

Security certifications compliance

These 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 4

Security certifications compliance modes

A security certifications compliance mode refers to a set of security standards established by the U.S. Department of Defense and global certification organizations. Organizations must use only equipment and software that comply with these standards.

Security certification standards

Secure Firewall supports compliance with these security certifications standards:

- **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 Cloud-Delivered Firewall Management Center web interface can be interpreted as references to DODIN APL.

- **Federal Information Processing Standards (FIPS) 140**: A requirements specification for encryption modules used in secure systems.

Note Cloud-Delivered Firewall Management Center does not provide CC, UCAPL, or FIPS compliance modes as administrator-selectable. You must select FedRAMP compliance during tenant provisioning, which enforces STIG-oriented hardening and FIPS cryptographic controls.

Organizations can enable security certifications compliance in CC mode or UCAPL mode for their managed devices. Enabling these modes does not guarantee compliance with every requirement of the selected security mode. For more information on hardening procedures, refer to the product guidelines provided by the certifying entity.

Caution After you enable a security certifications compliance mode, you cannot disable it. To remove an appliance from CC or UCAPL mode, you must reimage the appliance.

Security certifications compliance characteristics

Enabling CC or UCAPL modes result in certain changes to system behaviors and compliance characteristics on the managed devices. Restrictions on login accounts apply to command line access. These restrictions do not apply to web interface access.

Cloud-Delivered Firewall Management Center

Cloud-Delivered Firewall Management Center for a FedRAMP tenant has these behaviour and compliance characteristics:

- Applicable FIPS-mode cryptographic controls and startup self-tests are enabled.
- The system does not allow remote storage for backups or reports.
- The `admin` user is locked out after a maximum number of failed login attempts configurable through the web interface.
- The system automatically rekeys an SSH session with an appliance:
  - After a key has been in use for one hour of session activity.
  - After a key has been used to transmit 1 GB of data over the connection.
- The system performs a file system integrity check (FSIC) at boot-time and reports FSIC failures.

Managed Devices

System Change	Classic Managed Devices		Secure Firewall Threat Defense	
	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode
Applicable FIPS-mode cryptographic controls and startup self-tests are enabled.	Yes	Yes	Yes	Yes

System Change	Classic Managed Devices		Secure Firewall Threat Defense	
	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode
The system does not allow remote storage for backups or reports.	Not applicable	Not applicable	Not applicable	Not applicable
The system starts an additional system audit daemon.	No	Yes	No	No
The system boot loader is secured.	No	Yes	No	No
The system applies additional security to login accounts.	No	Yes	No	No
The system disables the reboot key sequence Ctrl+Alt+Del.	No	Yes	No	No
Passwords must be at least 14 characters long, and must consist of alphanumeric characters of mixed case and must include at least one numeric character and one non-alphanumeric character.	No	Yes	No	No
The minimum required password length for the local `admin` user can be configured using the local device CLI.	No	No	Yes	Yes
Passwords cannot be a word that appears in a dictionary nor include more than two consecutive occurrences of the same character.	No	Yes	No	No
The system locks out users other than `admin` after three failed login attempts in a row. In this case, the password must be reset by an administrator.	No	Yes	No	No
The system stores password history by default.	No	Yes	No	No
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the web interface.	Yes	Yes	—	—
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the local appliance CLI.	Yes, regardless of security certifications compliance enablement.	Yes, regardless of security certifications compliance enablement.	Yes	Yes
The system automatically rekeys an SSH session with an appliance: • After a key has been in use for one hour of session activity • After a key has been used to transmit 1 GB of data over the connection	Yes	Yes	Yes	Yes
The system performs a file system integrity check (FSIC) at boot-time. If the FSIC fails, Secure Firewall software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.	Yes	Yes	Yes	Yes

Security certifications compliance recommendations

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

- For all users, enable password strength checking and set the minimum password length to the value required by the certifying agency.
- When you configure Firewall Threat Defense on a Firepower 4100/9300 to operate in CC or UCAPL mode, you should also configure the Firepower 4100/9300 to operate in CC mode. For more information, see the *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide*.

Do not configure the system to use these features:

- Email reports, alerts, or data pruning notifications.
- Nmap Scan, Cisco IOS Null Route, Set Attribute Value, or ISE EPS remediations.
- 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.

Configure authentication and access settings appropriately for your security certifications compliance mode.

- 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 Cloud-Delivered Firewall Management Center FedRAMP tenant using the REST APIs.
- Disable access to the managed devices via the Secure Firewall REST API in deployments using CC or UCAPL mode.
- Enable CACs in deployments using UCAPL mode.
- Do not configure SSO in deployments using CC mode.

The system does not support CC or UCAPL mode for:

- Firewall Threat Defense clustering is not supported in UCAPL mode. CC mode clustering is supported only on certain releases of Firewall Threat Defense, and every cluster member must use the same compliance mode.
- Firewall Threat Defense container instances on the Firepower 4100/9300.
- Exporting event data to an external client using eStreamer.

Appliance hardening

To further harden your system, see the latest versions of the *Cisco Secure Firewall Management Center Hardening Guide* and the *Cisco Secure Firewall Threat Defense Hardening Guide*.

Refer to these topics for configuration steps:

Identity and access management

- Users

Monitoring, Auditing, and Compliance

- Security certifications compliance, on page 1

System and Network Configuration

- Licenses
- *SNMP* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Site-to-Site VPNs for Firewall Threat Defense* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *SMTP Server* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Configure SNMP for FXOS* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Configure Dynamic DNS* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Remote Access VPN* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *FlexConfig Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*

Alerting and Device-Level Security

- Create an email alert response
- Configure email alerting for intrusion events
- Create an SNMP alert response
- *Configure NTP Time Synchronization for Threat Defense* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *About Configuring Syslog* in the *Cisco Secure Firewall Management Center Device Configuration Guide*

Protect your network

This section provides links to features that you can configure to enhance and protect your network security. Refer to each feature's documentation for detailed configuration guidance.

- *Access Control Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- *Security Intelligence* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Getting Started with Intrusion Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Tuning Intrusion Policies Using Rules* in the *Cisco Secure Firewall Management Center Device Configuration Guide*

- *Custom Intrusion Rules* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- Intrusion rule updates
- *Transport and Network Layer Preprocessors* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Specific Threat Detection* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Application Layer Preprocessors* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Device Management* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- Updates