Which Application and Manager is Right for You?

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

Applications

You can use either the Secure Firewall ASA or the Secure Firewall Threat Defense (formerly Firepower Threat Defense) application on your hardware platform:

- ASA—The ASA is a traditional, advanced stateful firewall and VPN concentrator.
- Threat Defense—The threat defense is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS.

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.

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 multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. To get started with the management center on the Management network, see Threat Defense Deployment with the Management Center. To get started with the management center on a remote network, see Threat Defense Deployment with a Remote Management Center.
Secure Firewall Device Manager (formerly Firepower Device Manager)	The device manager is a simplified, on-device manager. Some threat defense features are not supported using the device manager. To get started with the device manager, see Threat Defense Deployment with the Device Manager.
Cisco Defense Orchestrator (CDO) Cloud-delivered Firewall Management Center	CDO's cloud-delivered Firewall Management Center has all of the configuration functionality of an on-premises management center. For the analytics functionality, you can use a cloud solution or an on-prem management center. CDO also manages other security devices, such as ASAs. To get started with CDO provisioning, see Threat Defense Deployment with CDO.
Secure Firewall Threat Defense REST API	The threat defense REST API lets you automate direct configuration of the threat defense. 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. To get started with ASDM, see ASA Deployment with ASDM.

Manager	Description
CLI	You can use the CLI to configure all ASA functionality. The CLI is not covered in this guide. For more information, see the ASA configuration guides.
CDO	CDO is a cloud-based, multi-device manager. CDO also manages other security devices, such as threat defenses. CDO for ASA is not covered in this guide. To get started with CDO, see the CDO home page.
Cisco Security Manager (CSM)	CSM is a multi-device manager that runs on its own server hardware. CSM does not support managing the threat defenses. CSM is not covered in this guide. For more information, see the CSM user guide.
ASA HTTP Interface	Using HTTP, an automation tool can execute commands on the ASAs by accessing specifically formatted URLs. The ASA HTTP interface is not covered in this guide. For more information, see the Cisco Secure Firewall ASA HTTP Interface for Automation.