



Which Application and Manager is Right for You?

Your hardware platform can run one of two applications: Secure Firewall Threat Defense or ASA. For each application, you have a choice of managers. This chapter explains the application and manager choices.

- [Applications, on page 1](#)
- [Managers, on page 1](#)

Applications

You can use either of the following applications on your hardware platform:

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

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



Note Secure Firewall Device Manager (formerly Firepower Device Manager) is not supported on the Secure Firewall 4200.

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	<p>The management center is a multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor.</p> <p>For a local management center, see Threat Defense Deployment with the Management Center.</p> <p>For a remote management center, see Threat Defense Deployment with a Remote Management Center.</p>
Cisco Defense Orchestrator (CDO) Cloud-delivered Firewall Management Center	<p>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.</p> <p>See Threat Defense Deployment with CDO.</p>
Secure Firewall Threat Defense REST API	<p>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 or CDO.</p> <p>The threat defense REST API is not covered in this guide. For more information, see the Cisco Secure Firewall Threat Defense REST API Guide.</p>
Secure Firewall Management Center REST API	<p>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.</p> <p>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.</p>

ASA Managers

Table 2: ASA Managers

Manager	Description
CLI	<p>You can use the CLI to configure all ASA functionality.</p> <p>The CLI is not covered in this guide. For more information, see the ASA configuration guides.</p>
Adaptive Security Device Manager (ASDM)	<p>ASDM is a Java-based, on-device manager that provides full ASA functionality.</p> <p>See ASA Deployment with ASDM.</p>
CDO	<p>CDO is a cloud-based, multi-device manager. CDO also manages other security devices, such as threat defenses.</p> <p>CDO for ASA is not covered in this guide. To get started with CDO, see the CDO home page.</p>

Manager	Description
Cisco Security Manager (CSM)	<p>CSM is a multi-device manager that runs on its own server hardware. CSM does not support managing the threat defenses.</p> <p>CSM is not covered in this guide. For more information, see the CSM user guide.</p>
ASA HTTP Interface	<p>Using HTTP, an automation tool can execute commands on the ASAs by accessing specifically formatted URLs.</p> <p>The ASA HTTP interface is not covered in this guide. For more information, see the Cisco Secure Firewall ASA HTTP Interface for Automation.</p>

