Security Certifications Compliance

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

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. Secure Firewall supports compliance with the following 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

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 access, not web interface access.)

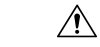
System Change	Secure Firewall Management Center		Classic Managed Devices		Secure Firewall Threat Defense	
	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode	CC Mode	UCAPL Mode
FIPS compliance is enabled.	Yes	Yes	Yes	Yes	Yes	Yes
The system does not allow remote storage for backups or reports.	Yes	Yes	—	—	—	—
The 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
The `admin` user can be locked out after a maximum number of failed login attempts configurable through the web interface.	Yes	Yes	Yes	Yes	—	—

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 local appliance CLI.	No	No	Yes, regardless of security certifications compliance enablement.	Yes, regardless of security certifications compliance enablement.	Yes	Yes
The system automtically 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:

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



Caution The Secure 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 Secure 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 Secure 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 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.
- 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 Secure 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.

Note The system does not support CC or UCAPL mode for:

- Secure Firewall Threat Defense devices in clusters
- Secure Firewall Threat Defense container instances on the Firepower 4100/9300
- Exporting event data to an external client using eStreamer.

Appliance Hardening

For information about features you can use 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*, as well as the following topics within this document:

- Licenses
- Users
- Logging into the Management Center
- Audit Log
- Audit Log Certificate
- Time Synchronization

- *Configure NTP Time Synchronization for Threat Defense* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Creating an Email Alert Response
- Configuring Email Alerting for Intrusion Events
- *Configure SMTP* in the Cisco Secure Firewall Management Center Device Configuration Guide
- *About SNMP for the Firepower 1000/2100* in the Cisco Secure Firewall Management Center Device Configuration Guide
- *Configure SNMP* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Creating an SNMP Alert Response
- *Configure Dynamic DNS* in the Cisco Secure Firewall Management Center Device Configuration Guide
- DNS Cache
- Audit and Syslog
- Access List
- Security Certifications Compliance, on page 1
- Configure SSH for Remote Storage
- Audit Log Certificate
- HTTPS Certificates
- Customize User Roles for the Web Interface
- Add or Edit an Internal User
- Session Timeout
- *About Configuring Syslog* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Schedule Management Center Backups
- *Site-to-Site VPNs for Threat Defense* 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

Protecting Your Network

See the following topics to learn about features you can configure to protect your network:

- Access Control Policies
- *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

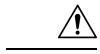
- *Tuning Intrusion Policies Using Rules* in the Cisco Secure Firewall Management Center Device Configuration Guide
- *Custom Intrusion Rules* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Update Intrusion Rules
- *Transport and Network Layer Preprocessors* in the Cisco 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
- Audit and Syslog
- Intrusion Events
- Event Search
- Workflows
- *Device Management* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Login Banner
- Updates

Enable Security Certifications Compliance

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 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. 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 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 be an Admin user to perform this task.

Procedure

Step 1 Depending on whether you are configuring a management center or a managed device:

- management center: Choose **System** (⚙) > **Configuration**.
- 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 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.