

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 3
- Enable security certifications compliance, on page 6

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 Secure 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.

Organizations can enable security certifications compliance in CC mode or UCAPL mode . 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. This table describes such changes to system behaviour.

System Change	Secure Firewall Management Center		Classic Managed Devices		Secure Firewall Threat Defense	
	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode
FIPS compliance is enabled.	Yes	Yes	Yes	Yes	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	No	Yes	No	No
The system boot loader is secured.	No	Yes	No	Yes	No	No
The system applies additional security to login accounts.	No	Yes	No	Yes	No	No
The system disables the reboot key sequence Ctrl+Alt+Del.	No	Yes	No	Yes	No	No
The system enforces a maximum of ten simultaneous login sessions.	No	Yes	No	Yes	No	No
Passwords must be at least 15 characters long, and must consist of alphanumeric characters of mixed case and must include at least one numeric character.	No	Yes	No	Yes	No	No
The minimum required password length for the local `admin` user can be configured using the local device CLI.	No	No	No	No	Yes	Yes
Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.	No	Yes	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	Yes	No	No
The system stores password history by default.	No	Yes	No	Yes	No	No

System Change	Secure Firewall Management Center		Classic Managed Devices		Secure Firewall Threat Defense	
	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the web interface.	Yes	Yes	Yes	Yes	—	—
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the local appliance CLI.	No	No	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	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	Yes	Yes

Security certifications compliance recommendations

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

- Enable security certifications compliance first on the Firewall Management Center, then enable it in the same mode on all managed devices.
- The Firewall 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.
- To use Firewall Management Centers in a high-availability configuration, configure them both to use the same security certifications compliance mode before forming the high availability pair.

- 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.
- Remote storage for backups or reports.
- 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 Firewall Management Center and 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 non-bundled platforms like Firepower 4100/9300 in cluster mode.
- Cluster creation is supported exclusively on the Firewall Management Center. Convert bundled platforms, such as Firewall Management Center Virtual, and Secure Firewall 3100/4200, to CC mode before initiating cluster creation. After you create and provision a cluster using Firewall Management Center, you cannot change from CC mode to Normal mode.
- The system supports CC mode for bundled platforms, such as Secure Firewall 3100/4200 in cluster mode running Version 7.4.7, 7.6.7, 7.7.20, 10.1.0, 10.5.0, and later.

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
- Custom user roles for the web interface
- Add or edit an internal user
- Logging into the Management Center

- Session timeouts

Monitoring, Auditing, and Compliance

- Audit and Syslog
- Audit logs
- Audit log certificates
- Security certifications compliance, on page 1

System and Network Configuration

- Licenses
- Time synchronization
- DNS caches
- Access lists
- HTTPS certificates
- Scheduling
- Configure SSH for remote storage
- *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*
- *Get Started with Snort 3 Intrusion Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Tune Intrusion Policies Using Rules* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- *Custom Rules in Snort 3* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- Intrusion rule updates
- *Application Layer Preprocessors* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- Audit and Syslog
- Intrusion Events
- Event Search
- Workflows
- *Device Management* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
- Login banners
- Updates

Enable security certifications compliance

Enable security certifications compliance to meet regulatory requirements for Common Criteria (CC) or Unified Capabilities Approved Products List (UCAPL) certification.

This configuration applies to either a Secure Firewall Management Center or managed device:

- For the Secure Firewall Management Center, this configuration is part of the system configuration.
- For a managed device, you apply this configuration from the Firewall Management Center 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. To disable CC or UCAPL mode, you must reimage the appliance.

Before you begin

- We recommend registering all devices that will be part of your deployment to the Firewall Management Center before enabling security certifications compliance on any appliances.
- Secure Firewall Threat Defense devices cannot use an evaluation license; your Smart Software Manager account must be enabled for export-controlled features.
- Secure Firewall Threat Defense devices must be deployed in routed mode.
- You must have administrative privileges to perform this task.

Procedure

Step 1 Depending on whether you are configuring a Firewall Management Center or a managed device:

- Firewall Management Center: Choose **Administration** > **Configuration**.
- Firewall Threat Defense device: Choose **Devices** > **Platform Settings** and create or edit a Secure Firewall Threat Defense policy.

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

Note Appliances reboot when you enable UCAPL or CC compliance. The Firewall Management Center 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

- Establish additional configuration changes as described in the guidelines for this product provided by the certifying entity.
- Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.