Préparer Identity Services Engine pour les restrictions étendues d'utilisation des clés dans les certificats émis par les autorités de certification publiques.

Table des matières

- Introduction
- Informations générales
- Définition du problème
  - Modification de la politique du programme racine Chrome
  - Principales exigences de stratégie
  - Calendrier
- Impact sur Cisco ISE
- Cas d'utilisation spécifiques
- Symptômes du problème
- Recommandations
  - Certificats d'audit ayant un impact potentiel et conformes aux recommandations
  - Solutions de contournement à court terme (avant juin 2026)
  - Option 1: Basculer vers des autorités de certification racines publiques fournissant des certificats EKU combinés
  - Option 2: Renouveler les certificats actuels pour prolonger leur validité
    - Stratégie de renouvellement
  - Option 3: Évaluation et migration vers d'autres fournisseurs CA
  - Solution à long terme (mise à niveau logicielle requise)
- Changement de comportement après installation du correctif
  - Certificat pxGrid
  - Certificat de service de messagerie ISE (IMS)
- Foire aux questions (FAQ)
- Ressources supplémentaires
  - Références externes
  - Ressources de l'autorité de certification
- Conclusion

Introduction

Ce document décrit l'impact des restrictions appliquées aux critères d'émission des certificats émis par les autorités de certification s'alignant sur le programme de certificat racine Chrome dans

Cisco Identity Services Engine (ISE).

Informations générales

Les certificats numériques sont des certificats électroniques émis par des autorités de certification (CA) qui sécurisent la communication entre les serveurs et les clients en garantissant l'authentification, l'intégrité des données et la confidentialité. L'utilisation de clé étendue (EKU) est un attribut qui définit l'objectif de la clé publique de certificat. Deux des valeurs EKU disponibles sont les suivantes :

- 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

Un seul certificat peut contenir à la fois des clés d'authentification serveur et client, ce qui lui permet de remplir deux fonctions. Cela est particulièrement important pour les produits comme ISE qui agissent comme serveur ou client selon le cas d'utilisation.

Définition du problème

Modification de la politique du programme racine Chrome

La mise en oeuvre de l'UER dépend de la signature du certificat par l'AC. L'utilisation de l'authentification serveur et de l'authentification client était une pratique courante.

Cependant, dans le cadre de la modification de la stratégie du programme racine Chrome, les autorités de certification qui s'alignent sur ces critères d'émission de certificat arrêtent la signature des certificats TLS qui incluent l'utilisation de clé étendue d'authentification du client (EKU). Les certificats récemment émis incluent uniquement l'EKU d'authentification serveur.

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 Client Authentication EKU dans ces certificats
- Les autorités de certification racine qui continuent à émettre des certificats avec l'EKU

d'authentification client sont finalement retirées du magasin racine Chrome provoquant le marquage de tels certificats comme "non approuvés" par le navigateur Chrome

Calendrier

- Octobre 2025 : Les AC qui s'alignent sur le programme (p. ex. DigiCert, Sectigo, etc.) ont commencé à émettre des certificats de serveur uniquement par défaut.
- Mai 2026 : Les autorités de certification alignées sur le programme arrêtent d'émettre des certificats EKU d'authentification client
- Mars 2027 : La politique du programme racine de Chrome devient pleinement efficace

Impact sur Cisco ISE

Toutes les versions de Cisco ISE sont concernées :

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



Remarque : La modification mentionnée a un impact sur toutes les versions d'ISE, y compris les versions inférieures à 3.x. Cependant, les modifications de code ne sont publiées que pour les versions mentionnées dans la section précédente. Cisco recommande de mettre à niveau ISE pour éviter tout impact.

Cas d'utilisation spécifiques

Le tableau 1 résume les services concernés par les modifications à venir de l'EKU d'authentification du client, ainsi que l'impact attendu pour chaque service.

Service	Incidence
pxGrid	Le service ISE pxGrid nécessite une communication entre les noeuds sur le canal pxGrid. Cela signifie que certains noeuds fonctionnent comme des serveurs et d'autres comme des clients.

	Par conséquent, la présence de l'EKU d'authentification du serveur et de l'EKU d'authentification du client est requise pour l'installation du certificat pxGrid. Par conséquent, l'installation des certificats d'autorité de certification publique nouvellement émis contenant uniquement l'EKU d'authentification du serveur est restreinte. ⚠ Mise en garde : Le service ISE pxGrid effectue la validation de l'EKU de certificat. Les certificats clients pxGrid externes doivent inclure l'EKU d'authentification client lors de la communication avec ISE ou lorsque la connexion est rejetée. Cisco recommande la vérification des certificats signés par l'autorité de certification publique utilisés dans les clients pxGrid externes pour éviter l'impact sur l'intégration. Pour en savoir plus sur ce point, consultez Impact du pare-feu sécurisé Cisco sur les modifications de l'unité d'authentification du client de l'autorité de certification publique à partir de mai 2026 pour les communications sécurisées.
Service de messagerie ISE (IMS)	ISE Messaging Services (IMS) est un canal sécurisé appliquant une validation mTLS stricte et utilisé pour la communication entre les noeuds. Par conséquent, la présence de l'EKU d'authentification du serveur et de l'EKU d'authentification du client est requise pour le bon fonctionnement du service. L'installation de certificats d'autorité de certification publique nouvellement émis ne contenant pas les deux unités EKU est limitée uniquement sur ISE 3.4 et 3.5. Les versions inférieures ne limitent pas l'installation. Cependant, le fonctionnement du service est affecté si les deux unités EKU ne sont pas présentes sur les certificats.
TC-NAC	Lors de la sélection du fournisseur TC-NAC Tenable Security Center : VA dans Administration > NAC Threat Centric > Ajouter un nouveau connecteur TC-NAC est créé. Une fois que le connecteur est prêt à être configuré, il est possible de sélectionner l'« authentification basée sur certificat » comme méthode d'authentification pour le connecteur TC-NAC, puis de sélectionner le « certificat d'administration ISE ». La connexion TC-NAC est établie entre le PSN ISE et la base de données VA, de sorte que le certificat

	d'administration du PSN spécifique est celui qui est utilisé comme certificat client. Si mTLS strict est activé sur Tenable alors l'EKU d'authentification client est requise. L'absence de l'EKU d'authentification du client peut entraîner le rejet du certificat du client ISE TC-NAC par le serveur.
LDAP, Syslog sécurisé, DTL RADIUS pour CoA	Ces trois services offrent la possibilité d'utiliser des certificats spécifiques en tant que « Certificats clients » pour l'authentification TLS. ISE ne procède à aucune validation EKU. Par conséquent, l'impact sur ces services dépend entièrement du côté serveur. si la validation de l'EKU du certificat est appliquée sur le serveur, alors le certificat spécifique utilisé par ISE nécessite l'EKU d'authentification du client ou l'authentification TLS échoue.

Tableau 1 : Services affectés

Symptômes du problème

Si vous tentez d'installer un certificat avec l'EKU d'authentification du serveur uniquement pour des services avec des exigences d'EKU spécifiques, l'erreur affichée dans l'image 1 se produit.

pxGrid et ISE Messaging Service (IMS) sont des services présentant de telles exigences d'utilisation améliorée de la clé.

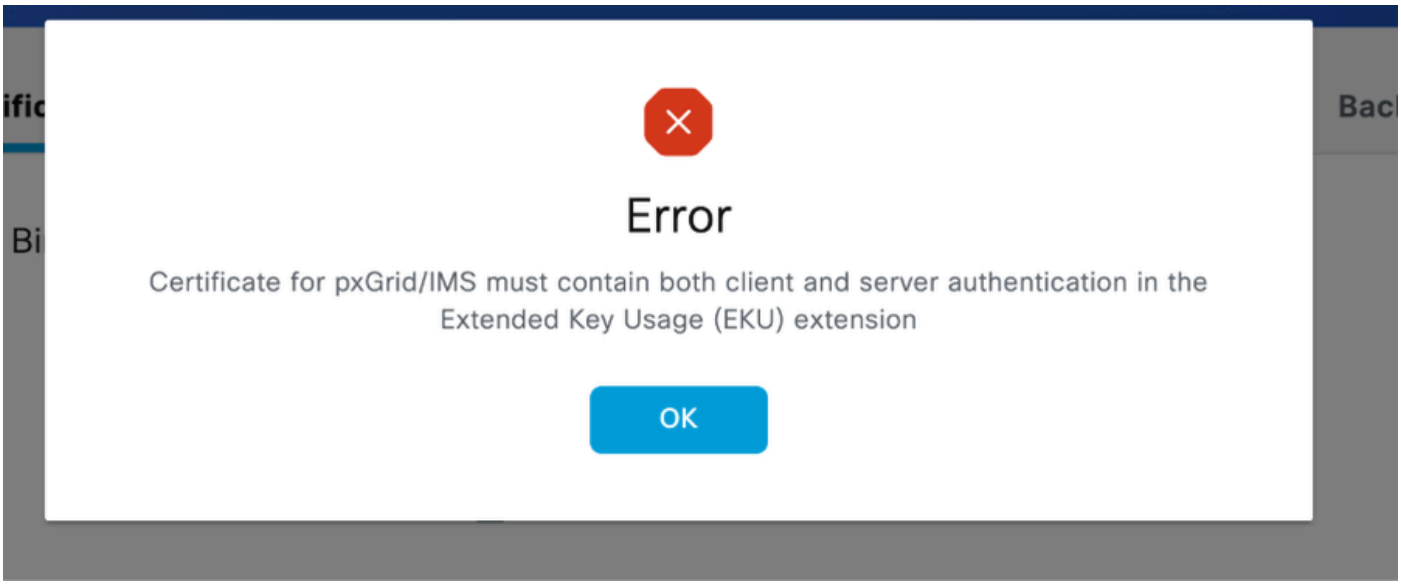


Image 1: Erreur affichée lors de la tentative d'installation d'un certificat non conforme aux exigences EKU

Recommandations

Certificats d'audit ayant un impact potentiel et conformes aux recommandations

- Utilisez le tableau 1 pour trouver les services ISE susceptibles d'avoir un impact. Vérifiez quels services parmi ceux mentionnés reposent sur des certificats publics signés par une autorité de certification ou sur des autorités de certification s'alignant sur le programme racine chrome.

- Documenter la chaîne d'AC pour chaque certificat et valider si cette AC met en oeuvre les changements dans les critères d'émission.
- Vérifier les dates d'expiration : Planifier les renouvellements de manière stratégique avant l'application des politiques. Gardez à l'esprit que l'EKU d'authentification du client peut être limitée selon la politique de CA.
- Utilisez le tableau 2 pour obtenir des recommandations spécifiques sur les services touchés par la modification des critères d'émission.
- ISE n'affiche pas les informations EKU sur les certificats. Si cela doit être validé, le certificat ISE spécifique doit être exporté et lu à l'aide d'outils externes.
- Pour exporter des certificats système ISE, accédez à Administration > System > Certificates > System Certificates > Sélectionnez le noeud spécifique que vous voulez exporter > Cliquez dans Export > Select Export Certificate Only > Cliquez sur le bouton Export.

Vous pouvez prendre la commande suivante comme référence pour vérifier les informations d'un fichier de certificat avec le nom de fichier "certnew.cer" et soupirer à la fois l'authentification du serveur et l'authentification du client EKU en utilisant openSSL.

```
mymachine% openssl x509 -noout -text -in "certnew.cer"

Certificate:

     Data:

         Version: 3 (0x2)

         Serial Number:

             XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

     Signature Algorithm: sha256WithRSAEncryption

         Issuer: DC=com, DC=mydc, CN=mycert-MYDC-DC-CA
```

```
Validity

    Not Before: Mar 10 22:01:51 2026 GMT

    Not After : Mar 10 22:11:51 2027 GMT

Subject: L=XX, O=XX, OU=XXX, CN=XXXX

Subject Public Key Info:

    Public Key Algorithm: rsaEncryption

        RSA Public-Key: (4096 bit)

        Modulus:

           <HEX STRING>

        Exponent: XXXXX (0xXXXX)

X509v3 extensions:

    X509v3 Key Usage:

        Digital Signature, Non Repudiation, Key Encipherment

    X509v3 Subject Key Identifier:

        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

    X509v3 Extended Key Usage:

        TLS Web Server Authentication, TLS Web Client Authentication

    X509v3 Subject Alternative Name:

        IP Address:x.x.x.x

    X509v3 Authority Key Identifier:

        keyid:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX

   .

   .

   .
```

Service	Actions recommandées
pxGrid	Si le certificat pxGrid sur ISE est émis par une autorité de certification publique et qu'un renouvellement ou une migration vers une autorité de certification publique est prévu, nous recommandons ce qui suit : 1. Vérifiez si l'EKU d'authentification du serveur et l'EKU d'authentification du client sont actuellement présents dans le certificat et s'il est possible de

	conserver les deux selon votre stratégie d'autorité de certification 2. Si la stratégie de l'autorité de certification ne permet pas la présence des deux unités EKU, nous recommandons de migrer le certificat pour qu'il soit signé par l'autorité de certification interne ISE. Pour effectuer la migration, accédez à : Administration > System > Certificates > System Certificates > Sélectionnez le certificat émis par l'autorité de certification interne ISE du noeud spécifique que vous souhaitez modifier > Edit > Cochez la case pxGrid sous la section usage > Save. Si un certificat émis par l'autorité de certification interne ISE n'existe pas, générez-en un. Utilisez la vidéo suivante comme guide pour générer le certificat.
Certificat de messagerie ISE (IMS)	Si le certificat du service de messagerie ISE est actuellement signé par une autorité de certification publique et qu'un renouvellement ou une migration vers une autorité de certification publique est prévu, nous vous recommandons de procéder comme suit : 1. Vérifiez si l'autorité de certification publique vers laquelle vous effectuez la migration ou que vous utilisez pour le renouvellement accepte l'utilisation des clés d'authentification serveur et client. 2. Si l'autorité de certification publique ne l'autorise pas, migrez le certificat de messagerie ISE pour utiliser l'autorité de certification interne ISE. Accédez à Administration > System > Certificates > Certificate Signing Request > Generate Certificate Signing Request (CSR) > sélectionnez « ISE Messaging Service » dans la liste déroulante Certificate(s) for > cochez la case Regenerate ISE Messaging Service Certificate > appuyez sur le bouton Generate ISE Messaging Service Certificate. Aucun redémarrage du service n'est nécessaire. Assurez-vous que tous les noeuds ISE sont opérationnels et accessibles à partir du PAN sur les ports 12001 et 443, afin que la modification du certificat soit propagée correctement à tous les noeuds.
TC-NAC	Le service TC-NAC s'appuie sur le certificat d'administration ISE du noeud spécifique pour l'authentification mTLS. Si le certificat est émis par une autorité de certification publique et qu'un renouvellement ou une migration vers une autorité de certification publique est prévu, nous recommandons ce qui suit : 1. Vérifiez si l'EKU d'authentification du serveur et l'EKU d'authentification du client sont actuellement présents dans le certificat et s'il est possible de conserver les deux selon votre stratégie d'autorité de certification

	2. Vérifiez si mTLS strict est activé sur Tenable. La désactivation de mTLS strict permet l'utilisation d'un certificat avec l'EKU d'authentification du serveur uniquement.
LDAP, Syslog sécurisé, DTL RADIUS pour CoA	ISE n'effectue pas de validation EKU pour les certificats clients de ces services. Si un renouvellement ou une migration vers une autorité de certification publique est prévu, vérifiez si l'unité EKU du certificat doit être modifiée après le renouvellement/la migration et si cela est en conflit avec la stratégie TLS côté serveur.

Tableau 2 : Actions recommandées pour éviter l'impact sur les services spécifiques.

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.
- Si la chaîne CA n'est pas préinstallée, installez la chaîne CA si nécessaire.
- 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

Directives générales :

- Renouveler les certificats EKU combinés avant l'expiration de la stratégie.
- Après le 15 mars 2026, les certificats émis par l'autorité de certification publique ne sont valides que pendant 200 jours.
- Les dates de mise en oeuvre et de stratégie des autorités de certification publiques peuvent varier.
- Certaines autorités de certification publiques ont cessé de délivrer des certificats EKU combinés.

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

Directives générales :

- Migrer vers une autre autorité de certification permettant la présence d'une clé d'authentification serveur et client
- Offre un contrôle à long terme sur les stratégies de certificat
- Lorsque vous émettez un certificat signé par une autorité de certification privée, vous devez partager les informations de 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 la chaîne d'autorité de certification correspondante

Solution à long terme (mise à niveau logicielle requise)

Les clients peuvent mettre à niveau ISE vers une version de correctif qui introduit un traitement des certificats mis à jour pour prendre en charge les certificats émis dans le cadre des nouvelles stratégies CA.

Les versions de correctifs suivantes incluent des changements de comportement afin d'aligner ISE sur les nouvelles restrictions. La date de publication prévue est 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

Changement de comportement après installation du correctif

⚠ Mise en garde : Ce correctif introduit des changements de comportement dans la logique de gestion des certificats.

Sauvegardez les certificats ISE et IMS avec leurs clés privées avant de les remplacer par de nouveaux certificats. La désinstallation de ce correctif après l'installation de certificats avec l'EKU d'authentification du serveur affecte uniquement la communication TLS des deux services.

Certificat pxGrid

Après l'installation du correctif :

- L'importation de certificats pxGrid contenant uniquement les EKU d'authentification du serveur, les EKU d'authentification du serveur et du client, ou aucune extension EKU est autorisée.
- Les certificats contenant uniquement l'EKU d'authentification client sont rejetés.

Certificat de service de messagerie ISE (IMS)

ISE 3.1, 3.2 et 3.3

Pour les versions 3.1, 3.2 et 3.3 de Cisco ISE, IMS continue d'exiger un certificat avec les clés d'authentification du serveur et du client. Après l'installation du correctif, la validation de l'EKU est appliquée, ce qui signifie que les certificats qui n'ont pas à la fois l'authentification du serveur et l'authentification du client sont rejetés pour l'installation.

Les clients doivent planifier la migration vers un certificat interne signé par une autorité de certification ISE une fois que le certificat actuel expire.

ISE 3.4 et 3.5

Après l'installation du correctif, la restriction EKU sur ISE est réduite. L'utilisation d'un certificat signé par une autorité de certification contenant une EKU d'authentification de serveur uniquement , à la fois des EKU d'authentification de serveur et de client, ou aucune EKU n'est autorisée.

Les certificats contenant uniquement l'EKU d'authentification client sont rejetés.

Le certificat IMS est utilisé pour l'authentification du serveur et du client dans la communication entre les noeuds ISE.



Remarque : Même si l'utilisation d'un certificat signé par une autorité de certification publique est prise en charge pour IMS. Cisco recommande d'utiliser le certificat d'autorité de certification interne ISE, car cette communication ne concerne que les transactions internes.

Foire aux questions (FAQ)

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

La stratégie appliquée par les autorités de certification privées est définie par chaque organisation. Si votre autorité de certification privée utilise les mêmes critères d'émission, les directives de ce document peuvent être utilisées.

Puis-je continuer à utiliser mes certificats existants ?

Oui, les certificats valides avec EKU combiné peuvent être utilisés jusqu'au moment de l'expiration.

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

Consultez la section Cas d'utilisation spécifiques.

Ressources supplémentaires

- ID de bogue Cisco CSCws83036 - Évaluation de l'impact de l'application ClientAuth EKU dans ISE
- Impact du pare-feu sécurisé Cisco sur l'authentification du client AC public Modifications de l'UKE à partir de mai 2026 pour les communications sécurisées

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 significatif 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 empêcher 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.