Cisco Secure Firewall Threat Defense Hardening Guide, Version 10.0

Introduction 3
Security Certifications Compliance 3
Monitor Cisco Security Advisories and Responses 4
Keep the System Up to Date 4
Enable CC or UCAPL Mode 6
Gain Traffic Visibility with NetFlow 6
Secure the Local Network Infrastructure 6
Harden Network Protocol Settings 8
Secure VPN Services 9
Harden Firewall Threat Defense User Access 11
Enforce Message-Authenticator Attribute in All RADIUS Responses 13
Protect Backups 13
Revert a Firewall Threat Defense Device Upgrade 14
Secure Data Export 14
Secure Syslog 15
Customize the Login Banner 15
Secure Connections to Servers Supporting Network User Authoritative Logins, Awareness, and Control 16
Secure Certificate Enrollment 17
Harden Object Group Search Settings 18

Harden Supporting Components 18

Disable Front Panel USB-A Port on Firepower 1000 and Secure Firewall 3100/4200 19

Secure HTTP Proxy Settings 19

Secure Loopback Interface 19

Secure Onboarding of Devices Using Device Registration Keys or Serial Numbers 19

Revised: December 1, 2025

Introduction

Secure Firewall Threat Defense protects your network assets and traffic from cyber threats, but you should also configure your deployment so that it is *hardened*—further reducing its vulnerability to cyber attack. This guide addresses hardening Firewall Threat Defense. For hardening information on other components of your deployment, see:

- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

This document refers to three different means of configuring Firewall Threat Defense, but is not intended as a detailed manual.

- You can configure some Firewall Threat Defense configuration settings using the Firewall Management Center web interface. For more information, see *Cisco Secure Firewall Management Center Device Configuration Guide*.
- You can configure some Firewall Threat Defense configuration settings using the Firewall Threat Defense Command Line Interface (CLI). For more information about all CLI commands referenced in this document, see *Cisco Firepower Threat Defense Command Reference*.
- You can configure Firewall Threat Defense configuration settings using the Secure Firewall Device Manager. For more information, see *Cisco Secure Firewall Device Manager Configuration Guide*.

Not all configurations discussed in this document are available in all Firewall Threat Defense versions. For detailed configuration information, see https://cisco.com/go/ftd-docs.

Security Certifications Compliance

Your organization might be required to use only equipment and software that comply with security standards established by the U.S. Department of Defense or other governmental certification organizations. Once certified by an appropriate certifying authority, and when configured in accordance with certification-specific guidance documents, Firewall Threat Defense is designed to comply with the following certification standards:

- Common Criteria (CC): a global standard established by the international Common Criteria Recognition Arrangement, defining requirements for security products.
- Department of Defense Information Network Approved Products List (DoDIN APL): a list of products meeting security requirements established by the U.S. Defense Information Systems Agency (DISA).

Note The U.S. Government has changed the name of the Unified Capabilities Approved Products List (UCAPL) to the DODIN APL. References to UCAPL in Firewall Management Center documentation and the web interface can be interpreted as references to DoDIN APL.

- Federal Information Processing Standards (FIPS) 140: a requirements specification for encryption modules.

Certification guidance documents are available separately once product certifications have completed; publication of this hardening guide does not guarantee completion of any of these product certifications.

The configuration settings described in this document do not guarantee strict compliance with all current requirements of the certifying entity. For more information on hardening procedures required, refer to the guidelines for this product provided by the certifying entity.

This document provides guidance for increasing the security of your Firewall Threat Defense, but some Firewall Threat Defense features do not support certification compliance even using the configuration settings described herein. For more information see

“Security Certifications Compliance Recommendations” in the *Cisco Secure Firewall Management Center Administration Guide*. We have endeavored to ensure that this hardening guide and the *Cisco Secure Firewall Management Center Administration Guide* do not conflict with certification-specific guidance. Should you encounter contradictions between Cisco documentation and certification guidance, use the certification guidance or consult with the system owner.

Monitor Cisco Security Advisories and Responses

The Cisco Product Security Incident Response Team (PSIRT) posts PSIRT Advisories for security-related issues in Cisco products. For less severe issues, Cisco also posts Cisco Security Responses. Security advisories and responses are available at Cisco Security Advisories and Alerts and Cisco Security Vulnerability Policy.

To maintain a secure network, stay aware of Cisco security advisories and responses. These advisories provide the information you need to evaluate the threats that vulnerabilities pose to your network. Refer to Risk Triage for Security Vulnerability Announcements for assistance with this evaluation process.

Keep the System Up to Date

Cisco periodically releases software updates to address issues and make improvements. Keeping your system software up to date is essential to maintaining a hardened system. Ensure your system software is properly updated. For more information see the “Updates” chapter of the *Cisco Secure Firewall Management Center Administration Guide*, and the *Secure Firewall Management Center Upgrade Guide*.

Cisco also periodically issues updates for the databases used to protect your network and assets. To provide optimum protection, keep the geolocation, intrusion rule, and vulnerability databases on the managing Firewall Management Center up to date. Before you update any component of your deployment you *must* read the *Cisco Secure Firewall Threat Defense Release Notes* that accompany the update. These provide critical and release-specific information, including compatibility, prerequisites, new capabilities, behavior changes, and warnings. Some updates may be large and take some time to complete; you should perform these updates during periods of low network use to reduce the impact on system performance.

Geolocation Database

The geolocation database (GeoDB) contains geographical data, such as country and city coordinates. When management center detects GeoDB information that matches a detected IP address, you can view the geolocation information associated with that IP address.

To update the GeoDB from the management center web interface, use **System** (⚙) > **Content Updates** > **Geolocation Updates**. You can:

- Update the GeoDB on a management center with no internet access.
- Update the GeoDB on a management center with internet access.
- Schedule recurring automatic updates of the GeoDB on a management center with internet access.

For more information, see "Update the Geolocation Database (GeoDB)" in the *Cisco Secure Firewall Management Center Administration Guide*.

Intrusion Rules

As new vulnerabilities become known, the Cisco Talos Security Intelligence and Research Group (Talos) releases intrusion rule updates (also known as Snort Rules Updates, or SRUs) that you can import onto your Firewall Management Center, and then implement by deploying the changed configuration to your managed devices. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules.

The management center web interface provides three approaches to updating the intrusion rules, all under **System** (⚙) > **Content Updates** > **Rule Updates**:

- Update intrusion rules on a Firewall Management Center with no internet access.
- Update intrusion rules on a Firewall Management Center with internet access.
- Schedule recurring automatic updates of intrusion rules on a Firewall Management Center with internet access.

For more information, see "Update Intrusion Rules" in the *Cisco Secure Firewall Management Center Administration Guide*.

You can also import local intrusion rules using **System** (⚙) > **Content Updates** > **Rule Updates**. You can create local intrusion rules using the instructions in the Snort users manual (available at http://www.snort.org). Before importing them to your Firewall Management Center, see "Best Practices for Importing Local Intrusion Rules" in the *Cisco Secure Firewall Management Center Administration Guide* and make certain your process for importing local intrusion rules complies with your security policies.

Vulnerabilities Database

Vulnerabilities Database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.

The Firewall Management Center web interface offers two approaches to updating the VDB:

- Manually update the VDB (**System** (⚙) > **Content Updates** > **VDB Updates**).
- Schedule VDB updates (**System** (⚙) > **Tools** > **Scheduling**).

For more information, see "Update the Vulnerability Database (VDB)" in the *Cisco Secure Firewall Management Center Administration Guide*.

Security Intelligence Lists and Feeds

Security Intelligence lists and feeds are collections of IP addresses, domain names, and URLs that you can use to quickly filter traffic that matches an entry on a list or feed.

There are system-provided feeds, and predefined lists. You can also use custom feeds and lists. To view these lists and feeds, choose **Objects** > **Object Management** > **Security Intelligence**. As part of system-provided feeds, Cisco provides the following feeds as Security Intelligence objects:

- Security Intelligence feeds are updated regularly with the latest threat intelligence from Talos:
    - Cisco-DNS-and-URL-Intelligence-Feed (under DNS Lists and Feeds)
    - Cisco-Intelligence-Feed (for IP addresses, under Network Lists and Feeds)

  You cannot delete the system-provided feeds, but you can change the frequency of (or disable) their updates. The Firewall Management Center can now update Cisco-Intelligence-Feed data for every 5 or 15 minutes.

- Cisco-TID-Feed (under Network Lists and Feeds)

  You must enable and configure Threat Intelligence Director to use this feed, which is a collection of TID observables data.

For more information, see "Custom Security Intelligence Lists and Feeds" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Enable CC or UCAPL Mode

To apply multiple hardening configuration changes with a single setting, choose CC or UCAPL mode for the Firewall Threat Defense. Apply this setting thorugh the Firewall Management Center web interface in the Firewall Threat Defense platform settings policy, found under **Devices** > **Platform Settings**. The change does not take effect on the Firewall Threat Defense until you deploy the new configuration; see “Enable Security Certifications Compliance” in the *Cisco Secure Firewall Management Center Administration Guide* for full details.

Choosing one of these configuration options puts into effect the changes listed under “Security Certifications Compliance Characteristics” in the *Cisco Secure Firewall Management Center Administration Guide*. Be aware that all appliances in your deployment should operate in the same security certifications compliance mode.

Caution After you enable this setting, you cannot disable it. Consult “Security Certifications Compliance” in the *Cisco Secure Firewall Management Center Administration Guide* for full information before enabling CC or UCAPL mode. If you need to reverse this setting, contact Cisco TAC for assistance.

Note Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. Additional settings recommended to harden your deployment above and beyond those provided by CC or UCAPL modes are described in this document. For full information on hardening procedures required for complete compliance, refer to the guidelines for this product provided by the certifying entity.

Gain Traffic Visibility with NetFlow

Cisco’s IOS NetFlow enables you to monitor traffic flows in your network in real time. Firewall Threat Defense can coordinate with some NetFlow features, such as viewing and resetting runtime counters. See the **show flow-export counters** and **clear flow-export counters** CLI commands.

Through the Firewall Management Center web interface you can disable Firewall Threat Defense syslog messages that are redundant with those captured by NetFlow. To do this, create an Firewall Threat Defense platform settings policy under **Devices** > **Platform Settings**, and choose **Syslog** from the menu. On the **Syslog Settings** tab check the **NetFlow Equivalent Syslogs** check box (Use the **show logging flow-export-syslogs** CLI command to determine which syslog messages are redundant.)

You can take advantage of these abilities if you configure network devices with NetFlow. Regardless of whether flow information is exported to a remote collector, you can use NetFlow reactively if needed. See “Netflow Data” in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.6* for more information.

Secure the Local Network Infrastructure

Your Secure Firewall deployment may interact with other network resources for a number of purposes. Hardening these other services can protect your Secure Firewall system as well as all your network assets. To identify everything that needs to be addressed, try diagramming the network and its components, assets, firewall configuration, port configurations, data flows, and bridging points.

Establish and adhere to an operational security process for your network that takes security issues into account.

Secure the Network Time Protocol Server

Synchronizing the system time on the Firewall Management Center and its managed devices is essential. We strongly recommend using a secure and trusted Network Time Protocol (NTP) server to synchronize system time on the Firewall Management Center and the devices it manages.

Configure NTP time synchronization for Firewall Threat Defense devices from the Firewall Management Center web interface by creating a Firewall Threat Defense platform settings policy under **Devices > Platform Settings**, and choosing the **Time Synchronization** tab within the policy page. For more information, see "Configure Time Synchronization" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

We recommend that you secure the communication with the NTP servers using MD5, SHA-1, or AES-128 CMAC symmetric key authentication.

Caution Unintended consequences may occur when time is not synchronized between the Firewall Management Center and managed devices. To ensure proper synchronization, configure the Firewall Management Center and all the devices it manages to use the same NTP server.

Secure the Domain Name System (DNS)

Computers communicating with each other in a networked environment depend on the DNS protocol to provide mapping between IP addresses and host names. Configuring a Firewall Threat Defense device to connect with a local DNS to support communication over its management interface is a part of the initial configuration process, described in the Quick Start Guide for your model.

Certain Firewall Threat Defense functions that use the data or diagnostic interfaces also use DNS—examples include NTP, access control policies, VPN services provided by the Firewall Threat Defense, ping, or traceroute. To configure DNS for the data or diagnostic interfaces, create a Firewall Threat Defense platform settings policy under **Devices > Platform Settings**, and choose **DNS** from the left pane. For more information, see "Configure DNS" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

DNS can be susceptible to specific types of attacks tailored to take advantage of weak points in a DNS server that is not configured with security in mind. Ensure your local DNS server is configured with industry-recommended best practices for security; Cisco offers guidelines in this document: DNS Best Practices, Network Protections, and Attack Identification.

Secure SNMP Polling and Traps

You can configure a Firewall Threat Defense to support SNMP polling and traps as described in "Configure SNMP" in the *Cisco Secure Firewall Management Center Device Configuration Guide*. If you choose to use SNMP polling, you should be aware that the SNMP Management Information Base (MIB) contains system details that could be used to attack your deployment, such as contact, administrative, location, and service information; IP addressing and routing information; and transmission protocol usage statistics. Choose configuration options to protect your system from SNMP-based threats.

To configure SNMP features for a Firewall Threat Defense, create a Firewall Threat Defense platform settings policy under **Devices > Platform Settings**, and choose **SNMP** from the left pane. For more information, see "Configure SNMP" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Use the following options to harden SNMP access to the Firewall Threat Defense device:

- When creating SNMP users, choose SNMPv3, which supports only encryption with AES128 and read-only users. For more information, see "Add SNMP Hosts" in the *Cisco Secure Firewall Management Center Device Configuration Guide, Version*.
- When creating SNMP users, choose SNMPv3, which supports:
    - Authentication algorithms such as SHA, SHA224, SHA256, and SHA384.

    - Encryption with AES256, AES192, and AES128.
    - Read-only users.

- Create SNMPv3 users with the following options:
    - Choose **Priv** for the **Security Level**.
    - Choose **Encrypted** for the **Encryption Password Type**.

  See “Add SNMPv3 Users” in the *Cisco Secure Firewall Management Center Device Configuration Guide* for full instructions.

Important Although you can establish a secure connection to an SNMP server from Firewall Management Center, the authentication module is not FIPS compliant.

Secure Network Address Translation (NAT)

Typically networked computers use NAT for reassigning source or destination IP addresses in network traffic. To protect your deployment as well as your overall network infrastructure from NAT-based exploits, configure the NAT service in your network in adherence with industry best practices as well as recommendations from your NAT provider.

For information about configuring your deployment to operate in a NAT environment, see “NAT Environments” in the *Cisco Secure Firewall Management Center Administration Guide*. Use this information at two stages when establishing your deployment:

- When performing the initial setup for your Firewall Management Center as described in the Cisco Firepower Management Center Getting Started Guide for your hardware model.
- When registering a managed device to the Firewall Management Center as described in "Add a Device to the Firewall Management Center Using a Device Template" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Secure the Appliances in Your Deployment

Your deployment includes the Firewall Threat Defense and security devices managed by the Firewall Management Center, each providing different means of access. Managed devices exchange information with the Firewall Management Center and their security is important to the security of your overall deployment. Analyze the appliances in your deployment and apply hardening configurations as appropriate, such as securing user access and closing unneeded communication ports.

Harden Network Protocol Settings

The Firewall Threat Defense device can interact with other network devices using a number of protocols; choose configuration settings for network communications to protect the Firewall Threat Defense device as well as the data it sends and receives.

- By default the Firewall Threat Defense device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to allow fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, fragmented packets are often used in Denial of Service (DoS) attacks, so we recommend that you do not allow fragments.
    - To configure the fragments settings for a Firewall Threat Defense device, create a Firewall Threat Defense platform settings policy under **Devices** > **Platform Settings**, and choose **Fragment Settings** from the left pane.

    - To disallow fragments in the network traffic handled by an Firewall Threat Defense device, set the **Chain (Packet)** option to 1.

  For complete instructions, see “Fragment Settings” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

- For Firewall Threat Defense devices managed by a Firewall Management Center, HTTPS connections with the Firewall Threat Defense can be used only to download packet capture files for troubleshooting.

  Configure Firewall Threat Defense to allow HTTPS access only for IP addresses that should be allowed to download packet captures. In the Firewall Management Center web interface create a Firewall Threat Defense platform settings policy under **Devices** > **Platform Settings**, and choose **HTTP Access** from the table of contents. See “HTTP Access” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

- By default, the Firewall Threat Defense can receive ICMP packets on any interface using either IPv4 or IPv6 with two exceptions:
    - The Firewall Threat Defense does not respond to ICMP echo requests directed to a broadcast address.
    - The Firewall Threat Defense responds only to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an Firewall Threat Defense interface to a far interface.

  To protect a Firewall Threat Defense device from ICMP-based attack, you can use ICMP rules to limit ICMP access to selected hosts, networks, or ICMP types. In the Firewall Management Center web interface, create an Firewall Threat Defense platform settings policy under **Devices** > **Platform Settings**, and choose **ICMP Access** from the table of contents. For details, see “ICMP Access” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

- The Firewall Threat Defense can be configured to provide DHCP and DDNS services (see “About DHCP and DDNS Services” in the *Cisco Secure Firewall Management Center Device Configuration Guide*). By their nature these protocols are vulnerable to attack. If you choose to configure your Firewall Threat Defense for DHCP or DDNS it is important to apply industry best practices for security, provide physical protection for your network assets, and harden user access to the Firewall Threat Defense device.

- You can enable LLDP on Firepower 1000 Series, 2100 Series, and Secure Firewall 3100. This feature enables the Firewall Threat Defense to exchange packets with its LLDP-enabled peers. By default, LLDP transmit and receive is disabled on a port. The information sent through LLDP is vulnerable to attack. If you choose to configure your Firewall Threat Defense device for LLDP, it is important to apply industry best practices for security, and harden user access to the Firewall Threat Defense. We recommend that you only enable the firewall to receive LLDP packets from its peers for enhanced security. This action ensures the firewall gets information about peer devices without revealing its identify to other peer devices. For more information, see "Enable the Physical Interface and Configure Ethernet Settings" in *Cisco Secure Firewall Management Center Device Configuration Guide*

Secure VPN Services

You can configure the Firewall Threat Defense to provide two kinds of Virtual Private Network (VPN) services: Remote Access VPN (RA VPN) and Site-to-site VPN. Depending on your device license, you can apply strong encryption to site-to-site and RA VPN transmissions. VPN with strong encryption requires special licensing; see "Licensing for Export-Controlled Functionality" in the *Cisco Secure Firewall Management Center Administration Guide*.

Remote Access Virtual Private Network

To secure message transmissions to and from remote clients over RA VPN connections, the Firewall Threat Defense can use Transport Layer Security (TLS) or IPsec IKEv2.

Before you deploy an RA VPN configuration to the Firewall Threat Defense, the Firewall Management Center ensures that the license prerequirements are met. For more information, see *Cisco Secure Firewall Management Center Device Configuration Guide*.

RA VPN on Firewall Threat Defense supports AD, LDAP, SAML identity providers, and RADIUS AAA servers for authentication. When a user configures AAA settings for RA VPN, we recommend that you use one of the following authentication methods for enhanced security:

- Client Certificate and SAML: Each user is authenticated with both a client certificate and a SAML server.
- Client Certificate and AAA: Each user is authenticated with both a client certificate and a AAA server.

RA VPN supports local authentication and multi-certificate authentication.

- Local Authentication: You can use this authentication method as the primary or secondary authentication method, or as a fallback in case the configured remote server can't be reached. We recommend that you use a strong password for the local authentication. For more information, see "Associate Local Realm with Remote Access VPN Policy" in *Cisco Secure Firewall Management Center Device Configuration Guide*.
- Multi-certificate Authentication: You can use this authentication method to validate the machine or device certificate using single certificate authentication. This authentication ensures that the device is a corporate-issued device and authenticates the user identity certificate to allow VPN access. We recommend that use this authentication method. For more information, see "Configuring Multiple Certificate Authentication" in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Site-to-Site Virtual Private Network

To secure message transmissions to and from remote networks over site-to-site VPN connections, the Firewall Threat Defense can use IPSEC IKEv1 or IPSEC IKEv2.

There are two types of site-to-site VPNs: Policy-based (Crypto Map) and Route-based (Virtual Tunnel Interface (VTI)). We recommend that you use route-based VTI VPN for enhanced security. For more information, see "Site-to-Site VPNs" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

When you configure the Firewall Threat Defense VPN IKE and IPsec options (**Devices** > **VPN** > **Site To Site** > **Add**, and click **IKE** or **IPsec** tabs), we recommend that you:

- Choose IKEv2.
- Use a strong key for the pre-shared manual key.
- Use the default IKEv2 policy. For example, AES-GCM-NULL-SHA-LATEST.
- Check the **Enable Security Association (SA) Strength Enforcement** check box.

  This option ensures that the encryption algorithm used by the child IPsec SA isn't stronger than the parent IKE SA.
- Check the **Enable Perfect Forward Secrecy** check box.

  This option generates and uses a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption. If you select this option, select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key from the **Modulus Group** drop-down list.

For more information about the above Firewall Threat Defense VPN IKE options, see *Cisco Secure Firewall Management Center Device Configuration Guide*.

To configure these services, see "VPN Overview" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

The Firewall Management Center supports a wide range of encryption and hash algorithms, and Diffie-Hellman groups from which to choose. Choosing strong encryption can worsen system performance, so you must find the balance between security and performance that provides sufficient protection without compromising efficiency. For more information, see “How Secure Should a VPN Connection Be?” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Harden Firewall Threat Defense User Access

The Firewall Threat Defense supports two types of users:

- Internal users—The device checks a local database for user authentication.
- External users—If the user is not present in the local database, the system queries an external LDAP or RADIUS authentication server.

You might consider establishing user access through an external authentication mechanism such as LDAP or RADIUS, to integrate user management with existing infrastructure in your network environment, or leverage capabilities such as two-factor authentication. Establishing external authentication requires creating an external authentication object within the Firewall Management Center web interface; external authentication objects can be shared to authenticate external users for the Firewall Management Center as well as the Firewall Threat Defense.

Be aware that using external authentication requires that you configure a DNS for your deployment. Be sure to follow hardening recommendations for your DNS. See Secure the Domain Name System (DNS), on page 7

Firewall Threat Defenses managed by Firewall Management Center provide a single means of user access: a command line interface which can be accessed using an SSH, serial, or keyboard and monitor connection for physical devices. With certain configuration settings in place these users can also access the Linux shell.

Restrict Config Privileges

By default, Firewall Threat Defense provide a single **admin** user with full administrator rights to all Firewall Threat Defense CLI commands. This user can create additional accounts and grant them one of two levels of access privilege with the **configure user access** CLI command:

- Basic: User can use Firewall Threat Defense CLI commands that do not affect system configuration
- Config: User can use all Firewall Threat Defense CLI commands, including those that provides significant system configuration abilities.

Consider carefully when assigning Config access rights to an account, and when choosing to which users you grant access to an account with Config access rights.

Restrict Linux Shell Access

The Firewall Threat Defense managed by the Firewall Management Center supports only CLI access through its management interface, using an SSH, serial, or keyboard and monitor connection. This is available to the **admin** account, internal users, and can be made available to external users.

Users with config level access can use the CLI **expert** command to access the Linux shell.

Caution On all devices, accounts with CLI Config level access or Linux shell access can obtain sudoers privileges in the Linux shell, which can present a security risk. To increase system security, we recommend:

- When giving users access to externally-authenticated accounts on Firewall Threat Defense keep in mind that all externally authenticated accounts on Firewall Threat Defense have CLI Config level access.
- Do not add new accounts directly in the Linux shell; on Firewall Threat Defense create new accounts using only the **configure user add** CLI command.
- Use the Firewall Threat Defense CLI command **configure ssh-access-list** to limit the IP addresses from which an Firewall Threat Defense will accept SSH connections on its management interface.

Administrators can also configure the Firewall Threat Defense to block all access to the Linux shell using the **system lockdown-sensor** CLI command. Once the system lockdown has completed, any user who logs in to the Firewall Threat Defense will have access only to the Firewall Threat Defense CLI commands. This can be a significant hardening action, but use it with careful consideration, because it cannot be reversed without a hotfix from Cisco TAC.

Harden Internal User Accounts

When configuring individual internal users, users with Config access can use the **configure user** Firewall Threat Defense CLI commands to harden the system against attacks through web interface login mechanisms. The following settings are available:

- Restrict the maximum number of failed logins before a user is locked out.
- Enforce a minimum password length (**configure user minpasswdlen**).
- Set the number of days passwords are valid (**configure user aging**).
- Require strong passwords (**configure user strengthcheck**).
- Assign user access privileges appropriate only to the type of access the user requires (**configure user access**).
- Force the user to reset the account password on the next login (**configure user forcereset**).

If your deployment uses multitenancy, consider the domain to which the Firewall Threat Defense belongs when granting users access to that device.

For more information, see “History for Domain Management” in the *Cisco Secure Firewall Management Center Administration Guide*.

Harden External User Accounts

If you choose to use an external server for Firewall Threat Defense user authentication, bear in mind that external users always have Config privileges; other user roles are not supported. Configure external authentication for Firewall Threat Defense users from the Firewall Management Center web interface by creating a Firewall Threat Defense platform settings policy under **Devices** > **Platform Settings** > Add/Edit Policy > **External Authentication**. Configuring external user accounts requires establishing a connection with an LDAP or RADIUS server though an external authentication object. For more information, see “Configure SSH and SSH Access List” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Important You can set up secure connections with LDAP or RADIUS servers from Firewall Management Center, but the authentication module is not FIPS compliant.

- Be aware that all Firewall Threat Defense external users have Config access, and unless you block access to the Linux shell with the **system lockdown-sensor** command, these users can gain access to the Linux shell. Linux shell users can gain root privileges, which presents a security risk.
- If you use LDAP for external authentication, under **Advanced Options**, configure TLS or SSL encryption.

Establish Session Timeouts

Limiting the duration of connections to a Firewall Management Center reduces the opportunity for unauthorized users to exploit unattended sessions.

To set session timeouts on the Firewall Management Center device, create the Firewall Management Center platform settings policy under **Device** > **Platform Settings** > Add/Edit Policy > **Timeouts**. See “Timeouts” in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more instructions.

Firewall Threat Defense REST API Considerations

The Firewall Threat Defense REST API provides a lightweight interface for third-party applications to view and manage appliance configuration using a REST client and standard HTTP methods. The API is described in the *Cisco Secure Firewall Threat Defense REST API Guide*.

Important Although you can establish secure connections between the Firewall Threat Defense and a REST API client using TLS, the authentication module is not FIPS compliant.

Enforce Message-Authenticator Attribute in All RADIUS Responses

You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Threat Defense VPN gateway securely verifies every response from the RADIUS server, whether for remote access VPN or access to the device itself. The RADIUS Server-Enabled Message Authenticator 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.

This parameter is available when you configure a RADIUS authentication object (choose **Administration** > **Users** > **External Authentication** > **Add External Authentication Object** > **RADIUS**).

Protect Backups

To protect system data and its availability, perform regular backups of your Firewall Threat Defense. The backup function appears under **System** > **Tools** > **Backup/Restore** in the Firewall Management Center web interface and is described in “Backup/Restore” in the *Cisco Secure Firewall Management Center Administration Guide*. To restore a saved Firewall Threat Defense configuration, use the Firewall Threat Defense CLI **restore** command.

The Firewall Management Center provides the ability to automatically store backups on a remote device. Using this feature is not recommended for a hardened system because the connection between the Firewall Management Center and the remote storage device cannot be secured.

Revert a Firewall Threat Defense Device Upgrade

If you learn that threat defense is vulnerable to attack within thirty days after an upgrade, you can revert if you saved a revert snapshot during upgrade (recommended). Reverting Firewall Threat Defense returns the software to its state just before the last major or maintenance upgrade. Reverting after patching necessarily removes patches as well.

For more information on reverting, including configurations that are and are not reverted, guidelines for reverting high availability and clustered devices, and any additional requirements, see the upgrade guide for the version currently running on the Firewall Management Center.

Secure Data Export

The Firewall Threat Defense CLI provides the ability to download certain files from the Firewall Threat Defense to a local computer. This capability is provided so you can collect information to provide to Cisco TAC when troubleshooting your system, and should not be used casually. Take precautions to protect any files you download from the Firewall Threat Defense; choose the most secure options available when downloading, secure the local computer where you store the data, and use the most secure protocols available when transmitting files to TAC. In particular, be aware of the possible risks when using the following commands:

- **show asp inspect-dp snort queue-exhaustion** [**snapshot** *snapshot_id*] [**export** *location*]

  The **export** option supports TFTP only.

- **file copy** *host_name user_id path filename_1* [*filename_2* ... *filename_n*]

  This command transfers files to remote host using unsecured FTP.

- **copy [/noverify] /noconfirm** {**/pcap capture:/**[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

  The following options for *src_url* and *dest_url* provide methods of securing the data copied:

  - Internal flash memory
  - System memory
  - Optional external flash drive
  - HTTPS secured with password
  - SCP secured with password, specifying target interface on SCP server
  - FTP secured with password
  - TFTP secured with password, specifying target interface on TFTP server

  We recommend against using the following *src_url* and *dest_url* options in a hardened system:

  - SMB UNIX server local file system
  - Cluster trace file system. (Systems with security certifications compliance enabled do not support clusters.)

- **cpu profile dump** *dest_url*

  The following options for *dest_url* provide methods of securing the data dump:

  - Internal flash memory
  - Optional external flash drive

  - HTTPS secured with password
  - SMB UNIX server local file system
  - SCP secured with password, specifying target interface on SCP server
  - FTP secured with password
  - TFTP secured with password, specifying target interface on TFTP server

  We recommend against using cluster file systems for *src_url* and *dest_url* options in a hardened system.

- **file secure-copy** *host_name user_id path filename_1* [*filename_2* ... *filename_n*]

  Copies file(s) to a remote host using SCP.

Secure Syslog

The Firewall Threat Defense can send syslog messages to an external syslog server; choose secure options when configuring syslog functionality:

1. Create a Firewall Threat Defense platform settings policy under **Devices** > **Platform Settings**, and choose **Syslog** from the left pane. When adding a syslog server under the **Syslog Servers** tab, choose the TCP protocol and check the **Enable secure syslog** check box. These options apply to syslog messages generated by the Firewall Threat Defense if you do not override them elsewhere in your device configuration.

   Note By default, when secure syslog is enabled, if a syslog server using TCP is down, the Firewall Threat Defense will not forward traffic. To override this behavior, check the **Allow user traffic to pass when TCP syslog server is down** check box.

With these two configuration settings in place the Firewall Threat Defense syslog behaves as follows:

- The syslog settings in the platform settings policy apply to syslog messages related to device and system health, and network configuration.
- The syslog settings in the platform settings apply to syslogs for connection and security intelligence events *unless* you override the setting for the access control policy in any of the places listed in “About Configuring the System to Send Security Event Data to Syslog” in the *Cisco Secure Firewall Management Center Administration Guide*. These overrides do not provide a secure syslog option, so we recommend against using them in a secure environment.
- The syslog settings in the platform settings policy apply to syslogs for intrusion events *unless* you override the setting for the access control policy in any of the places listed in “Configuration Locations for Security Event Syslogs” in the *Cisco Secure Firewall Management Center Administration Guide*. These overrides do not provide a secure syslog option, so we recommend against using them in a secure environment.

Customize the Login Banner

You can configure the Firewall Threat Defense device to convey essential information to users when they log in to the CLI. From a security perspective, the login banner should discourage unauthorized access; consider text such as this example:

> You have logged into a secure device. If you are not authorized to access this device, log out immediately or risk criminal charges.

To configure the login banner for a Firewall Threat Defense device, create a Firewall Threat Defense platform settings policy under **Device** > **Platform Settings**, and choose **Banner** from the left pane. See “Banner” in the *Cisco Secure Firewall Management Center Device Configuration Guide* for full instructions.

Secure Connections to Servers Supporting Network User Authoritative Logins, Awareness, and Control

Identity policies use identity sources to authenticate network users and collect user data for user awareness and control. Establishing user identity sources requires a connection between the Firewall Management Center or a managed device and one of the following types of servers:

- Microsoft Azure AD
- Microsoft Active Directory
- Linux Open LDAP
- RADIUS

Important Although you can set up a secure connection to LDAP, Microsoft AD, or RADIUS servers from Firewall Threat Defense, the authentication module is not FIPS compliant.

Note If you choose to use LDAP or Microsoft AD for external authentication, review the information in Harden External User Accounts, on page 12.

Note Firewall Threat Defense uses each of these servers to support a different combination of the possible user identity features. For full details, see “About User Identity Sources” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Securing Connections with Active Directory and LDAP Servers

Objects called *realms* describe connection settings associated with a domain on an Active Directory or LDAP server. For full information on configuring realms see “Realms” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

When you create a realm (**Integration** > **Other Integration** > **Realms** in the Firewall Management Center web interface) keep the following in mind to secure the connections with AD or LDAP servers:

For Realms Associated with Active Directory Servers:

- Choose strong passwords for the **AD Join Password** and **Directory Password**.
- When adding a directory to an Active Directory realm:
  - Select **STARTTLS** or **LDAPS** for the **Encryption** mode (do not choose **None**).

  - Specify an **SSL Certificate** to use for authentication to the Active Directory domain controller. We recommend using a certificate generated by globally known and trusted certificate authority.

For Realms Associated with LDAP Servers:

- Choose strong passwords for the **Directory Password**.
- When adding a directory to an LDAP realm:
  - Select **STARTTLS** or **LDAPS** for the **Encryption** mode (do not choose **None**).
  - Specify an **SSL Certificate** to use for authentication to the LDAP server. We recommend using a certificate generated by globally known and trusted certificate authority.

Securing Connections with RADIUS Servers

To configure a connection with a RADIUS server, create a RADIUS Server Group object (**Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** in the Firewall Management Center web interface) and add a RADIUS server to the group. To secure the connection with the RADIUS server, choose the following options in the **New RADIUS Server** dialog:

- Configure a **Key** and **Confirm Key** to encrypt data between the managed device and the RADIUS server.
- Specify an interface for the connection that can support secure data transmission.

Note Firewall Threat Defense connects with a RADIUS server for user identity only if a managed Firewall Threat Defense device in the deployment is configured to provide Remote Access VPN, which will be used as the user identity source. For information on configuring and securing Remote Access VPN, see Harden Network Protocol Settings, on page 8.

Secure Certificate Enrollment

Configuring Certificate Enrollment Using Enrollment over Secure Transport

You can configure certificate enrollment for Firewall Threat Defense over a secure channel. The device uses Enrollment over Secure Transport (EST) to obtain an identity certificate from the CA. EST uses TLS for secure message transport.

To configure EST:

1. Choose **Objects** > **Object Management** > **PKI** > **Certificate Enrollment**.
2. Click **Add Cert Enrollment** and click the **CA Information** tab.
3. From the **Enrollment Type** drop-down list, choose EST.

If you don’t want Firewall Threat Defense to validate the EST server certificate, we recommend that you don’t check the **Ignore EST Server Certificate Validations** check box. By default, Firewall Threat Defense validates the EST server certificate. EST enrollment type supports only RSA and ECDSA keys, and doesn’t support EdDSA keys. For more information, see "Certificate Enrollment Object EST Options" in *Cisco Secure Firewall Management Center Device Configuration Guide*.

On Firewall Management Center and Firewall Threat Defense, you can’t enroll certificates with RSA key sizes smaller than 2048 bits and keys using SHA-1. To override these restrictions, the **Enable Weak-Crypto** option is available (**Devices** > **Certificates**). By default, the weak-crypto option is disabled. We don’t recommend you to enable weak-crypto keys as these keys aren’t as secure as the ones with higher key sizes. You can enable weak-crypto to allow validation of peer certificates and so on. However, this configuration doesn't apply to the certificate enrollment.

Configuring Certificate Validations

You can use a specific CA certificate to validate SSL or IPSec clients, and use a CA certificate to validate connection from an SSL server. To configure the validation usage types:

1. Choose **Objects** > **Object Management** > **PKI** > **Certificate Enrollment**.
2. Click **Add Cert Enrollment** and click the **CA Information** tab.
3. **Validation Usage**—Choose from the options to validate the certificate during a VPN connection
    - IPsec Client—Validate an IPsec client certificate for a site-to-site VPN connection.
    - SSL Client—Validate an SSL client certificate during a remote access VPN connection attempt.
    - SSL Server—Select to validate an SSL server certificate, like as a Cisco Umbrella server certificate.

For more information, see "Adding Certificate Enrollment Objects" in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Harden Object Group Search Settings

The Firewall Threat Defense device expands access control rules into multiple access control list entries based on the contents of any network or interface objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search (**Devices** > **Device Management**, click **Edit** (✎). Then click **Device > Advanced Settings**). With object group search enabled, the system does not expand network or interface objects, but instead searches access rules for matches based on those group definitions.

It is important to note that object group search might also decrease rule lookup performance and thus increase CPU utilization. You should balance the CPU impact against the reduced memory requirements for your specific access control policy. For the low-end Firepower devices such as the 1000 series, 2110, and 2120, the increase in CPU utilization will make the device slow. In most cases, enabling object group search provides a net operational improvement. By default, object group search setting is enabled.

If you enable object group search and then configure and operate the device for a while, disabling the feature might lead to undesirable results. When you disable object group search, your existing access control rules will be expanded in the device's running configuration. If the expansion requires more memory than is available on the device, your device can be left in an inconsistent state and you might see a performance impact. If your device is operating normally, you should not disable object group search once you have enabled it. For more information, see "Configure Object Group Search" in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Harden Supporting Components

The Firewall Threat Defense software depends on complex underlying firmware and operating system software. These underlying software components carry their own security risks that must be addressed:

- Establish an operational security process for your network that takes security issues into account.
- For Firewall Threat Defense models 2100, 4100, and 9300 devices, secure the Firepower eXtensible Operating System the Firewall Threat Defense runs on; see the *Cisco Firepower 4100/9300 FXOS Hardening Guide*.

Disable Front Panel USB-A Port on Firepower 1000 and Secure Firewall 3100/4200

We recommend that you disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200 for security purposes as the port is enabled by default.

- Use the **system support usb show** command to view the current administrative and operational state of the USB port.
- Use the **system support usb port disable** command to disable the front panel USB port.

For more information, see *Cisco Secure Firewall Threat Defense Command Reference*.

Secure HTTP Proxy Settings

If there is no direct connection between the threat defense device and the Internet, you can set up an HTTP proxy for the management interface. The system will then use the proxy for all management connections. You can configure an HTTP proxy in the threat defense device CLI using the `configure network http-proxy` command. Ensure that you use a strong password when configuring the Proxy Password.

Secure Loopback Interface

A loopback interface is a software-only interface that emulates a physical interface. These interfaces helps to overcome path failures as they are accessible from any physical interface. If one interface goes down, you can access the loopback interface from another.

You can use loopback interfaces for services such as AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload (Secure Firewall 3100 and 4200 only), NetFlow, SNMP, SSH, Static and dynamic VTI tunnels, and Syslog. Ensure that you enable only the required services on the loopback interface.

For more information, see “Configure Loopback Interfaces” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Secure Onboarding of Devices Using Device Registration Keys or Serial Numbers

You can easily onboard devices to the Firewall Management Center using device serial numbers or registration keys, and bring up the devices with pre-provisioned configurations using device templates. We recommend that you secure the device serial numbers or registration keys before the onboarding process

For more information, see “Add a Device to the Firewall Management Center Using a Device Template” in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.