Préparer Expressway pour l’authentification client EKU Sunset dans les certificats de CA publique

Table des matières

- Introduction
- Informations de groupe secondaire
- Définition du problème
  - Modification de la politique du programme racine Chrome
  - Principales exigences de stratégie
  - Délai de réponse de l'AC publique
  - Documentation Cisco associée
- Impact sur la solution Expressway
  - Produits concernés
  - Double rôle d’Expressway
- Cas d'utilisation spécifiques
- Recommandations
  - Vérifier les certificats actuels (PREMIÈRE ÉTAPE OBLIGATOIRE)
  - 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
    - Considérations spéciales relatives au chiffrement des certificats
    - Éléments d'action pour le chiffrement des utilisateurs
  - Option 3: Évaluation et migration vers d'autres fournisseurs CA
    - Approche PKI privée
    - Solution à long terme (mises à niveau logicielles requises)
    - Détails sur la solution Cisco Expressway X15.4 (février 2026)
    - Détails sur la solution Cisco Expressway X15.5 (mai 2026)
- Arbre de décision
- Foire aux questions (FAQ)
  - Questions générales
  - Chiffrement des données spécifiques
  - Questions de mise à niveau
  - Spécifique à MRA (Mobile and Remote Access)
  - Gestion des certificats
  - Questions de calendrier
- Ressources supplémentaires
  - Documentation Cisco
  - Références externes

Ressources de l'autorité de certification

Conclusion

Points importants

Introduction

Ce document décrit les modifications de la politique du programme racine Chrome sur Cisco Expressway et l'EKU d'authentification client dans les certificats d'autorité de certification publics après le 26/06.

Informations de groupe secondaire

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 Expressway 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 compter de juin 2026, la politique du programme racine Chrome restreint les certificats de l'autorité de certification racine (CA) inclus dans le magasin racine Chrome, éliminant progressivement les racines polyvalentes pour aligner toutes les hiérarchies d'infrastructure à clé publique (PKI) afin de servir uniquement les cas d'utilisation d'authentification du serveur TLS.

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 du serveur pour maintenir la confiance du navigateur Google Chrome
- 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 : Juin 2026

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
- 11 février 2026 : Let's Encrypt arrête d'émettre des certificats avec l'EKU d'authentification client en utilisant le profil ACME classique
- Mai 2026 : Les serveurs CA publics arrêtent d'émettre des certifications EKU d'authentification client
- Juin 2026 : 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.

Documentation Cisco associée

- ID de bogue Cisco : CSCwr73373 - Prise en charge de certificats serveur et client distincts pour Expressway
- Avis de champ : FN74362
- Politique du programme racine de Chrome : documentation de la politique du programme racine de Chrome

Impact sur la solution Expressway

Produits concernés

Conformément à l'avis de champ FN74362, toutes les versions de Cisco Expressway sont concernées :

Product (produit)	Rejets affectés	Incidence
Expressway Core et Edge	X14 (toutes versions)	X14.0.0 à X14.3.7 - Toutes les versions affectées
Expressway Core et Edge	X15 (versions antérieures à X15.4)	X15.0.0 à X15.3.2 - Toutes les versions affectées

Double rôle d’Expressway

Les produits Cisco Expressway (Expressway-C et Expressway-E) agissent à la fois comme serveur et comme client dans divers scénarios de connexion, nécessitant des certificats avec des clés d’authentification serveur et client.

Expressway E en tant que serveur (authentification serveur EKU requise) :

- Accès au navigateur HTTPS
- Connexions de traversée UC SIP
- Connectivité audio/MRA Webex Edge

Expressway E en tant que client (authentification client EKU requise) :

- communications B2B
- Connexions MRA (Mobile and Remote Access)
- Fédération XMPP
- Connexions SIP Neighbor Zone/CMS
- Interactions avec les entités externes
- Connexion au cloud Cisco (intégration MRA)

Cas d'utilisation spécifiques

Le certificat public signé par l’autorité de certification avec l’UKE d’authentification du client actuellement utilisé pour les connexions mTLS dans Cisco Expressway est le certificat du serveur Expressway. Ce certificat est utilisé pour les connexions mTLS suivantes :

1. Appel B2B SIP sur mTLS - Expressway E devient client ou serveur sur une connexion mTLS, selon le site initié par la session
2. SIP IMP Federation over mTLS - Expressway E devient client ou serveur sur une connexion mTLS, selon le site initié par la session
3. UC Traversal Zone - Expressway C présente l’authentification client EKU
4. Zone de traversée avec configuration mTLS - Expressway C présente l’EKU d’authentification client
5. Zone de voisinage SIP avec configuration mTLS - Expressway devient client ou serveur sur une connexion mTLS, selon le site initié par la session, y compris les connexions avec :

- Cisco Unified Communications Manager (Unified CM)
- Cisco Unity
- Cisco Unified Border Element (CUBE)
- Serveur de réunion Cisco (CMS)
- Connexion au cloud Cisco - Intégration MRA (Expressway initie la connexion au cloud Cisco et présente l'EKU d'authentification client)

Recommandations

Vérifier les certificats actuels (PREMIÈRE ÉTAPE OBLIGATOIRE)

Conformément à l'avis FN74362, avant d'envisager une solution de contournement et des options de solution :

- Préparer un inventaire de tous les certificats TLS publics pour identifier les certificats qui contiennent l'EKU d'authentification du client
- Effectuez une sauvegarde de votre instance Cisco Expressway ou copiez manuellement le certificat signé et la clé privée
- Documenter l'utilisation des certificats : identifier les certificats utilisés pour les connexions mTLS
- 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

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 (selon FN74362) :

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 déploiement de création et d'utilisation de certificats Cisco Expressway (X14.0)
- Guide de déploiement de création et d'utilisation de certificats Cisco Expressway (X15.0)

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.

Considérations spéciales sur le chiffrement des certificats

Selon FN74362, si vous utilisez les certificats Let's Encrypt :

- Actuellement, Expressway utilise un profil ACME classique qui est codé en dur et qui ne peut pas être modifié par les utilisateurs
- Ce profil ACME classique est actuellement utilisé pour la demande de certificats qui incluent à la fois des unités EKU d'authentification serveur et client
- À partir du 11 février 2026, les demandes de certificat utilisant ce profil n'incluent plus l'EKU d'authentification client dans les certificats générés par Let's Encrypt

- Pour plus d'informations, consultez Ending TLS Client Authentication Certificate Support in 2026 - Let's Encrypt

Éléments d'action pour le chiffrement des utilisateurs

- Renouveler les certificats avant le 11 février 2026 - idéalement le plus près possible de cette date afin de maximiser la période de validité de 90 jours.
- Désactivez le planificateur automatisé ACME pour empêcher le renouvellement automatique des certificats après le 11 février 2026.
- Cette action permet d'éviter que les certificats soient écrasés par inadvertance avec des versions qui contiennent uniquement l'EKU d'authentification du serveur.
- Si vous ne renouvelez pas votre contrat avant le 11 février 2026, contactez le centre d'assistance technique Cisco.

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

Cette option s’applique à : Expressway C uniquement ; NON applicable à Expressway E.

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

---

⚠ Mise en garde : Cette option n’est pas viable pour Expressway-E, qui nécessite des certificats d’autorité de certification publics pour les services externes et la confiance du navigateur.

Solution à long terme (mises à niveau logicielles requises)

Conformément à la note de service FN74362, Cisco met en oeuvre des améliorations de produits dans des versions fixes afin de résoudre ce problème de manière exhaustive.

Calendrier de lancement fixe :

Product (produit)	Rejet Affecté	Déclenchement Fixe	Objectif de la correction	Disponibilité
Cisco Expressway	X14.x (toutes versions) X15.x (antérieure à X15.4)	X15,4	Solution intermittente : Permet le téléchargement supplémentaire du certificat signé ServerAuth EKU uniquement sur Expressway E et l'ajustement de la vérification du certificat pour le signal SIP MRA entre Expressway E et Expressway C	Février 2026
Cisco Expressway	X14.x (toutes versions) X15.x (antérieure à X15.5)	X15,5	Solution complète : Améliore l'interface utilisateur pour la séparation des certificats client et serveur et fournit des options aux administrateurs pour désactiver la vérification de l'UKE	Mai 2026

Remarque : Cisco Expressway E et Expressway C doivent être mis à niveau vers la même version.

Détails sur la solution Cisco Expressway X15.4 (février 2026)

Objectif : Solution intermittente pour prendre en charge les certificats avec ServerAuth EKU uniquement et pour activer les enregistrements MRA

Principales améliorations :

- Supprime la restriction sur les téléchargements de certificats
- Permet aux administrateurs de télécharger des certificats avec uniquement l'EKU d'authentification de serveur via l'interface utilisateur graphique Web sur Expressway E
- Auparavant, Expressway rejetait les certificats de serveur uniquement
- Ajuste la vérification du certificat pour MRA
- Modifie la vérification de certificat pour la signalisation SIP entre Expressway-E et Expressway-C dans les solutions MRA

- Autorise l'acceptation de certificats de serveur uniquement à partir d'applications tierces

Qui peut effectuer la mise à niveau vers X15.4 :

- si vous déployez un nouveau système ou redéployez un système Expressway-E pour MRA existant avec des certificats signés uniquement pour le serveur.
- Si vous utilisez des certificats ACME (Let's Encrypt) après le 11 février 2026.
- Les déploiements existants qui doivent mettre à niveau des certificats signés qui ne contiennent que l'EKU d'authentification du serveur.
- Si vous rencontrez des problèmes d'authentification liés aux certificats dans les connexions mTLS

Configuration requise importante pour X15.4 :

- Expressway-E et Expressway-C doivent être mis à niveau vers X15.4
- Planifier la mise à niveau pendant la fenêtre de maintenance pour minimiser les interruptions de service

Les limites de X15.4 sont les suivantes :

- Il s'agit d'une solution intermittente qui résout les problèmes de compatibilité immédiats
- Ne prend pas entièrement en charge les doubles certificats
- N'inclut pas de paramètre de service pour désactiver la vérification EKU
- Les connexions mTLS peuvent échouer en fonction du site lancé par la session

Détails sur la solution Cisco Expressway X15.5 (mai 2026)

Objectif : Solution complète pour répondre aux exigences globales du programme racine Google Chrome

Principales améliorations des produits :

- Séparation des certificats client et serveur
- Permet la prise en charge de deux certificats distincts sur la même interface
- Certificats Expressway avec EKU d’authentification serveur et EKU d’authentification client distincts
- Facilite les connexions mTLS appropriées avec des rôles de certificats séparés
- Améliorations de l'interface utilisateur et du back end
- Nouvelles interfaces de gestion des certificats pour la gestion individuelle des deux certificats
- Validation de l'EKU d'authentification client pendant le chargement du certificat pour éviter les pertes accidentelles de connexion MTLS
- Les administrateurs peuvent télécharger et gérer séparément les certificats serveur et client
- Options de désactivation de la vérification EKU d'authentification client
- Paramètre de service permettant aux administrateurs de désactiver le contrôle EKU d'authentification client en fonction des exigences de l'entreprise
- Permet à Cisco Expressway d’ignorer l’EKU de l’homologue distant (client) demandant

une connexion avec uniquement les certificats d’EKU d’authentification du serveur
- En l’absence d’un certificat EKU d’authentification client, permet à Expressway de (ré)utiliser le certificat EKU d’authentification serveur uniquement comme certificat client

---

Remarque : Dans ce cas, l'homologue distant doit également prendre en charge un modèle EKU d'authentification du client Ignore similaire

---

Arbre de décision

DÉBUT : Utilisez-vous des certificats d’autorité de certification publique sur Expressway ?

│

├─ 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 les connexions mTLS ? (Consultez les cas d'utilisation dans la section Cas d'utilisation spécifiques)

  │ │

  │ ├─ NON : Authentification du serveur uniquement

  │ │ └─ Impact minimal - Surveiller les modifications futures

  │ │

  │ └─ OUI : connexions mTLS avec EKU d'authentification client

  │ │

  │ └─ 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

│ │ ├─ Si nous allons chiffrer : Renouvellement avant le 11 février 2026

│ │ │ └─ Désactiver le planificateur ACME après le renouvellement

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

│ │ └─ Achète du temps jusqu'à l'expiration du certificat

│ │

│ ├─ Option C : Migrer vers une PKI privée (Expressway-C uniquement)

│ │ ├─ Configurer une infrastructure CA privée

│ │ ├─ Délivrer des certificats EKU combinés

│ │ ├─ Distribuer la racine à tous les homologues

│ │ └─ Contrôle à long terme, PAS pour Expressway-E

│ │

│ └─ Option D : Planifier la mise à niveau logicielle

│ ├─ Besoin urgent ? → Mise à niveau vers X15.4 (février 2026)

│ └─ Solution complète → Mise à niveau vers X15.5 (mai 2026)

│ └─ Obtenir ensuite des certificats serveur/client distincts

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 : Que faire si je n'utilise pas de connexions mTLS ?

R : Si vous utilisez uniquement le protocole TLS standard (authentification serveur), vous n'êtes pas affecté par cette stratégie. Vos certificats de serveur uniquement continuent à fonctionner. Cependant, vérifiez vos cas d'utilisation par rapport à la liste dans la section Cas d'utilisation spécifiques affectés, car certains cas d'utilisation utilisent par défaut mTLS.

Q : Mes connexions Web HTTPS standard à Expressway vont-elles cesser de fonctionner ?

R : Non. Les connexions TLS standard ne sont pas affectées. L'accès du navigateur Web à Expressway continue de fonctionner normalement, même avec des certificats EKU serveur uniquement.

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 : Revoir la section Cas d'utilisation spécifiques.

Q. Que puis-je faire maintenant ?

R : Cisco recommande vivement les mesures suivantes :

- Audit de vos certificats

  Identifier les certificats TLS publics utilisés pour mTLS

- Renouveler les certificats plus tôt

  Renouveler avant le 15 mars 2026 pour maximiser la validité

- Contrôle de l'automatisation ACME

  Désactiver les renouvellements automatiques qui peuvent remplacer les certificats de manière inattendue

- Coordonner avec votre CA

  Certains CA proposent des profils de certificat temporaires ou alternatifs

Q : CUCM SU3(a) est-il compatible avec X15.4 et X15.5 ?

A : Oui

Q : Existe-t-il une faille de sécurité avec la désactivation de la vérification de l'UKE du client dans Cisco Expressway E (avec la version X15.5) ?

R : Le certificat vérifie toujours CN/SAN pour vérifier la source de connexion est valide, seulement contourner la validation EKU (certificat pour le rôle de client) qui a été inclus par défaut jusqu'à ce

que Google soulève des problèmes de sécurité, par conséquent ne doit pas avoir problème de sécurité par rapport à avant.

Chiffrons les données spécifiques

Q : J’utilise Let’s Encrypt with ACME sur Expressway. Que puis-je faire ?

A :

1. Renouvelez votre certificat avant le 11 février 2026 (le plus près possible de cette date)
2. Désactiver le planificateur automatisé ACME immédiatement après le renouvellement
3. Prévoyez une mise à niveau vers X15.5 pour une solution à long terme

Q : Puis-je modifier le profil ACME pour continuer à obtenir des certificats EKU combinés ?

A : Non. Expressway utilise actuellement un profil ACME « classique » codé en dur qui ne peut pas être modifié par les utilisateurs. Veuillez contacter le TAC Cisco pour obtenir de l’aide sur le profil de certificat ACME.

Questions de mise à niveau

Q : Dois-je mettre à niveau Expressway-E et Expressway-C ?

A : Oui, absolument. Les deux doivent être mis à niveau vers la même version (X15.4 ou X15.5) pour un fonctionnement correct.

Q : Puis-je effectuer une mise à niveau vers X15.4 ou attendre X15.5 ?

A :

- Effectuez une mise à niveau vers X15.4 si vous rencontrez des problèmes urgents ou si vous devez accepter les certificats de serveur uniquement maintenant
- Si possible, attendez X15.5 (mai 2026) pour la solution complète avec prise en charge du double certificat

Q : Ma réplication de cluster est interrompue après le renouvellement du certificat. Que s'est-il passé ?

R : Il est probable que votre nouveau certificat ne dispose que de l'EKU d'authentification serveur, mais :

- Si aucune version antérieure à X15.4 avec TLS Verify = Application : Les homologues de cluster ne peuvent pas établir de connexions mTLS sans EKU d'authentification client
- Options de solution (l'une ou l'autre) :

  Définissez le mode de vérification TLS sur « Permissive » (moins sécurisé)

  Obtenir des certificats avec EKU combiné de la racine CA alternative

  Mise à niveau vers X15.4 ou version ultérieure, qui contourne la vérification de l'EKU

d'authentification du client pour ClusterDB

Q : Après la mise à niveau vers X15.4, puis-je utiliser le mode d'application avec des certificats de serveur uniquement dans ma grappe ?

R : Oui. À partir de X15.4, Expressway contourne la vérification de l'EKU d'authentification du client pour les connexions mTLS ClusterDB. Par conséquent, la vérification TLS peut être définie sur « Application » même si un ou plusieurs noeuds de cluster ont uniquement l'EKU d'authentification du serveur.

Q : Pourquoi ne puis-je pas télécharger mon certificat via l'interface utilisateur graphique d'Expressway Web ?

R : Avant X15.4, l'interface utilisateur graphique Web applique une validation codée en dur qui exige que les certificats aient l'EKU d'authentification client. Si votre certificat dispose uniquement de l'EKU d'authentification du serveur, vous avez deux options :

- Utilisez le protocole SCP (Secure Copy Protocol) pour télécharger le certificat directement sur le serveur (dossier /persistent/Certs)
- Mise à niveau vers X15.4 ou version ultérieure (Expressway-E uniquement), ce qui supprime cette restriction

Q : Après la mise à niveau vers X15.4, je ne peux toujours pas télécharger de certificats de serveur uniquement vers Expressway-E

R : Une fois mise à niveau, vérifiez que cette commande est activée

xConfiguration Certificat XCP TLS CVS EnableServerEkuUpload : On (activé)

Q : J'ai effectué une mise à niveau vers X15.4. Puis-je à présent télécharger des certificats de serveur uniquement sur Expressway-E et Expressway-C ?

R : Non. X15.4 supprime uniquement la restriction de téléchargement pour Expressway-E. Expressway-C nécessite toujours des certificats EKU combinés pour le téléchargement via l'interface graphique Web. En effet, Expressway-C agit fréquemment en tant que client TLS dans les zones de traversée UC et nécessite l'authentification client EKU. Assurez-vous que vous exécutez cette commande sur Expressway-E. Cette commande ne fonctionne pas sur Expressway-C

xConfiguration Certificat XCP TLS CVS EnableServerEkuUpload : On (activé)

Q : Je ne peux pas enregistrer la licence Smart après le renouvellement du certificat. Pourquoi ?

A : L'échec de la licence Smart après le renouvellement du certificat n'est généralement PAS lié à EKU :

- Vérifiez si Expressway peut atteindre tools.cisco.com (CSSM)
- Vérifier que les règles de pare-feu autorisent le trafic HTTPS sortant (port 443)
- Vérifiez si la configuration du proxy est correcte (si vous utilisez un proxy HTTP)

- Vérifier que le certificat du serveur CSSM est approuvé dans le magasin d’approbation Expressway
- Smart Licensing ne nécessite pas clientAuth, de sorte que cette modification de stratégie ne l'affecte pas

Spécifique à MRA (Mobile and Remote Access)

Q : Le MRA nécessite-t-il l’authentification client EKU sur Expressway-E ?

R : Cela dépend de la version Expressway :

- Avant X15.4 : Oui, indirectement requis

  Pendant la signalisation SIP MRA, Expressway-E envoie son certificat signé dans un message SIP SERVICE à Expressway-C

  Expressway-C valide le certificat, nécessitant à la fois l’authentification du client et l’authentification du serveur

  Sans EKU combiné, l'enregistrement MRA SIP échoue

- X15.4 et versions ultérieures : Non

  Expressway-C ne valide plus l’EKU d’authentification du client dans le message SIP SERVICE

  Expressway-E nécessite uniquement l’authentification serveur EKU pour MRA

  UC Traversal Zone fonctionne de manière unidirectionnelle (Expressway-C valide uniquement le certificat du serveur Expressway-E)

Q : Pourquoi mes zones voisines échouent après avoir téléchargé leEKU d’authentification serveur sur Expresswayx15.4

A : Si vous activez le mode de vérification TLS, vous devez disposer d'une clé d'authentification client. Vous pouvez donc désactiver la vérification TLS dans la configuration de la zone voisine

Q : Quels sont les certificats nécessaires au bon fonctionnement de MRA ?

A : Pour un déploiement MRA type :

Composante	Exigences du certificat	EKU requis	Remarques
Expressway-E (avant X15.4)	serverAuth + clientAuth	Les deux	Pour la validation SIP SERVICE par Exp-C
Expressway-E	serverAuth	Serveur	Vérification EKU du client

(X15.4+)	uniquement	uniquement	ignorée
Expressway-C	clientAuth + serverAuth	Les deux	Agit toujours comme client dans UC Traversal
Zone de traversée UC	Validation unidirectionnelle	Exp-E : serverAuth Exp-C : clientAuth	Exp-C valide le certificat de serveur Exp-E

Q : Mon ARM fonctionnait bien, mais après le renouvellement de mon certificat Expressway-E avec l'UKE serveur seulement, l'enregistrement SIP échoue. Qu'est-ce qui ne va pas ?

R : Si vous exécutez une version antérieure à X15.4, la signalisation SIP MRA nécessite qu'Expressway-E présente les clés d'authentification serveur et client dans le message SIP SERVICE. Vos options :

- Obtenir un certificat avec EKU combiné
- Basculer vers une racine CA alternative qui émet une UKE combinée
- Mettre à niveau Expressway-E et Expressway-C vers X15.4 ou version ultérieure (recommandé)

Gestion des certificats

Q : Comment puis-je obtenir un certificat avec EKU combiné de DigiCert ou IdenTrust ?

A : Contactez votre fournisseur d'autorité de certification et demandez un certificat à sa racine alternative qui émet toujours une clé d'activation combinée.

Q : Mon autorité de certification indique qu'elle ne peut fournir que des certificats de serveur uniquement. Que puis-je faire ?

A : Plusieurs options s'offrent à vous :

- Recherchez des racines alternatives : Demandez à votre autorité de certification si elle a d'autres racines qui génèrent une unité EKU combinée (comme DigiCert Assured ID ou IdenTrust Public Sector)
- Fournisseurs CA de commutateur : Recherchez les CA offrant EKU combiné à partir de racines non-Chrome de confiance
- Utiliser une PKI privée : Configurer une autorité de certification interne pour les certificats EKU combinés (déploiements Expressway-C uniquement)
- Mise à niveau vers X15.4 : Solution intermittente pour gérer les certificats avec ServerAuth EKU uniquement et pour activer les enregistrements MRA
- Mise à niveau vers X15.5 une fois disponible : Planifiez une architecture à double certificat où les certificats réservés aux serveurs sont acceptables et une solution complète pour

répondre aux exigences globales du programme racine Google Chrome

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 :

- 11 février 2026 : Let's Encrypt arrête l'EKU combiné via ACME classique
- 15 mars 2026 : Validité du certificat réduite à 200 jours
- Mai 2026 : La plupart des AC publiques arrêtent entièrement d'émettre des EKU combinés
- Juin 2026 : Politique Chrome pleinement appliquée

Ressources supplémentaires

Documentation Cisco

- Avis de zone FN74362 : Impact de Cisco Expressway sur la communication sécurisée en raison des modifications à venir apportées aux certificats TLS
- ID de bogue Cisco CSCwr73373: Prise en charge de certificats serveur et client distincts pour Expressway

Références externes

- Politique du programme racine Chrome
- Chiffrement en cours : Fin de la prise en charge des certificats d'authentification client TLS en 2026
- Exigences de base du forum CA/navigateur

Ressources de l'autorité de certification

- Portail d'assistance DigiCert
- Services de certificats IdenTrust
- Forum de la communauté Chiffrons
- Base de connaissances Sectigo

Conclusion

La suppression de l’UKE d’authentification client dans les certificats d’autorité de certification publique représente un changement significatif de la stratégie de sécurité qui a un impact sur les déploiements Cisco Expressway utilisant des connexions mTLS. Bien qu'il s'agisse d'un changement à l'échelle de l'industrie, la cote d'impact est CRITIQUE selon l'avis de secteur FN74362, et des mesures immédiates sont requises pour prévenir les interruptions de service.

Points importants

- Cela concerne TOUTES les versions d’Expressway (X14 et X15 avant X15.4)
- Auditer vos certificats MAINTENANT - C'est la première étape obligatoire
- Plusieurs solutions de contournement sont disponibles : choisissez la solution la mieux adaptée à votre environnement
- Mises à niveau logicielles requises pour la solution à long terme - Planifier pour X15.5
- Expressway-E et Expressway-C doivent être mis à niveau ensemble
- Chiffrons les utilisateurs avant la date limite la plus proche - 11 février 2026

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.