Notes de mise à jour pour ASDM de Cisco Secure Firewall, 7.19(x)

Première publication : 2022-11-29

Dernière modification : 2024-10-24

Notes de mise à jour pour ASDM de Cisco Secure Firewall, 7.19(x)

Ce document contient des informations sur la version 7.19(x) d'ASDM pour la série Secure Firewall ASA.

Remarques importantes

- **Aucune prise en charge dans l'ASA 9.19(1) et les versions ultérieures pour les Firepower 4110, 4120, 4140, 4150 et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.**L'ASA 9.18(x) est la dernière version prise en charge.
- **ASDM 7.19(1) requiert la version 8u261 d'Oracle Java ou une version ultérieure.**– Avant de passer à ASDM 7.19, assurez-vous de mettre à jour Oracle Java (si utilisé) à la version 8u261 ou plus récente. Cette version prend en charge TLSv1.3, qui est nécessaire pour mettre à jour le lanceur ASDM. OpenJRE n'est pas concerné.
- **Assistant de mise à niveau ASDM**– En raison d'un changement interne, à partir de mars 2022, l'assistant de mise à niveau ne fonctionnera plus avec les versions antérieures à ASDM 7.17(1.150). Vous devez procéder à une mise à niveau manuelle vers la version 7.17(1.150) ou ultérieure pour utiliser l'assistant.

Configuration requise

ASDM nécessite un ordinateur doté d'une unité centrale avec au moins 4 cœurs. Un nombre réduit de cœurs peut entraîner une utilisation élevée de la mémoire.

Exigences ASDM Java

Vous pouvez installer ASDM en utilisant Oracle JRE 8.0 (**asdm-*version*.bin**) ou OpenJRE 1.8.x (**asdm-openjre-*version*.bin**).

Remarque ASDM n'est pas testé sur Linux.

Tableau 1 : Système d'exploitation et navigateur requis pour l'ASDM

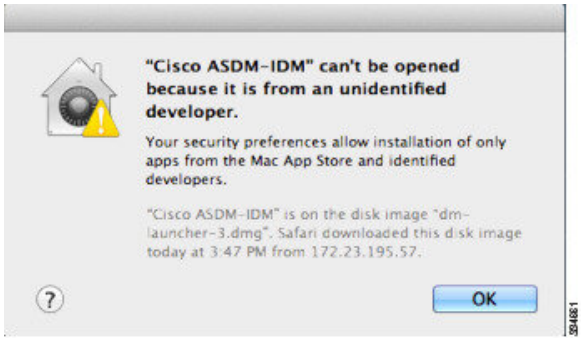
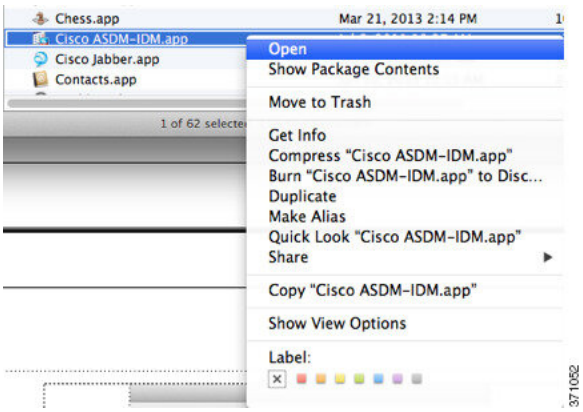
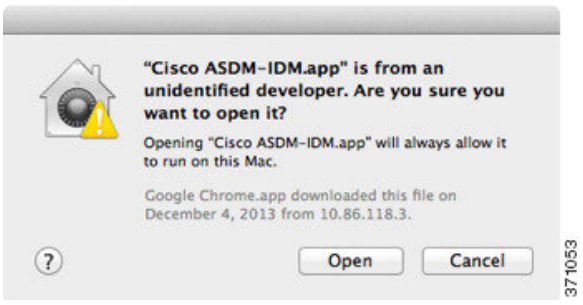
Système d'exploitation	Navigateur			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (anglais et japonais) : • 10 **Remarque** Voir Windows 10 dans Notes de compatibilité ASDM, à la page 2 si vous avez des problèmes avec le raccourci ASDM. • 8 • 7 • Server 2016 et Server 2019 • Serveur 2012 R2 • Serveur 2012 • Serveur 2008	Oui	Aucun soutien	Oui	8.0 version 8u261 ou ultérieure	1.8 **Remarque** Aucun soutien pour Windows 7 ou 10 de 32 bits
Apple OS X 10.4 et versions ultérieures	Oui	Oui	Oui (version 64 bits uniquement)	8.0 version 8u261 ou ultérieure	1.8

Notes de compatibilité ASDM

Le tableau suivant énumère les problèmes de compatibilité avec ASDM.

Modalités	Notes
Accès à l'annuaire Windows Active Directory	Dans certains cas, les paramètres Active Directory pour les utilisateurs Windows peuvent restreindre l'accès aux emplacements des fichiers de programme nécessaires pour lancer ASDM sur Windows. L'accès aux répertoires suivants est nécessaire : • Dossier du bureau • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems Si votre Active Directory restreint l'accès à l'annuaire, vous devez demander l'accès à votre administrateur Active Directory.

Modalités	Notes
Windows 10	Message d'erreur « **This app can't run on your PC** » (cette application ne peut pas fonctionner sur votre ordinateur personnel). Lorsque vous installez le lanceur ASDM, Windows 10 peut remplacer la cible du raccourci ASDM par le chemin de l'hôte Windows Scripting, ce qui provoque cette erreur. Pour fixer la cible du raccourci : **1.** Choisissez **Start (mémarrer)** > **Cisco ASDM-IDM Launcher (lanceur Cisco ASDM-IDM)** , et cliquez avec le bouton droit de la souris sur l'application **Cisco ASDM-IDM Launcher** (lanceur Cisco ASDM-IDM). **2.** Choisissez **More** > **Open file location** (Plus > Ouvrir l'emplacement du fichier.) Windows ouvre le répertoire avec l'icône du raccourci. **3.** Cliquez avec le bouton droit de la souris sur l'icône du raccourci et choisissez **Properties** (propriétés). **4.** Modifier la **Target** (cible) en : **C:\Windows\System32\wscript.exe invisible.vbs run.bat** **5.** Cliquez sur **OK**.
OS X	Sous OS X, vous pouvez être invité à installer Java la première fois que vous lancez ASDM; suivez les instructions si nécessaire. ASDM sera lancé une fois l'installation terminée.

Modalités	Notes
OS X 10.8 et versions ultérieures	Vous devez autoriser l'exécution d'ASDM, car il n'est pas signé avec un identifiant du développeur Apple. Si vous ne modifiez pas vos préférences de sécurité, un écran d'erreur s'affiche.  1. Pour permettre à ASDM de s'exécuter, faites un clic droit (ou Ctrl-Clic) sur l'icône du lanceur Cisco ASDM-IDM, et choisissez **Open** (ouvrir).  2. Un écran d'erreur similaire s'affiche, mais vous pouvez ouvrir ASDM à partir de cet écran. Cliquez sur **Open** (ouvrir) Le lanceur ASDM-IDM s'ouvre. 

Modalités	Notes
Requiert une licence de chiffrement fort (3DES/AES) sur l'ASA **Remarque** Les modèles de licence intelligents permettent un accès initial à ASDM sans la licence à chiffrement fort.	ASDM nécessite une connexion SSL avec l'ASA. Vous pouvez demander une licence 3DES à Cisco : **1.** Allez à www.cisco.com/go/license. **2.** Cliquez sur **Continue to Product License Registration (Continuer vers l'enregistrement de la licence du produit)**. **3.** Dans le portail des licences, cliquez sur **Get Other Licenses (Obtenir d'autres licences)** à côté du champ de texte. **4.** Choisissez **IPS, Crypto, Other… (IPS, Crypto, Autre…)** dans la liste déroulante. **5.** Tapez **ASA** dans le champ **Search by Keyword (Recherche par mot-clé)** . **6.** Sélectionnez **Cisco ASA 3DES/AES License** (licence Cisco ASA 3DES/AES) dans la liste **Product** (produit), puis cliquez sur **Next** (suivant). **7.** Saisissez le numéro de série de l'ASA et suivez les invites pour demander une licence 3DES/AES pour l'ASA.
• Certificat auto-signé ou certificat non fiable • IPv6 • Firefox et Safari	Lorsque l'ASA utilise un certificat auto-signé ou un certificat non fiable, Firefox et Safari ne peuvent pas ajouter d'exceptions de sécurité lors de la navigation avec HTTPS sur IPv6. Voir https://bugzilla.mozilla.org/show_bug.cgi?id=633001. Cette mise en garde concerne toutes les connexions SSL provenant de Firefox ou Safari vers l'ASA (y compris les connexions ASDM). Pour éviter cet inconvénient, configurez un certificat approprié pour l'ASA, délivré par une autorité de certification de confiance.
• Le chiffrement SSL sur l'ASA doit inclure à la fois RC4-MD5 et RC4-SHA1 ou désactiver le faux départ SSL dans Chrome. • Chrome	Si vous changez le chiffrement SSL sur l'ASA pour exclure les algorithmes RC4-MD5 et RC4-SHA1 (ces algorithmes sont activés par défaut), Chrome ne peut pas lancer ASDM à cause de la fonction « SSL false start » de Chrome. Nous suggérons de réactiver l'un de ces algorithmes (voir **Configuration** > **Device Management** > **Advanced** > **SSL Settings** [Configuration > Gestion des appareils > Avancés > Paramètres SSL]); ou vous pouvez désactiver le faux départ de SSL dans Chrome en utilisant le drapeau **--disable-ssl-false-start** conformément à Run Chromium with flags (exécuter Chromium avec des drapeaux).

Installer un certificat d'identité pour ASDM

Lorsque vous utilisez la mise à jour 51 de Java 7 et les versions ultérieures, le lanceur ASDM nécessite un certificat de confiance. Une méthode simple pour répondre aux exigences en matière de certificats consiste à installer un certificat d'identité autosigné. Vous pouvez utiliser Java Web Start pour lancer ASDM jusqu'à ce que vous installiez un certificat.

Consultez Install an Identity Certificate for ASDM (installer un certificat d'identité pour ASDM) pour installer un certificat d'identité autosigné sur l'ASA afin de l'utiliser avec ASDM, et pour enregistrer le certificat avec Java.

Augmenter la mémoire de configuration de l'ASDM

ASDM prend en charge une taille de configuration maximale de 512 Ko. Si vous dépassez cette quantité, vous risquez de rencontrer des problèmes de performance. Par exemple, lorsque vous chargez la configuration, la boîte de dialogue d'état indique le pourcentage de la configuration qui est terminée, mais avec des configurations importantes, elle cesse de s'augmenter et semble suspendre l'opération, même si ASDM est toujours en train de traiter la configuration. Si cette situation se produit, nous vous recommandons d'augmenter la mémoire vive du système ASDM.

Augmenter la mémoire de configuration de l'ASDM sous Windows

Pour augmenter la taille de la mémoire du tas ASDM, modifiez le fichier **run.bat** en suivant la procédure suivante.

Procédure

Étape 1 Aller dans le répertoire d'installation d'ASDM, par exemple C :\NProgram Files (x86)\NCisco Systems\NASDM.

Étape 2 Modifiez le fichier **run.bat** à l'aide d'un éditeur de texte.

Étape 3 Dans la ligne qui commence par « start javaw.exe », modifiez l'argument préfixé par « -Xmx » pour préciser la taille du tas souhaitée. Par exemple, remplacez-la par -Xmx768M pour 768 Mo ou -Xmx1G pour 1 Go.

Étape 4 Enregistrez le fichier **run.bat** .

Augmenter la mémoire de configuration de l'ASDM sous Mac OS

Pour augmenter la taille de la mémoire du tas ASDM, modifiez le fichier **Info.plist** en suivant la procédure suivante.

Procédure

Étape 1 Cliquez avec le bouton droit de la souris sur l'icône **Cisco ASDM-IDM** et choisissez **Show Package Contents** (afficher le contenu du paquet).

Étape 2 Dans le dossier **Contents** (contenus), double-cliquez sur le fichier **Info.plist**. Si les outils de développeur sont installés, ils s'ouvrent dans l'**Property List Editor** (Éditeur de liste de propriétés). Sinon, ils s'ouvremt dans **TextEdit**.

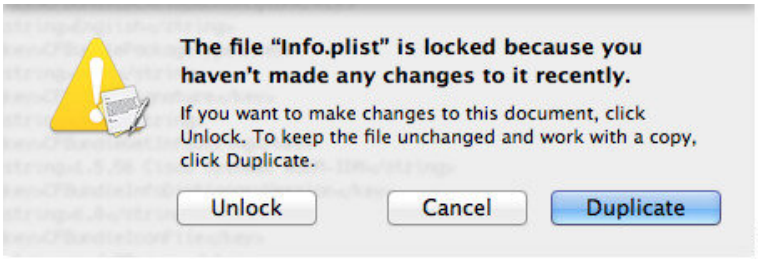
Étape 3 Sous **Java** > **VMOptions**, modifiez la chaîne préfixée par « -Xmx » pour préciser la taille du tas souhaitée. Par exemple, remplacez-la par -Xmx768M pour 768 Mo ou -Xmx1G pour 1 Go.

```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>


  <key>CFBundleDocumentTypes</key>
    <array>
```

Étape 4 Si ce fichier est verrouillé, une erreur telle que la suivante s'affiche :



Étape 5 Cliquez sur **Unlock** (déverrouiller) et enregistrez le fichier.

Si vous ne voyez pas la boîte de dialogue **Unlock** (déverrouiller), quittez l'éditeur, cliquez avec le bouton droit de la souris sur l'icône **Cisco ASDM-IDM**, choisissez **Copy Cisco ASDM-IDM** (copier Cisco ASDM-IDM), et collez-le à un endroit où vous avez des droits d'écriture, comme le bureau. Modifiez ensuite la taille du tas à partir de cette copie.

Compatibilité ASA et ASDM

Pour en savoir plus sur les exigences et la compatibilité du logiciel et du matériel ASA/ASDM, y compris la compatibilité des modules, consultez Cisco Cisco Secure Firewall ASA Compatibility (Cisco > Compatibilité).

Compatibilité VPN

Pour la compatibilité VPN, consultez Supported VPN Platforms, Cisco ASA 5500 Series (Plateformes VPN prises en charge, série Cisco ASA 5500).

Nouvelles fonctionnalités

Cette section énumère les nouvelles fonctionnalités de chaque version.

Remarque Les messages syslog nouveaux, modifiés et obsolètes sont répertoriés dans le guide des messages syslog.

Nouvelles fonctionnalités dans ASDM 7.19(1.95)

Publication : 5 juillet 2023

Il n'y a pas de nouvelles fonctionnalités dans cette version.

Nouvelles fonctionnalités dans l'ASA 9.19(1)/ASDM 7.19(1)

Publication : 29 novembre 2022

Fonctionnalités	Description
Caractéristiques de la plateforme	
Secure Firewall 3105	Nous avons présenté l'ASA pour le Secure Firewall 3105.
Solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle Azure	Vous pouvez maintenant déployer la solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle sur Microsoft Azure. Consultez les fonctionnalités Interfaces pour en savoir plus.
Caractéristiques du pare-feu	
Soutien aux groupes de service du réseau	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.
Fonctionnalités de haute disponibilité et d'évolutivité	
Suppression des propos tendancieux	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Regroupement virtuel d'ASA sur Amazon Web Services (AWS)	L'ASA virtuel prend en charge le regroupement d'interfaces individuelles pour un maximum de 16 nœuds sur AWS. Vous pouvez utiliser la mise en grappe avec ou sans équilibreur de charge de la passerelle AWS. ASDM n'est pas pris en charge.
Fonctionnalités de routage	
Prise en charge du redémarrage progressif de BGP pour IPv6	Nous avons ajouté la prise en charge du redémarrage progressif de BGP pour la famille d'adresses IPv6. Écrans nouveaux/modifiés : **Configuration** > **Configuration du appareil** > **Routage** > **BGP** > **Famille IPv6** > **Voisin**.
Prise en charge par ASDM des interfaces de bouclage pour le trafic BGP	ASDM prend en charge maintenant la configuration d'une interface avec boucle avec retour comme interface source pour le voisinage BGP. L'interface de bouclage permet de surmonter les défaillances du chemin. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Routing (routage)** > **BGP** > **IPv4 Family / IPv6 Family (famille IPv4 / famille IPv6)** > **Neighbor (voisin)** > **Add (ajouter)** > **General (général)**.

Fonctionnalités	Description
Caractéristiques de l'interface	
Prise en charge virtuelle de l'IPv6 par l'ASA	ASAv pour prendre en charge le protocole réseau IPv6 sur les plateformes du nuage privé et public. Les utilisateurs peuvent désormais : • Activer et configurer une adresse de gestion IPv6 via la configuration day0. • Attribuer des adresses IPv6 à l'aide de méthodes DHCP et statiques.
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charge de la passerelle Azure.	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charge de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired** ASDM n'est pas pris en charge.
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Edit Interface (éditer l'interface)** > **Configure Hardware Properties (configurer les propriétés du matériel)** > **FEC Mode (mode FEC)**
Prise en charge par ASDM des interfaces de bouclage	ASDM prend désormais en charge les interfaces de bouclage. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**.
Caractéristiques de la licence	
Prise en charge de la réservation de licences virtuelles permanentes pour l'ASAv5 sur KVM et VMware	Une nouvelle commande est disponible que vous pouvez exécuter pour remplacer la licence DPP par défaut et demander à Cisco Smart Software Manager (SSM) d'envoyer une licence DPP ASAv5 lorsque vous déployez ASAv avec 2GB RAM sur KVM et VMware. Vous pouvez modifier la même commande en ajoutant la forme <*no*> pour rétablir la licence de l'ASAv5 à la licence DPP par défaut en fonction de la configuration de la mémoire vive.
Fonctionnalités du VPN	
Prise en charge de l'interface de bouclage VTI	Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add VTI Interface (ajouter une interface VTI)** > **Advanced (avancé)**.

Fonctionnalités	Description
Prise en charge de l'interface de tunnel virtuel dynamique (VTI dynamique)	L'ASA est améliorée grâce à l'ITV dynamique. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Dynamique VTI prend en charge les rayons dynamiques (DHCP). Écrans nouveaux/modifiés : **Configuration > Device Setup > Interface Settings > Interfaces > Add > DVTI Interface**
Support VTI pour EIGRP et OSPF	Le routage EIGRP et OSPFv2/v3 est désormais pris en charge sur l'interface du tunnel virtuel. Vous pouvez maintenant utiliser ces protocoles de routage pour partager les informations de routage et pour acheminer le flux de trafic à travers le tunnel VPN basé sur VTI entre les pairs.
TLS 1.3 dans le VPN d'accès à distance.	Vous pouvez désormais utiliser TLS 1.3 pour chiffrer les connexions VPN d'accès à distance. TLS 1.3 ajoute la prise en charge des chiffrements suivants : • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Cette fonctionnalité nécessite Cisco Secure Client, version 5.0.01242 ou ultérieure. Écrans nouveaux/modifiés : **Configuration > Device Management > Advanced > SSL Settings (Configuration > Gestion des appareils > Avancé > Paramètres SSL)**
Prise en charge de la double pile pour les clients tiers IKEv2	Secure Firewall ASA prend désormais en charge les demandes d'IP à double pile provenant de clients VPN d'accès à distance tiers IKEv2. Si le client VPN d'accès à distance tiers demande des adresses IPv4 et IPv6, l'ASA peut désormais attribuer les deux versions d'adresses IP à l'aide de plusieurs sélecteurs de trafic. Cette fonction permet aux clients VPN d'accès à distance tiers d'envoyer des données IPv4 et IPv6 par le biais d'un seul tunnel IPsec.
Sélecteur de trafic pour l'interface VTI statique	Vous pouvez maintenant attribuer un sélecteur de trafic à une interface VTI statique.

Mettre à niveau le logiciel

Cette section fournit des informations sur le chemin de mise à niveau et un lien pour terminer la mise à niveau.

Chemin de mise à niveau de l'ASA

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information** (Accueil > Tableau de bord des appareils > Informations sur les appareils).
- Interface de ligne de commande : Utilisez la commande **show version** .

Ce tableau fournit des chemin sde mise à niveau pour l'ASA. Certaines versions plus anciennes nécessitent une mise à niveau intermédiaire avant de pouvoir passer à une version plus récente. Les versions recommandées sont en **gras**.

Remarque Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne.

Remarque Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Remarque 9.18(x) était la version finale pour les Firepower 4110, 4120, 4140, 4150, et les modules de sécurité SM-24, SM-36, et SM-44 pour le Firepower 9300.

ASA 9.16(x) était la version finale pour les ASA 5506-X, 5508-X et 5516-X.

ASA 9.14(x) est la version finale pour les ASA 5525-X, 5545-X et 5555-X.

ASA 9.12(x) est la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.

L'ASA 9.2(x) était la version finale de l'ASA 5505.

ASA 9.1(x) était la version finale pour les ASA 5510, 5520, 5540, 5550 et 5580.

Version actuelle	Version de mise à jour provisoire	Version cible
9.18(x)	—	L'un des éléments suivants : → **9.19(x)**
9.17(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)**
9.16(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x)
9.15(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)**

Version actuelle	Version de mise à jour provisoire	Version cible
9.14(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x)
9.13(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.12(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.10(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)

Version actuelle	Version de mise à jour provisoire	Version cible
9.9(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Version actuelle	Version de mise à jour provisoire	Version cible
9.6(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.4(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Version actuelle	Version de mise à jour provisoire	Version cible
9.3(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.2(x)	—	L'un des éléments suivants : → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), ou 9.1(7.4)	—	L'un des éléments suivants : → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	L'un des éléments suivants : → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

Version actuelle	Version de mise à jour provisoire	Version cible
9.0(2), 9.0(3) ou 9.0(4)	—	L'un des éléments suivants : → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	L'un des éléments suivants : → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	L'un des éléments suivants : → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	L'un des éléments suivants : → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	L'un des éléments suivants : → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) à 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	L'un des éléments suivants : → **9.12(x)** → 9.8(x) → 9.1(7.4)

Version actuelle	Version de mise à jour provisoire	Version cible
8.2(x) et antérieures	→ 9.0(4)	L'un des éléments suivants : → **9.12(x)** → 9.8(x) → 9.1(7.4)

Lien de mise à niveau

Pour terminer votre mise à niveau, consultez le guide de mise à niveau de l'ASA.

Bogues ouverts et résolus

Les bogues ouverts et résolus pour cette version sont accessibles via l'outil de recherche de bogues de Cisco. Cet outil Web vous permet d'accéder au système de suivi des bogues de Cisco, qui conserve les informations sur les bogues et les vulnérabilités de ce produit et d'autres produits matériels et logiciels de Cisco.

Remarque Vous devez avoir un compte Cisco.com pour vous connecter et accéder à l'outil de recherche de bogues de Cisco. Si vous n'en avez pas, vous pouvez vous inscrire pour obtenir un compte. Si vous n'avez pas de contrat d'assistance Cisco, vous ne pouvez rechercher les bogues que par leur numéro d'identification; vous ne pouvez pas effectuer de recherches.

Pour plus de renseignements sur l'outil de recherche de bogues de Cisco, consultez l'aide et FAQ de l'outil de recherche de bogues.

Bogues ouverts

Cette section dresse la liste des bogues non résolus dans chaque version.

Bogues ouverts dans la version 7.19(1.95)

Le tableau suivant répertorie une sélection de bogues ouverts au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCwc48458	L'utilisateur authentifié par Anyconnect ne paraît pas dans les résultats GET pour /api/monitoring/authusers

Bogues ouverts dans la version 7.19(1.90)

Le tableau suivant répertorie une sélection de bogues ouverts au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCwc48458	L'utilisateur authentifié par Anyconnect ne paraît pas dans les résultats GET pour /api/monitoring/authusers
CSCwd58653	Augmentation du temps de connexion/chargement initial de l'ASDM

Bogues ouverts dans la version 7.19(1)

Le tableau suivant répertorie une sélection de bogues ouverts au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCwc48458	L'utilisateur authentifié par Anyconnect ne paraît pas dans les résultats GET pour /api/monitoring/authusers
CSCwd58653	Augmentation du temps de connexion/chargement initial de l'ASDM

Bogues résolus

Cette section dresse la liste des bogues résolus par version.

Bogues résolus dans la version 7.19(1.95)

Le tableau suivant répertorie les bogues résolus au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCwd58653	Augmentation du temps de connexion/chargement initial de l'ASDM
CSCwd85545	ASDM supprimera toute la configuration class-map en raison de la suppression de l'ACL class-map configuré à partir de l'interface de ligne de commande.
CSCwd98702	L'option « Where used » (lieu d'utilisation) dans ASDM ne fonctionne pas
CSCwe00348	Impossible de mettre à jour le fichier hostscan à partir de l'ASDM, Impossible d'éditer le DAP si nous installons l'image hostscan
CSCwe34665	Impossible de modifier les objets ACL s'ils sont déjà utilisés, ce qui entraîne une exception.
CSCwe52019	ASDM ne se lance pas avec une erreur d'exception de sécurité – fichier de signature SHA1 invalide
CSCwf74697	ASDM version 7.19.1.94 openJRE version file in backend still showing OracleJRE version

Bogues résolus dans la version 7.19(1.90)

Aucun bogue n'a été résolu dans cette version.

Bogues résolus dans la version 7.19(1)

Le tableau suivant répertorie les bogues résolus au moment de la publication de cette note de mise à jour.

Identifiant	En-tête :
CSCwc21296	L'installateur MSI de Cisco ASDM n'est pas correctement signé
CSCwc63675	Certains contextes de l'ASA n'envoient pas les journaux vers les journaux en temps réel de l'ASDM.
CSCwc84975	La configuration SAML n'est pas persistante dans ASDM.
CSCwd16386	Config. ASDM :DAP manquant le type d'attributs AAA (Radius/LDAP)
CSCwd19658	ASDM définit incorrectement le groupe par défaut à DH 5 pour VPN de site à site, IKEv1

Contrat de licence de l'utilisateur final

Pour en savoir plus sur l'accord de licence de l'utilisateur final, consultez http://www.cisco.com/go/warranty.

Documentation associée

Pour en savoir plus sur l'ASA, consultez Navigating the Cisco Cisco Secure Firewall ASA Series Documentation (Orientation dans la documentation sur la gamme Cisco).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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.