Conformité des certifications de sécurité

Les rubriques suivantes décrivent comment configurer votre système pour se conformer aux normes de certification de sécurité :

Modes de conformité des certifications de sécurité

Votre entreprise peut être tenue d'utiliser uniquement de l'équipement et des logiciels conformes aux normes de sécurité établies par le département de la Défense des États-Unis et par des organismes de certification mondiaux. Firepower prend en charge la conformité aux normes de certification de sécurité suivantes :

- Common Criteria (CC) : norme mondiale établie dans le cadre de l'accord international de reconnaissance des critères communs, qui définit les propriétés des produits de sécurité.
- Liste unifiée des produits approuvés (UCAPL) : une liste des produits répondant aux exigences de sécurité établies par la Defense Information Systems Agency (DISA) des États-Unis

Remarque Le gouvernement américain a changé le nom de la liste unifiée des capacités approuvées (UCAPL) pour « liste des produits approuvés par le réseau d'information du ministère de la Défense » (DODIN APL). Les références à UCAPL dans cette documentation et dans l'interface Web Cisco Secure Firewall Management Center peuvent être interprétées comme des références à DODIN APL.

- Federal Information Processing Standards (FIPS) 140 : une spécification des exigences pour les modules de chiffrement

Vous pouvez activer la conformité des certifications de sécurité en mode CC ou en mode UCAPL. L'activation de la conformité aux certifications de sécurité ne garantit pas la stricte conformité de toutes les exigences du mode de sécurité sélectionné. Pour en savoir plus sur le renforcement des procédures, consultez les directives pour ce produit fournies par l'entité de certification.

⚠

Mise en garde Après avoir activé ce paramètre, vous ne pouvez pas le désactiver. Si vous devez sortir un périphérique du mode CC ou UCAPL, vous devez effectuer une réinitialisation.

Caractéristiques de conformité des certifications de sécurité

Le tableau suivant décrit les changements de comportement lorsque vous activez le mode CC ou UCAPL. (Les restrictions sur les comptes de connexion font référence à la ligne de commande , et non à l'accès à l'interface Web.)

Modification du système	Cisco Secure Firewall Management Center		Périphériques gérés classiques		Cisco Secure Firewall Threat Defense	
	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL
La conformité aux normes FIPS est activée.	Oui	Oui	Oui	Oui	Oui	Oui
Le système n'autorise pas le stockage à distance pour les sauvegardes ou les rapports.	Oui	Oui	—	—	—	—
Le système démarre un daemon d'audit du système supplémentaire.	Non	Oui	Non	Oui	Non	Non
Le chargeur de démarrage du système est sécurisé.	Non	Oui	Non	Oui	Non	Non
Le système applique une sécurité supplémentaire aux comptes de connexion.	Non	Oui	Non	Oui	Non	Non
Le système désactive la séquence de touches de redémarrage Ctrl + Alt + Suppr.	Non	Oui	Non	Oui	Non	Non
Le système applique un maximum de dix sessions de connexion simultanées.	Non	Oui	Non	Oui	Non	Non
Les mots de passe doivent comporter au moins 15 caractères, et doivent être composés de caractères alphanumériques, de casses minuscules et doivent inclure au moins un caractère numérique.	Non	Oui	Non	Oui	Non	Non
La longueur minimale requise du mot de passe pour l'utilisateur `admin` local peut être configurée à l'aide de l'interface de ligne de commande du périphérique local.	Non	Non	Non	Non	Oui	Oui
Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.	Non	Oui	Non	Oui	Non	Non

Modification du système	Cisco Secure Firewall Management Center		Périphériques gérés classiques		Cisco Secure Firewall Threat Defense	
	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL	Mode CC	Mode UCAPL
Le système verrouille les utilisateurs autres que `admin` après trois tentatives de connexion infructueuses de suite. Dans ce cas, le mot de passe doit être réinitialisé par un administrateur.	Non	Oui	Non	Oui	Non	Non
Le système stocke l'historique des mots de passe par défaut.	Non	Oui	Non	Oui	Non	Non
L'utilisateur `admin` peut être verrouillé après un nombre maximal de tentatives de connexion infructueuses configurables au moyen de l'interface Web.	Oui	Oui	Oui	Oui	—	—
L'utilisateur `admin` peut être verrouillé après un nombre maximal de tentatives de connexion infructueuses configurables par l'interface de ligne de commande du périphérique local.	Non	Non	Oui, quelle que soit l'activation de la conformité des certifications de sécurité.	Oui, quelle que soit l'activation de la conformité des certifications de sécurité.	Oui	Oui
Le système redemande la clé automatiquement pour une session SSH avec un appareil : • Après l'utilisation d'une clé pendant une heure d'activité de session • Lorsqu'une clé a été utilisée pour transmettre 1 Go de données sur la connexion	Oui	Oui	Oui	Oui	Oui	Oui
Le système effectue une vérification de l'intégrité du système de fichiers (FSIC) au démarrage. Si le FSIC échoue, le logiciel Firepower ne démarre pas, l'accès SSH à distance est désactivé et vous ne pouvez accéder au périphérique que depuis la console locale. Si cela se produit, communiquez avec le TAC de Cisco.	Oui	Oui	Oui	Oui	Oui	Oui

Recommandations en matière de conformité aux certifications de sécurité

Cisco vous recommande d'appliquer les bonnes pratiques suivantes lorsque vous utilisez un système pour lequel la conformité des certifications de sécurité est activée :

- Pour activer la conformité aux certifications de sécurité dans votre déploiement, activez-la d'abord sur Cisco Secure Firewall Management Center, puis activez-la dans le même mode sur tous les périphériques gérés.

Mise en garde Le Cisco Secure Firewall Management Center ne recevra pas de données d'événement d'un périphérique géré, sauf si les deux fonctionnent dans le même mode de conformité des certifications de sécurité.

- Pour tous les utilisateurs, activez la vérification de la force du mot de passe et définissez la longueur minimale de ce dernier à la valeur requise par l'organisme de certification.
- Si vous utilisez des Cisco Secure Firewall Management Centerdans une configuration à haute disponibilité, configurez les deux pour utiliser le même mode de conformité des certifications de sécurité.
- Lorsque vous configurez Cisco Secure Firewall Threat Defense sur un Firepower 4100/9300 pour fonctionner en mode CC ou UCAPL, vous devez également configurer Firepower 4100/9300 pour qu'il fonctionne en mode CC. Pour en savoir plus, reportez-vous au *Guide de configuration de Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager*.
- Ne configurez pas le système pour utiliser l'une des fonctionnalités suivantes :
  - Envoyer par courriel des rapports, alertes ou notifications de nettoyage des données.
  - Analyse Nmap, routage Cisco IOS nul, valeur d'attribut définie ou corrections de ISE et d'EPS.
  - Stockage à distance pour les sauvegardes ou les rapports.
  - Accès client tiers à la base de données du système.
  - Notifications ou alertes externes transmises par courriel (SMTP), déroutement SNMP ou syslog.
  - Messages du journal d'audit transmis à un serveur HTTP ou à un serveur syslog sans utiliser de certificats SSL pour sécuriser le canal entre le périphérique et le serveur.
- N'activez pas l'authentification externe à l'aide de LDAP ou de RADIUS dans les déploiements en mode CC.
- N'activez pas les certificats CAC dans les déploiements qui utilisent le mode CC.
- Désactiver l'accès à Cisco Secure Firewall Management Center et aux périphériques gérés par l'API REST Firepower dans les déploiements faisant appel au mode CC ou UCAPL.
- Activer les certificats CAC dans les déploiements utilisant le mode UCAPL.
- Ne configurez pas la connexion unique SSO dans les déploiements en mode CC.

- Ne configurez pas de périphériques Cisco Secure Firewall Threat Defense dans une paire à haute disponibilité, sauf si les deux systèmes utilisent le même mode de conformité des certifications de sécurité.

Remarque Le système ne prend pas en charge les modes CC ou UCAPL pour :

- des périphériques Cisco Secure Firewall Threat Defense en grappes
- instances de conteneur Cisco Secure Firewall Threat Defense sur le Firepower 4100/9300
- L'exportation de données d'événements vers un client externe à l'aide d'eStreamer.

Renforcement des appareils

Pour en savoir plus sur les fonctionnalités que vous pouvez utiliser pour renforcer votre système, consultez les dernières versions du *guide de durcissement de Cisco Firepower Management Center* et du *Guide sur le renforcement de Cisco Cisco Secure Firewall Threat Defense*, ainsi que les rubriques suivantes dans le document :

- Licences
- Utilisateurs
- *Configurer la synchronisation de l'heure NTP pour Threat Defense* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Création d'une réponse à une alerte par courriel
- Configuration des alertes par courriel pour les incidents d'intrusion
- *Configurer SMTP* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *À propos de SNMP pour les périphériques Firepower 1000/2100* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Configurer SNMP* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Création d'une réponse à une alerte SNMP
- *Configurer le DNS dynamique* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Conformité des certifications de sécurité, à la page 1
- *À propos de la configuration de Syslog* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *VPN de site à site pour Défense contre les menaces* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *VPN d'accès à distance* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- *Politiques FlexConfig* dans le Guide de configuration Cisco Secure Firewall Management Center Device

Protéger votre réseau

Consultez les rubriques suivantes pour en savoir plus sur les fonctionnalités que vous pouvez configurer pour protéger votre réseau :

- Politiques de contrôle d’accès
- *Renseignements sur la sécurité* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Mise en route des politiques de prévention des intrusions* dans le Guide de configuration Cisco Secure Firewall Management Center Device
- Réglage des politiques de prévention des intrusions à l’aide des règles de Guide de configuration Cisco Secure Firewall Management Center Device
- *Règles de prévention des intrusions personnalisées* dans Guide de configuration Cisco Secure Firewall Management Center Device
- Mettre à jour les règles de prévention des intrusions
- Limite globale pour la journalisation des incidents d'intrusion dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Préprocesseurs des couches transport et réseau* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Détection des menaces spécifiques* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Préprocesseurs de couche applicative* dans Guide de configuration Cisco Secure Firewall Management Center Device
- *Gestion des périphériques* dans Guide de configuration Cisco Secure Firewall Management Center Device
- Mises à jour

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.