description
Secure Firewall Threat Defense REST API	The threat defense REST API lets you automate direct configuration of the threat defense. This API is compatible with the device manager and CDO use because they can both discover the configuration on the firewall. You cannot use this API if you are managing the threat defense using the management center. The threat defense REST API is not covered in this guide. For more information, see the Cisco Secure Firewall Threat Defense REST API Guide.
Secure Firewall Management Center REST API	The management center REST API lets you automate configuration of management center policies that can then be applied to managed threat defenses. This API does not manage the threat defense directly. The management center REST API is not covered in this guide. For more information, see the Secure Firewall Management Center REST API Quick Start 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 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.
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 threat defenses, 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 the threat defenses. CSM is not covered in this guide. For more information, see the CSM user guide.

Manager	Description
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 Cisco ASA REST API Quick Start Guide.