

Security Certifications Compliance

The following topics describe how to configure your system to comply with security certifications standards:

- Security Certifications Compliance Modes, on page 1
- Security Certifications Compliance Characteristics, on page 2
- Security Certifications Compliance Recommendations, on page 2
- Enable Security Certifications Compliance, on page 3

Security Certifications Compliance Modes

Your organization might be required to use only equipment and software complying with security standards established by the U.S. Department of Defense and global certification organizations. The following security certifications standards are supported:

- Common Criteria (CC): a global standard established by the international Common Criteria Recognition Arrangement, defining properties for security products
- Unified Capabilities Approved Products List (UCAPL): 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 Department of Defense Information Network Approved Products List (DODIN APL). References to UCAPL in this documentation and the FMC web interface can be interpreted as references to DODIN APL.

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

You can enable security certifications compliance in CC mode or UCAPL mode. Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. For more information on hardening procedures, refer to the guidelines for this product provided by the certifying entity.

Caution After you enable this setting, you cannot disable it. If you need to take an appliance out of CC or UCAPL mode, you must reimage.

Security Certifications Compliance Characteristics

The following table describes behavior changes when you enable CC or UCAPL mode. (Restrictions on login accounts refers to command line or shell access, not web interface access.)

System Change	CC Mode	UCAPL Mode
FIPS compliance is enabled.	Yes	Yes
The system does not allow remote storage for backups or reports.	Yes	Yes
The system starts an additional system audit daemon.	No	Yes
The system boot loader is secured.	No	Yes
The system applies additional security to login accounts.	No	Yes
The system disables the reboot key sequence Ctrl-Alt-Del.	No	Yes
The system enforces a maximum of ten simultaneous login sessions.	No	Yes
The system does not support exporting event data using eStreamer.	Yes	Yes
The system applies more stringent safeguards for login accounts: • Passwords must be at least fifteen alphanumeric characters of mixed case and must include at least one numeric character. • Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters. • The system locks out a user after three failed login attempts in a row. In this case, the password must be reset by an administrator. • The system stores password history.	No	Yes

Security Certifications Compliance Recommendations

Cisco recommends that you observe the following best practices when using a system with security certifications compliance enabled:

- To enable security certifications compliance in your deployment, enable it first on the Firepower Management Center, then enable it in the same mode on all managed devices.



Caution The Firepower Management Center will not receive event data from a managed device unless both are operating in the same security certifications compliance mode.

- For all users, enable password strength checking and set the minimum password length to the value required by the certifying agency.

- If you are using Firepower Management Centers in a high-availability configuration, configure them both to use the same security certifications compliance mode.
- Do not configure the system to use any of the following features:
  - Email reports, alerts, or data pruning notifications.
  - Nmap Scan, Cisco IOS Null Route, Set Attribute Value, or ISE EPS remediations.
  - Remote storage for backups or reports.
  - Third-party client access to the system database.
  - External notifications or alerts transmitted via email (SMTP), SNMP trap, or syslog.
  - Audit log messages transmitted to an HTTP server or to a syslog server without using SSL certificates to secure the channel between the appliance and the server.
  - Exporting event data to an external client using eStreamer.
- Do not enable external authentication using LDAP or RADIUS in deployments using CC mode.
- Do not enable CACs in deployments using CC mode.
- Disable access to the Firepower Management Center and managed devices via the Firepower REST API in deployments using CC or UCAPL mode.
- Enable CACs in deployments using UCAPL mode.

Note The Firepower System does not support CC or UCAPL mode for classic devices in stacks or high availability pairs.

Enable Security Certifications Compliance

This configuration applies to either a Firepower Management Center or a Classic managed device:

- For the Firepower Management Center, this configuration is part of the system configuration.
- For a managed device, you apply this configuration from the FMC as part of a platform settings policy.

In either case, the configuration does not take effect until you save your system configuration changes or deploy the shared platform settings policy.

Caution After you enable this setting, you cannot disable it. If you need to take the appliance out of CC or UCAPL mode, you must reimage.

Before you begin

- We recommend you register all devices that you plan to be part of your deployment to the FMC before enabling security certifications compliance on any appliances.

- You must be an Admin user to perform this task.

Procedure

Step 1 Depending on whether you are configuring an FMC or a managed device:

- FMC: Choose **System** > **Configuration**.
- Classic device: Choose **Devices** > **Platform Settings** and create or edit a Firepower policy.

Step 2 Click **UCAPL/CC Compliance**.

Note Appliances reboot when you enable UCAPL or CC compliance. The FMC reboots when you save the system configuration; managed devices reboot when you deploy configuration changes.

Step 3 To *permanently* enable security certifications compliance on the appliance, you have two choices:

- To enable security certifications compliance in Common Criteria mode, choose **CC** from the drop-down list.
- To enable security certifications compliance in Unified Capabilities Approved Products List mode, choose **UCAPL** from the drop-down list.

Step 4 Click **Save**.

What to do next

- If you have not already, apply Control and Protection licenses to all Classic devices in your deployment.
- Establish additional configuration changes as described in the guidelines for this product provided by the certifying entity.
- Deploy configuration changes; see Deploy Configuration Changes.