General Operations Features

Getting Started

Table 1: Getting Started

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
ASA CLI for Configuration	**Limited Threat Defense CLI for Configuration, Full GUI Configuration** See: Getting Started Guides (console access), Command Reference, Device Configuration Guide	The threat defense CLI includes *limited* commands for initial configuration only and some special operations. Configuration needs to be performed in the management center, which has limited device configuration discovery.
ASA CLI for Monitoring	**Threat Defense CLI for Monitoring** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: Getting Started Guides (console access), Command Reference, Using the Threat Defense CLI from the Web Interface	You can use the same **show** commands that are available on the ASA. You can access the CLI at the console, using SSH, or you can use the CLI web tool.
Initial Configuration	**Initial Configuration** See: Getting Started Guides (console access)	Use the CLI or the device manager to set network settings and register with the management center.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Configuration Changes	**Configuration Deployment** UI path: **Deploy** See: Configuration Deployment	You need to deploy any changes from the management center.
Smart Licenses	**Smart Licenses** UI path: **System** > **Licenses** > **Smart Licenses** See: Licenses How To: Register the Management Center with Cisco Smart Account	Licenses are consumed and assigned by the management center.
Transparent or Routed Firewall Mode	**Transparent or Routed Firewall Mode** See: Transparent or Routed Firewall Mode	Like the ASA, you need to change the firewall mode using the CLI before you register the device to the management center.

High Availability and Scalability

Table 2: High Availability and Scalability

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Multiple Context Mode	**Multi-instance Mode** or **Virtual Routers** UI path: • Firepower 4100/9300 Multi-Instance: **Logical Devices** > **Add** (chassis manager) • Virtual Routers: **Devices** > **Device Management** > **Edit** > **Routing** > **Manage Virtual Routers** See: Using Multi-Instance Capability on the Firepower 4100/9300, Virtual Routers How To: Create a Virtual Router, Assign Interfaces to Virtual Routers, Configure NAT for a Virtual Router, Provide Internet Access with Overlapping Address Spaces, Configure Routing Policy	In many cases, your customers may only need separate routing tables rather than full separation. In this case, you can use virtual routers. For complete configuration separation, use mutli-instance mode on supported platforms. This implementation is different from the ASA multiple context mode, but the functionality is similar.
Active/Standby Failover	**High Availability** UI path: **Devices** > **Device Management** > **Add** > **High Availability** See: High Availability How To: Create a high availability (HA) pair	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Clustering	**Clustering** UI path: • Firepower 4100/9300: **Logical Devices** > **Add** (chassis manager) **Devices** > **Device Management** > **Add** > **Device** (management center) • Threat Defense Virtual for public cloud: **Devices** > **Device Management** > **Add** > **Device** • Secure Firewall 3100: **Devices** > **Device Management** > **Add** > **Cluster** • Threat Defense Virtual for private cloud: **Devices** > **Device Management** > **Add** > **Cluster** See: Deploy a Cluster for Threat Defense on the Secure Firewall 3100, Deploy a Cluster for Threat Defense on the Firepower 4100/9300, Deploy a Cluster for Threat Defense Virtual in a Public Cloud, Deploy a Cluster for Threat Defense Virtual in a Private Cloud How To: Create a Cluster, Modify an Existing Cluster, Add Nodes to an Existing Cluster, Remove a Data Node from a Cluster, Break a Cluster, Delete a Cluster, Break a Node from Clustering, Delete a Data Node from Clustering	Inter-site clustering and distributed site-to-site VPN is not supported.

Interfaces

For the threat defense, interfaces are configured per device. However, for most features, you assign interfaces to security zones and then apply policies to *zones*, not directly to interfaces. Zones, like the security policy itself, are configured as objects that can be shared across multiple devices.

Note The threat defense supports regular firewall interfaces like the ASA, but it also supports a different type of IPS-only interface.

Table 3: Interfaces

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Management Interface	**Management Interface** UI path: **Devices** > **Device Management** > **Edit** > **Devices** > **Management** See: Complete the Threat Defense Initial Configuration	The ASA has a management-only interface that has its own routing table, but operates for the most part like data interfaces. The threat defense has a Management interface separate from the data interfaces. It is used to set up and register the device to the management center. It uses its own IP address and static routing.
Physical Interfaces	**Physical Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Interface Overview How To: Configure Interface Settings	
Firepower 1010 Switch Ports	**Firepower 1010 Switch Ports** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Firepower 1010 Switch Ports	
EtherChannels	**EtherChannels** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure EtherChannel Interfaces	
Loopback Interfaces	**Loopback Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Loopback Interfaces	
VLAN Subinterfaces	**VLAN Subinterfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure VLAN Subinterfaces and 802.1Q Trunking	
VXLAN Interfaces	**VXLAN Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure VXLAN Interfaces	
Routed and Transparent Mode Interfaces	**Routed and Transparent Mode Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Routed and Transparent Mode Interfaces	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Advanced Interface Configuration	**Advanced Interface Configuration** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Advanced Interface Settings	
Traffic Zones	**ECMP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **ECMP** See: ECMP	

Basic Settings

Table 4: Basic Settings

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
DNS Server	**DNS Server** UI path: • **Objects** > **Object Management** > **DNS Server Group** • **Devices** > **Platform Settings** > **DNS** See: DNS Server Group, Configure DNS, FlexConfig Policies	DNS servers are part of platform settings that can be applied to multiple devices. **Note** The DNS server for the threat defense dedicated Management interface is configured at the CLI using the **configure network dns servers** and **configure network dns searchdomains** commands
ISA 3000 Hardware Bypass	**ISA 3000 Hardware Bypass** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: How to Configure Automatic Hardware Bypass for Power Failure (ISA 3000)	This feature can be configured using FlexConfig.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
ISA 3000 Precision Time Protocol	**ISA 3000 Precision Time Protocol** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: How to Configure Precision Time Protocol (ISA 3000)	This feature can be configured using FlexConfig.
ISA 3000 Dual Power Supply	**ISA 3000 Precision Dual Power Supply** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: FlexConfig Policies	This feature can be configured using FlexConfig.
DHCP Server	**DHCP Server** UI path: • IPv4: **Devices** > **Device Management** > **Edit** > **DHCP** > **DHCP Server** • IPv6: **Devices** > **Device Management** > **Edit** > **Interfaces** > **IPv6** > **DHCP** See: Configure the DHCPv4 Server, Configure the DHCPv6 Stateless Server	
DHCP Relay Agent	**DHCP Relay Agent** UI path: **Devices** > **Device Management** > **Edit** > **DHCP** > **DHCP Relay** See: Configure the DHCP Relay Agent	
DDNS	**DDNS** UI path: **Devices** > **Device Management** > **Edit** > **DHCP** > **DDNS** See: Configure Dynamic DNS	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Digital Certificates	**Certificates, PKI** UI path: • **Objects** > **Object Management** > **PKI** • **Devices** > **Certificates** See: PKI, Certificates How To: • Certificate Authentication for Remote Access (RA) VPN—Creating a Certificate Map for Certificate Authentication in RA VPN, Associating a Certificate Map to a Connection Profile • Create and Install an Identity Certificate on Device for Remote Access VPN Configuration—PKCS12 Cert Enrollment Object, Manual Cert Enrollment Object, Self-signed Cert Enrollment Object, SCEP Cert Enrollment Object, Install Manual Certificate, Install PKCS12, SCEP, or Self-Signed Certificate, Configure Remote Access VPN • Configuring VPN—Renew a certificate using manual re-enrollment, Renew a certificate using Self-signed, SCEP, or EST enrollment	Create reusable certificate objects and then apply them per device.
ARP Inspection and the MAC Address Table	**ARP Inspection and the MAC Address Table** UI path: • **Devices** > **Device Management** > **Edit** > **Interfaces** > **Advanced** > **ARP and MAC** • **Devices** > **Platform Settings** > **ARP Inspection** See: Advanced Interface Settings, Configure ARP Inspection	ARP inspection is part of platform settings that can be applied to multiple devices.
WCCP	**WCCP** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: FlexConfig Policies	This feature can be configured using FlexConfig.

Routing

Routing is configured per-device.

Table 5: Routing

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Data and Management Routing Tables	**Data and Management Routing Tables** See: Reference for Routing How To: Configure Routing Policy	The ASA and the threat defense have different defaults for which traffic defaults to the management routing table vs. the data routing table. **Note** The dedicated Management interface has a separate Linux routing table that you can configure at the CLI.
Static and Default Routes	**Static and Default Routes** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **Static Route** See: Static and Default Routes How To: Configure a Static Route for VTI	
Policy Based Routing	**Policy Based Routing** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **Policy Based Routing** See: Policy Based Routing	
Route Maps	**Route Maps** UI path: **Objects** > **Object Management** > **Route Map** See: Route Map	
Bidirectional Forwarding Detection Routing	**Bidirectional Forwarding Detection Routing** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **BFD** See: Bidirectional Forwarding Detection Routing	
BGP	**BGP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **BGP** See: BGP How To: Configure BGP routing for VTI	
OSPF	**OSPF** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **OSPF** See: OSPF	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
ISIS	**ISIS** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: FlexConfig Policies	This feature can be configured using FlexConfig.
EIGRP	**EIGRP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **EIGRP** See: EIGRP	
Multicast Routing	**Multicast Routing** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **Multicast Routing** See: Multicast	
RIP	**RIP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **RIP** See: RIP	

AAA Servers

On the threat defense, AAA servers can be used for VPN access. For AAA servers and the local database for management access, see System Administration, on page 10.

Table 6: AAA Servers

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
RADIUS for VPN	**RADIUS for VPN** UI path: **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** See: Add a RADIUS Server Group	
LDAP for VPN	**LDAP for VPN** UI path: **Integration** > **Other Integrations** > **Realms** See: Create an Active Directory Realm and Realm Directory How To: Configure LDAP attribute map for remote access VPN	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
SAML Single Sign-On for VPN	**SAML Single Sign-On for VPN** UI path: **Objects** > **Object Management** > **AAA Server** > **Single Sign-On Server** See: Add a Single Sign-on Server How To: Add SAML Single Sign-On server object	

System Administration

Table 7: System Administration

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Local Database for Device Management	**Internal User (management center)** UI path: **System** (⚙) > **Users** See: Add an Internal User **Users (threat defense)** See: Add an Internal User at the CLI	The management center and threat defense maintain separate user databases. You can configure management center users for web access and CLI access. To add threat defense users, you need to use the CLI. The threat defense users have SSH access.
RADIUS for Device Management	**RADIUS (management center)** UI path: **System** (⚙) > **Users** > **External Authentication** See: Add a RADIUS External Authentication Object for Management Center **RADIUS (threat defense)** UI path: • **System** (⚙) > **Users** > **External Authentication** • **Devices** > **Platform Settings** > **Edit** > **External Authentication** See: Configure External Authentication for SSH	For threat defense users, you enable the RADIUS authentication object as part of the platform settings.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
LDAP for Device Management	**LDAP (management center)** UI path: **System** (⚙) > **Users** > **External Authentication** See: Add an LDAP External Authentication Object for Management Center **LDAP (threat defense)** UI path: • **System** (⚙) > **Users** > **External Authentication** • **Devices** > **Platform Settings** > **Edit** > **External Authentication** See: Configure External Authentication for SSH	For threat defense users, you enable the LDAP authentication object as part of the platform settings.
SSH	**Access List (management center)** UI path: **System** (⚙) > **Configuration** > **Access List** See: Access List **Secure Shell (threat defense)** UI path: **Devices** > **Platform Settings** > **Secure Shell** See: Configure Secure Shell	For the management center, SSH is enabled by default. You can limit access in the system configuration. For the threat defense, SSH is enabled by default for the dedicated Management interface. You can limit access using the **configure ssh-access-list** command. For SSH to data interfaces, enable it in platform settings. Platform settings can be applied to multiple devices.
HTTPS	**Access List** UI path: **System** (⚙) > **Configuration** > **Access List** See: Access List	You can control HTTPS access to the management center in the system configuration. The threat defense does not support HTTPS access when managed by the management center.
Upgrade the Software	**Upgrade the Software** UI path: **System** (⚙) > **Updates** See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center How To: Upgrade Secure Firewall Threat Defense	Perform all upgrades using the management center.
Downgrading	**Reverting** UI path: **Devices** > **Device Management** > **More** > **Revert Upgrade** See: Revert the Upgrade	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Backup and Restore	**Backup and Restore** UI path: **System** (⚙) > **Tools** > **Backup/Restore** See: Backup and Restore	
Hot Swap an SSD (Secure Firewall 3100)	**Hot Swap an SSD (Secure Firewall 3100)** See: Hot Swap an SSD on the Secure Firewall 3100	Use the CLI to perform the hot swap.
Debugging Messages	**Debugging Messages** See: debug command in the Command Reference	
Packet Capture	**Packet Capture** UI path: **Devices** > **Packet Capture** See: Use the Capture Trace How To: Collect packet capture for threat defense device	
Packet Tracer	**Packet Tracer** UI path: **Devices** > **Packet Tracer** See: Use the Packet Tracer How To: Collect packet trace to troubleshoot threat defense device	
Ping	**Ping** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: ping command in the Command Reference	
Traceroute	**Traceroute** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: traceroute command in the Command Reference	
Connection monitoring	**Connection monitoring** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: show conn command in the Command Reference	
show asp drop	**ASP Drop** UI path: **System** (⚙) > **Health** > **Policy** See: Health Modules	

Monitoring

Table 8: Monitoring

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Logging	**Syslog** UI path: • ASA-style syslogs: **Devices** > **Platform Settings** > **Syslog** • Alerts for file and malware, connection, Security Intelligence, and intrusion events: **Policies** > **Access Control** > **Edit** > **Logging** • Alerts for access control rules, intrusion rules, and other advanced services: **Policies** > **Actions** > **Alerts** See: Configure Syslog, About Sending Syslog Messages for Security Events, Creating a Syslog Alert Response	The threat defense supports the same syslog capability as the ASA. But it also supports logging and alerts generated by the next-generation IPS support that only the threat defense supports. Syslog settings are part of platform settings that can be applied to multiple devices.
SNMP	**SNMP** UI path: **Devices** > **Platform Settings** > **SNMP** See: Configure SNMP	SNMP settings are part of platform settings that can be applied to multiple devices.
Cisco Success Network	**Cisco Success Network** UI path: **Integration** > **SecureX** > **Cisco Cloud Support** See: Configure Cisco Success Network Enrollment	
Alarms for the ISA 3000	**Alarms for the ISA 3000** UI path: **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** See: Alarms for the Cisco ISA 3000	This feature can be configured using FlexConfig.