Cisco Secure Firewall Management Center Hardening Guide, Version 7.2

First Published: 2022-06-27

Introduction

From Version 7.2, Firepower Management Center (FMC) is rebranded as Secure Firewall Management Center (management center). Firepower Threat Defense (FTD) is rebranded as Secure Firewall Threat Defense (threat defense).

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

- *Cisco Firepower Threat Defense Hardening Guide, Version 7.2*
- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

Not all configuration settings discussed in this manual are available in all management center versions. For more information about new and deprecated features for each release, see Cisco Secure Firewall Management Center New Features by Release. For detailed information about configuring your management center deployment, see the Cisco Secure Firewall Threat Defense documentation for your version for your version.

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, 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 management center documentation and 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 management center, but some management center 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, 7.2*. We have endeavored to ensure that this hardening guide and the *Cisco Secure Firewall Management Center Administration Guide, 7.2* 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 management center 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 "System Updates" chapter of the *Cisco Secure Firewall Management Center Administration Guide, 7.2*, and the *Secure Firewall Management Center Upgrade Guide*.

Cisco also periodically issues updates for the databases management center uses to protect your network and assets. To provide optimum protection, keep the geolocation, intrusion rules, and vulnerabilities databases 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

Geolocation Database (GeoDB) is a database of geographical data (such as country and city coordinates) and connection-related data (such as Internet service provider, domain name, connection type) associated with routable IP addresses. When management center detects GeoDB information that matches a detected IP address, you can view the geolocation information associated with that IP address. To view any geolocation details other than country or continent, you must install the GeoDB on your system.

To update the GeoDB from the management center web interface, use **System** > **Updates** > **Geolocation Updates**, and choose one of the following methods:

- Update the GeoDB on an management center with no internet access.
- Update the GeoDB on an management center with internet access.

- Schedule recurring automatic updates of the GeoDB on an management center with internet access.

For more information, see "Update the Geolocation Database" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

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 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** > **Updates** > **Rule Updates**:

- Update intrusion rules on an management center with no internet access.
- Update intrusion rules on an management center with internet access.
- Schedule recurring automatic updates of intrusion rules on an management center with internet access.

For more information, see "Update Intrusion Rules" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

You can also import local intrusion rules using **System** > **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 management center, see "Best Practices for Importing Local Intrusion Rules" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2* 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 management center web interface offers two approaches to updating the VDB:

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

For more information, see "Update the Vulnerability Database" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

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 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 "Security Intelligence Lists and Feeds" in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Enable CC or UCAPL Mode

To apply multiple hardening configuration changes with a single setting, choose CC or UCAPL mode for the management center. This setting appears under **System** > **Configuration** > **UCAPL/CC Compliance** in the management center web interface.

Choosing one of these configuration options puts into effect the changes listed under “Security Certification Compliance Characteristics” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*. 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, 7.2* 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.

Secure the Local Network Infrastructure

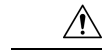
Your deployment may interact with other network resources for a number of purposes. Hardening these other services can protect your system as well as all your network assets. To identify everything that needs to be addressed, try diagramming the network and its components, assets, firewall configuration, 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 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 management center and the devices it manages. From the management center web interface use **System** > **Configuration** > **Time Synchronization** and use the instructions in “Synchronize Time Using a Network NTP Server” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

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 management center and managed devices. To ensure proper synchronization, configure the 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 the management center to connect with a local DNS server is part of the initial configuration process, described in the Cisco Secure Firewall Management Center Getting Started Guide for your hardware model.

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. Be sure your local DNS server is configured in keeping with industry-recommended best practices for security; Cisco offers guidelines in DNS Best Practices, Network Protections, and Attack Identification.

Secure SNMP Polling

You can monitor the management center using SNMP polling as described in "SNMP Polling" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*. 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. For this reason you should choose configuration options to protect your system from SNMP-based threats.

When you configure SNMP polling (under **System** > **Configuration** > **SNMP** in the management center web interface) use the following options to harden SNMP in your deployment:

- Choose SNMPv3, which supports:
  - Authentication algorithms such as SHA, SHA224, SHA256, and SHA384.
  - Encryption with AES256, AES192, and AES128.
  - Read-only users.
- Use strong passwords when configuring the **Authentication Password** for network management access.
- Use strong passwords when configuring the **Privacy Password**.
- Choose the **Privacy Protocol** as AES128.

In addition, you should restrict your access list for SNMP access to the specific hosts that will be used to poll for the MIB. This option appears in the management center web interface under **System** > **Configuration** > **Access List**. See "Configuring the Access List for Your System" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

The management center also supports sending external alerts to an SNMP server. To secure this function, see Block Third-Party Database Access.

Important Although you can establish a secure connection to an SNMP server from the 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, 7.2*. Use this information at two stages when establishing your deployment:

- When performing the initial setup for your management center as described in the Cisco Firepower Management Center Getting Started Guide for your hardware model.
- When registering a managed device to the management center as described in "Add Devices to the Firepower Management Center" in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Secure Access to Managed Devices

Your deployment includes security devices managed by the management center, each providing different means of access. These devices exchange information with the management center and their security is important to the security of your overall deployment. Analyze these devices in your deployment and apply hardening configurations as appropriate, such as securing user access and closing unneeded communication ports.

Harden Management Center User Access

Internal and External Users

The management center supports two types of users:

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

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 management center web interface; external authentication objects can be shared to authenticate external users for the management center as well as managed devices.

Types of User Access

The management center supports two types of user access:

- A web interface (HTTP)—Available to both internal and external user accounts.

- Command line access using SSH, serial, or keyboard and monitor connection—Available to the CLI/shell access **admin** account and can be made available to external users.

Restrict Administration Privileges

The management center supports two **admin** accounts:

- One **admin** account for accessing the management center through the web interface (HTTP).
- One **admin** account for CLI/shell access using SSH, serial, or keyboard and monitor connection. In the default configuration this account has direct access to the Linux shell. You can configure this account to access the management center auxiliary CLI rather than the Linux shell (see Restrict Shell Access, on page 7). From within the management center CLI this account can directly access the Linux shell using the CLI **expert** command (unless you disable the **expert** command; again, see Restrict Shell Access, on page 7).

Note In the management center initial configuration, the passwords for both these **admin** accounts are the same, but they are not the same accounts, and the system validates these passwords against different databases.

The **admin** accounts have configuration rights over and above other users, including the right to create additional accounts with the same privileges. Consider carefully when choosing to which users you grant access to any account with administration privileges.

For more information, see “User Accounts for Management Access” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Restrict Shell Access

By default, users with command line access gain direct access to the Linux shell when they log in. CLI or shell users must take the additional step of entering the CLI **expert** command to access the Linux shell.

Note On all devices, after a user makes three consecutive failed attempts to log into the CLI or shell via SSH, the system terminates the SSH connection.

Caution On all devices, users with CLI/shell access can obtain root privileges in the shell, which can present a security risk. For system security reasons, we strongly recommend:

- If you establish external authentication, make sure that you restrict the list of users with CLI/shell access appropriately.
- Do not add users directly in the shell; create new accounts using only the procedures described in the Secure Firewall Management Center Configuration Guide for your version.
- Do not access the management center using the shell or CLI **expert** mode unless directed by Cisco TAC.

For more information on types of management center access, see "Web Interface and CLI Access" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

The most secure hardening action you can take with regards to Linux shell access for the management center is to block all access to the shell:

- Log into the management center using an SSH, serial or keyboard and monitor connection (See the Getting Started Guide for your management center model.)
- Enter the **system lockdown** command. (*Cisco Secure Firewall Management Center Administration Guide, 7.2*.)

After you use the **system lockdown** command, any user who logs in to the management center with command line credentials will have access only to the management center CLI commands. This can be a significant hardening action, but use it with careful consideration, because it can only be reversed with a hotfix from Cisco TAC.

For more information on the management center CLI, see *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Use Multitenancy to Segment User Access to Managed Devices, Configurations, and Events

Administrators can group the managed devices, configurations, and events in a deployment into *domains*, and grant management center users access to selected domains as appropriate to their needs. Users operate within the access restrictions imposed by their domain assignment in addition to those imposed by their user role(s). You can, for instance, grant a selected account full administrator access within one domain, Security Analyst access within another domain, and no access to a third domain.

Create and manage domains from the management center web interface using the **System** > **Domains**. For more information about implementing multitenancy, see *Cisco Secure Firewall Management Center Administration Guide, 7.2* under "Domains".

Assign users rights within domains from the management center web interface using **System** > **Users** > **Users** For more information, see “Add an Internal User ” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Harden Internal User Accounts

Internal users have access to the management center only through the web interface. Administrators can use the following settings under **System** > **Users** > **Users** to harden the system against attacks through web interface login mechanisms:

- Restrict the maximum number of failed web interface logins before an account is locked out
- Enforce a minimum password length
- Set the number of days passwords are valid
- Require strong passwords
- Do not exempt users from web interface session timeout
- Assign user role(s) appropriate only to the type of access the account requires
- Assign a domain appropriate to the type of access the user requires
- Force the user to reset the account password on the next login

For more information on these settings, see "Users" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Administrators can also configure the following settings globally for all internal web interface users under **System** > **Configuration** > **User Configuration**:

- Limit password reuse
- Track successful logins
- Block web interface access for temporarily users who fail a selected number of login attempts

For more information on these settings, see "Global User Configuration Settings" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Harden External User Accounts

The management center authenticates external user accounts against a user database stored on an external server (LDAP or RADIUS).

Note If you choose to use external authentication, review the information in Secure Connections to Servers Supporting Network User Authoritative Logins, Awareness, and Control, on page 16.

Note To use external authentication the management center must use DNS. Configuring an management center to use DNS is usually done during the initial configuration process. Be sure your local DNS is configured in keeping with industry-recommended best practices for security; see Secure the Domain Name System (DNS), on page 5.

Important Although you can set up a secure connection with LDAP or RADIUS servers from the management center, the authentication module is not FIPS compliant.

To configure an external server for management center user authentication, you must create an external authentication object under **System** > **Users** > **External Authentication**. Use the following options in your external authentication object to harden your management center against possible attacks through externally-authenticated user accounts:

- Carefully restrict users' access to accounts with shell access. Shell users can gain root privileges, which presents a security risk.
- Do not grant accounts more access than they need:
  - If using LDAP, associate the appropriate management center user roles with LDAP users or user groups.
  - If using RADIUS, associate the appropriate management center user roles with RADIUS attributes.
- If using LDAP, under **Advanced Options** when configuring an external authentication object, configure TLS or SSL encryption.

For more information see "Configure External Authentication" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Establish Session Timeouts

Limiting the length of account login sessions reduces the opportunity for unauthorized users to exploit unattended sessions.

To set session timeouts on the management center, use **System > Configuration > Session Timeout**. From there you can configure the following interface timeout values in minutes:

- **Browser Session Timeout**—Management Center web interface session timeout.
- **CLI Timeout**—CLI access timeout.

These settings apply to internal and external accounts, regardless of their access role(s). See "Session Timeouts" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Disable REST API Access

The management center REST API provides a lightweight interface for third-party applications to view and manage appliance configuration using a REST client and standard HTTP methods. For more information on the management center REST API, see the Secure Firewall Management Center REST API Quick Start Guide for your version.

By default, the management center allows requests from applications using the REST API. To harden the management center, you should disable this access; in the management center web interface select **System** > **Configuration** > **REST API Preferences** and uncheck the **Enable REST API** check box. For more information, see "REST API Preferences" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Restrict Remote Access

On the management center you can use access lists to limit access to the system by IP address and port. By default, the following ports are enabled for any IP address:

- 443 (HTTPS) – Used for web interface access
- 22 (SSH) – Used for CLI/shell access

You can also add access to poll for SNMP information over port 161.

Important Although you can set up a secure connection to an SNMP server from management center, the authentication module is not FIPS compliant.

To operate in a more secure environment, configure your management center to permit these forms of access only to specific IP addresses, and disable the default rules that allow HTTPS or SSH access to any IP address. These options appear under **System > Configuration > Access List** in the management center web interface. For more information, see "Access List" in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Do Not Use Remediations

A remediation is a program that management center launches in response to a correlation policy violation. You can configure several types of remediations on the management center, but they all require that the management center communicate with entities outside in an unsecured fashion. For this reason, we recommend

against configuring a hardened management center to use remediations. For information, see “Remediations” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Secure Communications Between the Management Center and the Web Browser

Secure the information transmitted between the management center and your local computer by using both client and server HTTPS certificates to secure the connection between the management center and the browser running the web interface. The management center uses a default self-signed certificate, but we recommend replacing that with a certificate generated by globally known and trusted certificate authority.

To configure HTTPS certificates for your management center, use **System** > **Configuration** > **HTTPS Certificate** in the management center web interface; see “HTTPS Certificates” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Lock Access Control Policy

You can lock an access control policy to prevent other administrators from editing it. Locking the policy ensures that your changes are not invalidated if another administrator edits the policy and saves changes before you save your changes. Without locking, if multiple administrators edit the policy simultaneously, the first user who saves changes overwrites the changes of all other users. The lock is for the access control policy and does not apply to the objects used in the policy. When locked, other administrators have read-only access to the policy. However, other administrators can assign a locked policy to a managed device. We recommend that you lock an access control policy when you edit the policy:

1. Choose **Policies** > **Access Control**.
2. Click **Edit** next to the access control policy you want to lock or unlock.
3. Click the lock icon next to the policy name to lock or unlock the policy.

To unlock a policy that is locked by another administrator, you must update the following permission: **Policies** > **Access Control** > **Access Control Policy** > **Modify Access Control Policy** > **Override Access Control Policy Lock**. By default, this permission is enabled for the Administrator user role. We recommend that you do not enable this permission. For more information, see "Locking an Access Control Policy" in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Protect Backups

To protect system data and its availability, perform regular backups of your management center. The backup function appears under **System** > **Tools** > **Backup/Restore** in the management center web interface. For more information, see "Back up the management center" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

The 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 management center and the remote storage device cannot be secured.

Revert a Threat Defense Upgrade

You can revert major and maintenance upgrades to threat defense using the management center. Reverting returns the software to its state just before the last major or maintenance upgrade, also called a snapshot. Reverting after patching removes patches. The revert happens only if communications between the management

center and device are disrupted. In high availability or scalability deployments, revert is more successful when all units are reverted simultaneously.

Configurations that are reverted include: snort version, device-specific configurations, objects used by your device-specific configurations. Configurations that are not reverted include shared policies that can be used by multiple devices.

If you want to revert after a successful upgrade, choose **System** > **Updates** on the management center to upgrade the threat defense, and set the **Enable revert after successful upgrade** option. By default, this option is enabled. We recommend that you enable this option.

The revert snapshot is saved on the management center and the device for thirty days, after which it is automatically deleted and you can no longer revert. You can manually delete the snapshot from either appliance to save disk space, but this removes your ability to revert. For more details, see "Revert the Upgrade" in the *Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2*.

Protect Configuration Export and Import

The management center provides the ability to export a number of system configurations (such as policies, custom tables, and report templates) to a file. You can import these configurations to another management center running the same version. This can be a timesaving feature for administrators adding new appliances to a deployment, but it must be used with care to prevent security breaches. Keep the following precautions in mind when using the export/import feature:

- Secure the communications between the management center and the web browser to protect the configuration information being transferred. See Secure Communications Between the Management Center and the Web Browser, on page 11.
- Secure access to the local computer where the exported configuration file is stored; protecting this file is important to the security of your deployment.
- Be aware that if you export a configuration that uses PKI objects containing private keys, the system decrypts the private keys before export; the exported private keys are stored in clear text. On import the system encrypts the keys with a randomly generated key.

The configuration export and import functions appear in the management center web interface under **System** > **Tools** > **Import/Export**. For full information on this feature, see "Import/Export" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Protect Management Connection Using Auto Rollback

You can enable auto rollback of the configuration if a deployment causes the management connection between the management center and the threat defense to go down. The auto rollback of the deployment occurs if you use the data interface for management center access, and you misconfigure the data interface.

We recommend that you enable the auto rollback settings using **Devices > Device Management > Device > Deployment Settings**, and configure the connectivity monitor interval. Auto rollback is not supported for high availability or clustering deployments, and transparent modes. For more information, see "Edit Deployment Settings" in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Protect Reports

Management Center offers several types of reports, all of which contain sensitive information you should protect from access by unauthorized personnel. You can download all types of reports from the management

center to your local computer in unencrypted form. Before downloading reports, secure the communications between the management center and the web browser to protect the information being transferred. (See Secure Communications Between the Management Center and the Web Browser.) In addition, secure access to the local computer where any reports are stored.

- Standard reports are detailed customizable reports about all aspects of your system, available in HTML, CSV, and PDF formats. Risk reports are HTML format summaries of risks found in your organization.

  On the management center web interface, both standard and risk reports appear under **Overview** > **Reporting**. For these reports, there are two storage options along with local download, each of which presents a security risk:

  - You can automatically email the report to a selected server. We do not recommend using this feature in a hardened system as the email cannot be secured.
  - You can automatically store reports on a remote device. We do not recommend using this feature for a hardened system as the connection between the management center and the remote storage device cannot be secured.

  For full information on designing and generating standard reports and risk reports, see "Reports" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

- Health monitor reports for troubleshooting contain information that Cisco TAC can use to diagnose system problems should any arise. To generate these reports from the management center web interface, use **System** > **Health** > **Monitor**, and follow the instructions under “Health Monitor Reports for Troubleshooting” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*. The management center produces troubleshooting files in .tar and .gz formats.

- Policy reports are PDF files providing details on a policy’s current saved configuration. To generate a policy report, access the management page for the policy for which you want a report and click the report icon ( .) For a full list of the policies that support reports, see “Generating Current Policy Reports” in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

- Use comparison reports to review policy changes for compliance with your organization's standards or to optimize system performance. You can examine the differences between two policies or between a saved policy and the running configuration. To generate a comparison report (available in PDF format only), access the management page for the type of policies you want to compare, and select **Compare Policies**. See “Comparing Policies” in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Secure External Alerting

You can configure the management center to issue notifications called *alert responses* to external servers when selected events occur. While these alerts are useful in monitoring system activity, they can present a security risk if the connection to the external server cannot be secured.

The management center supports sending alert responses in three different forms:

- Alert responses sent to syslog cannot be secured. Choose **Policies** > **Actions** > **Alerts** > **Create Alert** > **Create Syslog Alert** in the management center web interface; we do not recommend configuring your management center to send such alerts in a hardened environment.

- Information the management center sends to an external server via email can be secured if you configure the connection with the mail relay host to use encryption (TLS or SSLv3) and require a username and password. Do this through the management center web interface using **System** > **Configuration** >

Email Notification. For more information see "Configuring a Mail Relay Host and Notification Address" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Once you have secured the connection with the mail relay host, this protects data the management center transmits with the following features:

- Email alert responses, described in "Creating an Email Alert Response" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*. (Configure this setting using **Polices** > **Actions** > **Alerts** > **Create Alert** > **Create Email Alert** in the management center web interface.)
- Data pruning notifications, described in "Configuring Database Event Limits" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*. (Configure this setting under **System** > **Configuration** > **Database** in the management center web interface.)

- Alerts sent to an SNMP server can be secured by using the following options under **Policies** > **Actions** > **Alerts** > **Create Alert** > **Create SNMP Alert** in the management center web interface:
  - Choose SNMP v3 for the **Version**. This protocol supports:
    - Authentication algorithms such as SHA, SHA224, SHA256, and SHA384.
    - Encryption with AES256, AES192, and AES128.
    - Read-only users.
  - Choose an **Authentication Protocol** to secure the connection (MD5 or SHA) and supply a **Password**.
  - Choose DES, AES, or AES128 as the **Privacy Protocol** and supply a **Password**. A longer key provides higher security but a reduction in performance.
  - Supply an **Engine ID** which the system will use to encode messages. We recommend that you use the hexadecimal version of the management center's IP address. For example, if the management center has an IP address of 10.1.1.77, use 0a01014D0.

  You should restrict your access list for SNMP access to the specific hosts to which the management center will send SNMP alerts. Choose **System** > **Configuration** > **Access List**. See "Configure an Access List" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

  The management center also supports SNMP polling. To secure this function, see Secure SNMP Polling.

Important Although you can set up secure connections to an SNMP or SMTP server from the management center, the authentication module is not FIPS compliant.

For full information on external alerting, see "External Alerting with Alert Responses" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Protect Audit Logs

The management center maintains read-only logs of user activity, configured through **System** > **Configuration** > **Audit Log**. To conserve memory resources on the management center you can store these logs externally (streaming to the Syslog or to an HTTP server). However, doing so can present a security risk unless you secure the channel for audit log streaming by enabling TLS and establishing mutual authentication

using TLS certificates. For more information, see “Securely Stream Audit Logs” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Secure the Connection to eStreamer

The Event Streamer (eStreamer) allows you to stream several kinds of event data from an management center to a custom-developed client application. For more information, see the Secure Firewall eStreamer Integration Guide for your version. If your organization chooses to create and use an eStreamer client, take the following precautions:

- Develop your application using industry best practices for security.
- Configure the connection between the management center and the eStreamer client so that the data is transmitted securely. Do this in the management center web interface under **Integrations** > **Other Integrations** > **eStreamer** > **Create Client** by providing a password to encrypt the certificate file that secures the connection with the host running the eStreamer client. For more information, see “Configuring eStreamer Client Communications” in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Secure the Connection to Cisco Security Analytics and Logging

You can configure Cisco Security Analytics and Logging (On Premises) to store your threat defense event data for increased storage at a larger retention period.

The query from the management center to the Cisco Secure Network Analytics Manager is through a TLS-encrypted connection. By default, Security Analytics and Logging uses a self-signed certificate that the management center can download automatically. To secure the connection to Security Analytics and Logging, we recommend that you:

- Transfer the certificate manually over a secure channel and upload it to the management center.
- Use a certificate generated by a globally known and trusted certificate authority.

The events are sent to Cisco Security Analytics and Logging (On Premises) using syslog. Ensure that you choose secure options when configuring syslog functionality.

Block Third-Party Database Access

Ensure that third party client applications do not have access to the management center database; in the management center web interface, under **System** > **Configuration** > **External Database Access**, be sure the **Allow External Database Access** check box is unchecked. For more information, see "External Database Access Settings" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

Customize the Login Banner

Users with and without authorized access to the management center can view the system login page. Customize your login banner so it displays only the information appropriate for anyone to see. On the management center web interface, use **System** > **Configuration** > **Login Banner**. For full information see "Login Banners" in the *Cisco Secure Firewall Management Center Administration Guide, 7.2*.

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

Management Center 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 management center or a managed device and one of the following types of servers:

- Microsoft Active Directory
- Linux Open LDAP
- RADIUS

Important Although you can set up a secure connection to LDAP, Microsoft AD, or RADIUS servers from management center, 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 9.

Note Management Center 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, 7.2*.

Note Management Center can use also RADIUS servers to supply a VPN capability for your network. For more information, see "VPN Overview" in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

Securing Connections with Active Directory and LDAP Servers

Management Center objects called *realms* describe connection settings associated with a domain on an Active Directory or LDAP server. For full information on configuring realms see “Create and Manage Realms” in the *Cisco Secure Firewall Management Center Device Configuration Guide, 7.2*.

When you create a realm (**Integration** > **Other Integrations** > **Realms** in the 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** > **RADIUS Server Group** in the 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:

- Supply 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.

Secure Certificate Enrollment

Configuring Certificate Enrollment Using Enrollment over Secure Transport

You can configure certificate enrollment for 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 > Cert 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 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, 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, 7.2*.

On management center and threat defense Versions 7.0 and higher, you can’t enroll certificates with RSA key sizes smaller than 2048 bits and keys using SHA-1. To override these restrictions on management center 7.0 managing threat defense running versions lesser than 7.0, 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. For management center and threat defense versions 7.0 and higher, 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 > Cert 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, 7.2*

Harden Object Group Search Settings

The 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 > 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, 7.2*

Harden Supporting Components

The management center 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 management center models 1000, 1600, 2000, 2500, 2600, 4000, 4500, and 4600, to harden components of the hardware device that underlie the management center software, see the *Cisco UCS Hardening Guide*.