Cisco Firepower Management Center Hardening Guide, Version 6.4

First Published: 2019-05-10

Cisco Firepower Management Center Hardening Guide, Version 6.4

Firepower protects your network assets and traffic from cyber threats, but you should also configure Firepower itself so that it is *hardened*—further reducing its vulnerability to cyber attack. This guide addresses hardening your Firepower deployment, with a focus on the Firepower Management Center (FMC). For hardening information on other components of your Firepower deployment see the following documents:

- *Cisco Firepower Threat Defense Hardening Guide, Version 6.4*
- *Cisco Firepower 4100/9300 FXOS Hardening Guide*

This guide refers to configuration settings in the FMC web interface but is not intended as a detailed manual for that interface. Feature descriptions refer to Version 6.4 of the Firepower system, and cross-references refer to Version 6.4 of the *Firepower Management Center Configuration Guide*. Not all configuration settings discussed in this manual are available in all Firepower versions. For detailed information about configuring your Firepower deployment, see the Firepower 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, Firepower 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 Firepower documentation and the Firepower Management Center 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 Firepower 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 FMC, but some FMC features do not support certification compliance even using the configuration settings described herein. For more information see "Security Certifications Compliance Recommendations" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*. We have endeavored to ensure that this hardening guide and the *Cisco Firepower Management Center Configuration Guide, Version 6.4* 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 the Cisco Security Advisories and Alerts page. More information about these communication vehicles is available in the Cisco Security Vulnerability Policy.

To maintain a secure network, stay aware of Cisco security advisories and responses. These 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 Firepower software updates to address issues and make improvements. Keeping your system software up to date is essential to maintaining a hardened system. To ensure your system software is properly updated, use the information in the "System Updates" chapter of the *Firepower Management Center Configuration Guide, Version 6.4*, and the *Firepower Management Center Upgrade Guide*.

Cisco also periodically issues updates for the databases Firepower 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 Firepower deployment you *must* read the Cisco Firepower 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 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 Firepower 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 FMC web interface, use **System** > **Updates** > **Geolocation Updates**, and choose one of the following methods:

- Update the GeoDB on an FMC with no internet access.
- Update the GeoDB on an FMC with internet access.

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

For more information, see "Update the Geolocation Database" in the *Firepower Management Center Configuration Guide, Version 6.4*.

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 FMC, 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 FMC web interface provides three approaches to updating the intrusion rules, all under **System** > **Updates** > **Rule Updates**:

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

For more information, see "Update Intrusion Rules" in the *Firepower Management Center Configuration Guide, Version 6.4*.

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 FMC, consult "Guidelines for Importing Local Intrusion Rules" in the *Firepower Management Center Configuration Guide, Version 6.4* 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 FMC 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 *Firepower Management Center Configuration Guide, Version 6.4*.

Enable CC or UCAPL Mode

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

Choosing one of these configuration options puts into effect the changes listed under "Security Certification Compliance Characteristics" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*. Be aware that all appliances in your Firepower 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 Firepower Management Center Configuration Guide, Version 6.4* 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 Firepower deployment may interact with other network resources for a number of purposes. Hardening these other services can protect your Firepower 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 FMC and its managed devices is essential to successful operation of Firepower. We strongly recommend using a secure and trusted Network Time Protocol (NTP) server to synchronize system time on the FMC and the devices it manages. From the FMC web interface use **System** > **Configuration** > **Time Synchronization** and use the instructions in "Synchronize Time Using a Network NTP Server" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Caution Unintended consequences may occur when time is not synchronized between the FMC and managed devices. To ensure proper synchronization, configure the FMC 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 an FMC to connect with a local Domain Name System server is part of the initial configuration process, described in the Cisco Firepower 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 this document: http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html.

Secure SNMP Polling

You can monitor the FMC using SNMP polling as described in "SNMP Polling" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*. 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 FMC web interface) use the following options to harden SNMP in your Firepower deployment:

- Choose SNMPv3, which supports only encryption with AES128 and read-only users.
- Use strong passwords when configuring the **Authentication Password** field for network management access.

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 FMC web interface under **System** > **Configuration** > **Access List**. See "Configuring the Access List for Your System" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

The FMC 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 Firepower, the authentication module is not FIPS compliant.

Secure Network Address Translation (NAT)

Typically networked computers use Network Address Translation (NAT) for reassigning source or destination IP addresses in network traffic. To protect your Firepower 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 Firepower deployment to operate in a NAT environment, see "NAT Environments" in the *Firepower Management Center Configuration Guide, Version 6.4*. Use this information at two stages when establishing your deployment:

- When performing the initial setup for your FMC as described in the Cisco Firepower Management Center Getting Started Guide for your hardware model.
- When registering a managed device to the FMC as described in "Add Devices to the Firepower Management Center" in the *Firepower Management Center Configuration Guide, Version 6.4*.

Secure Access to Managed Devices

Your Firepower deployment includes security devices managed by the FMC, each providing different means of access. These devices exchange information with the FMC 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 FMC User Access

Internal and External Users

The FMC supports two types of users:

- Internal users—The system 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 FMC web interface; external authentication objects can be shared to authenticate external users for the FMC as well as managed devices.

Types of User Access

The FMC supports two types of user access:

- A web interface (HTTP). This is available to both internal and external user accounts.
- Command line access using SSH, serial, or keyboard and monitor connection. This is available to the CLI/shell access **admin** account and can be made available to external users.

This discussion of user management refers to features available in Firepower Version 6.4; not all user account configuration features addressed in this section apply to all Firepower versions. For information specific to your system, see the Firepower Management Center Configuration Guide for your version.

Restrict Administration Privileges

The FMC supports two **admin** accounts:

- One **admin** account for accessing the FMC 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 FMC auxiliary CLI rather than the Linux shell (see Restrict Shell Access, on page 7). From within the FMC 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 FMC 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 *Firepower Management Center Configuration Guide, Version 6.4*.

Restrict Shell Access

By default, users with command line access gain direct access to the Linux shell when they log in.Administrators can configure these accounts to initially access the FMC CLI on login using the web interface selection **System** > **Configuration** > **Console Configuration** > **Enable CLI Access**.Once the FMC CLI is enabled, 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 Firepower Management Center Configuration Guide for your version.
- Do not access the FMC using the shell or CLI **expert** mode unless directed by Cisco TAC.

For more information on types of FMC access, see "Web Interface, CLI, or Shell Access" in the *Firepower Management Center Configuration Guide, Version 6.4*.

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

- Enable the FMC CLI from the web interface using **System** > **Configuration** > **Console Configuration** > **Enable CLI Access**.
- Log into the FMC using an SSH, serial or keyboard and monitor connection (See the Getting Started Guide for your FMC model.)
- Enter the **system lockdown** command. (See Appendix C of the *Firepower Management Center Configuration Guide, Version 6.4*.)

Once the system lockdown has completed, any user who logs in to the FMC with command line credentials will have access only to the FMC 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 full information on the FMC CLI, see See Appendix C of the *Firepower Management Center Configuration Guide, Version 6.4*.

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

Administrators can group the managed devices, configurations, and events in a Firepower deployment into *domains*, and grant FMC 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 FMC web interface using the **System** > **Domains** menu option. Full information about implementing multitenancy can be found in the *Cisco Firepower Management Center Configuration Guide, Version 6.4* under "Domain Management".

Assign users rights within domains from the FMC web interface using **System** > **Users** > **Users** For full details see “Add an Internal User at the Web Interface” in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Harden Internal User Accounts

Internal users have access to the FMC 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 and must be reactivated by an administrator
- 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 “User Accounts for Management Access” in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*FMC" .

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
- Temporarily block web interface access for users who fail a selected number of login attempts

For more information on these settings, see “Global User Configuration Settings” in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Harden External User Accounts

The FMC 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 14.

Note To use external authentication the FMC must use DNS. Configuring an FMC 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 4.

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

To configure an external server for FMC 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 FMC 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 Firepower user roles with LDAP users or user groups.
  - If using RADIUS, associate the appropriate Firepower 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 Firepower Management Center Configuration Guide, Version 6.4*.

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 FMC, use **System** > **Configuration** > **Shell Timeout**. From there you can configure the following interface timeout values in minutes:

- **Browser Session Timeout** : FMC web interface session timeout.
- **Shell Timeout**: CLI/shell access timeout.

These settings apply to internal and external accounts, regardless of their access role(s). See "Session Timeouts" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Disable REST API Access

The Firepower 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 Firepower REST API, see the Firepower Management Center REST API Quick Start Guide for your version.

By default, the FMC allows requests from applications using the REST API. To harden the FMC, you should disable this access; in the FMC web interface select **System** > **Configuration** > **REST API Preferences** and uncheck the **Enable REST API** checkbox. For full information, see "REST API Preferences" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Restrict Remote Access

On the FMC 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 Firepower, the authentication module is not FIPS compliant.

To operate in a more secure environment, configure your FMC 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 FMC web interface. For more information, see "Access List" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Do Not Use Remediations

A remediation is a program that Firepower launches in response to a correlation policy violation. You can configure several types of remediations on the FMC, but they all require that the FMC communicate with entities outside of the Firepower in an unsecured fashion. For this reason, we recommend against configuring a hardened Firepower System to use remediations. For information, see "Remediations" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4* .

Secure Communications Between the FMC and the Web Browser

Secure the information transmitted between the FMC and your local computer by using both client and server HTTPS certificates to secure the connection between the FMC and the browser running the web interface. The FMC 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 FMC, use **System** > **Configuration** > **HTTPS Certificate** in the FMC web interface; see "HTTPS Certificates" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Protect Backups

To protect system data and its availability, perform regular backups of your FMC. The backup function appears under **System** > **Tools** > **Backup/Restore** in the FMC web interface. For more information, see "Back up the Firepower Management Center" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4* .

The FMC 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 FMC and the remote storage device cannot be secured.

Protect Configuration Export and Import

The FMC provides the ability to export a number of system configurations (such as policies, custom tables, and report templates) to a file which can then be used to import those same configurations to another FMC running the same Firepower 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 FMC and the web browser to protect the configuration information being transferred. See Secure Communications Between the FMC and the Web Browser, on page 10.
- Secure access to the local computer where the exported configuration file is stored; protecting this file is important to the security of your Firepower 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 FMC web interface under **System** > **Tools** > **Import/Export**. For full information on this feature, see "Configuration Import and Export" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Protect Reports

The Firepower system offers several types of reports, all of which contain sensitive information you should protect from access by unauthorized personnel. All of the report types discussed here can be downloaded from the FMC to your local computer in unencrypted form. Before downloading reports, secure the communications between the FMC and the web browser to protect the information being transferred. (See Secure Communications Between the FMC 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 FMC web interface, both standard and risk reports appear under **Overview** > **Reporting**. For these reports Firepower offers two storage options in addition to 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 FMC and the remote storage device cannot be secured.

  For full information on designing and generating standard reports and risk reports, see "Working with Reports" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4* .

- 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 FMC web interface, use **System** > **Health** > **Monitor**, and follow the instructions under "Health Monitor Reports for Troubleshooting" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*. The FMC produces troubleshooting files in `.tar.gz` format.

- 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 on the report icon () For a full list of the policies that support reports, see "Generating Current Policy Reports" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.
- 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 Firepower Management Center Configuration Guide, Version 6.4*.
- Incident Reports can include information about incidents of suspected security policy violations such as summary, status, and information specific to events you add to the incident. These reports can be formatted as HTML, PDF, or CSV formats. In the FMC web interface, generate these reports from the incident analysis page at **Analysis** > **Intrusions** > **Incidents**, and use the instructions under "Generating Incident Reports" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*
- The intrusion events clipboard is a holding area where you can copy events from any of the intrusion event views, and generate reports about those events in HTML, PDF or CSV formats. In the FMC web interface, you must first add events to the clipboard, then you can generate these reports using **Analysis** > **Intrusions** > **Clipboard**. See "The Intrusion Events Clipboard" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Secure External Alerting

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

The FMC supports sending alert responses in three different forms:

- Alert responses sent to syslog cannot be secured. (**Policies** > **Actions** > **Alerts** > **Create Alert** > **Create Syslog Alert** in the FMC web interface); we do not recommend configuring your FMC to send such alerts in a hardened environment.
- Information the FMC 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 FMC web interface using **System** > **Configuration** > **Mail Relay Host**. For more information see "Configuring a Mail Relay Host and Notification Address" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

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

  - Email alert responses, described in "Creating an Email Alert Response" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*. (Configure this setting using **Polices** > **Actions** > **Alerts** > **Create Alert** > **Create Email Alert** in the FMC web interface.)
  - Data pruning notifications, described in "Configuring Database Event Limits" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*. (Configure this setting under **System** > **Configuration** > **Database** in the FMC 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 FMC web interface:
  - Choose SNMP v3 for the **Version**. This protocol supports:
    - Encryption with AES128 and read-only users.
  - Choose an **Authentication Protocol** to secure the connection (MD5 or SHA) and supply a **Password**.
  - Choose DES for the **Privacy Protocol** and supply a **Password**.
  - Supply an **Engine ID** which the system will use to encode messages. We recommend that you use the hexadecimal version of the FMC's IP address. For example, if the FMC has an IP address of 10.1.1.77, use 0a01014D0.

In addition, you should restrict your access list for SNMP access to the specific hosts to which the FMC will send SNMP alerts. (This option appears in the FMC web interface under **System** > **Configuration** > **Access List**. See "Configure an Access List" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.)

The FMC 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 Firepower, the authentication module is not FIPS compliant.

For full information on external alerting, see "External Alerting with Alert Responses" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Protect Audit Logs

The FMC maintains read-only logs of user activity, configured through **System** > **Configuration** > **Audit Log**. To conserve memory resources on the FMC 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 Firepower Management Center Configuration Guide, Version 6.4*.

Secure the Connection to eStreamer

The Event Streamer (eStreamer) allows you to stream several kinds of event data from an FMC to a custom-developed client application. For more information, see the Firepower 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 FMC and the eStreamer client so the data is transmitted securely. Do this in the FMC web interface under **System** > **Integration** > **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 Firepower Management Center Configuration Guide, Version 6.4*.

Block Third-Party Database Access

Ensure that third party client applications do not have access to the FMC database; in the FMC web interface, under **System** > **Configuration** > **External Database Access**, be sure the **Allow External Database Access** checkbox is unchecked. For more information, see "External Database Access Settings" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Customize the Login Banner

The system login page is likely to be seen by people both with and without authorized access to the FMC. Customize your login banner so it displays only the information appropriate for anyone to see. On the FMC web interface, use **System** > **Configuration** > **Login Banner**. For full information see "Login Banners" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

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

Firepower 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 FMC 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 Firepower, 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 8.

Note Firepower 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 Firepower Management Center Configuration Guide, Version 6.4*.

Note Firepower can use also RADIUS servers to supply a VPN capability for your network. For more information, see "Firepower Threat Defense VPN" in the *Cisco Firepower Management Center Configuration Guide, Version 6.4*.

Securing Connections with Active Directory and LDAP Servers

Firepower 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 Firepower Management Center Configuration Guide, Version 6.4*.

When you create a realm (**System** > **Integration** > **Realms** in the FMC 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 FMC 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.

Harden Supporting Components

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