Paramètres SSL

Paramètres SSL

Configurez les paramètres SSL à l'un des emplacements suivants :

- **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > SSL Settings (Paramètres SSL)**
- **Configuration > Remote Access VPN (VPN d'accès à distance) > Advanced (Avancé) > SSL Settings (Paramètres SSL)**

L'ASA utilise le protocole SSL (Secure Sockets Layer) et le protocole TLS (Transport Layer Security) pour prendre en charge la transmission sécurisée des messages pour ASDM, Clientless SSL VPN, VPN et les sessions basées sur le navigateur. En outre, DTLS est utilisé pour les connexions des clients VPN Secure Client . Le volet SSL Settings (Paramètres SSL) vous permet de configurer les versions SSL et les algorithmes de chiffrement pour les clients et les serveurs. Il vous permet également d'appliquer des points de confiance configurés précédemment à des interfaces spécifiques et de configurer un point de confiance de repli pour les interfaces qui n'ont pas de point de confiance associé.

Remarque Pour la version 9.3(2), SSLv3 a été abandonné. La valeur par défaut est maintenant **tlsv1** au lieu de **any**. Le mot-clé **any** est maintenant obsolète. Si vous choisissez **any**, **sslv3** ou **sslv3**-only, les paramètres sont acceptés avec un avertissement. Cliquez sur **OK** pour continuer. Dans la prochaine version majeure d'ASA, ces mots-clés seront supprimés de l'ASA.

Pour la version 9.4(1), tous les mots-clés SSLv3 ont été supprimés de la configuration ASA et la prise en charge SSLv3 a été supprimée de l'ASA. Si SSLv3 est activé, une erreur de démarrage s'affichera à partir de la commande avec l'option SSLv3. L'ASA reviendra ensuite à l'utilisation par défaut de TLSv1.

Le récepteur mobile Citrix peut ne pas prendre en charge les protocoles TLS 1.1/1.2; veuillez consulter https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf pour connaître la compatibilité

Champs

- **Server SSL Version** (Version SSL du serveur) : spécifiez la version minimale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit en tant que serveur dans la liste déroulante.

N'importe quel	Accepte les messages client hello SSLv2 et négocie la version commune la plus élevée.
SSLv3	Accepte les messages client hello SSLv2 et négocie SSLv3 (ou une version supérieure).
TLS V1	Accepte les messages client hello SSLv2 et négocie TLSv1 (ou version supérieure).
TLSV1.1	Accepte les messages client hello SSLv2 et négocie TLSv1.1 (ou version supérieure).
TLSV1.2	Accepte les messages client hello SSLv2 et négocie TLSv1.2 (ou version supérieure).
TLSV1.3	Accepte les hellos de clients SSLv2 et négocie TLSv1.3 (ou version ultérieure).
DTLSv1	Accepte les messages client hello DTLSv1 et négocie DTLSv1 (ou version supérieure).
DTLS1.2	Accepte les messages client hello DTLSv1.2 et négocie DTLSv1.2 (ou une version supérieure).

Remarque La configuration et l'utilisation de DTLS s'appliquent uniquement aux .

Assurez-vous que la session TLS est aussi sécurisée ou plus sécurisée que la session DTLS en utilisant une version de TLS égale ou supérieure à celle de DTLS. DTLSV1.2 prend en charge TLSV1.2 et TLSV1.3. Toute version TLS peut être utilisée avec DTLS1, car elles sont toutes égales ou supérieures à DTLS 1.

TLSv1.3 nécessite Cisco Secure Client version 5.0 ou ultérieure.

- **Client SSL Version** (Version SSL du client) : précisez la version minimale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme client, dans la liste déroulante. (DTLS non disponible pour le rôle de client SSL)

N'importe lequel	Transmet les messages client hello SSLv3 et négocie SSLv3 (ou version supérieure).
SSL v3	Transmet les messages client hello SSLv3 et négocie SSLv3 (ou version supérieure).
TLS V1	Transmet les messages client hello TLSv1 et négocie TLSv1 (ou version supérieure).
TLSV1.1	Transmet les messages client hello TLSv1.1 et négocie TLSv1.1 (ou version supérieure).
TLSV1.2	Transmet les messages client hello TLSv1.2 et négocie TLSv1.2 (ou version supérieure).
TLSv1.3	Transmet les messages client hello TLSv1.3 (ou version ultérieure).

- **Diffie-Hellmann group to be used with SSL**(Groupe Diffie-Hellman à utiliser avec SSL : choisissez un groupe dans la liste déroulante. Les options disponibles sont Group1 - module de 768 bits, Group2 - module de 1024 bits, Group5 - module de 1536 bits, Group14 - module de 2048 bits, ordre premier de 224 bits, et Group24 - module de 2048 bits, ordre premier de 256 bits. La valeur par défaut est Group2.

- **ECDH group to be used with SSL** (Groupe ECDH à utiliser avec SSL) : choisissez un groupe dans la liste déroulante. Les options disponibles sont Groupe19 – EC 256 bits, Groupe20 – EC 384 bits et Groupe21 – EC 521 bits. La valeur par défaut est Group19.

Remarque Les chiffrements ECDSA et DHE ont la priorité la plus élevée.

- **Encryption** (Chiffrement) : spécifiez la version, le niveau de sécurité et les algorithmes de chiffrement SSL que vous souhaitez prendre en charge. Cliquez sur **Edit** (Modifier) pour définir ou modifier une entrée du tableau à l'aide de la boîte de dialogue Configure Cipher Algorithms/Custom String (Configurer les algorithmes de chiffrement / la chaîne personnalisée). Choisissez le niveau de sécurité du chiffrement SSL, puis cliquez sur **OK**.
  - **Cipher Version** (Version du chiffrement) : répertorie la version du chiffrement que l'ASA prend en charge et utilise pour les connexions SSL.
  - **Cipher Security Level** (Niveau de sécurité du chiffrement) : répertorie les niveaux de sécurité du chiffrement que l'ASA prend en charge et utilise pour les connexions SSL. Choisissez une des options suivantes :

    Tout comprend tous les chiffrements, y compris NULL-SHA.

    Faible comprend tous les chiffrements, sauf NULL-SHA.

    Medium (Moyen) : comprend tous les chiffrements, sauf NULL-SHA, DES-CBC-SHA, RC4-MD5 (valeur par défaut), RC4-SHA et DES-CBC3-SHA.

    High (Élevé) : comprend uniquement AES-256 avec les chiffrements SHA-2 et s'applique uniquement à TLS version 1.2 et aux chiffrements pris en charge par TLS version 1.3.

    Personnalisé comprend un ou plusieurs chiffrements que vous spécifiez dans la zone Algorithmes de chiffrement/chaîne personnalisée. Cette option vous fournit un contrôle total de la suite de chiffrement à l'aide de chaînes de définition de chiffrement OpenSSL.
  - **Cipher Algorithms/Custom String** (Algorithmes de chiffrement/chaîne personnalisée) : répertorie les algorithmes de chiffrement que l'ASA prend en charge et utilise pour les connexions SSL. Pour plus d'informations sur les chiffrements à l'aide d'OpenSSL, consultez https://www.openssl.org/docs/manmaster/man1/ciphers.html

    L'ASA spécifie l'ordre de priorité des chiffrements pris en charge comme suit : d'abord les chiffrements pris en charge uniquement par TLSv1.3/TLSv1.2, puis les chiffrements non pris en charge par TLSv1.1, TLSv1.2 ou TLSv1.3.

Les chiffrements suivants sont pris en charge :

- **Server Name Indication (SNI)** (Indication du nom de serveur) : spécifie le nom de domaine et le point de confiance à associer à ce domaine. Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour définir ou modifier, pour chaque interface, un domaine et un point de confiance à l'aide de la boîte de dialogue Add/Edit Server Name Indication (SNI) (Ajouter/Modifier l'indication du nom de serveur [SNI]).

Chiffre	TLSv1.1/DTLSv1	TLSv1.2 / DTLSV 1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	Non	Non	Oui

Chiffre	TLSv1.1/DTLSv1	TLSv1.2 / DTLSV 1.2	TLSv13
TLS_CHACHA20_POLY1305_SHA256	Non	Non	Oui
TLS_AES_256_GCM_SHA384	Non	Non	Oui
AES128-GCM-SHA256	Non	Oui	Non
AES128-SHA	Oui	oui	Non
AES128-SHA256	Non	Oui	Non
AES256-GCM-SHA384	Non	Oui	Non
AES256-SHA	Oui	oui	Non
AES256-SHA256	Non	Oui	Non
DERS-CBC-SHA	Non	Non	Non
DES-CBC-SHA	Oui	oui	Non
DHE-RSA-AES128-GCM-SHA256	Non	Oui	Non
DHE-RSA-AES128-SHA	Oui	oui	Non
DHE-RSA-AES128-SHA256	Non	Oui	Non
DHE-RSA-AES256-GCM-SHA384	Non	l	Non
DHE-RSA-AES256-SHA	Oui	oui	Non
ECDHE-ECDSA-AES128-GCM-SHA256	Non	Oui	Non
ECDHE-ECDSA-AES128-SHA256	Non	Oui	Non
ECDHE-ECDSA-AES256-GCM-SHA384	Non	Oui	Non
ECDHE-ECDSA-AES256-SHA384	Non	Oui	Non
ECDHE-RSA-AES128-GCM-SHA256	Oui	oui	Non
ECDHE-RSA-AES128-SHA256	Non	Oui	Non
ECDHE-RSA-AES256-GCM-SHA384	Non	Oui	Non
ECDHE-RSA-AES256-SHA384	Non	Oui	Non
NULL-SHA	Non	Non	Non
RC4-MD5	Non	Non	Non
RC4-SHA	Non	Non	Non

Remarque Le tunnel DTLS1.2 fonctionne avec TLSv1.3, cependant, DTLS1.2 ne prend pas en charge les chiffrements TLSv1.3. Le chiffrement pris en charge de priorité la plus élevée est choisi pour le tunnel DTLS1.2.

  - Specify domain (Préciser le domaine) : saisissez le nom de domaine.
  - Select trustpoint to associate with domain (Sélectionner le point de confiance à associer au domaine) : choisissez le point de confiance dans la liste déroulante

- **Certificates** (Certificats) : attribuez les certificats à utiliser pour l'authentification SSL sur chaque interface. Cliquez sur **Edit** (Modifier) pour définir ou modifier le point de confiance pour chaque interface à l'aide de la boîte de dialogue Select SSL Certificate (Sélectionner le certificat SSL).
  - Primary Enrolled Certificate (Certificat inscrit principal) : sélectionnez le point de confiance à utiliser pour les certificats sur cette interface.
  - Load Balancing Enrolled Certificate (Certificat inscrit pour l'équilibrage de charge) : sélectionnez un point de confiance à utiliser pour les certificats lorsque l'équilibrage de charge VPN est configuré.
- **Fallback Certificate** (Certificat de repli) : cliquez pour choisir un certificat à utiliser pour les interfaces auxquelles aucun certificat n'est associé. Si vous choisissez **None** (Aucun), l'ASA utilise la paire de clés et le certificat RSA par défaut.
- **Forced Certification Authentication Timeout** (Délai d'authentification de certification forcée) : configurez le nombre de minutes à attendre avant l'expiration de l'authentification par certificat.
- **Apply** (Appliquer) : cliquez pour enregistrer vos modifications.
- **Reset** (Réinitialiser) : cliquez pour annuler les modifications apportées et rétablir les paramètres SSL aux valeurs précédemment définies.

Paramètres SSL

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.