安全认证合规性

以下主题介绍如何配置系统来符合安全认证标准：

安全认证合规性模式

组织只能使用符合由美国国防部和全球认证组织制定的安全标准的设备和软件。Firepower 支持符合以下安全认证标准：

- 通用标准 (CC)：国际共同标准承认协定建立的全球标准，用于定义安全产品的属性
- 统一功能获批产品列表 (UCAPL)：符合美国国防信息系统机构 (DISA) 建立的安全要求的产品列表

注释 美国政府已将统一功能获批产品列表 (UCAPL) 的名称改为国防部信息网络获批产品列表 (DODIN APL)。本文档和 Cisco Secure Firewall Management CenterWeb 接口中对 UCAPL 的引用可以解释为对 DODIN APL 的引用。

- 联邦信息处理标准 (FIPS) 140：加密模块的要求规范

可以在 CC 模式或 UCAPL 模式下启用安全认证合规性。启用安全认证合规性不保证严格符合所选安全模式的所有要求。有关强化操作步骤的详细信息，请参阅由认证实体提供的此产品的相关准则。

注意 启用此设置后，您将无法将其禁用。如果设备需要退出 CC 或 UCAPL 模式，必须重新映像。

安全认证合规性特征

下表描述了启用 CC 或 UCAPL 模式时的行为更改。（对登录账户的限制是指命令行访问，而不是 Web 界面访问。）

系统更改	Cisco Secure Firewall Management Center		经典受管设备		Cisco Secure Firewall Threat Defense	
	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式
启用 FIPS 合规性。	兼容	兼容	兼容	兼容	兼容	兼容
系统不允许远程存储备份或报告。	兼容	兼容	—	—	—	—
系统启动额外的系统审核后台守护程序。	不兼容	是	否	是	否	不兼容
系统引导加载程序受到保护。	不兼容	是	否	是	否	不兼容
系统对登录帐户应用额外保护。	不兼容	是	否	是	否	不兼容
系统禁用重启按键序列 Ctrl+Alt+Del。	不兼容	是	否	是	否	不兼容
系统最多同时执行 10 个登录会话。	不兼容	是	否	是	否	不兼容
密码必须至少包含 15 个字符，且必须由大小写混合的字母数字字符组成，还必须至少包含一个数字字符。	不兼容	是	否	是	否	不兼容
可以使用本地设备 CLI 配置对本地 `admin` 用户要求的最低密码长度。	不兼容	不兼容	不兼容	不兼容	兼容	兼容
密码中包含的单词不能是在词典中出现过的单词或包含连续的重复字符。	不兼容	是	否	是	否	不兼容
连续三次登录尝试失败后，系统会锁定除 `admin` 以外的用户。在这种情况下，管理员必须重置密码。	不兼容	是	否	是	否	不兼容
默认情况下，系统会存储密码历史记录。	不兼容	是	否	是	否	不兼容
在失败次数超过可通过 Web 界面配置的最大失败登录尝试次数之后，`admin` 用户会被锁定。	兼容	兼容	兼容	兼容	—	—
在失败次数超过可通过本地设备 CLI 配置的最大失败登录尝试次数之后，`admin` 用户会被锁定。	不兼容	不兼容	是，无论是否启用安全认证合规性。	是，无论是否启用安全认证合规性。	兼容	兼容

系统更改	Cisco Secure Firewall Management Center		经典受管设备		Cisco Secure Firewall Threat Defense	
	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式	CC 模式	UCAPL 模式
系统会自动为与设备进行的 SSH 会话重新生成密钥： • 某个密钥用于会话活动达一小时后 • 某个密钥用于通过连接传输 1 GB 的数据后	兼容	兼容	兼容	兼容	兼容	兼容
系统在启动时执行文件系统完整性检查(FSIC)。如果 FSIC 失败，则 Firepower 软件无法启动，远程 SSH 访问会被禁用，您只能通过本地控制台访问该设备。如果出现此问题，请联系思科 TAC。	兼容	兼容	兼容	兼容	兼容	兼容

安全认证合规性建议

在使用启用安全认证合规性的系统时，思科建议您遵循以下最佳实践：

- 要在部署中启用安全认证合规性，请首先在 Cisco Secure Firewall Management Center上将其启用，然后在所有托管设备上的同一模式下将其启用。

⚠

注意 Cisco Secure Firewall Management Center不会接受来自受管设备的事件数据，除非两者在同一安全认证合规性模式下运行。

- 对于所有用户，启用密码强度检查，并将最小密码长度设置为认证机构要求的值。
- 如果您在高可用性配置下使用 Cisco Secure Firewall Management Center，请将它们配置为使用同一安全认证合规性模式。
- 如果将 Firepower 4100/9300机箱上的 Cisco Secure Firewall Threat Defense配置为以 CC 或 UCAPL 模式运行，还应将 Firepower 4100/9300 配置为以 CC 模式运行。有关详细信息，请参阅 *Cisco Firepower 4100/9300 FXOS Firepower* 机箱管理器配置指南。
- 请勿将系统配置为使用以下任意一种功能：
  - 邮件报告、警报或数据修剪通知。
  - Nmap 扫描、思科 IOS 空路由、设置属性值或 ISE EPS 补救。
  - 备份或报告的远程存储。
  - 第三方客户端访问系统数据库。

  - 通过邮件 (SMTP) 传送的外部通知或警报、SNMP 陷阱或系统日志。
  - 审核未使用 SSL 证书传输到 HTTP 服务器或系统日志服务器的日志消息，以保护设备和服务器之间的通道。

- 请勿在使用 CC 模式的部署中使用 LDAP 或 RADIUS 启用外部身份验证。
- 请勿使用 CC 模式在部署中启用 CAC。
- 使用 CC 或 UCAPL 模式在部署中通过 Firepower REST API 禁用访问 Cisco Secure Firewall Management Center和受管设备。
- 使用 UCAPL 模式在部署中启用 CAC。
- 请勿使用 CC 模式在部署中配置 SSO。
- 请勿将 Cisco Secure Firewall Threat Defense设备配置为高可用性对，除非它们都使用相同的安全认证合规模式。

注释 系统对于以下各项不支持 CC 或 UCAPL 模式：

- 集群中的 Cisco Secure Firewall Threat Defense设备
- Cisco Secure Firewall Threat Defense 容器实例，位于 Firepower 4100/9300
- 使用 eStreamer 将事件数据导出到外部客户端。

设备强化

有关可用于进一步强化系统的功能的信息，请参阅最新版本的 *Cisco Firepower* 管理中心强化指南 和 *Cisco Cisco Secure Firewall Threat Defense* 强化指南，以及本文档中的以下主题：

- 许可证
- 管理中心 的
- 登录到管理中心
- 审核日志
- 审核日志 ID证书
- 时间同步
- 在 《Cisco Secure Firewall Management Center 设备配置指南》中为威胁防御配置 NTP 时间同步
- 创建邮件警报响应
- 配置入侵事件的邮件警报
- 在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SMTP*

- 关于在 《Cisco Secure Firewall Management Center 设备配置指南》中适用于 *Firepower 1000/2100* 的 *SNMP*
- 在《Cisco Secure Firewall Management Center 设备配置指南》中配置 *SMTP*
- 创建 SNMP 警报响应
- 《Cisco Secure Firewall Management Center 设备配置指南》中的配置动态 *DNS*
- DNS 缓存
- 审核和系统日志
- 访问列表
- 安全认证合规性， 第 1 页
- 为远程存储配置 SSH
- 审核日志 ID证书
- HTTPS 证书
- 自定义 Web 界面的用户角色
- 添加或编辑内部用户
- 会话超时
- 关于在 《Cisco Secure Firewall Management Center 设备配置指南》中配置系统日志
- 计划 管理中心 备份
- 《Cisco Secure Firewall Management Center 设备配置指南》中的适用于 威胁防御的站点间 *VPN*
- 《Cisco Secure Firewall Management Center 设备配置指南》中的远程接入 *VPN*
- 《Cisco Secure Firewall Management Center 设备配置指南》中的*FlexConfig* 策略

保护您的网络

请参阅以下主题以了解可配置用于网络保护的功能：

- 访问控制策略
- 《Cisco Secure Firewall Management Center 设备配置指南》安全情报
- 《Cisco Secure Firewall Management Center 设备配置指南》侵策略使用入门
- 使用《Cisco Secure Firewall Management Center 设备配置指南》规则调整入侵策略
- 自定义《Cisco Secure Firewall Management Center 设备配置指南》入侵规则
- 更新入侵规则
- 《Cisco Secure Firewall Management Center 设备配置指南》入侵事件日志记录的全局限制

- 《Cisco Secure Firewall Management Center 设备配置指南》传输层和网络层预处理器
- 《Cisco Secure Firewall Management Center 设备配置指南》具体威胁检测
- 《Cisco Secure Firewall Management Center 设备配置指南》应用层预处理器
- 审核和系统日志
- 入侵事件
- 事件搜索
- 工作流程
- 《Cisco Secure Firewall Management Center 设备配置指南》设备管理
- 登录标识
- 更新

启用安全认证合规

此配置适用于 Cisco Secure Firewall Management Center 或托管设备：

- 对于 Cisco Secure Firewall Management Center，此配置是系统配置的一部分。
- 对于托管设备，将 管理中心 中的配置作为平台设置策略的一部分进行应用。

无论采用何种方式，配置在您保存系统配置更改或部署共享平台设置策略后才会生效。

注意 启用此设置后，您将无法将其禁用。如果设备需要退出 CC 或 UCAPL 模式，必须重新映像。

开始之前

- 在任何设备上启用安全认证合规性之前，我们建议注册您计划让其成为部署到管理中心的一部分的所有设备。
- Cisco Secure Firewall Threat Defense 设备不能使用评估许可证；您的 智能软件管理器 账户必须启用出口管制功能。
- Cisco Secure Firewall Threat Defense 设备必须在路由模式下部署。
- 您必须是管理员用户才能执行此任务。

过程

步骤 1 根据配置的是 管理中心 还是典型托管设备，请执行以下操作：

- 管理中心： 选择 **系统**（⚙）> **配置**。
- 威胁防御 设备：选择 **设备** > **平台设置** 并创建或编辑 Cisco Secure Firewall Threat Defense 策略。

步骤 2 点击 **UCAPL/CC 合规性 (UCAPL/CC Compliance)**。

注释 在您启用UCAPL或CC合规性时设备会重启。管理中心在您保存系统配置时重启；托管设备在您部署配置更改时重启。

步骤 3 要在设备上永久启用安全认证合规性，您有两种选择：

- 要在通用条件模式中启用安全认证合规性，请从下拉列表中选择 **CC**。
- 要在统一功能获批产品列表模式中启用安全认证合规性，请从下拉列表中选择 **UCAPL**。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 根据认证实体提供的本产品指南中的说明，确定其他配置更改。
- 部署配置更改；请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。