Préparer Cisco ISE pour le créneau d'EKU d'authentification client dans les certificats d'autorité de certification publique

Table des matières

Introduction

Ce document décrit l'impact sur les services ISE en raison des modifications à venir apportées aux certificats TLS émis par les autorités de certification publiques avec l'EKU d'authentification client.

Informations générales

Les certificats numériques sont des informations d'identification électroniques émises par des autorités de certification (CA) de confiance qui sécurisent la communication entre les serveurs et les clients en garantissant l'authentification, l'intégrité des données et la confidentialité. Ces certificats contiennent des champs d'utilisation de clé étendue (EKU) qui définissent leur objectif :

- EKU d'authentification du serveur (id-kp-serverAuth) : Utilisé lorsqu'un serveur présente son certificat pour prouver son identité
- EKU d'authentification du client (id-kp-clientAuth) : Utilisé dans les connexions TLS mutuelles (mTLS) où les deux parties s'authentifient mutuellement

Traditionnellement, un seul certificat peut contenir à la fois des UEC d'authentification de serveur et de client, ce qui lui permet de remplir deux fonctions. Ceci est particulièrement important pour les produits tels que Cisco ISE qui agissent à la fois comme serveur et comme client dans différents scénarios de connexion.

Définition du problème

Modification de la politique du programme racine Chrome

À partir de mai 2026, de nombreuses autorités de certification publiques cesseront d'émettre des certificats TLS (Transport Layer Security) incluant l'utilisation de la clé étendue d'authentification du client (EKU). Les certificats nouvellement émis incluent généralement l'EKU d'authentification du serveur uniquement.

Principales exigences de stratégie

- Les autorités de certification racine publiques doivent affirmer l'utilisation de clé étendue (EKU) UNIQUEMENT pour l'authentification du serveur (id-kp-serverAuth)
- Les certificats doivent inclure UNIQUEMENT l'EKU d'authentification serveur.
- Il est interdit d'inclure l'authentification client EKU dans ces certificats
- Les autorités de certification racine qui continuent à émettre des certificats avec l'EKU d'authentification client sont finalement supprimées du Chrome Root Store
- Plus d'autorités de certification racine à usage mixte pour les certificats TLS de serveur public
- Délai d'application : Mars 2027.

Délai de réponse de l'AC publique

- Octobre 2025 : Par défaut, de nombreuses autorités de certification publiques (DigiCert, Sectigo, SSL) ont commencé à émettre des certificats de serveur uniquement.
- Mai 2026 : De nombreux serveurs CA publics arrêtent d'émettre des certifications EKU d'authentification client
- Mars 2027 : La politique du programme racine de Chrome devient pleinement efficace

---

Remarque : Cette politique s'applique uniquement aux certificats émis par des autorités de certification publiques. L'ICP privée et les certificats auto-signés ne sont pas affectés par cette stratégie.

Impact sur Cisco ISE

Produits concernés

Toutes les versions de Cisco ISE sont concernées :

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3.4
- ISE 3.5

Remarque : Les versions de Cisco ISE 2.x sont également affectées ; cependant, aucune correction n'est prévue car ces versions ont atteint leur fin de vie (EOL).

Double rôle de Cisco ISE

ISE agit à la fois comme serveur et comme client dans divers scénarios de connexion, nécessitant des certificats avec les EKU d'authentification serveur et client.

Cisco ISE en tant que serveur (clé d'authentification de serveur requise) :

- PxGrid
- Service de messagerie ISE

Cisco ISE en tant que client (clé d'authentification client requise) :

- TC-NAC
- Syslog sécurisé
- LDAPS
- Radius DTLS

Cas d'utilisation spécifiques

Le tableau ci-dessous résume les services Cisco ISE susceptibles d'être affectés par les modifications à venir de l'UKE d'authentification client, ainsi que l'impact attendu pour chaque service.

Service	Incidence
pxGrid	Les certificats pxGrid sont utilisés pour la communication entre les noeuds ISE et les intégrations pxGrid externes. Alors que les intégrations pxGrid externes nécessitent uniquement l'EKU d'authentification du serveur, Cisco ISE exige actuellement que les certificats pxGrid importés contiennent à la fois l'EKU d'authentification du serveur et l'EKU d'authentification du client en raison d'une restriction d'interface utilisateur. Par conséquent, les certificats pxGrid émis par l'autorité de certification publique sont généralement déployés avec les deux unités EKU.
Service de messagerie ISE (IMS)	IMS est utilisé pour la communication back-end entre les services ISE internes. Cisco ISE exige actuellement que les certificats IMS contiennent à la fois l'EKU d'authentification serveur et l'EKU d'authentification client. Les certificats renouvelés par une autorité de certification publique avec EKU d'authentification de serveur uniquement ne peuvent pas être utilisés pour IMS, ce qui peut entraîner des échecs de communication ISE interne.
TC-NAC	Si le certificat Admin contient uniquement l'EKU d'authentification du serveur, l'authentification basée sur certificat pour TC-NAC peut être affectée lorsque le mode FIPS est activé ou lorsque Tenable est configuré avec mTLS (introduit dans les versions ISE 3.4P3 et 3.5).
Syslog sécurisé	
LDAP	
RADIUS DTLS	

⚠ Mise en garde : Les clients doivent vérifier le type de certificat utilisé par les clients pxGrid externes. Lors du renouvellement, les certificats publics signés par une autorité de certification ne peuvent plus inclure d'EKU d'authentification client. Les intégrations client pxGrid externes doivent inclure l'EKU d'authentification client lors de la communication

avec ISE, sinon la connexion sera rejetée.

Symptômes du problème

Après le déploiement des certificats Server Authentication EKU uniquement dans Cisco ISE, les clients constateront des échecs d'importation de certificats dans l'interface utilisateur graphique de Cisco ISE lorsqu'ils essaieront de télécharger des certificats pxGrid ou ISE Messaging Service (IMS) qui ne répondent pas aux exigences actuelles d'utilisation de clé étendue (EKU) pour le service sélectionné.

Un exemple de message d'erreur affiché dans l'interface utilisateur graphique est présenté ci-dessous.

Recommandations

Vérifier les certificats actuels (PREMIÈRE ÉTAPE OBLIGATOIRE)

- Préparer un inventaire de tous les certificats TLS publics pour identifier les certificats qui contiennent l'EKU d'authentification du client
- Documenter l'utilisation des certificats : identifiez les certificats utilisés conformément au tableau ci-dessus qui sont signés avec Public-CA.
- Vérifiez les informations CA et racine : Documenter l'autorité de certification et le racine qui ont émis chaque certificat
- Vérifier les dates d'expiration : Planification stratégique des renouvellements avant l'application des politiques

Suggestions pour les services qui nécessitent une clé d'activation client

Le tableau ci-dessous fournit les actions recommandées pour les services et intégrations Cisco ISE qui reposent sur des certificats contenant l'EKU d'authentification client.

Service	Actions recommandées
TC-NAC	• Lorsque Tenable est utilisé, la validation EKU stricte peut être désactivée du côté Tenable pour maintenir la connectivité.
Syslog sécurisé	
LDAP	
RADIUS DTLS	

Clients PxGrid (CatC, FMC...etc.)	
EAP-TLS	

Solutions de contournement à court terme (avant juin 2026)

Les administrateurs peuvent choisir l'une des solutions de contournement suivantes :

Option 1: Basculer vers des autorités de certification racines publiques fournissant des certificats EKU combinés

Certaines autorités de certification de racine publique (telles que DigiCert et IdenTrust) émettent des certificats avec EKU combiné à partir d'une racine alternative, qui ne peut pas être inclus dans le magasin de confiance du navigateur Chrome.

Exemples d'AC racine publiques et de types d'UER :

Fournisseur CA	Type EKU	Autorité de certification racine	Émission/sous-AC
FiducieIden	clientAuth + serverAuth	IdenTrust Public Sector Root CA 1	IdenTrust Public Sector Server CA 1
DigiCert	clientAuth + serverAuth	ID garanti DigiCert - Racine G2	ID certifié DigiCert CA G2

Conditions préalables à cette approche :

- Coordonnez-vous avec votre fournisseur d'autorité de certification pour vérifier la disponibilité de ces certificats.
- Avant de déployer des certificats, assurez-vous que le serveur qui présente le certificat et tous les clients qui l'utilisent font confiance à l'autorité de certification racine correspondante.
- Échanger des informations de certificat racine avec des homologues de communication.
- Cette approche permet d'éviter les mises à niveau logicielles immédiates.

Références de gestion des certificats :

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.3
- Configurer les renouvellements de certificats sur ISE

Option 2: Renouveler les certificats actuels pour prolonger leur validité

Les certificats délivrés par les autorités de certification publiques racine avant mai 2026 qui disposent à la fois d'une clé d'authentification serveur et client continuent d'être honorés jusqu'à l'expiration de leur durée.

Stratégie de renouvellement

Les recommandations générales sont :

- Renouveler les certificats EKU combinés avant la temporisation de la stratégie
- Pour une validité maximale des certificats, prévoyez de renouveler les certificats avant le 15 mars 2026.
- Après cette date, les certificats émis par l'autorité de certification publique ne sont valides que pendant 200 jours.
- Cisco vous recommande vivement de renouveler vos certificats avant cette date si vous souhaitez poursuivre cette option.
- Les dates de mise en oeuvre et de stratégie des autorités de certification publiques peuvent varier.
- Certaines autorités de certification publiques ont cessé d'émettre des certificats EKU combinés et ne peuvent pas en fournir un par défaut.
- Pour générer un certificat avec une UKE combinée, travaillez avec votre autorité de certification et utilisez un profil spécial fourni par les autorités de certification publiques.

Option 3: Évaluation et migration vers d'autres fournisseurs CA

Approche PKI privée

- Évaluer la faisabilité de la transition vers l'ICP privée
- Configurez une autorité de certification privée pour émettre des certificats uniques avec une unité EKU combinée (certificats serveur et client avec les unités EKU requises)
- Lors de l'émission d'un certificat signé par une autorité de certification privée, vous devez partager les informations du certificat racine avec l'homologue.
- Avant d'émettre ou de déployer un certificat, assurez-vous que le serveur qui présente le certificat et tous les clients qui l'utilisent font confiance à l'autorité de certification racine correspondante.
- Les CA privées ne sont pas soumises à la politique du programme racine Chrome
- Offre un contrôle à long terme sur les stratégies de certificat

Solution à long terme (mise à niveau logicielle requise)

Les clients doivent mettre à niveau Cisco ISE vers une version de correctif qui introduit une gestion des certificats mise à jour pour prendre en charge les certificats émis dans le cadre des nouvelles stratégies CA.

Les versions de correctifs suivantes répondent à ce problème, prévu pour avril 2026 :

Version de Cisco ISE	Version du

	correctif
ISE 3.1	Patch 11
ISE 3.2	Patch 10
ISE 3.3	Patch 11
ISE 3.4	Correctif 6
ISE 3.5	Correctif 3

Comportement après installation du correctif

Certificat PxGrid

Après l'installation du correctif :

- L'exigence actuelle de l'interface utilisateur qui applique l'EKU d'authentification du serveur et l'EKU d'authentification du client pour les certificats pxGrid sera supprimée.
- Cisco ISE autorise l'importation de certificats pxGrid contenant uniquement l'EKU d'authentification du serveur, les EKU d'authentification du serveur et du client, ou aucune extension EKU.
- Les certificats contenant uniquement l'EKU d'authentification client ne seront pas acceptés.

Certificat de service de messagerie ISE (IMS)

Pour ISE 3.1, 3.2 et 3.3

Il n'y a aucun changement de comportement après l'installation du correctif. Le service de messagerie ISE continuera d'exiger un certificat avec l'unité d'évaluation du client et du serveur. Les clients doivent prévoir d'utiliser un certificat de CA interne ISE une fois que le certificat actuel expire.

Pour ISE 3.4 et 3.5

IMS prend désormais en charge les certificats CA publics contenant uniquement l'EKU d'authentification serveur. Cependant, étant donné que IMS est utilisé uniquement pour la communication interne de Cisco ISE, Cisco recommande d'utiliser le certificat ISE Internal CA lorsque le certificat est renouvelé.

Arbre de décision

DÉBUT : Utilisez-vous des certificats d'autorité de certification publique sur Cisco ISE ?

│

├─ NON : PKI privé ou auto-signé

│ └─ Aucune action requise - Non affecté par la politique

│

└─ OUI : Certificats CA publics en cours d'utilisation

  │

  ├─ Sont-ils utilisés pour l'un des services mentionnés dans la section « Cas d'utilisation particuliers touchés » ?

  │ │

  │ ├─ Services quand ISE agit en tant que client TLS

  │ │ └─ Examiner la section « Suggestions de services qui nécessitent une clé d'activation du client ».

  │ │

  │ └─ Services lorsqu'ISE agit en tant que serveur TLS (PxGrid OU IMS)

  │ │

  │ └─ Choisissez VOTRE approche :

  │ │

  │ ├─ Option A : Basculer vers une CA racine alternative

  │ │ ├─ Contacter le fournisseur CA pour l'UKE combinée à partir de la racine alternative

  │ │ ├─ S S’assurer que tous les homologues font confiance à la nouvelle racine

  │ │ └─ Aucune mise à niveau logicielle immédiate requise

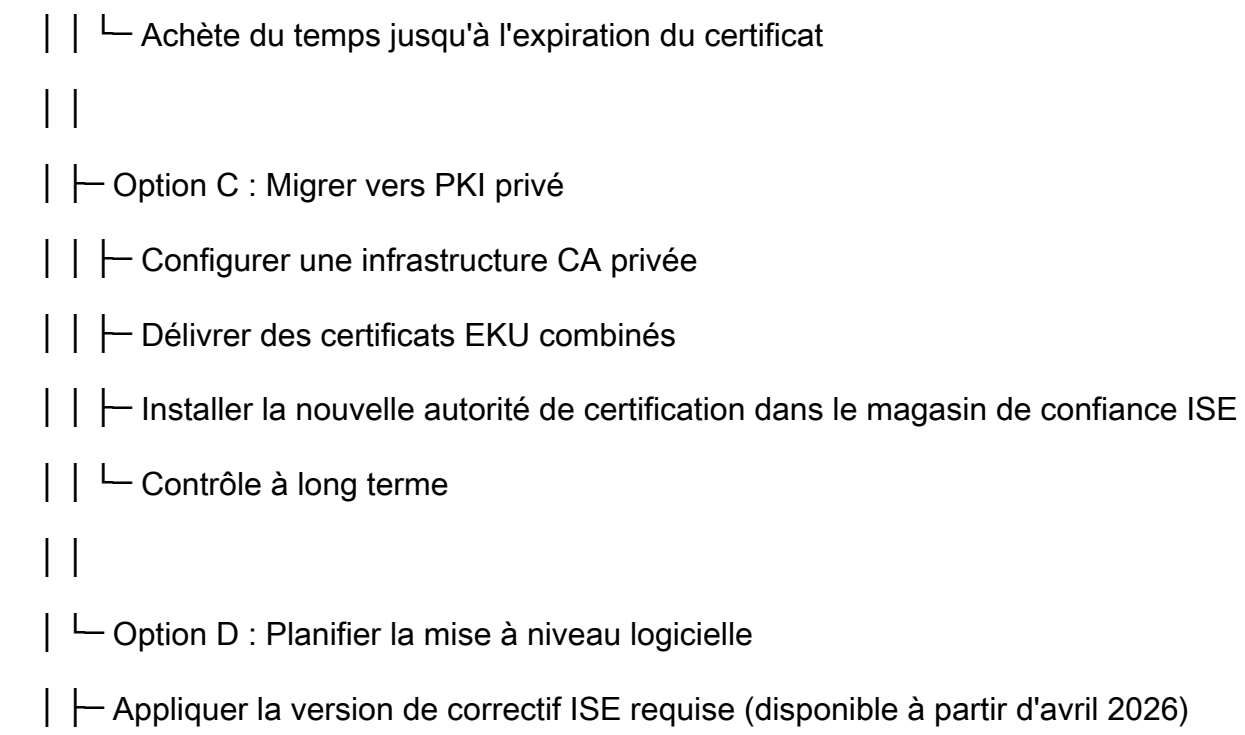
  │ │

  │ ├─ Option B : Renouveler les certificats avant les dates limites

  │ │ ├─ Cela vous aidera à vous libérer de l'urgence d'appliquer des correctifs à Cisco ISE

  │ │ │

  │ │ ├─ Pour une validité maximale : Renouveler avant le 15 mars 2026



Foire aux questions (FAQ)

Questions générales

Q : Dois-je m'en inquiéter si j'utilise une ICP privée ?

A : Non. Cette stratégie affecte uniquement les certificats émis par les autorités de certification racines publiques. L'ICP privée et les certificats auto-signés ne sont pas affectés.

Q : Puis-je continuer à utiliser mes certificats existants ?

A : Oui, les certificats existants avec EKU combiné restent valides jusqu'à leur expiration. Le problème se pose lorsque vous devez renouveler votre contrat. Ils fonctionnent à la fois pour les connexions TLS et mTLS jusqu'à expiration.

Q : Comment puis-je savoir si j'utilise mTLS ou TLS standard ?

A : Consultez la section Cas d'utilisation spécifiques affectés.

Questions de mise à niveau

Gestion des certificats

Questions de calendrier

Q : Que se passe-t-il le 15 juin 2026 ?

A : Chrome cesse d'approuver les certificats TLS publics contenant à la fois des EKU d'authentification serveur et client. Les services utilisant de tels certificats peuvent échouer.

Q : Pourquoi dois-je renouveler mon contrat avant le 15 mars 2026 ?

A : Après le 15 mars 2026, la validité du certificat passe de 398 à 200 jours. Le renouvellement avant cette date vous donne la durée de vie maximale du certificat.

Q : Quel est le délai d'action ?

A : Il existe plusieurs délais :

- 15 mars 2026 : Validité du certificat réduite à 200 jours
- Mai 2026 : La plupart des AC publiques arrêtent entièrement d'émettre des EKU combinés
- Mars 2027 : Politique Chrome pleinement appliquée

Ressources supplémentaires

- ID de bogue Cisco : CSCws83036- Évaluation de l'impact de l'application EKU ClientAuth dans ISE

Références externes

- Politique du programme racine Chrome

Ressources de l'autorité de certification

- Portail IdenTrust

Conclusion

L'arrêt de l'EKU d'authentification client dans les certificats d'autorité de certification publique représente un changement important de la stratégie de sécurité qui affecte les déploiements Cisco ISE utilisant des connexions mTLS. Bien qu'il s'agisse d'un changement à l'échelle du secteur, l'évaluation de l'impact est CRITIQUE et une action immédiate est requise pour éviter les interruptions de service.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.