

Getting Started

The following topics explain how to get started configuring the Firewall Threat Defense device using Firewall Device Manager.

- Is This Guide for You?, on page 1
- New Features in Firewall Device Manager/Firewall Threat Defense Version 7.4, on page 1
- Default Configuration, on page 6
- Logging Into the System, on page 12
- Setting Up the System, on page 17
- Configuration Basics, on page 23
- Communication Port and Internet Access Requirements, on page 33

Is This Guide for You?

This guide explains how to configure Firewall Threat Defense using the Firewall Device Manager web-based configuration interface included on the Firewall Threat Defense devices.

The Firewall Device Manager lets you configure the basic features of the software that are most commonly used for small or mid-size networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many Firewall Threat Defense devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that Firewall Threat Defense allows, use the Firewall Management Center to configure your devices instead of the integrated Firewall Device Manager.

New Features in Firewall Device Manager/Firewall Threat Defense Version 7.4

Released: December 13, 2023

The following table lists the new features available in Firewall Threat Defense 7.4 when configured using the Firewall Device Manager.

Feature	Description
Platform Features	
Network modules for the Secure Firewall 3130 and 3140.	We introduced these network modules for the Secure Firewall 3130 and 3140: • 2-port 100G QSFP+ network module (FPR3K-XNM-2X100G) See: *Cisco Secure Firewall 3100 Series Hardware Installation Guide*
IMDSv2 support for AWS deployments.	Threat defense virtual for AWS now supports Instance Metadata Service Version 2 (IMDSv2), a security improvement over IMDSv1. When you enable the instance metadata service on AWS, IMDSv2 Optional mode is still the default, but we recommend you choose IMDSv2 Required. We also recommend you switch your upgraded instances. See: Secure Firewall Threat Defense Virtual getting started guides
Firewall and IPS Features	
Sensitive data detection and masking.	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. Requires Snort 3.
VPN Features	
IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100.	**Upgrade impact. Qualifying connections start being offloaded.** On the Secure Firewall 3100, qualifying IPsec connections through the VTI loopback interface are now offloaded by default. Previously, this feature was only supported on physical interfaces. This feature is automatically enabled by the upgrade. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command.
Interface Features	

Feature	Description
Merged management and diagnostic interfaces.	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later, and you did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. If you upgraded to 7.4 or later, and you have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including management) in the configuration. New/modified screens: • **Devices** > **Interfaces** > **Management** interface • (Moved to Interfaces) **System Settings** > **Management Interface** • **Devices** > **Interfaces** > **Merge Interface action needed** > **Management Interface Merge** New/modified commands: **show management-interface convergence**
Deploy without the diagnostic interface on threat defense virtual for Azure and GCP.	You can now deploy without the diagnostic interface on threat defense virtual for Azure and GCP. Azure deployments still require at least two data interfaces, but GCP requires that you replace the diagnostic interface with a data interface, for a new minimum of three. (Previously, threat defense virtual deployments required one management, one diagnostic, and at least two data interfaces.) Restrictions: This feature is supported for new deployments only. It is not supported for upgraded devices. See: Secure Firewall Threat Defense Virtual getting started guides
Inline sets for Firepower 1000 series, Firepower 2100, and Secure Firewall 3100.	You can configure inline sets on Firepower 1000 series, Firepower 2100, and Secure Firewall 3100 devices. We added the inline sets tab to the Interface page.
Licensing Features	

Feature	Description
Changes to license names and support for the Carrier license.	Licenses have been renamed: • Threat is now IPS • Malware is now Malware Defense • Base is now Essentials • AnyConnect Apex is now Secure Client Premier • AnyConnect Plus is now Secure Client Advantage • AnyConnect VPN Only is now Secure Client VPN Only In addition, you can now apply the Carrier license, which allows you to configure GTP/GPRS, Diameter, SCTP, and M3UA inspections. Use FlexConfig to configure these features.
Administrative and Troubleshooting Features	
Default NTP server updated.	**Upgrade impact. The system connects to new resources.** The default NTP servers have changed from sourcefire.pool.ntp.org to time.cisco.com. To use a different NTP server, select **Device**, then click **Time Services** in the **System Settings** panel.
SAML servers for HTTPS management user access.	You can configure a SAML server to provide external authentication for HTTPS management access. You can configure external users with the following types of authorization access: Administrator, Audit Admin, Cryptographic Admin, Read-Write User, Read-Only User. You can use Common Access Card (CAC) for login when using a SAML server. We updated the SAML identity source object configuration, and the **System Settings** > **Management Access** page to accept them.
Detect configuration mismatches in threat defense high availability pairs.	You can now use the CLI to detect configuration mismatches in threat defense high availability pairs. New/modified CLI commands: **show failover config-sync error**, **show failover config-sync stats** See: *Cisco Secure Firewall Threat Defense Command Reference*
Capture dropped packets with the Secure Firewall 3100.	Packet losses resulting from MAC address table inconsistencies can impact your debugging capabilities. The Secure Firewall 3100 can now capture these dropped packets. New/modified CLI commands: [**drop** { **disable** | **mac-filter** }] in the **capture** command. See: *Cisco Secure Firewall Threat Defense Command Reference*

Feature	Description
Firmware upgrades included in FXOS upgrades.	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1+ now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*
Quick recovery after data plane failure for the Firepower 1000/2100 and Firepower 4100/9300.	When the data plane process on the Firepower 1000/2100 or the Firepower 4100/9300 crashes, the system reloads the process instead of rebooting the device. Reloading the data plane also restarts other processes, including Snort. If the data plane crashes during bootup, the device follows the normal reload/reboot sequence; this avoids a reload loop. This feature is enabled by default for both new and upgraded devices. To disable it, use FlexConfig. New/modified ASA CLI commands: **data-plane quick-reload**, **show data-plane quick-reload status** New/modified threat defense CLI commands: **show data-plane quick-reload status** See: *Cisco Secure Firewall Threat Defense Command Reference* and *Cisco Secure Firewall ASA Series Command Reference*.

Feature	Description
Require the Message-Authenticator attribute in all RADIUS responses.	**Upgrade impact. For the Firepower 4100/9300, check FXOS compatibility before you upgrade Firewall Threat Defense. After Firewall Threat Defense upgrade, enable the option for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Firewall Threat Defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **Require Message-Authenticator for all RADIUS Responses** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New CLI commands: **message-authenticator-required** Version restrictions: Requires Version 7.0.7, 7.2.10, 7.4.3, 7.6.1, or 7.7+. For the Firepower 4100/9300, may require an FXOS upgrade; for minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Default Configuration

The default configuration of your device depends on whether you have completed initial setup.

Default Configuration Prior to Initial Setup

Before you initially configure the Firewall Threat Defense device using the local manager (Firewall Device Manager), the device includes the following default configuration.

For many models, this configuration assumes that you open the device manager through the inside interface, typically by plugging your computer directly into the interface, and use the DHCP server defined on the inside interface to supply your computer with an IP address. Alternatively, you can plug your computer into the Management interface and use DHCP to obtain an address. However, some models have different default configurations and management requirements. See the table below for details.

Note You can pre-configure many of these settings using the CLI setup ((Optional) Change Management Network Settings at the CLI, on page 18) before you perform setup using the wizard.

Default Configuration Settings

Setting	Default	Can be changed during initial configuration?
Password for admin user.	Admin123 Firepower 4100/9300: Set the password when you deploy the logical device. AWS: The default is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.	Yes. You must change the default password.
Management IP address.	Obtained through DHCP. Firewall Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300: Set the management IP address when you deploy the logical device.	No. For Firepower 4100/9300: Yes.
Management gateway.	The data interfaces on the device. Typically the outside interface becomes the route to the Internet. This gateway works for from-the-device traffic only. If the device receives a default gateway from the DHCP server, then that gateway is used. Firepower 4100/9300: Set the gateway IP address when you deploy the logical device. ISA 3000: 192.168.45.1. Firewall Threat Defense Virtual: 192.168.45.1	No. For Firepower 4100/9300: Yes.
DNS servers for the management interface.	The OpenDNS public DNS servers, IPv4: 208.67.220.220 and 208.67.222.222; IPv6: 2620:119:35::35. DNS servers obtained from DHCP are never used. Firepower 4100/9300: Set the DNS servers when you deploy the logical device.	Yes
Inside interface IP address.	192.168.95.1/24 Firepower 4100/9300: Data interfaces are not pre-configured. ISA 3000: BVI1 IP address is not preconfigured. BVI1 includes all inside and outside interfaces. Firewall Threat Defense Virtual: 192.168.45.1/24	No.

Setting	Default	Can be changed during initial configuration?
DHCP server for inside clients.	Running on the inside interface with the address pool 192.168.95.5 - 192.168.95.254. Firepower 4100/9300: No DHCP server enabled. ISA 3000: No DHCP server enabled. Firewall Threat Defense Virtual: The address pool on the inside interface is 192.168.45.46 - 192.168.45.254.	No.
DHCP auto-configuration for inside clients. (Auto-configuration supplies clients with addresses for WINS and DNS servers.)	Enabled on outside interface.	Yes, but indirectly. If you configure a static IPv4 address for the outside interface, DHCP server auto-configuration is disabled.
Outside interface IP address.	IPv4: Obtained through DHCP from Internet Service Provider (ISP) or upstream router. IPv6: Autoconfiguration. Firepower 4100/9300: Data interfaces are not pre-configured. ISA 3000: BVI1 IP address is not preconfigured. BVI1 includes all inside and outside interfaces.	Yes.

Default Interfaces by Device Model

You cannot select different inside and outside interfaces during initial configuration. To change the interface assignments after configuration, edit the interface and DHCP settings. You must remove an interface from the bridge group before you can configure it as a non-switched interface.

Device Model	Outside Interface	Inside Interface
Firepower 1010	Ethernet1/1	VLAN1, which includes all other switch ports except the outside interface, which is a physical firewall interface.
Firepower 1120, 1140, 1150	Ethernet1/1	Ethernet1/2
Firepower 2100	Ethernet1/1	Ethernet1/2
Secure Firewall 3100	Ethernet1/1	Ethernet1/2
Firepower 4100	Data interfaces are not pre-configured.	Data interfaces are not pre-configured.
Firepower 9300	Data interfaces are not pre-configured.	Data interfaces are not pre-configured.

Device Model	Outside Interface	Inside Interface
Firewall Threat Defense Virtual	GigabitEthernet0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 and GigabitEthernet1/3 GigabitEthernet1/1 (outside1) and 1/2 (inside1), and GigabitEthernet1/3 (outside2) and 1/4 (inside2) (non-fiber models only) are configured as Hardware Bypass pairs. All inside and outside interfaces are part of BVI1.	GigabitEthernet1/2 and GigabitEthernet1/4

Configuration After Initial Setup

After you complete the setup wizard, the device configuration will include the following settings. The table shows whether a particular setting is something you explicitly chose or whether it was defined for you based on your other selections. Validate any "implied" configurations and edit them if they do not serve your needs.



Note The Firepower 4100/9300 and ISA 3000 do not support the setup wizard. For the Firepower 4100/9300 , all initial configuration is set when you deploy the logical device from the chassis. For the ISA 3000, a special default configuration is applied before shipping.

Setting	Configuration	Explicit, implied, or default configuration
Password for admin user.	Whatever you entered.	Explicit.
Management IP address.	Obtained through DHCP. Firewall Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300 : The management IP address you set when you deployed the logical device.	Default.
Management gateway.	The data interfaces on the device. Typically the outside interface becomes the route to the Internet. The management gateway works for from-the-device traffic only. If the device receives a default gateway from the DHCP server, then that gateway is used. Firepower 4100/9300 : The gateway IP address you set when you deployed the logical device. ISA 3000: 192.168.45.1 Firewall Threat Defense Virtual: 192.168.45.1	Default.

Setting	Configuration	Explicit, implied, or default configuration
DNS servers for the management interface.	The OpenDNS public DNS servers, IPv4: 208.67.220.220, 208.67.222.222; IPv6: 2620:119:35::35, or whatever you entered. DNS servers obtained from DHCP are never used. Firepower 4100/9300 : The DNS servers you set when you deployed the logical device.	Explicit.
Management hostname.	**firepower** or whatever you entered. Firepower 4100/9300 : The hostname you set when you deployed the logical device.	Explicit.
Management access through data interfaces.	A data interface management access list rule allows HTTPS access through the inside interface. SSH connections are not allowed. Both IPv4 and IPv6 connections are allowed. Firepower 4100/9300 : No data interfaces have default management access rules. ISA 3000: No data interfaces have default management access rules. Firewall Threat Defense Virtual: No data interfaces have default management access rules.	Implied.
System time.	The time zone and NTP servers you selected. Firepower 4100/9300 : System time is inherited from the chassis. ISA 3000: Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org.	Explicit.
Smart license.	Either registered with a base license, or the evaluation period activated, whichever you selected. Subscription licenses are not enabled. Go to the smart licensing page to enable them.	Explicit.
Inside interface IP address.	192.168.95.1/24 Firepower 4100/9300 : Data interfaces are not pre-configured. ISA 3000: None. You must set the BVI1 IP address manually. Firewall Threat Defense Virtual: 192.168.45.1/24	Default.
DHCP server for inside clients.	Running on the inside interface with the address pool 192.168.95.5 - 192.168.95.254. Firepower 4100/9300 : No DHCP server enabled. ISA 3000: No DHCP server enabled. Firewall Threat Defense Virtual: The address pool on the inside interface is 192.168.45.46 - 192.168.45.254.	Default.

Setting	Configuration	Explicit, implied, or default configuration
DHCP auto-configuration for inside clients. (Auto-configuration supplies clients with addresses for WINS and DNS servers.)	Enabled on outside interface if you use DHCP to obtain the outside interface IPv4 address. If you use static addressing, DHCP auto-configuration is disabled.	Explicit, but indirectly.
Data interface configuration.	• 1010—The outside interface, Ethernet1/1, is a physical firewall interface. All other interfaces are switch ports that are enabled and part of VLAN1, the inside interface. You can plug end points or switches into these ports and obtain addresses from the DHCP server for the inside interface. • Firepower 4100/9300 —All data interfaces are disabled. • ISA 3000—All data interfaces are enabled and part of the same bridge group, BVI1. GigabitEthernet1/1 and 1/3 are outside interfaces, and GigabitEthernet1/2 and 1/4 are inside interfaces. GigabitEthernet1/1 (outside1) and 1/2 (inside1), and GigabitEthernet1/3 (outside2) and 1/4 (inside2) (non-fiber models only) are configured as Hardware Bypass pairs. • All other models—The outside and inside interfaces are the only ones configured and enabled. All other data interfaces are disabled.	Default.
Outside physical interface and IP address.	The default outside port based on the device model. See Default Configuration Prior to Initial Setup, on page 6. The IP address is obtained by DHCP and IPv6 autoconfiguration, or it is a static address as entered (IPv4, IPv6, or both). Firepower 4100/9300 : Data interfaces are not pre-configured. ISA 3000: None. You must set the BVI1 IP address manually.	Interface is Default. Addressing is Explicit.
Static routes.	If you configure a static IPv4 or IPv6 address for the outside interface, a static default route is configured for IPv4/IPv6 as appropriate, pointing to the gateway you defined for that address type. If you select DHCP, the default route is obtained from the DHCP server. Network objects are also created for the gateway and the "any" address, that is, 0.0.0.0/0 for IPv4, ::/0 for IPv6.	Implied.

Setting	Configuration	Explicit, implied, or default configuration
Security zones.	**inside_zone**, containing the inside interfaces. For the Firepower 4100/9300 , you need to add interfaces manually to this security zone. **outside_zone**, containing the outside interfaces. For the Firepower 4100/9300 , you need to add interfaces manually to this zone. (You can edit these zones to add other interfaces, or create your own zones.)	Implied.
Access control policy.	A rule trusting all traffic from the inside_zone to the outside_zone. This allows without inspection all traffic from users inside your network to get outside, and all return traffic for those connections. The default action for any other traffic is to block it. This prevents any traffic initiated from outside to enter your network. Firepower 4100/9300 : There are no pre-configured access rules. ISA 3000: A rule trusting all traffic from the inside_zone to the outside_zone, and a rule trusting all traffic from the outside_zone to the inside_zone. Traffic is not blocked. The device also has rules trusting all traffic between the interfaces in the inside_zone and in the outside_zone. This allows without inspection all traffic between users on the inside, and between users on the outside.	Implied.
NAT	An interface dynamic PAT rule translates the source address for any IPv4 traffic destined to the outside interface to a unique port on the outside interface's IP address. There are additional hidden PAT rules to enable HTTPS access through the inside interfaces, and routing through the data interfaces for the management address. These do not appear in the NAT table, but you will see them if you use the **show nat** command in the CLI. Firepower 4100/9300 : NAT is not pre-configured. ISA 3000: NAT is not pre-configured.	Implied.

Logging Into the System

There are two interfaces to the Firewall Threat Defense device:

Firewall Device Manager Web Interface

The Firewall Device Manager runs in your web browser. You use this interface to configure, manage, and monitor the system.

Command Line Interface (CLI, Console)

Use the CLI for troubleshooting. You can also use it for initial setup instead of the Firewall Device Manager.

The following topics explain how to log into these interfaces and manage your user account.

Your User Role Controls What You Can See and Do

Your username is assigned a role, and your role determines what you can do or what you can see in the Firewall Device Manager. The locally-defined **admin** user has all privileges, but if you log in using a different account, you might have fewer privileges.

The upper-right corner of the Firewall Device Manager window shows your username and privilege level.



The privileges are:

- **Administrator**—You can see and use all features.
- **Read-Write User**—You can do everything a read-only user can do, but also edit and deploy the configuration. The only restrictions are for system-critical actions, which include installing upgrades, creating and restoring backups, viewing the audit log, and ending the sessions of other Firewall Device Manager users.
- **Read-Only User**—You can view dashboards and the configuration, but you cannot make any changes. If you try to make a change, the error message explains that this is due to lack of permission.
- **Cryptographic Admin**—You can configure encryption-related features such as certificates, decryption policies, and secret keys. Read-only access to other features.
- **Audit Admin**—You can view user login history and the audit log and perform auditing-related actions. Read-only access to configuration features.

These privileges are not related to those available for CLI users.

Logging Into the Firewall Device Manager

Use the Firewall Device Manager to configure, manage, and monitor the system. The features that you can configure through the browser are not configurable through the command-line interface (CLI); you must use the web interface to implement your security policies.

Use a current version of the following browsers: Firefox, Chrome, Safari, Edge.

Note If you type in the wrong password and fail to log in on 3 consecutive attempts, your account is locked for 5 minutes. You must wait before trying to log in again.

Before you begin

Initially, you can log into the Firewall Device Manager using the **admin** username only. However, you can then configure authorization for additional users defined in an external AAA server, as described in Managing Firewall Device Manager and Firewall Threat Defense User Access.

There can be up to 5 active logins at one time. This includes users logged into the device manager and active API sessions, which are represented by non-expired API tokens. If you exceed this limit, the oldest session, either the device manager login or API token, is expired to allow the new session. These limits do not apply to SSH sessions.

Procedure

Step 1 Using a browser, open the home page of the system, for example, https://ftd.example.com.

You can use any of the following addresses. You can use the IPv4 or IPv6 address or the DNS name, if you have configured one.

- The management address. By default (on most platforms), the Management interface is a DHCP client, so the IP address depends on your DHCP server.
- The address of a data interface that you have opened for HTTPS access. By default (on most platforms), the "inside" interface allows HTTPS access, so you can connect to the default inside address 192.168.95.1. See Default Configuration Prior to Initial Setup, on page 6 for details about your model's inside IP address.

  If you changed the HTTPS data port, you must include the custom port in the URL. For example, if you changed the port to 4443: https://ftd.example.com:4443

Tip
If your browser is not configured to recognize the server certificate, you will see a warning about an untrusted certificate. Accept the certificate as an exception, or in your trusted root certificate store.

Step 2 If the login screen includes text, such as a warning or disclaimer, read the information, then select the checkbox to acknowledge your agreement.

Step 3 (Local User and RADIUS only.)Enter your username and password defined for the device, then click **Login**.

You can use the **admin** username, which is a pre-defined user. The default admin password is Admin123. On AWS, the default admin password is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

Your session will expire after 30 minutes of inactivity, and you will be prompted to log in again. You can log out by selecting **Log Out** from the user icon drop-down menu in the upper right of the page.



Step 4 (SAML server only.) Click the **Single-Sign On (SSO)** link next to the **Login** button.

This will take you to the SAML server for login. Do not enter credentials, just click the link. If you enter local credentials and click Login, that logs you in using the local database.

When on the SAML server's login page, log in as you would normally do. If you use a Common Access Card (CAC) for login, click the link to sign in using certificates. The device manager does not directly deal with CAC authentication.

Logging Into the Command Line Interface (CLI)

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session.

To log into the CLI, do one of the following:

- Use the console cable included with the device to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your device for more information about the console cable.



Note On the Firepower and Secure Firewall device models, the CLI on the Console port is the Secure Firewall eXtensible Operating System (FXOS). For the some device models, you can get to the Firewall Threat Defense CLI using the **connect ftd** command. For the Firepower 4100/9300, see Connect to the Console of the Application. Use the FXOS CLI for chassis-level troubleshooting only. Use the Firewall Threat Defense CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands.

- For the Firewall Threat Defense Virtual, open the virtual console.
- Use an SSH client to make a connection to the management IP address. You can also connect to the address on a data interface if you open the interface for SSH connections (see Configuring the Management Access List). SSH access to data interfaces is disabled by default. Log in using the **admin** username or another CLI user account. The default admin password is Admin123. On AWS, the default admin password for the Firewall Threat Defense Virtual is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

Tips

- If the administrator added text to the login process, such as a warning or disclaimer, you need to acknowledge that you read and agree to the statement.
- After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see Cisco Firepower Threat Defense Command Reference at http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.
- You can create local user accounts that can log into the CLI using the **configure user add** command. However, these users can log into the CLI only. They cannot log into the Firewall Device Manager web interface.
- You can create user accounts for SSH access in an external server. For information about configuring external authentication for SSH access, see Configuring External Authorization (AAA) for the Firewall Threat Defense CLI (SSH) Users.

Changing Your Password

You should periodically change your password. The following procedure explains how to change the password while logged into Firewall Device Manager.

Note If you are logged into the CLI, you can change your password using the **configure password** command. You can change the password for a different CLI user with the **configure user password** *username* command.

Before you begin

This procedure applies to local users only. If your user account is defined on an external AAA server, you must change your password with that server.

Procedure

Step 1 Select **Profile** from the user icon drop-down list in the upper right of the menu.



Step 2 Click the **Password** tab.

Step 3 Enter your current password.

Step 4 Enter your new password and then confirm it.

You can click **Generate** to have a random 16 character password generated for you. Click the Show Password () button to see the passwords unmasked. Then, click the **Copy To Clipboard** link so you can paste the password in the confirmation field.

The page includes the minimum requirements for a password. You cannot change these minimum requirements. Passwords must:

- Be 8 – 128 characters
- Have at least one lower and one upper case letter
- Have at least one digit
- Have at least one special character
- Not contain repeated letters

Step 5 Click **Change**.

Setting User Profile Preferences

You can set preferences for the user interface and change your password.

Procedure

Step 1 Select **Profile** from the user icon drop-down list in the upper right of the menu.



Step 2 On the **Profile** tab, configure the following and click **Save**.

- **Time Zone for Scheduling Tasks**—Select the time zone you want to use for scheduling tasks such as backups and updates. The browser time zone is used for dashboards and events, if you set a different zone.
- **Color Theme**—Select the color theme you want to use in the user interface.

Step 3 On the **Password** tab, you can enter a new password and click **Change**.

Viewing Pages in Languages Other Than English

You can view the GUI and online help in the following languages.

- Chinese
- English (the default)
- Japanese
- Korean

To use these languages, you must select that language in your browser settings. There is no language setting in the product itself.

If your browser does not support a particular language, the product will not appear in that language. For example, the French version appears only if you configure the browser to use Canadian French. Selecting another type of French leaves the product in English.

Setting Up the System

You must complete an initial configuration to make the system function correctly in your network. Successful deployment includes attaching cables correctly and configuring the addresses needed to insert the device into your network and connect it to the Internet or other upstream router. The following procedure explains the process.

Before you begin

Before you start the initial setup, the device includes some default settings. For details, see Default Configuration Prior to Initial Setup, on page 6.

Procedure

Step 1 Connect the Interfaces, on page 18

Step 2 Complete the Initial Configuration Using the Setup Wizard, on page 20

For details about the resulting configuration, see Configuration After Initial Setup, on page 9.

Connect the Interfaces

The default configuration assumes that certain interfaces are used for the inside and outside networks. Initial configuration will be easier to complete if you connect network cables to the interfaces based on these expectations.

The default configuration for most models is designed to let you attach your management computer to the inside interface. Alternatively, you can also directly attach your workstation to the Management port. The interfaces are on different networks, so do not try to connect any of the inside interfaces and the Management port to the same network.

Do not connect any of the inside interfaces to a network that has an active DHCP server. This will conflict with the DHCP server already running on the inside interface . If you want to use a different DHCP server for the network, disable the unwanted DHCP server after initial setup.

See the getting started guide for your model for cabling diagrams.

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in the GUI.

Note You do not need to use this procedure for the Firepower 4100/9300, because you set the IP address manually when you deployed.

Note You cannot repeat the CLI setup script unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See *Cisco Secure Firewall Threat Defense Command Reference*.

Procedure

Step 1 Connect to the Firewall Threat Defense console port. See Logging Into the Command Line Interface (CLI), on page 15 for more information.

Step 2 Log in with the username **admin**.

The default admin password is Admin123. On AWS, the default admin password for the Firewall Threat Defense Virtual is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

Step 3 The first time you log into the Firewall Threat Defense, you are prompted to accept the End User License Agreement (EULA) and to change the admin password. You are then presented with the CLI setup script.

Defaults or previously-entered values appear in brackets. To accept previously entered values, press **Enter**.

See the following guidelines:

- **Enter the IPv4 default gateway for the management interface**—If you set a manual IP address, enter either **data-interfaces** or the IP address of the gateway router. The **data-interfaces** setting sends outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the Firewall Device Manager (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that the Firewall Device Manager management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP and uses the **data-interfaces** as a fallback method if DHCP doesn't provide a gateway.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **yes** to use the Firewall Device Manager. A **no** answer means you intend to use the on-premises or cloud-delivered Firewall Management Center to manage the device.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
```

```
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Step 4 Log into the Firewall Device Manager on the new Management IP address.

Complete the Initial Configuration Using the Setup Wizard

When you initially log into the Firewall Device Manager, you are taken through the device setup wizard to complete the initial system configuration.

If you plan to use the device in a high availability configuration, please read Prepare the Two Units for High Availability.

Note The Firepower 4100/9300 and ISA 3000 do not support the setup wizard, so this procedure does not apply to these models. For the Firepower 4100/9300, all initial configuration is set when you deploy the logical device from the chassis. For the ISA 3000, a special default configuration is applied before shipping.

Before you begin

Ensure that you connect a data interface to your gateway device, for example, a cable modem or router. For edge deployments, this would be your Internet-facing gateway. For data center deployments, this would be a back-bone router. Use the default "outside" interface for your model (see Connect the Interfaces, on page 18 and Default Configuration Prior to Initial Setup, on page 6).

Then, connect your management computer to the "inside" interface for your hardware model. Alternatively, you can connect to the Management interface. For the Firewall Threat Defense Virtual, simply ensure that you have connectivity to the management IP address.

(Except for the Firewall Threat Defense Virtual, which requires connectivity to the internet from the management IP address.) The Management interface does not need to be connected to a network. By default, the system obtains system licensing and database and other updates through the data interfaces, typically the outside interface, that connect to the internet. If you instead want to use a separate management network, you can connect the Management interface to a network and configure a separate management gateway after you complete initial setup.

To change the Management interface network settings if you cannot access the default IP address, see (Optional) Change Management Network Settings at the CLI, on page 18.

Procedure

Step 1 Log into the Firewall Device Manager.

a) Assuming you did not go through initial configuration in the CLI, open the Firewall Device Manager at **https://***ip-address*, where the address is one of the following.

- If you are connected to the inside interface: **https://192.168.95.1**.
- (Firewall Threat Defense Virtual) If you are connected to the Management interface: **https://192.168.45.45**.
- (All other models) If you are connected to the Management interface: **https://***dhcp_client_ip*

b) Log in with the username **admin**. The default admin password is Admin123. On AWS, the default admin password for the Firewall Threat Defense Virtual is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment..

Step 2 If this is the first time logging into the system, and you did not use the CLI setup wizard, you are prompted to read and accept the End User License Agreement and change the admin password.

You must complete these steps to continue.

Step 3 Configure the following options for the outside and management interfaces and click **Next**.

Caution
Your settings are deployed to the device when you click **Next**. The interface will be named "outside" and it will be added to the "outside_zone" security zone. Ensure that your settings are correct.

Outside Interface

- **Configure IPv4**—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. Do not configure an IP address on the same subnet as the default inside address (see Default Configuration Prior to Initial Setup, on page 6), either statically or through DHCP. PPPoE is not supported on WAN interfaces, including interfaces that you use as VPN tunnel sources. Use DHCP or a static IPv4 address for WAN interfaces..
- **Configure IPv6**—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

Management Interface

- **DNS Servers**—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers, or the DNS servers you obtain from the DHCP server. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields. Your ISP might require that you use specific DNS servers. If after completing the wizard, you find that DNS resolution is not working, see Troubleshooting DNS for the Management Interface.
- **Firewall Hostname**—The hostname for the system's management address.

Step 4 Configure the system time settings and click **Next**.

- **Time Zone**—Select the time zone for the system.
- **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

Step 5 Configure the smart licenses for the system.

You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

To register the device now, select the option to register the device, click the link to log into your Smart Software Manager account, generate a new token, and copy the token into the edit box. You must also select your services region, and decide whether to send usage data to the Cisco Success Network. The on-screen text explains these settings in more detail.

If you do not want to register the device yet, select the evaluation mode option. The evaluation period last up to 90 days. To later register the device and obtain smart licenses, click **Device**, then click the link in the **Smart Licenses** group.

Step 6 Click **Finish**.

What to do next

- If you want to use features covered by optional licenses, such as category-based URL filtering, intrusion inspection, or malware prevention, enable the required licenses. See Enabling or Disabling Optional Licenses.
- Connect the other data interfaces to distinct networks and configure the interfaces. For information on configuring interfaces, see How to Add a Subnet and Interfaces.
- If you are managing the device through the inside interface, and you want to open CLI sessions through the inside interface, open the inside interface to SSH connections. See Configuring the Management Access List.
- Go through the use cases to learn how to use the product. See Best Practices: Use Cases for Firewall Threat Defense.

What to Do if You Do Not Obtain an IP Address for the Outside Interface

The default device configuration includes a static IPv4 address for the inside interface. You cannot change this address through the initial device setup wizard, although you can change it afterwards.

The default inside IP address might conflict with other networks attached to the device. This is especially true if you use DHCP on the outside interface to obtain an address from your Internet Service Provider (ISP). Some ISPs use the same subnet as the inside network as the address pool. Because you cannot have two data interfaces with addresses on the same subnet, conflicting addresses from the ISP cannot be configured on the outside interface.

If there is a conflict between the inside static IP address and the DHCP-provided address on the outside interface, the connection diagram should show the outside interface as administratively UP, but with no IPv4 address.

The setup wizard will complete successfully in this case, and all the default NAT, access, and other policies and settings will be configured. Simply follow the procedure below to eliminate the conflict.

Before you begin

Verify that you have a healthy connection to the ISP. Although a subnet conflict will prevent you from getting an address on the outside interface, you will also fail to get one if you simply do not have a link to the ISP.

Procedure

Step 1 Click **Device**, then click the link in the **Interfaces** summary.

Step 2 Mouse over the **Actions** column for the inside interface and click the edit icon ( ).

Step 3 On the **IPv4 Address** tab, enter a static address on a unique subnet, for example, 192.168.2.1/24 or 192.168.46.1/24. Note that the default management address is 192.168.45.45/24, so do not use that subnet.

You also have the option to use DHCP to obtain an address if you have a DHCP server already running on the inside network. However, you must first click **Delete** in the **DHCP SERVER IS DEFINED FOR THIS INTERFACE** group to remove the DHCP server from the interface.

Step 4 In the **DHCP SERVER IS DEFINED FOR THIS INTERFACE** area, click **Edit** and change the DHCP pool to a range on the new subnet, for example, 192.168.2.5-192.168.2.254.

Step 5 Click **OK** to save the interface changes.

Step 6 Click the **Deploy** button in the menu to deploy your changes.



Step 7 Click **Deploy Now**.

After deployment completes, the connection graphic should show that the outside interface now has an IP address. Use a client on the inside network to verify you have connectivity to the Internet or other upstream network.

Configuration Basics

The following topics explain the basic methods for configuring the device.

Configuring the Device

When you initially log into Firewall Device Manager, you are guided through a setup wizard to help you configure basic settings. Once you complete the wizard, use the following method to configure other features and to manage the device configuration.

If you have trouble distinguishing items visually, select a different color scheme in the user profile. Select **Profile** from the user icon drop-down menu in the upper right of the page.



Procedure

Step 1 Click **Device** to get to the **Device Summary**.

The dashboard shows a visual status for the device, including enabled interfaces and whether key settings are configured (colored green) or still need to be configured. For more information, see Viewing Interface and Management Status, on page 29.

Above the status image is a summary of the device model, software version, VDB (System and Vulnerability Database) version, and the last time intrusion rules were updated. This area also shows high availability status, including links to configure the feature; see High Availability (Failover). It also shows cloud registration status, where you see the account to which the device is registered if you are using cloud management; see Configuring Cloud Services.

Below the image are groups for the various features you can configure, with summaries of the configurations in each group, and actions you can take to manage the system configuration.

Step 2 Click the links in each group to configure the settings or perform the actions.

Following is a summary of the groups:

- **Interface**—You should have at least two data interfaces configured in addition to the management interface. See Interfaces.
- **Routing**—The routing configuration. You must define a default route. Other routes might be necessary depending on your configuration. See Routing.
- **Updates**—Geolocation, intrusion rule, and vulnerability database updates, and system software upgrades. Set up a regular update schedule to ensure that you have the latest database updates if you use those features. You can also go to this page if you need to download an update before the regularly schedule update occurs. See Updating System Databases and Feeds.
- **System Settings**—This group includes a variety of settings. Some are basic settings that you would configure when you initially set up the device and then rarely change. See System Settings.
- **Smart License**—Shows the current state of the system licenses. You must install the appropriate licenses to use the system. Some features require additional licenses. See Licensing the System.
- **Backup and Restore**—Back up the system configuration or restore a previous backup. See Backing Up and Restoring the System.
- **Troubleshoot**—Generate a troubleshooting file at the request of the Cisco Technical Assistance Center. See Creating a Troubleshooting File.
- **Site-to-Site VPN**—The site-to-site virtual private network (VPN) connections between this device and remote devices. See Managing Site-to-Site VPNs.
- **Remote Access VPN**—The remote access virtual private network (VPN) configuration that allows outside clients to connect to your inside network. See Configuring Remote Access VPN.
- **Advanced Configuration**—Use FlexConfig and Smart CLI to configure features that you otherwise cannot configure using Firewall Device Manager. See Advanced Configuration.
- **Device Administration**—View the audit log or export a copy of the configuration. See Auditing and Change Management.

Step 3 Click the **Deploy** button in the menu to deploy your changes.



Changes are not active on the device until you deploy them. See Deploying Your Changes, on page 26.

What to do next

Click **Policies** in the main menu and configure the security policy for the system. You can also click **Objects** to configure the objects needed in those policies.

Configuring Security Policies

Use the security policies to implement your organization's acceptable use policy and to protect your network from intrusions and other threats.

Procedure

Step 1 Click **Policies**.

The Security Policies page shows the general flow of a connection through the system, and the order in which security policies are applied.

Step 2 Click the name of a policy and configure it.

You might not need to configure each policy type, although you must always have an access control policy. Following is a summary of the policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it. See Configuring SSL Decryption Policies.
- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address. See Configuring Identity Policies.
- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to selected IP addresses or URLs. By blocking known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence block lists update dynamically. Using feeds, you do not need to edit the policy to add or remove items in the block lists. See Configuring Security Intelligence.
- **NAT** (Network Address Translation)—Use the NAT policy to convert internal IP addresses to externally routeable addresses. See Configure NAT.
- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering. See Configuring the Access Control Policy.
- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules. See Intrusion Policies.

Step 3 Click the **Deploy** button in the menu to deploy your changes.



Changes are not active on the device until you deploy them. See Deploying Your Changes, on page 26.

Searching for Rules or Objects

You can use full-text search on lists of policy rules or objects to help you find the item you want to edit. This is especially helpful when dealing with policies that have hundreds of rules, or long object lists.

The method for using search on rules and objects is the same for any type of policy (except the intrusion policy) or object: in the **Search** field, enter a string to find, and press Enter.

This string can exist in any part of the rule or object, and it can be a partial string. You can use the asterisk * as a wildcard that matches zero or more characters. Do not include the following characters, they are not supported as part of the search string: ?~!{}<>:%. The following characters are ignored: ;#&.

The string can appear within an object in the group. For example, you can enter an IP address and find the network objects or groups that specify that address.

When done, click the **x** on the right side of the search box to clear the filter.

Deploying Your Changes

When you update a policy or setting, the change is not immediately applied to the device. There is a two step process for making configuration changes:

1. Make your changes.
2. Deploy your changes.

This process gives you the opportunity to make a group of related changes without forcing you to run a device in a “partially configured” manner. In most cases, the deployment includes just your changes. However, if necessary, the system will reapply the entire configuration, which might be disruptive to your network. In addition, some changes require inspection engines to restart, with traffic dropping during the restart. Thus, consider deploying changes when potential disruptions will have the least impact.



Note If the deployment job fails, the system must roll back any partial changes to the previous configuration. Rollback includes clearing the data plane configuration and redeploying the previous version. This will disrupt traffic until the rollback completes.

After you complete the changes you want to make, use the following procedure to deploy them to the device.

Caution The Firewall Threat Defense device drops traffic when the inspection engines are busy because of a software resource issue, or down because a configuration requires the engines to restart during configuration deployment. For detailed information on changes that require a restart, see Configuration Changes that Restart Inspection Engines, on page 28.

Procedure

Step 1 Click the **Deploy Changes** icon in the upper right of the web page.

The icon is highlighted with a dot when there are undeployed changes.



The Pending Changes window shows a comparison of the deployed version of the configuration with the pending changes. These changes are color-coded to indicate removed, added, or edited elements. See the legend in the window for an explanation of the colors.

If the deployment requires that inspection engines be restarted, the page includes a message that provides detail on what changed that requires a restart. If momentary traffic loss at this time would be unacceptable, close the dialog box and wait until a better time to deploy changes.

If the icon is not highlighted, you can still click it to see the date and time of the last successful deployment job. There is also a link to show you the deployment history, which takes you to the audit page filtered to show deployment jobs only.



Step 2 If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately.

The window will show that the deployment is in progress. You can close the window, or wait for deployment to complete. If you close the window while deployment is in progress, the job does not stop. You can see results in the task list or audit log. If you leave the window open, click the **Deployment History** link to view the results.

Optionally, you can do the following:

- **Name the Job**—To name the deployment job, click the drop-down arrow on the **Deploy Now** button and select **Name the Deployment Job**. Enter a name, then click **Deploy**. The name will appear in the audit and deployment history as part of the job, which might make it easier for you to find the job.

  For example, if you name a job "DMZ Interface Configuration," a successful deployment will be named "Deployment Completed: DMZ Interface Configuration." In addition, the name is used as the Event Name in Task Started and Task Completed events related to the deployment job.

- **Force a full deployment**—If you are having problems and would like to force the system to deploy the full configuration, rather than just the changes, you can click the drop-down arrow on the **Deploy Now** button and select **Apply Full Deployment**. A full deployment results in traffic interruption, so you must acknowledge that you want to perform this action before you can click **Deploy**.

- **Discard Changes**—To discard all pending changes, click **More Options** > **Discard All**. You are prompted for confirmation.
- **Copy Changes**—To copy the list of changes to the clipboard, click **More Options** > **Copy to Clipboard**. This option works only if there are fewer than 500 changes.
- **Download Changes**—To download the list of changes as a file, click **More Options** > **Download as Text**. You are prompted to save the file to your workstation. The file is in YAML format. You can view it in a text editor if you do not have an editor that specifically supports YAML format.

Configuration Changes that Restart Inspection Engines

Any of the following configurations or actions restart inspection engines when you deploy configuration changes.



Caution When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires inspection engines to restart, which interrupts traffic inspection and drops traffic.

Deployment

Some changes require that inspection engines be restarted, which will result in momentary traffic loss. Following are the changes that require inspection engine restart:

- SSL decryption policy is enabled or disabled.
- The MTU changed on one or more physical interfaces (but not subinterfaces).
- You add or remove a file policy on an access control rule.
- The VDB was updated.
- Creating or breaking the high availability configuration.

In addition, some packets might be dropped during deployment if the Snort process is busy, with the total CPU utilization exceeding 60%. You can check the current CPU utilization for Snort using the **show asp inspect-dp snort** command.

System Database Updates

If you download an update to the Rules database or VDB, you must deploy the update for it to become active. This deployment might restart inspection engines. When you manually download an update, or schedule an update, you can indicate whether the system should automatically deploy changes after the download is complete. If you do not have the system automatically deploy the update, the update is applied the next time you deploy changes, at which time inspection engines might restart.

System Updates

Installing a system update or patch that does not reboot the system and includes a binary change requires inspection engines to restart. Binary changes can include changes to inspection engines, a preprocessor, the

vulnerability database (VDB), or a shared object rule. Note also that a patch that does not include a binary change can sometimes require a Snort restart.

Configuration Changes that Force a Full Deployment

In most cases, the deployment includes just your changes. However, if necessary, the system will reapply the entire configuration, which might be disruptive to your network. Following are some changes that force a full deployment.

- The Security Intelligence or Identity policies are initially enabled.
- Both the Security Intelligence and Identity policies are disabled.
- Creating an EtherChannel when you reuse data.
- Deleting an EtherChannel.
- Modifying the member interface associations of an EtherChannel.
- Deleting any interface that is used in the configuration. For example, deleting a subinterface that is part of a security zone used by an access control rule.
- Changing a FlexConfig object that is part of the FlexConfig policy, or deleting an object from the policy, when that object does not include negate lines. Omitting negate lines forces the system to full deploy, because there is no specific way to remove the configuration produced by the FlexConfig object. You can avoid this problem by always including the appropriate negate lines in each FlexConfig object.

Viewing Interface and Management Status

The Device Summary includes a graphical view of your device and select settings for the management address. To open the Device Summary, click **Device**.

Elements on this graphic change color based on the status of the element. Mousing over elements sometimes provides additional information. Use this graphic to monitor the following items.



Note The interface portion of the graphic, including interface status information, is also available on the **Interfaces** page and the **Monitoring** > **System** dashboard.

Interface Status

Mouse over a port to see its IP addresses, and enabled and link statuses. The IP addresses can be statically assigned or obtained using DHCP. Mousing over a Bridge Virtual Interface (BVI) also shows the list of member interfaces.

Interface ports use the following color coding:

- Green—The interface is configured, enabled, and the link is up.
- Gray—The interface is not enabled.
- Orange/Red—The interface is configured and enabled, but the link is down. If the interface is wired, this is an error condition that needs correction. If the interface is not wired, this is the expected status.

Inside, Outside Network Connections

The graphic indicates which port is connected to the outside (or upstream) and inside networks, under the following conditions.

- Inside Network—The port for the inside network is shown for the interface named “inside” only. If there are additional inside networks, they are not shown. If you do not name any interface “inside,” no port is marked as the inside port.
- Outside Network—The port for the outside network is shown for the interface named “outside” only. As with the inside network, this name is required, or no port is marked as the outside port.

Management Setting Status

The graphic shows whether the gateway, DNS servers, NTP servers, and Smart Licensing are configured for the management address, and whether those settings are functioning correctly.

Green indicates that the feature is configured and functioning correctly, gray indicates that it is not configured or not functioning correctly. For example, the DNS box is gray if the servers cannot be reached. Mouse over the elements to see more information.

If you find problems, correct them as follows:

- Management port and gateway—Select **System Settings** > **Management Interface**.
- DNS servers—Select **System Settings** > **DNS Server**.
- NTP servers—Select **System Settings** > **NTP**. Also see Troubleshooting NTP.
- Smart License—Click the **View Configuration** link in the Smart License group.

Viewing System Task Status

System tasks include actions that occur without your direct involvement, such as retrieving and applying various database updates. You can view a list of these tasks and their status to verify that these system tasks are completing successfully.

The task list shows consolidated status for system tasks and deployment jobs. The audit log contains more detailed information, and is available under **Device** > **Device Administration** > **Audit Log**. For example, the audit log shows separate events for task start and task end, whereas the task list merges those events into a single entry. In addition, the audit log entry for a deployment includes detailed information about the deployed changes.

Procedure

Step 1 Click the **Task List** button in the main menu.



The task list opens, displaying the status and details of system tasks.

Step 2 Evaluate the task status.

If you find a persistent problem, you might need to fix the device configuration. For example, a persistent failure to obtain database updates could indicate that there is no path to the Internet for the device's management IP address. You might need to contact the Cisco Technical Assistance Center (TAC) for some issues as indicted in the task descriptions.

You can do the following with the task list:

- Click the **Success** or **Failures** buttons to filter the list based on these statuses.
- Click the delete icon ( ) for a task to remove it from the list.
- Click **Remove All Completed Tasks** to empty the list of all tasks that are not in progress.

Using the CLI Console to Monitor and Test the Configuration

Firewall Threat Defense devices include a command line interface (CLI) that you can use for monitoring and troubleshooting. Although you can open an SSH session to get access to all of the system commands, you can also open a CLI Console in the Firewall Device Manager to use read-only commands, such as the various **show** commands and **ping**, **traceroute**, and **packet-tracer**. If you have Administrator privileges, you can also enter the **failover**, **reboot**, and **shutdown** commands.

You can keep the CLI Console open as you move from page to page, configure, and deploy features. For example, after deploying a new static route, you could use **ping** in the CLI Console to verify that the target network is reachable.

The CLI Console uses the base Firewall Threat Defense CLI. You cannot enter the diagnostic CLI, expert mode, or FXOS CLI (on models that use FXOS) using the CLI Console. Use SSH if you need to enter those other CLI modes.

For detailed information on commands, see Cisco Firepower Threat Defense Command Reference, https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

Notes:

- Although **ping** is supported in CLI Console, the **ping system** command is not supported.
- The system can process at most 2 concurrent commands. Thus, if another user is issuing commands (for example, using the REST API), you might need to wait for other commands to complete before entering a command. If this is a persistent problem, use an SSH session instead of the CLI Console.
- Commands return information based on the deployed configuration. If you make a configuration change in the Firewall Device Manager, but do not deploy it, you will not see the results of your change in the command output. For example, if you create a new static route but do not deploy it, that route will not appear in **show route** output.

Procedure

Step 1 Click the **CLI Console** button in the upper right of the web page.



Step 2 Type the commands at the prompt and press **Enter**.

Some commands take longer to produce output than others, please be patient. If you get a message that the command execution timed out, please try again. You will also get a time out error if you enter a command that requires interactive responses, such as **show perfstats**. If the problem persists, you might need to use an SSH client instead of the CLI Console.

Following are some tips on how to use the window.

- Press the **Tab** key to automatically complete a command after partially typing it. Also, Tab will list out the parameters available at that point in the command. Tab works down to three levels of keyword. After three levels, you need to use the command reference for more information.
- You can stop command execution by pressing Ctrl+C.
- To move the window, click and hold anywhere in the header, then drag the window to the desired location.
- Click the **Expand** () or **Collapse** () button to make the window bigger or smaller.
- Click the **Undock Into Separate Window** () button to detach the window from the web page into its own browser window. To dock it again, click the **Dock to Main Window** () button.
- Click and drag to highlight text, then press Ctrl+C to copy output to the clipboard.
- Click the **Clear CLI** () button to erase all output.
- Click the **Copy Last Output** () button to copy the output from the last command you entered to the clipboard.

Step 3 When you are finished, simply close the console window. Do not use the **exit** command.

Although the credentials you use to log into the Firewall Device Manager validate your access to the CLI, you are never actually logged into the CLI when using the console.

Using Firewall Device Manager and the REST API Together

When you set up the device in local management mode, you can configure the device using the Firewall Device Manager and the Firewall Threat Defense REST API. In fact, the Firewall Device Manager uses the REST API to configure the device.

However, please understand that the REST API can provide additional features than the ones available through the Firewall Device Manager. Thus, for any given feature, you might be able to configure settings using the REST API that cannot appear when you view the configuration through the Firewall Device Manager.

If you do configure a feature setting that is available in the REST API but not in the Firewall Device Manager, and then make a change to the overall feature (such as remote access VPN) using the Firewall Device Manager, that setting might be undone. Whether an API-only setting is preserved can vary, and in many cases, API changes to settings not available in the Firewall Device Manager are preserved through the Firewall Device Manager edits. For any given feature, you should verify whether your changes are preserved.

In general, you should avoid using both the Firewall Device Manager and the REST API simultaneously for any given feature. Instead, choose one method or the other, feature by feature, for configuring the device.

You can view, and try out, the API methods using API Explorer. Click the more options button (⋮) and choose **API Explorer**.

Communication Port and Internet Access Requirements

The following topics describe the ports that need to be open on the device, and the internet sites to which access is required, to operate all features available on the device. If you are operating in a limited or air-gapped manner, some or all of these ports and internet sites can be blocked to meet your requirements. Otherwise, ensure these ports and sites are open and accessible.

Communication Ports Used by the Device

The following tables list the ports that need to be open for various services. Use access control rules to ensure access to these ports are open on the interfaces that face the services, or that face users who should be able to gain access to the device using the associated protocol. If you do not use a feature, you can leave those ports closed.

Table 1: Inbound Ports

Inbound Port	Protocol/Feature	Details
TCP/22	SSH	Secure remote connections to the appliance command line interface. **Note** If you use the **copy** command, or another command that performs external communication, you need to open that outbound port. For example, TCP/20, 21 if you intend to use FTP.
UDP/161	SNMP	Allow access to MIBs via SNMP polling.
TCP/443	HTTPS	Used for the following services: • Management connections to Firewall Device Manager. • Firewall Threat Defense REST API. • Remote access VPN SSL connections. If you configure a custom port for RA VPN, open that port.
TCP/885	Captive portal	Communicate with a captive portal identity source. This is the default port. If you configure a different port, open your custom port. For more information, see Configure Identity Policy Settings.
TCP/8989	Cisco Support Diagnostics	Accepts authorized requests. Also initiates connections on this port.

Table 2: Outbound Ports

Outbound Port	Protocol/Feature	Details
UDP/53 (If used.) TCP/53	DNS	DNS. Normally, UDP/53 is used for DNS. But if you use DNS over TCP, open TCP/53 as well.
UDP/67 UDP/68	DHCP	DHCP.
UDP/123	NTP	Synchronize time.
UDP/162	SNMP	Send SNMP alerts to a remote trap server.
TCP/389 TCP/636	LDAP, LDAPS	Communicate with an LDAP server for external authentication. If you configure custom ports, open those ports. See Configuring AD Identity Realms.
TCP/443	HTTPS	Send and receive data from the internet, such as downloading database updates..
UDP/514	Syslog	Send system log messages to a remote syslog server.
UDP/1812 UDP/1813	RADIUS	Communicate with a RADIUS server for external authentication and accounting. If you configure custom ports, open those ports. See Configure RADIUS Servers.
UDP/8514	Secure Network Analytics Manager	Send syslog messages to the cloud.
TCP/8989	Cisco Support Diagnostics	Transmits usage information and statistics. Also accepts connections on this port.

Internet Resources Accessed by the Device

The following features must have access to the associated internet resources to operate correctly. The device uses ports TCP/80 and TCP/443 as needed.

Table 3: Internet Resources Accessed by the Device

Feature	Reason	High Availability	Resource
CA certificate bundles	Queries for new CA certificates at a daily system-defined time. The local CA bundle contains certificates to access several Cisco services. This feature is configured in the CLI using the **configure cert-update auto-update** command. Available in versions 7.0(5), 7.1(0.3), 7.2(4), 7.3 and higher.	Each peer downloads its own certificates.	cisco.com/security/pki
Malware Defense 1	Secure Malware Analytics Cloud lookups.	Both peers perform lookups.	Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations
	Download signature updates for file preclassification and local malware analysis.	Active peer downloads, syncs to standby.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Submit files for dynamic analysis. Query for dynamic analysis results.	Both peers submit or query for dynamic analysis reports.	fmc.api.threatgrid.com fmc.api.threatgrid.eu fmc.api.threatgrid.ca fmc.api.threatgrid.com.au fmc.api.threatgrid.in
Security intelligence	Download security intelligence feeds.	Active peer downloads, syncs to standby.	intelligence.sourcefire.com

Feature	Reason	High Availability	Resource
URL filtering	Download URL category and reputation data. Manually query (look up) URL category and reputation data. Query for uncategorized URLs.	Active peer downloads, syncs to standby.	URLs: • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com IPv4 blocks: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 blocks: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Cisco Smart Software Manager	Communicate with the Smart Software Manager.	Active peer communicates.	www.cisco.com smartreceiver.cisco.com
Cisco Success Network	Transmit usage information and statistics.	Active peer communicates.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	Accepts authorized requests and transmits usage information and statistics.	Active peer communicates.	api-sse.cisco.com:8989
General cloud services	—	—	api-sse.cisco.com
Cisco XDR integration	Configure devices to send events to the Security Cloud Control.	Active peer communicates.	Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide
Time synchronization	Synchronize time in your deployment. Not supported with a proxy server.	Both peers communicate with the NTP server.	User configured. Default servers: • 0.sourcefire.pool.ntp.org • 1.sourcefire.pool.ntp.org • 2.sourcefire.pool.ntp.org

Feature	Reason	High Availability	Resource
Intrusion rules	Download intrusion rules (SRU/LSP).	Active peer downloads, syncs to standby.	talosintelligence.com
Vulnerability database	Download VDB updates.	Active peer downloads, syncs to standby.	support.sourcefire.com
Geolocation database	Download GeoDB updates.	Active peer downloads, syncs to standby.	support.sourcefire.com