

Certificats numériques

Ce chapitre décrit comment configurer les certificats numériques.

- À propos des certificats numériques, à la page 1
- Lignes directrices pour les certificats numériques, à la page 9
- Configurer les certificats numériques, à la page 12
- Définir une alerte d’expiration de certificat (pour les certificats d’identité ou CA), à la page 29
- Supervision des certificats numériques, à la page 30
- Historique de gestion des certificats, à la page 30

À propos des certificats numériques

Les certificats numériques fournissent une identification numérique aux fins d’authentification. Un certificat numérique contient des renseignements permettant d’identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l’entreprise, le service ou l’adresse IP. Les autorités de certification sont chargées de gérer les demandes de certificat et d’émettre des certificats numériques. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l’identité du périphérique ou de l’utilisateur.

Un certificat numérique inclut également une copie de la clé publique de l’utilisateur ou du périphérique. Une autorité de certification peut être un tiers de confiance, comme VeriSign, ou une autorité de certification privée (interne) que vous établissez au sein de votre organisation. Les autorités de certification émettent des certificats numériques dans le contexte d’une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité.

Pour l’authentification à l’aide de certificats numériques, au moins un certificat d’identité et son certificat CA d’émission doivent exister sur un ASA. Cette configuration autorise plusieurs identités, racines et hiérarchies de certificat. L’ASA évalue les certificats tiers par rapport aux CRL, également appelées listes de révocation d’autorité, depuis le certificat d’identité jusqu’à la chaîne des autorités de certification subordonnées.

Voici une description de plusieurs types de certificats numériques disponibles :

- Un certificat d'autorité de certification est utilisé pour signer les autres certificats. Il est autosigné et appelé certificat racine. Un certificat émis par un autre certificat CA s'appelle un certificat subordonné.
- Les autorités de certification délivrent également des certificats d’identité, qui sont des certificats pour des systèmes ou des hôtes spécifiques.
- Les certificats de signataire de code sont des certificats spéciaux utilisés pour créer des signatures numériques pour signer le code, le code signé révélant lui-même l’origine du certificat.

Dans une hiérarchie avec une racine et deux certificats CA intermédiaires, une validation de CRL pour l'accès à distance échoue sur la tête de réseau exécutant la version 9.13 ou une version ultérieure lorsque le certificat d'ID est signé par une CA intermédiaire, mais que la CRL est signée par une autre CA intermédiaire. La défaillance se produit même si la tête de réseau fait confiance aux deux intermédiaires lorsque ceux-ci sont signés par la même racine.

Par conséquent, chaque signataire doit conserver sa propre CRL. Chaque signataire précisera ensuite l'emplacement de la CRL dans la liste d'URL de chaque certificat qu'il signe. Sinon, vous pouvez configurer un remplacement d'URL dans le point de confiance de chaque signataire pointant vers le bon emplacement de CRL.

La CA locale intègre une fonctionnalité d'autorité de certificat indépendante sur l'ASA, déploie les certificats et assure une vérification sécurisée de la révocation des certificats émis. La CA locale fournit une autorité interne sécurisée et configurable pour l'authentification des certificats avec inscription des utilisateurs via une page de connexion au site Web.

Remarque Les certificats CA et les certificats d'identité s'appliquent à la fois aux connexions VPN de site à site et aux connexions VPN d'accès à distance. Les procédures dans ce document font référence à l'utilisation du VPN d'accès à distance dans l'interface graphique utilisateur du gestionnaire ASDM.

Astuces Pour un exemple de scénario comprenant la configuration des certificats et l'équilibrage de charges, consultez l'URL suivante : https://supportforums.cisco.com/docs/DOC-5964.

Cryptographie à clé publique

Les signatures numériques, activées par le chiffrement à clé publique, fournissent un moyen d'authentifier les appareils et les utilisateurs. Dans le chiffrement à clé publique, comme le système de chiffrement RSA, chaque utilisateur dispose d'une paire de clés contenant une clé publique et une clé privée. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre.

En termes simples, une signature se forme lorsque les données sont chiffrées avec une clé privée. La signature est jointe aux données et envoyée au récepteur. Le récepteur applique la clé publique de l'expéditeur aux données. Si la signature envoyée avec les données correspond au résultat de l'application de la clé publique aux données, la validité du message est établie.

Ce processus repose sur le récepteur ayant une copie de la clé publique de l'expéditeur et sur un degré élevé de confiance que cette clé appartient à l'expéditeur, et non à une personne se faisant passer pour l'expéditeur.

L'obtention de la clé publique d'un expéditeur est normalement gérée en externe ou par le biais d'une opération effectuée lors de l'installation. Par exemple, la plupart des navigateurs Web sont configurés avec les certificats racine de plusieurs autorités de certification par défaut. Pour le VPN, le protocole IKE, un composant IPsec, peut utiliser des signatures numériques pour authentifier les périphériques homologues avant de configurer des associations de sécurité.

Évolutivité des certificats

Sans certificats numériques, vous devez configurer manuellement chaque homologue IPsec pour chaque homologue avec lequel il communique; par conséquent, chaque nouvel homologue que vous ajoutez à un réseau nécessite une modification de configuration sur chaque homologue avec lequel il doit communiquer de manière sécurisée.

Lorsque vous utilisez des certificats numériques, chaque homologue est inscrit auprès d'une CA. Lorsque deux homologues tentent de communiquer, ils échangent des certificats et signent numériquement les données pour s'authentifier. Lorsqu'un nouvel homologue est ajouté au réseau, vous inscrivez cet homologue auprès d'une CA et aucun des autres homologues ne nécessite de modification. Lorsque le nouvel homologue tente une connexion IPsec, les certificats sont automatiquement échangés et l'homologue peut être authentifié.

Avec une CA, un homologue s'authentifie auprès de l'homologue distant en lui envoyant un certificat et en effectuant une cryptographie à clé publique. Chaque homologue envoie son certificat unique, qui a été émis par la CA. Ce processus fonctionne, car chaque certificat encapsule la clé publique de l'homologue associé, chaque certificat est authentifié par la CA et tous les homologues participants reconnaissent la CA comme une autorité d'authentification. Le processus s'appelle IKE avec une signature RSA.

L'homologue peut continuer à envoyer son certificat pour plusieurs sessions IPsec et à plusieurs homologues IPsec jusqu'à l'expiration du certificat. Lorsque son certificat expire, l'administrateur homologue doit en obtenir un nouveau auprès de la CA.

Les CA peuvent également révoquer les certificats d'homologues qui ne participent plus à IPsec. Les certificats révoqués ne sont pas reconnus comme valides par les autres homologues. Les certificats révoqués sont répertoriés dans une CRL, que chaque homologue peut vérifier avant d'accepter un certificat d'un autre homologue.

Certaines CA disposent d'une autorité d'enregistrement dans le cadre de leur mise en œuvre. Une autorité d'enregistrement est un serveur qui agit en tant que mandataire pour la CA, de sorte que les fonctions CA puissent continuer à fonctionner lorsque la CA n'est pas disponible.

Paires de clés

Les paires de clés sont des clés d'algorithme de signature numérique à courbe elliptique (ECDSA), qui ont les caractéristiques suivantes :

- Les clés RSA peuvent être utilisées pour SSH ou SSL.
- L'inscription SCEP prend en charge la certification des clés RSA.
- La taille de clé RSA maximum est de 4 096 et la valeur par défaut est de 2 048.
- La longueur maximum de la clé ECDSA est de 521, et la valeur par défaut est de 384.
- Vous pouvez générer une paire de clés RSA à usage général, utilisée à la fois pour la signature et le chiffrement, ou vous pouvez générer des paires de clés RSA distinctes pour chaque objectif. Des clés de signature et de chiffrement distinctes aident à réduire l'exposition des clés, car SSL utilise une clé pour le chiffrement, mais pas pour la signature. Cependant, IKE utilise une clé pour la signature, mais pas pour le chiffrement. En utilisant des clés distinctes pour chacune, l'exposition des clés est réduite au minimum.

Point de confiance

Les points de confiance vous permettent de gérer et de suivre les autorités de certification et les certificats. Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de configuration spécifiques à l'autorité de certification et une association avec un certificat d'identité inscrit.

Après avoir défini un point de confiance, vous pouvez le référencer par son nom dans les commandes nécessitant de spécifier une CA. Vous pouvez configurer de nombreux points de confiance.



Remarque Si l'ASA a plusieurs points de confiance qui partagent la même CA, un seul de ces points de confiance partageant la CA peut être utilisé pour valider les certificats d'utilisateur. Pour contrôler le partage du point de confiance qu'une CA utilise pour la validation des certificats d'utilisateur émis par cette CA, utilisez la commande **support-user-cert-validation**.

Pour l'inscription automatique, un point de confiance doit être configuré avec une URL d'inscription, et la CA que représente le point de confiance doit être disponible sur le réseau et doit prendre en charge SCEP.

Vous pouvez exporter et importer la paire de clés et les certificats émis associés à un point de confiance au format PKCS12. Ce format est utile pour dupliquer manuellement une configuration de point de confiance sur un autre ASA.

Inscription de certificat

L'ASA a besoin d'un certificat CA pour chaque point de confiance et d'un ou deux certificats pour lui-même, selon la configuration des clés utilisées par le point de confiance. Si le point de confiance utilise des clés RSA distinctes pour la signature et le chiffrement, l'ASA a besoin de deux certificats, un pour chaque fonction. Dans les autres configurations de clés, un seul certificat est nécessaire.

L'ASA prend en charge l'inscription automatique avec SCEP et l'inscription manuelle, ce qui vous permet de coller un certificat codé en base 64 directement dans le terminal. Pour les VPN de site à site, vous devez inscrire chaque ASA. Pour les VPN d'accès à distance, vous devez inscrire chaque ASA et chaque client VPN d'accès à distance.

Serveur mandataire pour les demandes SCEP

L'ASA peut servir de mandataire pour les demandes SCEP entre Secure Client (services client sécurisés) et une CA tierce. La CA ne doit être accessible à l'ASA que si celui-ci agit en tant que mandataire. Pour que l'ASA fournisse ce service, l'utilisateur doit s'authentifier à l'aide de l'une des méthodes prises en charge par AAA avant que l'ASA envoie une demande d'inscription. Vous pouvez également utiliser l'analyse de l'hôte et des politiques d'accès dynamique pour appliquer des règles d'admissibilité à l'inscription.

L'ASA prend en charge cette fonctionnalité uniquement avec une session VPN Secure Client (services client sécurisés) SSL ou IKEv2. Il prend en charge toutes les autorités de certification conformes à SCEP, y compris Cisco IOS CS, Windows Server 2003 CA et Windows Server 2008 CA

L'accès sans client (par navigateur) ne prend pas en charge le mandataire SCEP, bien que WebLaunch (Secure Client (services client sécurisés) initié sans client) le prenne en charge.

L'ASA ne prend pas en charge l'interrogation des certificats.

L'ASA prend en charge l'équilibrage de charges pour cette fonctionnalité.

Vérification de la révocation

Lorsqu'un certificat est émis, il est valide pour une période fixe. Parfois, une CA révoque un certificat avant l'expiration de cette période; par exemple, en raison de problèmes de sécurité ou d'un changement de nom ou d'association. Les CA publient périodiquement une liste signée des certificats révoqués. L'activation de la vérification de la révocation force l'ASA à vérifier que la CA n'a pas révoqué un certificat chaque fois qu'il l'utilise pour l'authentification.

Lorsque vous activez la vérification de la révocation, l'ASA vérifie l'état de révocation du certificat pendant le processus de validation du certificat PKI, qui peut utiliser la vérification des CRL, OCSP ou les deux. Le protocole OCSP est uniquement utilisé lorsque la première méthode renvoie une erreur (par exemple, indiquant que le serveur n'est pas disponible).

Lors de la vérification des CRL, l'ASA récupère, analyse et met en mémoire cache les CRL, qui fournissent une liste complète des certificats révoqués (et non révoqués) avec leurs numéros de série. L'ASA évalue les certificats en fonction des CRL, également appelées listes de révocation d'autorité, à partir du certificat d'identité jusqu'à la chaîne des autorités de certification subordonnées.

Le protocole OCSP offre une méthode plus évolutive de vérification de l'état de révocation dans la mesure où il localise l'état du certificat auprès d'une autorité de validation, à laquelle il demande l'état d'un certificat spécifique.

Serveurs CA pris en charge

L'ASA prend en charge les serveurs CA suivants :

CS Cisco IOS, CA local ASA et les prestataires CA tiers conformes à X.509, y compris, sans s'y limiter :

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

Les CRL fournissent à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration des CRL fait partie de la configuration d'un point de confiance.

Vous pouvez configurer l'ASA pour rendre les vérifications de CRL obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check crl**. Vous pouvez également rendre la vérification

de la CRL facultative en utilisant la commande **revocation-check crl none**, qui permet de réussir l'authentification par certificat lorsque la CA n'est pas disponible pour fournir des données CRL mises à jour.

Remarque La commande **revocation-check crl none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'ASA peut récupérer les CRL des autorités de certification à l'aide de HTTP, SCEP ou LDAP. Les CRL extraites pour chaque point de confiance sont mises en cache pour une durée configurable pour chaque point de confiance.

Remarque Même si le serveur CRL répond par l'indicateur HTTP « Connection: Keep-alive » (Connexion : Keepalive) pour indiquer une connexion persistante, l'ASA ne demande pas la prise en charge de la connexion persistante. Modifiez les paramètres sur le serveur CRL pour répondre par « Connection: Close » (Connexion : Fermer) lorsque la liste est envoyée.

Lorsque l'ASA a mis en cache une CRL plus longtemps que la configuration de la mise en cache des CRL, l'ASA considère la CRL comme trop ancienne pour être fiable ou « obsolète ». L'ASA tente de récupérer une version plus récente de la CRL la prochaine fois qu'une authentification par certificat nécessite une vérification de la CRL obsolète.

Vous pourriez recevoir un échec de *vérification de la révocation* pour une connexion ou un certificat utilisateur si vous dépassez la limite de taille de 16 Mo pour la CRL.

L'ASA met les CRL en cache pendant une durée déterminée par les deux facteurs suivants :

- Le nombre de minutes spécifié avec la commande **cache-time**. La valeur par défaut est de 60 minutes.
- Le champ NextUpdate dans les CRL extraites, qui peut être absent des CRL. Vous contrôlez si l'ASA requiert et utilise le champ NextUpdate avec la commande **enforcenextupdate**.

L'ASA utilise ces deux facteurs de la manière suivante :

- Si le champ NextUpdate n'est pas obligatoire, l'ASA marque les CRL comme obsolètes après la durée définie par la commande **cache-time**.
- Si le champ NextUpdate est obligatoire, l'ASA marque les CRL comme obsolètes à la première des deux fois spécifiées par la commande **cache-time** et le champ NextUpdate. Par exemple, si la commande **cache-time** est définie à 100 minutes et que le champ NextUpdate indique que la prochaine mise à jour est à 70 minutes, l'ASA marque les CRL comme obsolètes en 70 minutes.

Si l'ASA a une mémoire insuffisante pour stocker toutes les CRL mises en cache pour un point de confiance donné, il supprime la CRL la moins récemment utilisée pour faire de la place pour une CRL nouvellement récupérée. Les grandes CRL nécessitent un surdébit de calcul important pour les analyser. Par conséquent, pour de meilleures performances, utilisez de nombreuses CRL de plus petite taille plutôt que quelques grandes CRL, ou de préférence, utilisez OCSP.

Consultez les tailles de cache suivantes :

- Mode de contexte unique : 128 Mo
- Mode de contexte multiple : 16 Mo par contexte

OCSP

L'OCSP fournit à l'ASA un moyen de déterminer si un certificat qui se trouve dans sa plage de temps valide a été révoqué par la CA émettrice. La configuration de l'OCSP fait partie de la configuration du point de confiance.

L'OCSP localise l'état du certificat sur une autorité de validation (un serveur OCSP, également appelé *répondeur*) que l'ASA interroge pour connaître l'état d'un certificat en particulier. Cette méthode offre une meilleure évolutivité et un état de révocation plus à jour que la vérification des CRL, et aide les entreprises avec de grandes installations PKI à déployer et à étendre des réseaux sécurisés.



Remarque L'ASA autorise un décalage de cinq secondes pour les réponses OCSP.

Vous pouvez configurer l'ASA pour rendre les vérifications OCSP obligatoires lors de l'authentification d'un certificat à l'aide de la commande **revocation-check ocsp**. Vous pouvez également rendre la vérification OCSP facultative en utilisant la commande **revocation-check ocsp none**, qui permet de réussir l'authentification par certificat lorsque l'autorité de validation n'est pas disponible pour fournir des données OCSP mises à jour.



Remarque La commande **revocation-check ocsp none**, qui a été supprimée dans la version 9.13(1), a été restaurée.

L'OCSP fournit trois façons de définir l'URL du serveur OCSP. L'ASA utilise ces serveurs dans l'ordre suivant :

1. L'URL OCSP définie dans une règle de remplacement de certificat de correspondance à l'aide de la commande **match certificate**).
2. L'URL OCSP configurée à l'aide de la commande **ocsp url**.
3. Le champ AIA du certificat client.



Remarque Pour configurer un point de confiance pour valider un certificat de répondeur OCSP autosigné, vous devez importer le certificat de répondeur autosigné dans son propre point de confiance en tant que certificat CA de confiance. Ensuite, vous devez configurer la commande **match certificate** dans le point de confiance de validation du certificat client pour utiliser le point de confiance qui comprend le certificat de répondeur OCSP autosigné pour valider le certificat de répondeur. Utilisez la même procédure pour configurer la validation des certificats de répondeur externes au chemin de validation du certificat client.

Le certificat du serveur OCSP (répondeur) signe généralement la réponse OCSP. Après avoir reçu la réponse, l'ASA tente de vérifier le certificat du répondeur. La CA définit normalement la durée de vie du certificat de répondeur OCSP sur une période relativement courte pour réduire au minimum les risques de compromission. La CA comprend généralement une extension ocsp-no-check dans le certificat du répondeur, qui indique que ce certificat n'a pas besoin de vérification de l'état de révocation. Cependant, si cette extension est absente, l'ASA tente de vérifier l'état de révocation en utilisant la même méthode que spécifiée dans le point de confiance. Si le certificat du répondeur n'est pas vérifiable, les vérifications de révocation échouent. Pour éviter cette possibilité, utilisez la commande **revocation-check none** pour configurer le point de confiance de validation du certificat du répondeur et utilisez la commande **revocation-check ocsp** pour configurer le certificat client.

Certificats et coordonnées de connexion de l'utilisateur

La section suivante décrit les différentes méthodes d'utilisation des certificats et des coordonnées de connexion de l'utilisateur (nom d'utilisateur et mot de passe) pour l'authentification et l'autorisation. Ces méthodes s'appliquent à IPsec, Secure Client (services client sécurisés) et au SSL VPN sans client.

Dans tous les cas, l'autorisation LDAP n'utilise pas le mot de passe comme identifiant. L'autorisation RADIUS utilise un mot de passe commun pour tous les utilisateurs ou le nom d'utilisateur comme mot de passe.

Informations d'authentification de l'utilisateur

La méthode par défaut pour l'authentification et l'autorisation utilise les coordonnées de connexion de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation dans le groupe de tunnels (également appelé profil de connexion ASDM)
  - Utilise le nom d'utilisateur comme identifiant

Certificats

Si des certificats numériques d'utilisateur sont configurés, l'ASA valide d'abord le certificat. Cependant, il n'utilise aucun des DN des certificats comme nom d'utilisateur pour l'authentification.

Si l'authentification et l'autorisation sont toutes deux activées, l'ASA utilise les coordonnées de connexion de l'utilisateur pour l'authentification et l'autorisation de l'utilisateur.

- Authentification
  - Activé par le paramètre du groupe de serveurs d'authentification
  - Utilise le nom d'utilisateur et le mot de passe comme identifiant
- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise le nom d'utilisateur comme identifiant

Si l'authentification est désactivée et que l'autorisation est activée, l'ASA utilise le champ DN principal pour l'autorisation.

- Authentification
  - DÉSACTIVÉ (défini sur Aucun) par le paramètre du groupe de serveurs d'authentification
  - Aucun identifiant utilisé

- Autorisation
  - Activé par le paramètre du groupe de serveurs d'autorisation
  - Utilise la valeur du nom d'utilisateur du champ DN principal du certificat comme identifiant

Remarque Si le champ de DN principal n'est pas présent dans le certificat, l'ASA utilise la valeur du champ DN secondaire comme nom d'utilisateur pour la demande d'autorisation.

Prenons par exemple un certificat d'utilisateur qui comprend les champs et les valeurs de DN du sujet suivants :

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

Si le DN principal = EA (adresse courriel) et le DN secondaire = CN (nom commun), le nom d'utilisateur utilisé dans la demande d'autorisation serait anyuser@example.com.

Lignes directrices pour les certificats numériques

Cette section comprend des lignes directrices et des limites que vous devez vérifier avant de configurer les certificats numériques.

Directives relatives au mode contextuel

- Pris en charge en mode de contexte unique seulement pour les autorités de certification tierces.

Directives en matière de basculement

- Ne prend pas en charge la réplication des sessions dans le basculement dynamique.
- Ne prend pas en charge le basculement pour les autorités de certification locales.
- Les certificats sont automatiquement copiés sur l'unité de secours si vous configurez le basculement dynamique. Si vous constatez qu'un certificat est manquant, utilisez la commande **write standby** sur l'unité active.

Directives IPv6

Ne prend pas en charge IPv6.

Certificats de CA locale

- Assurez-vous que l'ASA est configuré correctement pour prendre en charge les certificats. Un ASA mal configuré peut entraîner l'échec de l'inscription ou demander un certificat contenant des renseignements inexacts.
- Assurez-vous que le nom d'hôte et le nom de domaine de l'ASA sont configurés correctement. Pour afficher le nom d'hôte et le nom de domaine actuellement configurés, saisissez la commande **show running-config**.

- Assurez-vous que l'horloge ASA est réglée avec précision avant de configurer la CA. Les certificats ont une date et une heure de validité et d'expiration. Lorsque l'ASA s'inscrit auprès d'une CA et obtient un certificat, l'ASA vérifie que l'heure actuelle se situe dans la plage de validité du certificat. Si ce n'est pas le cas, l'inscription échoue.
- Trois jours avant l'expiration du certificat de CA locale, un certificat de renouvellement de remplacement est généré et un message de journal système informe l'administrateur qu'il est temps de procéder au renouvellement du certificat de CA locale. Le nouveau certificat de CA locale doit être importé sur tous les périphériques nécessaires avant l'expiration du certificat actuel. Si l'administrateur ne répond pas en installant le certificat de renouvellement comme nouveau certificat de CA locale, les validations peuvent échouer.
- Le certificat de CA locale est renouvelé automatiquement après son expiration en utilisant la même paire de clés. Le certificat de renouvellement peut être exporté au format base 64.

  L'exemple suivant montre un certificat de CA locale codé en base 64 :

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

Prise en charge du mandataire SCEP

- Assurez-vous que l'ASA et les nœuds de service de politique Cisco ISE sont synchronisés à l'aide du même serveur NTP.
- Secure Client (services client sécurisés) 3.0 ou une version ultérieure doit être en cours d'exécution sur le terminal.
- La méthode d'authentification, configurée dans le profil de connexion pour votre stratégie de groupe, doit être définie pour utiliser à la fois AAA et l'authentification par certificat.
- Un port SSL doit être ouvert pour les connexions VPN IKEv2.
- La CA doit être en mode d'octroi automatique.

Directives supplémentaires

- Le type de certificat que vous pouvez utiliser est limité par les types de certificats pris en charge par les applications qui utiliseront le certificat. Les certificats RSA sont généralement pris en charge par toutes les applications qui utilisent des certificats. Cependant, les certificats EDDSA peuvent ne pas être pris en charge par les systèmes d'exploitation des ordinateurs, les navigateurs, ASDM ou Secure Client (services client sécurisés). Par exemple, vous devez utiliser un certificat RSA pour l'identité et l'authentification VPN d'accès à distance. Pour le VPN de site à site, où l'ASA est l'application qui utilise le certificat, EDDSA est pris en charge.
- Pour les ASA configurés en tant que serveurs ou clients CA, limitez la période de validité du certificat à une date antérieure à la date de fin recommandée, soit le 19 janvier 2038 à 03:14:08 UTC. Ces lignes directrices s'appliquent également aux certificats importés de fournisseurs tiers.

- L'ASA établit une connexion LDAP/SSL uniquement si l'un des critères de certification suivants est satisfait :
  - Le certificat du serveur LDAP est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA) et est valide.
  - Un certificat d'autorité de certification des serveurs émettant la chaîne est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA), et tous les certificats d'autorité de certification subordonnés de la chaîne sont complets et valides.
- Lorsqu'une inscription de certificat est terminée, l'ASA stocke un fichier PKCS12 contenant la paire de clés et la chaîne de certificat de l'utilisateur, ce qui nécessite environ 2 Ko de mémoire flash ou d'espace disque par inscription. La quantité réelle d'espace disque dépend de la configuration de la clé RSA et des champs de certificat. Gardez ces lignes directrices à l'esprit lors de l'ajout d'un grand nombre d'inscriptions de certificat en attente sur un ASA avec une quantité limitée de mémoire flash disponible, car ces fichiers PKCS12 sont stockés dans la mémoire flash pendant toute la durée du délai d'expiration de récupération de l'inscription configuré. Nous vous conseillons d'utiliser une taille de clé d'au moins 2048.
- Vous devez configurer l'ASA pour utiliser un certificat d'identité afin de protéger le trafic ASDM et le trafic HTTPS vers l'interface de gestion. Les certificats d'identité qui sont automatiquement générés avec SCEP sont régénérés après chaque redémarrage, alors assurez-vous d'installer manuellement vos propres certificats d'identité. Pour obtenir un exemple de cette procédure qui s'applique uniquement à SSL, consultez l'URL suivante : http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml.
- L'ASA et le Secure Client (services client sécurisés) ne peuvent valider que les certificats dans lesquels le champ X520Serialnumber (numéro de série dans le nom d'objet) est au format PrintableString. Si le format du numéro de série utilise un encodage tel que UTF8, l'autorisation de certificat échouera.
- Utilisez uniquement des caractères et des valeurs valides pour les paramètres de certificat lorsque vous les importez sur l'ASA. Dans l'ASA, ces certificats sont décodés afin d'être intégrés dans des structures de données internes. Les certificats comportant des champs vides sont interprétés comme non conformes aux normes de décodage et, par conséquent, la validation de l'installation échoue. Cependant, à partir de la version 9.16, les valeurs vides des champs facultatifs n'ont aucune incidence sur les critères de décodage et de validation d'installation.
- Pour utiliser un caractère générique (*), assurez-vous d'utiliser l'encodage sur le serveur CA qui autorise ce caractère dans la valeur de chaîne. Bien que la RFC 5280 recommande d'utiliser un UTF8String ou PrintableString, vous devez utiliser UTF8String, car PrintableString ne reconnaît pas le caractère générique comme un caractère valide. L'ASA rejette le certificat importé si un caractère ou une valeur non valide est détecté pendant l'importation. Par exemple :

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕv°3é¼p0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

Configurer les certificats numériques

Après avoir établi des certificats de confiance, vous pouvez commencer d'autres tâches fondamentales telles que l'établissement de certificats d'identité ou des configurations plus avancées telles que l'établissement de certificats de signature de code.

Avant de commencer

Lisez les renseignements sur les certificats numériques et établissez des certificats de confiance. Les certificats CA sans clé privée sont utilisés par tous les protocoles VPN, et sont configurés dans des points de confiance pour valider les certificats clients entrants.

Procédure

Étape 1 Un certificat d'identité est un certificat configuré sur l'ASA avec une clé privée correspondante. Il est utilisé pour le chiffrement sortant ou pour la génération de signatures lors de l'activation des services SSL et IPsec sur l'ASA et est obtenu par l'inscription du point de confiance. Pour configurer les certificats d'identité, consultez Configuration des certificats d'identité, à la page 12.

Étape 2 Pour configurer les CA, consultez Configuration des certificats CA, à la page 20.

Prochaine étape

Configurez une alerte d'expiration de certificat ou surveillez les certificats numériques et l'historique de gestion des certificats.

Configuration des certificats d'identité

Un certificat d'identité peut être utilisé pour authentifier l'accès VPN par l'ASA.

Dans le volet Identity Certificates Authentication (Authentification par certificats d'identité), vous pouvez effectuer les tâches suivantes :

- Ajouter ou importer un certificat d'identité, à la page 13.
- Activer les inscriptions CMPv2 à la demande d'une CA
- Afficher les détails d'un certificat d'identité.
- Supprimer un certificat d'identité existant.
- Exporter un certificat d'identité, à la page 17.
- Définir des alertes d'expiration de certificat.
- Vous inscrire pour un certificat d'identité avec Entrust Générer une requête de signature de certificat, à la page 18.

Ajouter ou importer un certificat d'identité

Pour ajouter ou importer une nouvelle configuration de certificat d'identité, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité) apparaît, avec le nom du point de confiance sélectionné affiché en haut.

Étape 3 Cliquez sur le bouton radio **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** (Importer le certificat d'identité à partir d'un fichier (format PKCS12 avec certificat(s) + clé privée)) pour importer un certificat d'identité à partir d'un fichier existant.

Étape 4 Entrez la phrase secrète utilisée pour déchiffrer le fichier PKCS12.

Étape 5 Saisissez le nom du chemin d'accès au fichier ou cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Import ID Certificate File** (Importer le fichier de certificat d'ID). Recherchez le fichier de certificat, puis cliquez sur **Import ID Certificate File** (Importer le fichier de certificat d'ID).

Étape 6 Cliquez sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité) pour ajouter un nouveau certificat d'identité.

Étape 7 Cliquez sur **New** (Nouveau) pour afficher la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés).

Étape 8 Choisissez le type de clé **RSA**, **ECDSA** ou **EdDSA**.

Étape 9 Si vous choisissez **EdDSA**, l'option **Edwards Curve** (Courbe d'Edwards) s'affiche. Cliquez sur le bouton radio EdDSA1.

Étape 10 Cliquez sur le bouton radio **Use default keypair name** (Utiliser le nom de la paire de clés par défaut) pour utiliser le nom de la paire de clés par défaut.

Étape 11 Cliquez sur le bouton radio **Enter a new key pair name** (Entrer un nouveau nom de paire de clés), puis saisissez le nouveau nom.

Étape 12 Choisissez la taille du module partir de la liste déroulante. Si **Edwards Curve** (Courbe d'Edwards) est sélectionné, choisissez Ed25519. Si vous n'êtes pas sûr de la taille du module, consultez Entrust.

Pour ASA 9.16(1) et les versions ultérieures, assurez-vous de sélectionner une taille de module RSA de 2 048 ou plus. La validation du certificat CA échoue lorsque la taille de la clé RSA est inférieure à 2 048 bits. Pour remplacer cette restriction, activez l'option d'autorisation de chiffrement faible. (Voir Autoriser le chiffrement faible pour les certificats CA, à la page 27).

Étape 13 Choisissez l'utilisation de la paire de clés en cliquant sur le bouton radio **General purpose** (Usage général) (par défaut) ou **Special** (Spécial). Lorsque vous choisissez le bouton radio **Special** (Spécial), l'ASA génère deux paires de clés, une pour la signature et une pour le chiffrement. Cette sélection indique que deux certificats sont requis pour l'identité correspondante.

Étape 14 Cliquez sur **Generate Now** (Générer maintenant) pour créer de nouvelles paires de clés, puis cliquez sur **Show** (Afficher) pour afficher la boîte de dialogue **Key Pair Details** (Détails de la paire de clés), qui contient les informations d'affichage uniquement :

- Le nom de la paire de clés dont la clé publique doit être certifiée.
- L'heure et la date auxquelles la paire de clés est générée.

- L'utilisation d'une paire de clés RSA.
- La taille du module (bits) des paires de clés : 512, 768, 1 024, 2 048, 3 072 et 4 096. La valeur par défaut est 2 048.
- Les données de clé, qui comprennent les données de clé spécifiques au format texte.

Étape 15 Cliquez sur **OK** lorsque vous avez terminé.

Étape 16 Choisissez un DN de sujet de certificat pour former le DN dans le certificat d'identité, puis cliquez sur **Select** (Sélectionner) pour afficher la boîte de dialogue **Certificate Subject DN** (DN du sujet du certificat).

Étape 17 Choisissez un ou plusieurs attributs de DN que vous souhaitez ajouter dans la liste déroulante, saisissez une valeur, puis cliquez sur **Add** (Ajouter). Les attributs X.500 disponibles pour le DN du sujet de certificat sont les suivants :

- **Nom usuel**
- **Service (OU)**
- **Nom de la société (O)**
- **Pays (C)**
- **État/Province (ST)**
- **Emplacement (L)**
- **Adresses de courriel (EA)**

Étape 18 Cliquez sur **OK** lorsque vous avez terminé.

Étape 19 Cochez la case **Generate self-signed certificate** (Générer un certificat autosigné) pour créer des certificats autosignés.

Étape 20 Cochez la case **Act as local certificate authority and issue dynamic certificates to TLS proxy** (Agir en tant qu'autorité de certification locale et émettre des certificats dynamiques au mandataire TLS) pour que le certificat d'identité agisse en tant qu'autorité CA locale.

Étape 21 Cliquez sur **Advanced** (Avancé) pour établir des paramètres de certificat d'identité supplémentaires.

La boîte de dialogue **Advanced Options** (Options avancées) apparaît, avec les trois onglets suivants : **Certificate Parameters** (Paramètres de certificat), **Enrollment Mode** (Mode d'inscription) et **SCEP Challenge Password** (Mot de passe du défi SCEP).



Remarque Les paramètres du mode d'inscription et le mot de passe du défi SCEP ne sont pas disponibles pour les certificats autosignés.

Étape 22 Cliquez sur l'onglet **Certificate Parameters** (Paramètres de certificat), puis saisissez les renseignements suivants :

- Le FQDN, un nom de domaine non ambivalent, pour indiquer la position du nœud dans la hiérarchie DNS.
- L'adresse courriel associée au certificat d'identité.
- L'adresse IP de l'ASA sur le réseau en notation décimale à quatre parties séparées par des points.

- Cochez la case **Include serial number of the device** (Inclure le numéro de série du périphérique) pour ajouter le numéro de série de l'ASA aux paramètres de certificat.

Étape 23 Cliquez sur l'onglet **Enrollment Mode** (Mode d'inscription), puis saisissez les renseignements suivants :

- Choisissez la méthode d'inscription en cliquant sur le bouton radio **Request by manual enrollment** (Demande par inscription manuelle) ou sur le bouton radio **Request from a CA** (Demande d'une autorité de certification). Si vous choisissez **Request from a CA** (Demande d'une autorité de certification), pour en savoir plus sur l'activation des inscriptions CMPV2, consultez Activer les inscriptions CMPv2 à la demande d'une CA , à la page 16.
- Choisissez le protocole d'inscription : scep, cmp, ou est.

Remarque Seules les clés RSA et ECDSA sont prises en charge pour l'inscription de certificat CMP .

- L'URL d'inscription du certificat à installer automatiquement par le biais de SCEP.
- Le nombre maximum de minutes autorisées pour réessayer d'installer un certificat d'identité. La valeur par défaut est d'une minute.
- Le nombre maximum de tentatives autorisées pour l'installation d'un certificat d'identité. La valeur par défaut est zéro, ce qui indique un nombre illimité de tentatives dans la période de réessai.

Étape 24 Cliquez sur l'onglet **SCEP Challenge Password** (Mot de passe du défi SCEP), puis saisissez les renseignements suivants :

- Le mot de passe SCEP
- La confirmation du mot de passe SCEP

Étape 25 Cliquez sur **OK** lorsque vous avez terminé.

Étape 26 Cochez la case **Enable CA flag in basic constraints extension** (Activer l'indicateur de CA dans l'extension de contraintes de base) si ce certificat doit être en mesure de signer d'autres certificats.

L'extension des contraintes de base détermine si le sujet du certificat est une autorité de certification (CA), auquel cas le certificat peut être utilisé pour signer d'autres certificats. L'indicateur de d'autorité de certification fait partie de cette extension. La présence de ces éléments dans un certificat indique que la clé publique du certificat peut être utilisée pour valider les signatures de certificat. Il n'y a aucun mal à laisser cette option sélectionnée.

Étape 27 Cliquez sur **Add Certificate** (Ajouter un certificat) dans la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité).

Le nouveau certificat d'identité apparaît dans la liste des certificats d'identité.

Étape 28 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du nouveau certificat d'identité.

Étape 29 Cliquez sur **Show Details** (Afficher les détails) pour afficher la boîte de dialogue **Certificate Details** (Détails du certificat), qui comprend les trois onglets d'affichage uniquement suivants :

- L'onglet **General** (Général) affiche les valeurs pour le type, le numéro de série, l'état, l'utilisation, le type de clé publique, le point de distribution de la CRL, les délais de validité du certificat et les points de confiance associés. Les valeurs s'appliquent à l'état disponible et à l'état en attente.
- L'onglet **Issued to** (Émis pour) affiche les champs X.500 du DN du sujet ou du propriétaire du certificat visé ainsi que leurs valeurs. Les valeurs s'appliquent uniquement à l'état disponible.
- L'onglet **Issued by** (Émis par) affiche les champs X.500 de l'entité qui accorde le certificat. Les valeurs s'appliquent uniquement à l'état disponible.

Étape 30 Pour supprimer une configuration de certificat d'identité, sélectionnez-la, puis cliquez sur **Delete** (Supprimer).

Remarque Après avoir supprimé une configuration de certificat, elle ne peut pas être restaurée. Pour recréer le certificat supprimé, cliquez sur **Add** (Ajouter) pour saisir à nouveau tous les renseignements de configuration du certificat.

Activer les inscriptions CMPv2 à la demande d'une CA

Pour être placé en tant qu'appareil de passerelle de sécurité dans les réseaux LTE sans fil, l'ASA prend en charge certaines fonctions de gestion des certificats à l'aide du protocole de gestion des certificats (CMPv2). En utilisant CMPv2 pour l'inscription de certificats de périphérique ASA, vous pouvez effectuer l'inscription manuelle, pour le certificat principal et secondaire de l'autorité de certification compatible avec CMPv2, ou des mises à jour de certificat manuelles, pour le remplacement d'un certificat précédemment émis à l'aide de la même paire de clés. Les certificats reçus sont stockés en dehors de la configuration traditionnelle et sont utilisés dans les configurations IPsec compatibles avec les certificats.

Remarque Vous n'aurez pas la fonctionnalité CMPv2 complète sur l'ASA.

Une demande initiale établit la confiance avec l'autorité de certification et obtient le premier certificat. Un certificat CA doit être préconfiguré dans un point de confiance. L'authentification a lieu lorsque vous reconnaissez l'empreinte digitale du certificat installé.

Après avoir cliqué sur **Request from a CA** (Demande d'une autorité de certification) dans l'onglet Enrollment Mode (Mode d'inscription) de la fenêtre Advanced Options (Options avancées), procédez comme suit pour les inscriptions CMPv2 :

Avant de commencer

- Suivez les étapes dans Ajouter ou importer un certificat d'identité, à la page 13.
- La licence de l'opérateur doit être incluse pour permettre l'inscription au CMP.

Procédure

Étape 1 Choisissez CMP comme protocole d'inscription et saisissez l'URL du CMP dans la zone http://.

Étape 2 Pour générer automatiquement de nouvelles paires de clés pour toutes les inscriptions CMP manuelles et automatiques, choisissez **RSA** ou **EDCSA**.

Si vous choisissez RSA, choisissez une valeur dans le menu déroulant Modules. Si vous choisissez EDCSA, choisissez une valeur dans le menu déroulant elliptic-curve (courbe elliptique).

Étape 3 (Facultatif) Cliquez sur **Regenerate the key pair** (Régénérer la paire de clés) pour générer une paire de clés lors du renouvellement du certificat ou avant de créer la demande d'inscription.

Étape 4 Cliquez sur **Shared Key** (Clé partagée) et saisissez une valeur fournie hors bande par la CA. Cette valeur est utilisée par la CA et l'ASA pour confirmer l'authentificité et l'intégrité des messages qu'ils échangent.

Étape 5 Cliquez sur **Signing Trustpoint** (Point de confiance de signature) et entrez le nom du point de confiance qui contient un certificat d'appareil émis précédemment utilisé pour signer la demande d'inscription au CMP.

Ces options ne sont disponibles que lorsque le protocole d'inscription auprès du point de confiance est défini sur CMP. Lorsqu'il s'agit d'un point de confiance CMP, le secret partagé ou le certificat de signature peut être spécifié, mais pas les deux.

Étape 6 Cliquez sur **Browse Certificate** (Parcourir le certificat) pour spécifier le certificat CA.

Étape 7 (Facultatif) Cliquez sur la case **Auto Enroll** (Inscription automatique) pour déclencher l'inscription automatique de CMPv2.

Étape 8 Dans le champ Auto Enroll Lifetime (Durée de vie de l'inscription automatique), saisissez le pourcentage de la durée de vie absolue du certificat après lequel l'inscription automatique sera nécessaire.

Étape 9 Cliquez sur **Auto Enroll Regenerate Key** (Regénérer la clé pour l'inscription automatique) pour regénérer une nouvelle clé lors du renouvellement du certificat.

Exporter un certificat d'identité

Pour exporter un certificat d'identité, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Export** (Exporter) pour afficher la boîte de dialogue **Export Certificate** (Exporter le certificat).

Étape 2 Saisissez le nom du fichier de format PKCS12 à utiliser pour exporter la configuration du certificat. Sinon, cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Export ID Certificate File** (Exporter le fichier de certificat d'ID) pour trouver le fichier vers lequel vous souhaitez exporter la configuration du certificat.

Étape 3 Choisissez le format de certificat en cliquant sur le bouton radio **PKCS12 Format** (Format PKCS12) ou le bouton radio **PEM Format** (Format PEM).

Étape 4 Entrez la phrase secrète utilisée pour chiffrer le fichier PKCS12 pour l'exportation.

Étape 5 Confirmez la phrase secrète de chiffrement.

Étape 6 Cliquez sur **Export Certificate** (Exporter le certificat) pour exporter la configuration du certificat.

Une boîte de dialogue d'information s'affiche et vous informe que le fichier de configuration du certificat a été exporté avec succès vers l'emplacement que vous avez spécifié.

Générer une requête de signature de certificat

Pour générer une requête de signature de certificat à envoyer à EnTrust, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Enroll ASA SSL VPN with Entrust** (Enregistrer ASA SSL VPN auprès d'Entrust) pour afficher la boîte de dialogue **Generate Certificate Signing Request** (Générer une requête de signature de certificat).

Étape 2 Exécutez les étapes suivantes dans la zone **Key Pair** (Paire de clés) :

a) Choisissez l'une des paires de clés configurées dans la liste déroulante.
b) Cliquez sur **Show** (Afficher) pour afficher la boîte de dialogue **Key Details** (Détails de la clé), qui fournit des renseignements sur la paire de clés sélectionnée, y compris la date et l'heure de génération, l'utilisation (générale ou spéciale), la taille du module et les données de la clé.
c) Cliquez sur **OK** lorsque vous avez terminé.
d) Cliquez sur **New** (Nouveau) pour afficher la boîte de dialogue **Add Key Pair** (Ajouter une paire de clés). Lorsque vous générez la paire de clés, vous pouvez l'envoyer à l'ASA ou l'enregistrer dans un fichier.

Étape 3 Saisissez les renseignements suivants dans le champ **Certificate Subject DN** (DN du sujet du certificat) :

a) Le FQDN ou l'adresse IP de l'ASA.
b) Le nom de l'entreprise.
c) Le code pays à deux lettres.

Étape 4 Effectuez les étapes suivantes dans la zone **Optional Parameters** (Paramètres facultatifs) :

a) Cliquez sur **Select** (Sélectionner) pour afficher la boîte de dialogue **Additional DN Attributes** (Attributs de DN supplémentaires).
b) Choisissez l'attribut à ajouter dans la liste déroulante, puis saisissez une valeur.
c) Cliquez sur **Add** (Ajouter) pour ajouter chaque attribut au tableau d'attributs.
d) Cliquez sur **Delete** (Supprimer) pour supprimer un attribut du tableau d'attributs.
e) Cliquez sur **OK** lorsque vous avez terminé.

Les attributs ajoutés apparaissent dans le champ **Additional DN Attributes** (Attributs de DN supplémentaires).

Étape 5 Saisissez des renseignements supplémentaires sur le nom de domaine complet si la CA le demande.

Étape 6 Cliquez sur **Generate Request (**Générer la demande) pour générer la requête de signature de certificat, que vous pouvez ensuite envoyer à Entrust ou enregistrer dans un fichier et envoyer ultérieurement.

La boîte de dialogue **Enroll with Entrust** (S'inscrire auprès d'Entrust) apparaît, avec la CSR.

Étape 7 Terminez le processus d'inscription en cliquant sur le lien **request a certificate from Entrust** (demande de certificat auprès d'Entrust). Copiez et collez ensuite la CSR fournie et soumettez-la à l'aide du formulaire web Entrust, fourni à l'adresse http://www.entrust.net/cisco/. Sinon, pour vous inscrire ultérieurement, enregistrez la CSR générée dans un fichier, puis cliquez sur le lien **enroll with Entrust** (s'inscrire auprès d'Entrust) dans le volet **Identity Certificates** (Certificats d'identité).

Étape 8 Entrust émet un certificat après avoir vérifié l'authentification de votre demande, ce qui peut prendre plusieurs jours. Vous devez ensuite installer le certificat en sélectionnant la demande en attente dans le volet **Identity Certificate** (Certificat d'identité) et en cliquant sur **Install** (Installer).

Étape 9 Cliquez sur **Close** (Fermer) pour fermer la boîte de dialogue **Enroll with Entrust** (S'inscrire auprès d'Entrust).

Installer des certificats d'identité

Pour installer un nouveau certificat d'identité, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Add** (Ajouter) dans le volet **Identity Certificates** (Certificats d'identité) pour afficher la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité).

Étape 2 Cliquez sur le bouton radio **Add a new identity certificate** (Ajouter un nouveau certificat d'identité).

Étape 3 Modifiez la paire de clés ou créez-en une nouvelle. Une paire de clés est requise.

Étape 4 Saisissez les renseignements sur le DN du sujet du certificat, puis cliquez sur **Select** (Sélectionner) pour afficher la boîte de dialogue **Certificate Subject DN** (DN du sujet du certificat).

Étape 5 Spécifiez tous les attributs de DN du sujet requis par la CA concernée, puis cliquez sur **OK** pour fermer la boîte de dialogue **Certificate Subject DN** (DN du sujet du certificat).

Étape 6 Dans la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité), cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue **Advanced Options** (Options avancées).

Étape 7 Pour continuer, consultez les étapes 17 à 23 de Ajouter ou importer un certificat d'identité, à la page 13.

Étape 8 Dans la boîte de dialogue **Add Identity Certificate** (Ajouter un certificat d'identité), cliquez sur **Add Certificate** (Ajouter un certificat).

La boîte de dialogue **Identity Certificate Request** (Demande de certificat d'identité) apparaît.

Étape 9 Saisissez le nom de fichier CSR du type, du texte, tel que c:\verisign-csr.txt, puis cliquez sur **OK**.

Étape 10 Envoyez le fichier texte CSR à la CA. Vous pouvez également coller le fichier texte dans la page d'inscription à la CSR sur le site Web de la CA.

Étape 11 Lorsque la CA vous renvoie le certificat d'identité, accédez au volet **Identity Certificates** (Certificats d'identité), sélectionnez l'entrée de certificat en attente, puis cliquez sur **Install** (Installer).

La boîte de dialogue **Install Identity Certificate** (Installer le certificat d'identité) apparaît.

Étape 12 Choisissez l'une des options suivantes en cliquant sur le bouton radio applicable :

- **Install from a file** (Installer à partir d'un fichier).

  Sinon, cliquez sur **Browse** (Parcourir) pour rechercher le fichier.

- **Paste the certificate data in base-64 format** (Coller les données de certificat au format base-64).

  Collez les données de certificat copiées dans la zone fournie.

Étape 13 Cliquez sur **Install Certificate** (Installer le certificat).

Étape 14 Cliquez sur **Apply** (Appliquer) pour enregistrer le certificat nouvellement installé avec la configuration ASA.

Étape 15 Pour afficher des renseignements détaillés sur le certificat d'identité sélectionné, cliquez sur **Show Details** (Afficher les détails) pour afficher la boîte de dialogue **Certificate Details** (Détails du certificat), qui comprend les trois onglets d'affichage uniquement suivants :

L'onglet **General** (Général) affiche les valeurs pour le type, le numéro de série, l'état, l'utilisation, le type de clé publique, le point de distribution de la CRL, les délais de validité du certificat et les points de confiance associés. Les valeurs s'appliquent à l'état disponible et à l'état en attente.

L'onglet **Issued to** (Émis pour) affiche les champs X.500 du DN du sujet ou du propriétaire du certificat visé ainsi que leurs valeurs. Les valeurs s'appliquent uniquement à l'état disponible.

L'onglet **Issued by** (Émis par) affiche les champs X.500 de l'entité qui accorde le certificat. Les valeurs s'appliquent uniquement à l'état disponible.

Étape 16 Pour supprimer une configuration de certificat de signataire de code, sélectionnez-la, puis cliquez sur **Delete** (Supprimer).

Remarque Après avoir supprimé une configuration de certificat, elle ne peut pas être restaurée. Pour recréer le certificat supprimé, cliquez sur **Import** (Importer) pour saisir à nouveau tous les renseignements de configuration du certificat.

Configuration des autorités de certification

Configuration des certificats CA

Cette page vous permet de gérer les certificats CA. Les rubriques suivantes expliquent ce que vous pouvez faire.

Ajouter ou installer un certificat CA

Pour ajouter ou installer un certificat CA, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Install Certificate** (Installer le certificat) s'affiche.

Étape 3 Cliquez sur le bouton radio **Install from a file** (Installer à partir d'un fichier) pour ajouter une configuration de certificat à partir d'un fichier existant (il s'agit du paramètre par défaut).

Étape 4 Saisissez le chemin d'accès et le nom du fichier, ou cliquez sur **Browse** (Parcourir) pour rechercher le fichier. Cliquez ensuite sur **Install Certificate** (Installer le certificat).

Étape 5 La boîte de dialogue **Certificate Installation** (Installation du certificat) s'affiche avec un message de confirmation indiquant que le certificat a été installé avec succès. Cliquez sur **OK** pour fermer cette boîte de dialogue.

Étape 6 Cliquez sur le bouton radio **Paste certificate in PEM format** (Coller le certificat dans le format PEM) pour vous inscrire manuellement.

Étape 7 Copiez et collez le certificat au format PEM (base64 ou hexadécimal) dans la zone fournie, puis cliquez sur **Install Certificate** (Installer le certificat).

Étape 8 La boîte de dialogue **Certificate Installation** (Installation du certificat) s'affiche avec un message de confirmation indiquant que le certificat a été installé avec succès. Cliquez sur **OK** pour fermer cette boîte de dialogue.

Étape 9 Cliquez sur le bouton radio **Use SCEP** (Utiliser SCEP) pour l'inscription automatique. L'ASA communique avec la CA à l'aide de SCEP, obtient les certificats et les installe sur le périphérique. Pour utiliser SCEP, vous devez vous inscrire auprès d'une CA qui prend en charge SCEP et vous devez vous inscrire par Internet. L'inscription automatique à l'aide de SCEP nécessite que vous fournissiez les renseignements suivants :

- Le chemin d'accès et le nom de fichier du certificat à installer automatiquement.
- Le nombre maximum de minutes pour réessayer l'installation du certificat. La valeur par défaut est d'une minute.
- Le nombre de tentatives d'installation d'un certificat. La valeur par défaut est zéro, ce qui indique un nombre illimité de tentatives dans la période de réessai.

Étape 10 Cliquez sur **More Options** (Plus d'options) pour afficher des options de configuration supplémentaires pour les nouveaux certificats et les certificats existants.

Le volet **Configuration Options for CA Certificates** (Options de configuration des certificats CA) apparaît.

Étape 11 Pour modifier la configuration d'un certificat CA existant, sélectionnez-le, puis cliquez sur **Edit** (Modifier).

Étape 12 Pour supprimer la configuration d'un certificat CA, sélectionnez-le, puis cliquez sur **Delete** (Supprimer).



Remarque Après avoir supprimé une configuration de certificat, elle ne peut pas être restaurée. Pour recréer le certificat supprimé, cliquez sur **Add** (Ajouter) pour saisir à nouveau tous les renseignements de configuration du certificat.

Étape 13 Cliquez sur **Show Details** (Afficher les détails) pour afficher la boîte de dialogue **Certificate Details** (Détails du certificat), qui comprend les trois onglets d'affichage uniquement suivants :

- L'onglet **General** (Général) affiche les valeurs pour le type, le numéro de série, l'état, l'utilisation, le type de clé publique, le point de distribution de la CRL, les délais de validité du certificat et les points de confiance associés. Les valeurs s'appliquent à l'état disponible et à l'état en attente.
- L'onglet **Issued to** (Émis pour) affiche les champs X.500 du DN du sujet ou du propriétaire du certificat visé ainsi que leurs valeurs. Les valeurs s'appliquent uniquement à l'état disponible.
- L'onglet **Issued by** (Émis par) affiche les champs X.500 de l'entité qui accorde le certificat. Les valeurs s'appliquent uniquement à l'état disponible.

Configurer les certificats CA pour la révocation

Pour configurer les certificats CA pour la révocation, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **Revocation Check** (Vérification de la révocation).

Étape 3 Cliquez sur le bouton radio **Do not check certificates for revocation** (Ne pas vérifier les certificats pour la révocation) pour désactiver la vérification de la révocation des certificats.

Étape 4 Cliquez sur le bouton radio **Check certificates for revocation** (Vérifier les certificats pour la révocation) pour sélectionner une ou plusieurs méthodes de vérification de la révocation (CRL ou OCSP).

Étape 5 Cliquez sur **Add** (Ajouter) pour déplacer une méthode de révocation vers la droite et la rendre disponible. Cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour modifier l'ordre des méthodes.

Les méthodes que vous choisissez sont mises en œuvre dans l'ordre dans lequel vous les ajoutez. Si une méthode renvoie une erreur, la méthode de vérification de la révocation suivante s'active.

Étape 6 Cochez la case **Consider certificate valid if revocation information cannot be retrieved (Considérer le certificat valide si les informations de révocation ne peuvent pas être récupérées)** pour ignorer les erreurs de vérification de la révocation lors de la validation du certificat.

Étape 7 Cliquez sur **OK** pour fermer l'onglet **Revocation Check** (Vérification de la révocation).

Configurer la politique de récupération des CRL

Pour configurer la politique de récupération des CRL, procédez comme suit :

Avant de commencer

- Pour attribuer des URL statiques :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cochez la case **Use CRL Distribution Point from the certificate** (Utiliser le point de distribution CRL du certificat) pour diriger la vérification de la révocation vers le point de distribution de la CRL à partir du certificat en cours de vérification.

Étape 3 Cochez la case **Use Static URLs configured below** (Utiliser les URL statiques configurées ci-dessous) pour répertorier les URL précises à utiliser pour la récupération des CRL. Les URL que vous sélectionnez sont mises en œuvre dans l'ordre dans lequel vous les ajoutez. Si une erreur se produit avec l'URL indiquée, l'URL suivante est prise dans l'ordre.

Étape 4 Cliquez sur **Add** (Ajouter) dans l'onglet la zone **Static Configuration** (Configuration statique).

La boîte de dialogue **Add Static URL** (Ajouter une URL statique) apparaît.

Étape 5 Saisissez l'URL statique à utiliser pour la distribution des CRL, puis cliquez sur **OK**.

L'URL que vous avez saisie apparaît dans la liste **Static URLs** (URL statiques).

Étape 6 Cliquez sur **OK** pour fermer cette boîte de dialogue.

Configurer les méthodes de récupération des CRL

Pour configurer les méthodes de récupération des CRL, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **CRL Retrieval Methods** (Méthodes de récupération des CRL) dans le volet **Configuration Options for CA Certificates** (Options de configuration pour les certificats CA).

Étape 3 Choisissez l'une des trois méthodes de récupération suivantes :

- Pour activer LDAP pour la récupération des CRL, cochez la case **Enable Lightweight Directory Access Protocol (LDAP)** (Activer le protocole LDAP). Avec LDAP, la récupération des CRL démarre une session LDAP en se connectant à un serveur LDAP nommé, accessible par un mot de passe. La connexion s'effectue sur le port TCP 389 par défaut. Entrez les paramètres requis suivants :
  - **Nom**
  - **Mot de passe**
  - **Confirmer le mot de passe**
  - **Serveur par défaut** (nom du serveur)
  - **Port par défaut** (389)
- Pour activer HTTP pour la récupération des CRL, cochez la case **Enable HTTP** (Activer HTTP).

Étape 4 Cliquez sur **OK** pour fermer cet onglet.

Configurer les règles OCSP

Pour configurer les règles OCSP afin d'obtenir l'état de révocation d'un certificat numérique X.509, procédez comme suit.

Avant de commencer

Assurez-vous d'avoir configuré une carte de certificat avant d'essayer d'ajouter des règles OCSP. Si aucune carte de certificat n'a été configurée, un message d'erreur s'affiche.

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **OCSP Rules** (Règles OCSP) dans le volet **Configuration Options for CA Certificates** (Options de configuration pour les certificats CA).

Étape 3 Choisissez la carte de certificat à faire correspondre à cette règle OCSP. Les cartes de certificats correspondent aux autorisations des utilisateurs à des champs spécifiques d'un certificat. Le nom de la CA utilisée par l'ASA pour valider les certificats du répondeur apparaît dans le champ **Certificat** (Certificate). Le numéro de priorité de la règle apparaît dans le champ **Index**. L'URL du serveur OCSP pour ce certificat apparaît dans le champ **URL**.

Étape 4 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add OCSP Rule** (Ajouter une règle OCSP) apparaît.

Étape 5 Sélectionnez le mappage de certificats à utiliser dans la liste déroulante.

Étape 6 Sélectionnez le certificat à utiliser dans la liste déroulante.

Étape 7 Saisissez le numéro de priorité de la règle.

Étape 8 Saisissez l'URL du serveur OCSP pour ce certificat.

Étape 9 Lorsque vous avez terminé, cliquez sur **OK** pour fermer cette boîte de dialogue.

La règle OCSP nouvellement ajoutée apparaît dans la liste.

Étape 10 Cliquez sur **OK** pour fermer cet onglet.

Configurer les paramètres avancés de la CRL et de l'OCSP

Pour configurer des paramètres CRL et OCSP supplémentaires, procédez comme suit :

Procédure

Étape 1 Sélectionnez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)** > **Add (Ajouter)** pour afficher la boîte de dialogue **Install Certificates** (Installer les certificats). Cliquez sur **More Options** (Plus d'options).

Étape 2 Cliquez sur l'onglet **Advanced** (Avancé) dans le volet **Configuration Options for CA Certificates** (Options de configuration pour les certificats CA).

Étape 3 Saisissez le nombre de minutes entre les actualisations du cache dans la zone **CRL Options** (Options CRL). La valeur par défaut est de 60 minutes. La plage autorisée est de 1 à 1440 minutes. Pour éviter d'avoir à récupérer la même CRL d'une autorité de certification à plusieurs reprises, l'ASA peut stocker les CRL extraites localement, ce qui s'appelle la mise en cache des CRL. La capacité du cache CRL varie selon la plateforme et est cumulative dans tous les contextes. Si une tentative de mise en cache d'une CRL nouvellement extraite dépassait ses limites de stockage, l'ASA supprime la CRL la moins récemment utilisée jusqu'à ce que plus d'espace se libère.

Étape 4 Cochez la case **Enforce next CRL update** (Appliquer la prochaine mise à jour de la CRL) pour exiger que les CRL valides aient une valeur de prochaine mise à jour qui n'a pas expiré. Décochez la case **Enforce next CRL update** (Appliquer la prochaine mise à jour de la CRL) pour laisser les CRL valides sans valeur de mise à jour suivante ou si la valeur de mise à jour suivante a expiré.

Étape 5 Saisissez l'URL du serveur OCSP dans le champ **OCSP Options** (Options OCSP). L'ASA utilise les serveurs OCSP selon l'ordre suivant :

a) URL OCSP dans une règle de remplacement de certificat de correspondance
b) URL OCSP configurée dans l'attribut OCSP Options (Options OCSP) sélectionné
c) Champ AIA d'un certificat d'utilisateur

Étape 6 Par défaut, la case **Disable nonce extension** (Désactiver l'extension de nonce) est cochée, ce qui lie cryptographiquement les requêtes aux réponses pour éviter les attaques par relecture. Ce processus fonctionne en faisant correspondre l'extension dans la demande à celle dans la réponse, en s'assurant qu'elles sont identiques. Décochez la case **Disable nonce extension** (Désactiver l'extension de nonce) si le serveur OCSP que vous utilisez envoie des réponses prégénérées qui n'incluent pas cette extension de nonce correspondante.

Étape 7 Choisissez l'une des options suivantes dans la zone **Other Options** (Autres options) :

- Cochez la case **Accept certificates issued by this CA** (Accepter les certificats émis par cette autorité de certification) pour indiquer que l'ASA doit accepter les certificats de la CA spécifiée.
- Cochez la case **Accept certificates issued by the subordinate CAs of this CA** (Accepter les certificats émis par les autorités de certification subordonnées de cette autorité de certification) pour indiquer que l'ASA doit accepter les certificats de la CA subordonnée.

Étape 8 Cliquez sur **OK** pour fermer cet onglet, puis cliquez sur **Apply** (Appliquer) pour enregistrer les modifications de votre configuration.

Gérer les certificats de l'utilisateur

Pour modifier l'état du certificat, procédez comme suit :

Procédure

Étape 1 Sélectionnez des certificats spécifiques par nom d'utilisateur ou par numéro de série de certificat dans le volet **Manage User Certificates** (Gérer les certificats d'utilisateur).

Étape 2 Choisissez une des options suivantes :

- Cliquez sur **Revoke** (Révoquer) pour supprimer l'accès utilisateur si la durée de validité du certificat utilisateur est expirée. La CA locale marque également le certificat comme révoqué dans la base de données des certificats, met automatiquement à jour les renseignements réémet la liste CRL.
- Sélectionnez un certificat révoqué et cliquez sur **Unrevoke** (Annuler la révocation) pour rétablir l'accès. La CA locale marque également le certificat comme non révoqué dans la base de données des certificats, met automatiquement à jour les renseignements du certificat et réémet une liste CRL mise à jour.

Étape 3 Cliquez sur **Apply** (Appliquer) lorsque vous avez terminé pour enregistrer vos modifications.

Configurer les identités de référence

Lorsque l'ASA agit en tant que client TLS, il prend en charge les règles de vérification de l'identité d'un serveur d'applications, comme défini dans la RFC 6125. Cette RFC spécifie les procédures pour représenter les identités de référence (configurées sur l'ASA) et les vérifier par rapport aux identités présentées (envoyées par le serveur d'applications). Si l'identité présentée ne peut pas être comparée à l'identité de référence configurée, la connexion n'est pas établie et une erreur est enregistrée.

Le serveur présente son identité en incluant un ou plusieurs identifiants dans le certificat de serveur présenté à l'ASA lors de l'établissement de la connexion. Les identités de référence sont configurées sur l'ASA pour être comparées à l'identité présentée dans un certificat de serveur lors de l'établissement de la connexion. Ces identifiants sont des instances spécifiques des quatre types d'identifiants spécifiés dans la RFC 6125. Les quatre types d'identifiants sont les suivants :

- CN_ID : nom distinctif relatif (RDN) dans un champ d'objet de certificat qui ne contient qu'une seule paire d'attributs types et de valeurs de type de nom commun (CN), dans lequel la valeur correspond à la forme globale d'un nom de domaine. La valeur CN ne peut pas être en texte libre. Un identifiant de référence CN-ID n'identifie pas un service d'application.
- DNS-ID : une entrée subjectAltName de type dNSName. Il s'agit d'un nom de domaine DNS. Un identifiant de référence DNS-ID n'identifie pas un service d'application.
- SRV-ID : une entrée subjectAltName de type otherName dont le format de nom est SRVName comme défini dans la RFC 4985. Un identifiant SRV-ID peut contenir à la fois un nom de domaine et un type de service d'application. Par exemple, un SRV-ID de « _imaps.example.net » serait divisé en une partie de nom de domaine DNS de « example.net » et une partie de type de service d'application de « imaps ».
- URI-ID : Une entrée subjectAltName de type uniformResourceIdentifier dont la valeur comprend à la fois (i) un schéma et (ii) un composant « hôte » (ou son équivalent) qui correspond à la règle « reg-name » spécifiée dans la RFC 3986. Un identifiant URI-ID doit contenir le nom de domaine DNS, pas l'adresse IP et pas seulement le nom d'hôte. Par exemple, un URI-ID de « sip:voice.example.edu » serait divisé en une partie de nom de domaine DNS de « voice.example.edu » et un type de service d'application de « sip ».

Une identité de référence est créée lors de la configuration d'une identité avec un nom précédemment inutilisé. Une fois qu'une identité de référence a été créée, les quatre types d'identifiants et leurs valeurs associées peuvent être ajoutés ou supprimés de l'identité de référence. Les identifiants de référence PEUVENT contenir des renseignements identifiant le service d'application et doivent contenir des renseignements identifiant le nom de domaine DNS.

Avant de commencer

- Les identités de référence sont utilisées lors de la connexion au serveur de journal système et au serveur de licences Smart uniquement. Aucune autre connexion en mode client SSL ASA ne prend actuellement en charge la configuration ou l'utilisation des identités de référence.
- L'ASA met en œuvre toutes les règles de correspondance des identifiants décrites dans la RFC 6125, à l'exception des certificats épinglés et du système de secours pour les clients interactifs.
- La possibilité d'épingler des certificats n'est pas mise en œuvre. Par conséquent, `aucune correspondance n'a été trouvée, le certificat épinglé` ne se produira pas. De plus, un utilisateur n'aura pas la possibilité d'épingler un certificat si aucune correspondance n'est trouvée, car notre mise en œuvre n'est pas un client interactif.

Procédure

Étape 1 Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Advanced (Avancé) > Reference Identity (Identité de référence)**.

Les identités de référence configurées sont répertoriées. Vous pouvez en **ajouter** une nouvelle, choisir et **modifier** une existante, ou choisir et **supprimer** une existante. Une identité de référence en cours d'utilisation ne peut pas être supprimée.

Étape 2 Créez ou modifiez les ID de référence en sélectionnant **Add** (Ajouter) ou **Edit** (Modifier).

Utilisez cette boîte de dialogue Add or Edit Reference Identity (Ajouter ou modifier l'identité de référence) pour choisir et préciser vos ID de référence.

- Plusieurs identifiants de référence de tout type peuvent être ajoutés à l'identité de référence.
- Vous ne pouvez pas modifier le nom une fois qu'il est défini, supprimer et recréer une identité de référence pour modifier le nom.

Prochaine étape

Utilisez l'identité de référence lors de la configuration des connexions du journal système et du serveur Smart Call Home.

Autoriser le chiffrement faible pour les certificats CA

Lorsque les attributs suivants sont présents, l'opération de validation du certificat CA échoue :

- Certificats signés avec le SHA-1 avec algorithme de chiffrement RSA.
- Certificats avec une taille de clé RSA inférieure à 2 048 bits.

Cependant, vous pouvez remplacer ces restrictions en configurant l'option d'autorisation de chiffrement faible. Lorsqu'elle est activée, l'ASA autorise l'utilisation des attributs ci-dessus lors de la validation des certificats. Nous déconseillons d'autoriser les clés au chiffrement faible, car ces clés ne sont pas aussi sécurisées que celles dont la taille est plus élevée.

Procédure

Étape 1 Accédez à **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificate (Certificat d'identité)** ou **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Identity Certificate (Certificat d'identité)** ou **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Certificate Management (Gestion des certificats)** > **Code Signer (Signataire du code)**.

Étape 2 Pour autoriser des tailles de clés inférieures à 2 048 bits et des algorithmes de signature SHA-1, sous **Weak Crypto Configurations** (Configurations de chiffrement faible), cochez la case **Allow Weak Key Sizes and Hash Algorithms** (Autoriser des tailles de clé faible et des algorithmes de hachage).

Certificat de signataire de code

Importer un certificat de signataire de code

Pour importer un certificat de signataire de code, procédez comme suit :

Procédure

Étape 1 Dans le volet **Code Signer** (Signataire du code), cliquez sur **Import** (Importer) pour afficher la boîte de dialogue **Import Certificate** (Importer le certificat).

Étape 2 Entrez la phrase secrète utilisée pour déchiffrer le fichier au format PKCS12.

Étape 3 Saisissez le nom du fichier à importer ou cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Import ID Certificate File** (Importer le fichier de certificat d'ID) et rechercher le fichier.

Étape 4 Sélectionnez le fichier à importer et cliquez sur **Import ID Certificate File** (Importer le fichier de certificat d'ID).

Le fichier de certificat sélectionné apparaît dans la boîte de dialogue **Import Certificate** (Importer le certificat).

Étape 5 Cliquez sur **Import Certificate** (Importer le certificat).

Le certificat importé apparaît dans le volet **Code Signer** (Signataire du code).

Étape 6 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration du certificat de signataire de code nouvellement importée.

Exporter un certificat de signataire de code

Pour exporter un certificat de signataire de code, procédez comme suit :

Procédure

Étape 1 Dans le volet **Code Signer** (Signataire du code), cliquez sur **Export** (Exporter) pour afficher la boîte de dialogue **Export Certificate** (Exporter le certificat).

Étape 2 Saisissez le nom du fichier de format PKCS12 à utiliser pour exporter la configuration du certificat.

Étape 3 Dans la zone **Certificate Format** (Format de certificat), pour utiliser la norme de cryptographie à clé publique, qui peut être codée en base64 ou au format hexadécimal, cliquez sur le bouton radio **PKCS12 format** (Format PKCS12). Sinon, cliquez sur le bouton radio **PEM format** (Format PEM).

Étape 4 Cliquez sur **Browse** (Parcourir) pour afficher la boîte de dialogue **Export ID Certificate File** (Exporter le fichier de certificat d'ID) pour trouver le fichier vers lequel vous souhaitez exporter la configuration du certificat.

Étape 5 Sélectionnez le fichier et cliquez sur **Export ID Certificate File** (Exporter le fichier de certificat d'ID).

Le fichier de certificat sélectionné apparaît dans la boîte de dialogue **Export Certificate** (Exporter le certificat).

Étape 6 Saisissez la phrase secrète utilisée pour déchiffrer le fichier au format PKCS12 pour l'exportation.

Étape 7 Confirmez la phrase secrète de déchiffrement.

Étape 8 Cliquez sur **Export Certificate** (Exporter le certificat) pour exporter la configuration du certificat.

Définir une alerte d'expiration de certificat (pour les certificats d'identité ou CA)

L'ASA vérifie tous les certificats CA et d'ID des points de confiance pour déterminer leur expiration une fois toutes les 24 heures. Si un certificat est sur le point d'expirer, un journal système sera émis en tant qu'alerte.

En plus du rappel de réabonnement, si un certificat déjà expiré est détecté dans la configuration, un journal système est généré une fois par jour pour rectifier la configuration en renouvelant le certificat ou en supprimant le certificat expiré.

Par exemple, supposons que les alertes d'expiration sont configurées pour commencer à 60 jours et se répètent ensuite tous les 6 jours. Si l'ASA est redémarré au bout de 40 jours, une alerte est envoyée ce jour-là et l'alerte suivante est envoyée le 36e jour.

Remarque La vérification de l'expiration n'est pas effectuée sur les certificats de groupe de confiance. Le point de confiance CA local est également traité comme un point de confiance normal pour la vérification de l'expiration.

Procédure

Étape 1 Accédez à **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **Identity Certificate/CA Certificate (Certificat d'identité/Certificat CA)**.

Étape 2 Cochez la case **Enable Certificate Expiration Alert** (Activer l'alerte d'expiration du certificat).

Étape 3 Indiquez le nombre de jours souhaité :

- Envoyer la première alerte avant : configurez le nombre de jours (de 1 à 90) avant l'expiration auxquels la première alerte sera émise.
- Répéter l'alerte pour : configurez la fréquence d'alerte (1 à 14 jours) si le certificat n'est pas renouvelé. Par défaut, la première alerte est envoyée 60 jours avant l'expiration et une fois par semaine après, jusqu'à ce que le certificat soit renouvelé et supprimé. De plus, une alerte est envoyée le jour de l'expiration, puis une fois par jour par la suite, et quelle que soit la configuration de l'alerte, une alerte est envoyée chaque jour pendant la dernière semaine précédant l'expiration.

Supervision des certificats numériques

Consultez les commandes suivantes pour superviser l'état du certificat numérique :

- **Monitoring (Supervision) > Properties (Propriétés) > CRL**

  Ce volet affiche les détails de la CRL.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique de gestion des certificats

Tableau 1 : Historique de gestion des certificats

Nom de la caractéristique	Versions de plateforme	Description
Certificate Management	7.0(1)	Les certificats numériques (y compris les certificats CA, les certificats d'identité et les certificats de signataire de code) fournissent une identification numérique pour l'authentification. Un certificat numérique contient des renseignements permettant d'identifier un appareil ou un utilisateur, tels que le nom, le numéro de série, l'entreprise, le service ou l'adresse IP. Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur. Les autorités de certification émettent des certificats numériques dans le contexte d'une PKI, qui utilise le chiffrement par clé publique ou par clé privée pour assurer la sécurité. Nous avons introduit les écrans suivants : Configuration > Remote Access VPN (VPN d'accès à distance) > Certificate Management Configuration (Configuration de la gestion des certificats) > Site-to-Site VPN (VPN de site à site) > Certificate Management (Gestion des certificats). Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Certificate Management (Gestion des certificats) > CA Certificates Configuration (Configuration des certificats CA) > Device Management (Gestion des périphériques) > Certificate Management (Gestion des certificats) > CA Certificates (Certificats CA).
Certificate Management	7.2(1)	
Certificate Management	8.0(2)	

Nom de la caractéristique	Versions de plateforme	Description
Mandataire SCEP	v 8.4(1)	Nous avons introduit cette fonctionnalité, qui permet un déploiement sécurisé des certificats de périphérique à partir d'autorités de certification tierces.
Identités de référence	9.6(2)	Le traitement du client TLS prend désormais en charge les règles de vérification de l'identité de serveur définies dans la RFC 6125, section 6. La vérification de l'identité sera effectuée pendant la validation PKI pour les connexions TLS au serveur de journal système et au serveur de licences Smart uniquement. Si l'identité présentée ne correspond pas à l'identité de référence configurée, la connexion n'est pas établie. Nous avons modifié les écrans suivants : Configuration > Remote Access VPN (VPN d'accès à distance) > Advanced Configuration (Configuration avancée) > Device Management (Gestion des périphériques) > Logging (Journalisation) > Syslog Servers (Serveurs de journal système) > Add/Edit Configuration (Ajouter/Modifier la configuration) > Device Management (Gestion des périphériques) > Smart Call Home
Serveur CA local	9.12(1)	Pour que le FQDN de l'URL d'inscription soit configurable au lieu d'utiliser le FQDN configuré de l'ASA, une nouvelle option d'interface de ligne de commande est introduite. Cette nouvelle option est ajoutée au mode smpt du serveur CA de chiffrement. Nous avons rendu obsolète le serveur CA local et le supprimerons dans une version ultérieure : lorsque l'ASA est configuré en tant que serveur CA local, il est en mesure d'émettre des certificats numériques, de publier des listes de révocation de certificats (CRL) et de révoquer en toute sécurité les certificats émis. Cette fonctionnalité a été abandonnée et, par conséquent, la commande du serveur CA de chiffrement l'a été aussi.
Serveur CA local	9.13(1)	Nous avons supprimé la prise en charge du serveur CA local. Ainsi, la commande **crypto ca server** et ses sous-commandes sont supprimées. Nous avons supprimé les commandes suivantes : **crypto ca server** et toutes ses sous-commandes.
Modifications des commandes du point de distribution de la CRL	9.13(1)	Les commandes de configuration d'URL de CDP statiques sont supprimées et déplacées vers la commande de certificat correspondante. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats CA)**

Nom de la caractéristique	Versions de plateforme	Description
Taille du cache de la CRL augmentée	9.13(1)	Pour éviter l'échec de téléchargements de CRL volumineux, la taille du cache a été augmentée et la limite du nombre d'entrées dans une CRL individuelle a été supprimée. • Augmentation de la taille totale du cache de la CRL à 16 Mo par contexte pour le mode de contexte multiple. • Augmentation de la taille totale du cache de la CRL à 128 Mo pour le mode de contexte unique.
Option de restauration des contrôles de validité du certificat de contournement	9.15(1)	L'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP, qui avait été supprimée dans la version 9.13(1), a été rétablie.
Modifications apportées aux commandes de certificat correspondantes pour prendre en charge l'URL du point de distribution de la CRL statique	9.15(1)	La commande de configuration d'URL de CDP statiques a permis aux CDP statiques d'être mappés de façon unique à chaque certificat d'une chaîne validée. Cependant, un seul de ces mappages était pris en charge pour chaque certificat. Cette modification permet aux CDP configurés de manière statique d'être mappés à une chaîne de certificats pour l'authentification.
Les modifications apportées à la paire de clés du point de confiance et à la clé de chiffrement génèrent des commandes	9.16(1)	La prise en charge des certificats avec des tailles de clé inférieures à 2 048 a été supprimée. Toute configuration utilisant des options de 512, 768 ou 1 024 bits est transférée vers la version 2 048 avec notification dûe. La prise en charge de l'utilisation de l'algorithme de hachage SHA1 pour la certification a été supprimée. **Remarque** La commande **crypto ca permit-weak-crypto** a été introduite pour remplacer ces restrictions. La nouvelle option de clé EDDSA a été ajoutée aux options RSA et ECDSA existantes.

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.