Certificat SAML ISE

Contenu

Introduction

Ce document décrit les certificats système SAML (Security Assertion Markup Language) dans Cisco Identity Services Engine (ISE). Il couvre le but des certificats SAML, comment effectuer le renouvellement, et enfin répond aux fréquentes FAQ. Il couvre ISE de la version 2.4 à la version 3.0, cependant, il doit être similaire ou identique à d'autres versions de logiciel ISE 2.x et 3.x, sauf indication contraire.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

1. Cisco ISE
2. Terminologie utilisée pour décrire différents types de déploiements ISE et AAA (Authentication, Authorization and Accounting)
3. Notions de base sur les protocoles RADIUS et AAA
4. protocole SAML
5. Certificats SSL/TLS et x509
6. Notions de base sur l'infrastructure à clé publique (PKI)

Components Used

Les informations de ce document sont basées sur Cisco Identity Services Engine (ISE), versions 2.4 à 3.0

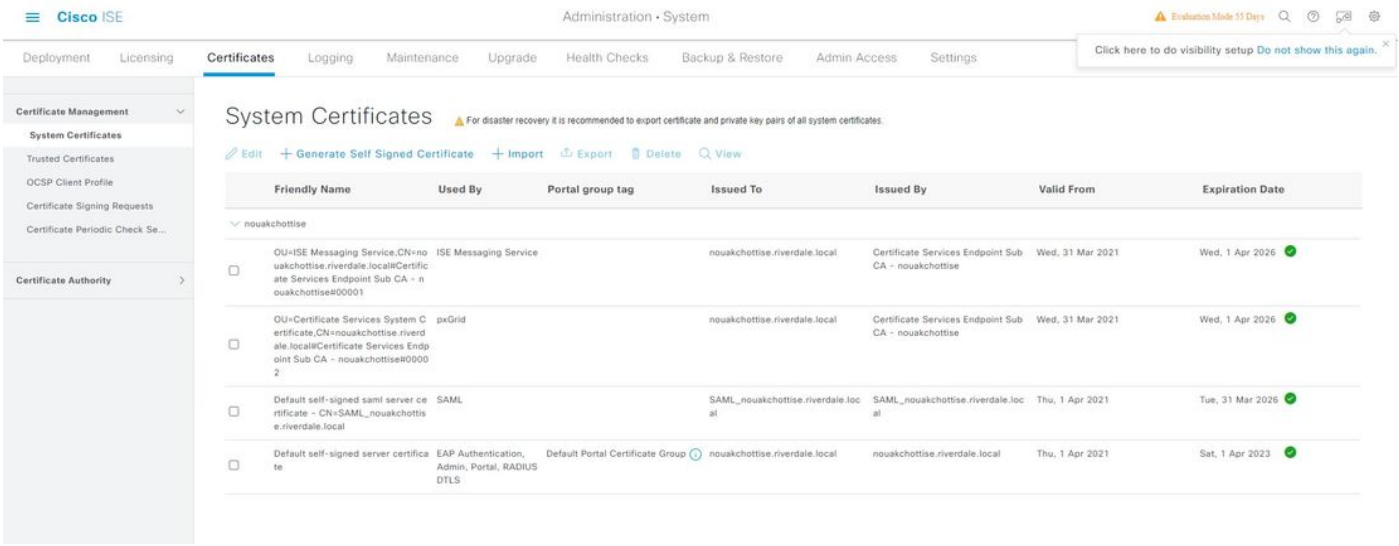
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute commande ou configuration.

Certificats SSL dans ISE

Un certificat SSL (Secure Sockets Layer) est un fichier numérique qui identifie un individu, un serveur ou toute autre entité numérique et associe cette entité à une clé publique. Un certificat auto-signé est signé par son créateur. Les certificats peuvent être autosignés ou signés numériquement par une autorité de certification externe (CA) - généralement le propre serveur d'autorité de certification d'une société ou un fournisseur d'autorité de certification connu. Un certificat numérique signé par une autorité de certification est considéré comme une norme de l'industrie et plus sûr qu'un certificat autosigné.

Cisco ISE s'appuie sur PKI pour fournir une communication sécurisée avec les points d'extrémité et les administrateurs, entre ISE et d'autres serveurs/services, et entre les noeuds Cisco ISE dans un déploiement multinoeud. PKI utilise des certificats numériques X.509 pour transférer des clés publiques pour le chiffrement et le déchiffrement des messages et pour vérifier l'authenticité d'autres certificats représentant les utilisateurs et les périphériques. Grâce au portail d'administration de Cisco ISE, vous pouvez gérer ces certificats X.509.

Dans ISE, les certificats système sont des certificats de serveur qui identifient un noeud Cisco ISE à d'autres applications (terminaux, autres serveurs, etc.). Chaque noeud Cisco ISE possède ses propres certificats système qui sont stockés sur le noeud avec les clés privées correspondantes. Chaque certificat système peut être mappé à des rôles qui indiquent l'objectif du certificat tel qu'illustré dans l'image.



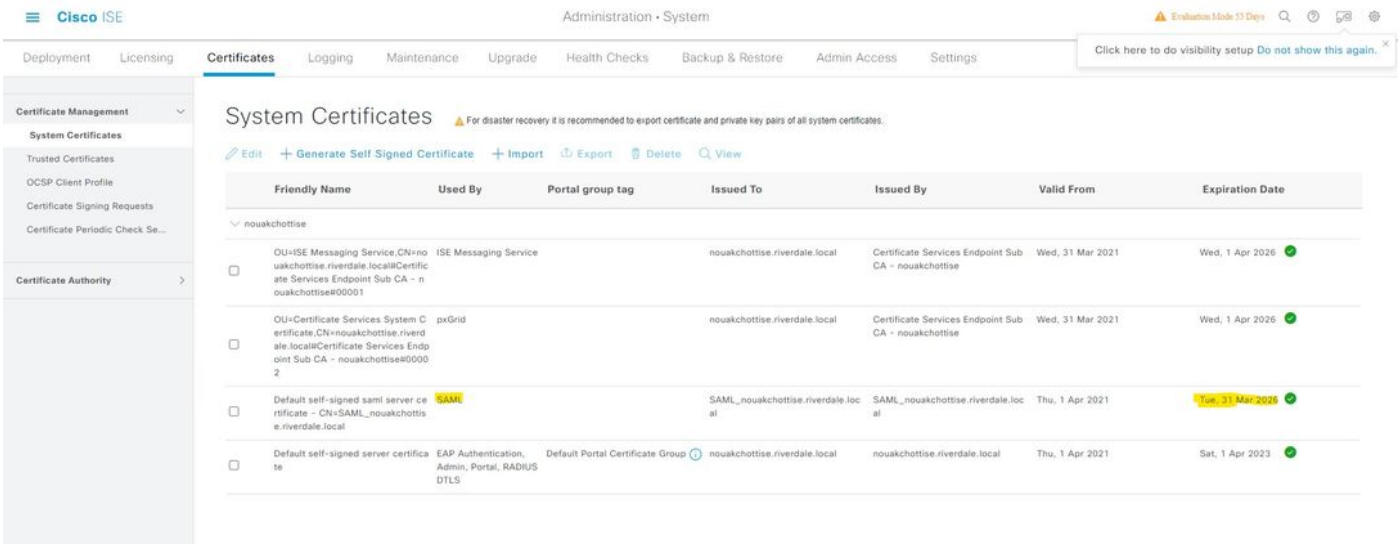
Certificats système ISE 3.0

La portée de ce document est uniquement pour le certificat SAML. Pour obtenir d'autres certificats dans ISE et plus d'informations sur les certificats SSL dans ISE en général, reportez-vous à ce document : Certificats TLS/SSL dans ISE - Cisco

Certificat SAML dans ISE

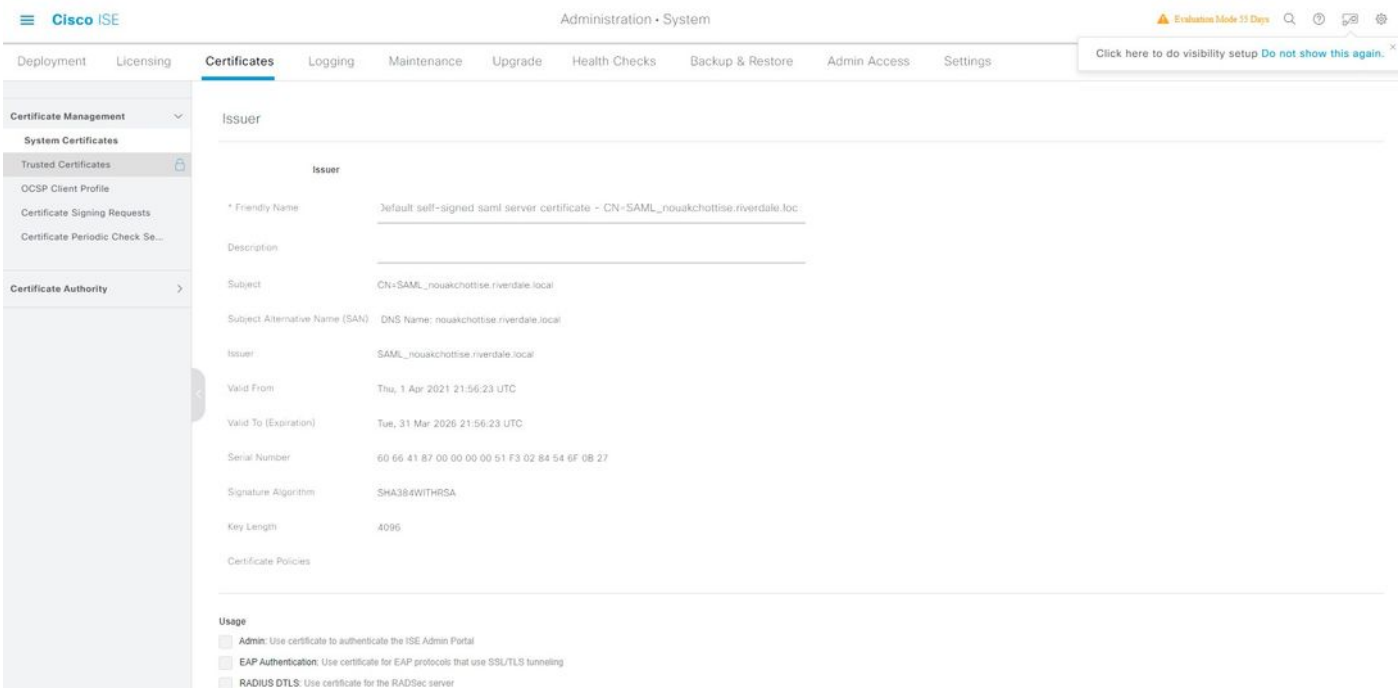
Le certificat SAML dans ISE est déterminé en recherchant les certificats système ayant l'entrée SAML dans le champ Utilisations. Ce certificat sera utilisé pour communiquer avec les fournisseurs d'identité SAML (IdP), comme vérifier que les réponses SAML sont reçues de l'IdP correct et sécuriser la communication avec l'IdP. Remarque : les certificats désignés pour l'utilisation SAML ne peuvent pas être utilisés pour un autre service, tel qu'Admin, l'authentification

EAP, etc.



Pour la première installation d'ISE, ISE est livré avec un certificat de serveur SAML autosigné qui possède les propriétés suivantes :

Taille de clé : 2048
Validité : un an
Utilisation des clés : Signature numérique (signature)
Utilisation de clé étendue : Authentification du serveur Web TLS (1.3.6.1.5.5.7.3.1)



Note: Il est recommandé de ne pas utiliser de certificat qui contient la valeur 2.5.29.37.0 pour l'identificateur d'objet Any Purpose dans l'attribut Extended Key Usage. Si vous utilisez un certificat qui contient la valeur 2.5.29.37.0 pour l'identificateur d'objet Any Purpose dans l'attribut Extended Key Usage, le certificat est considéré comme non valide et le message d'erreur suivant s'affiche : « source=local ; type=fatal ; message=« certificat non pris en charge ».

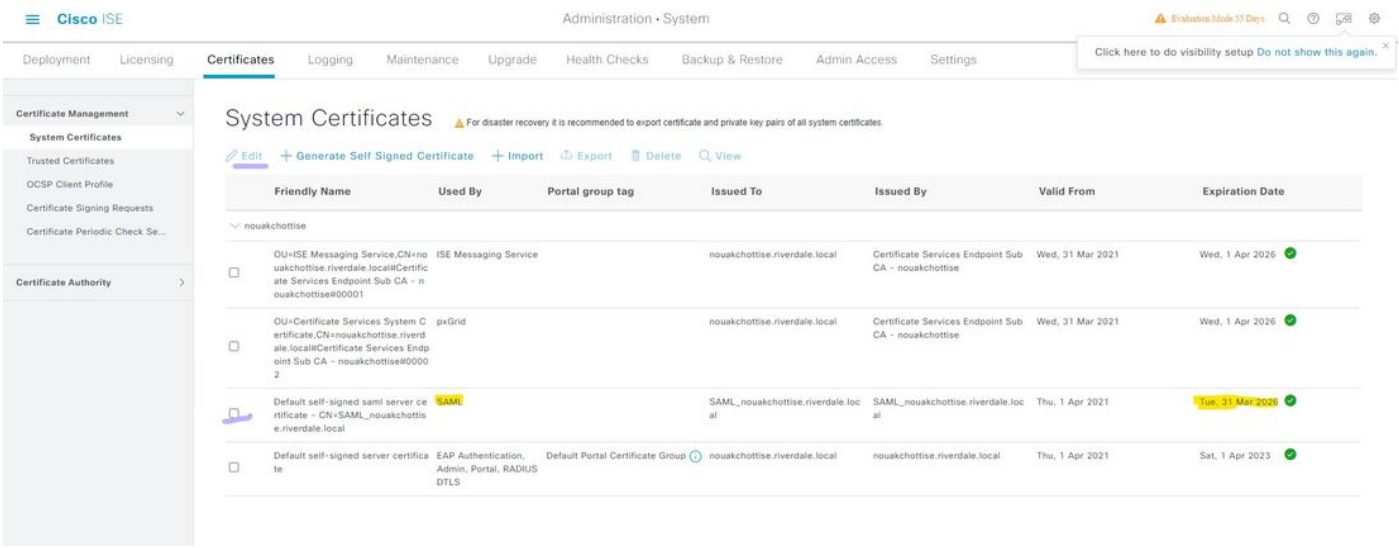
Les administrateurs ISE devront renouveler ce certificat SAML autosigné avant expiration, même si la fonctionnalité SAML n'est pas utilisée activement.

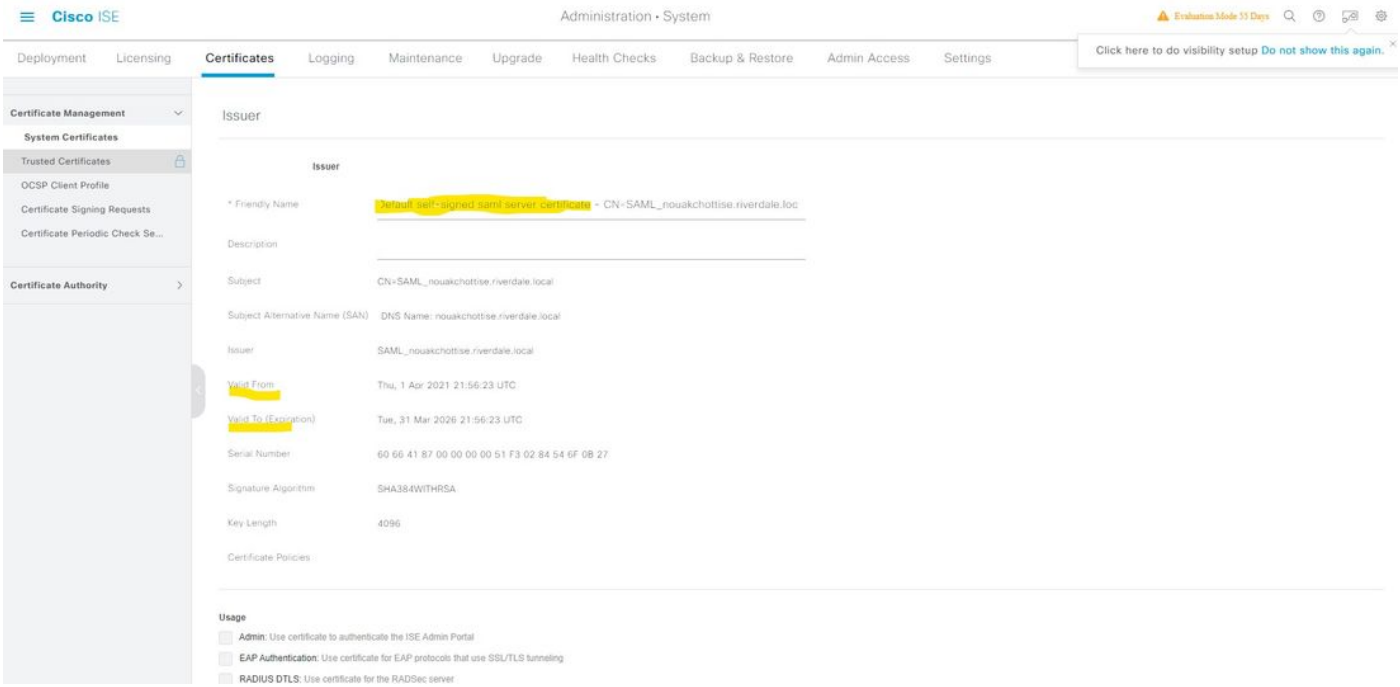
Renouveler un certificat SAML auto-signé dans ISE

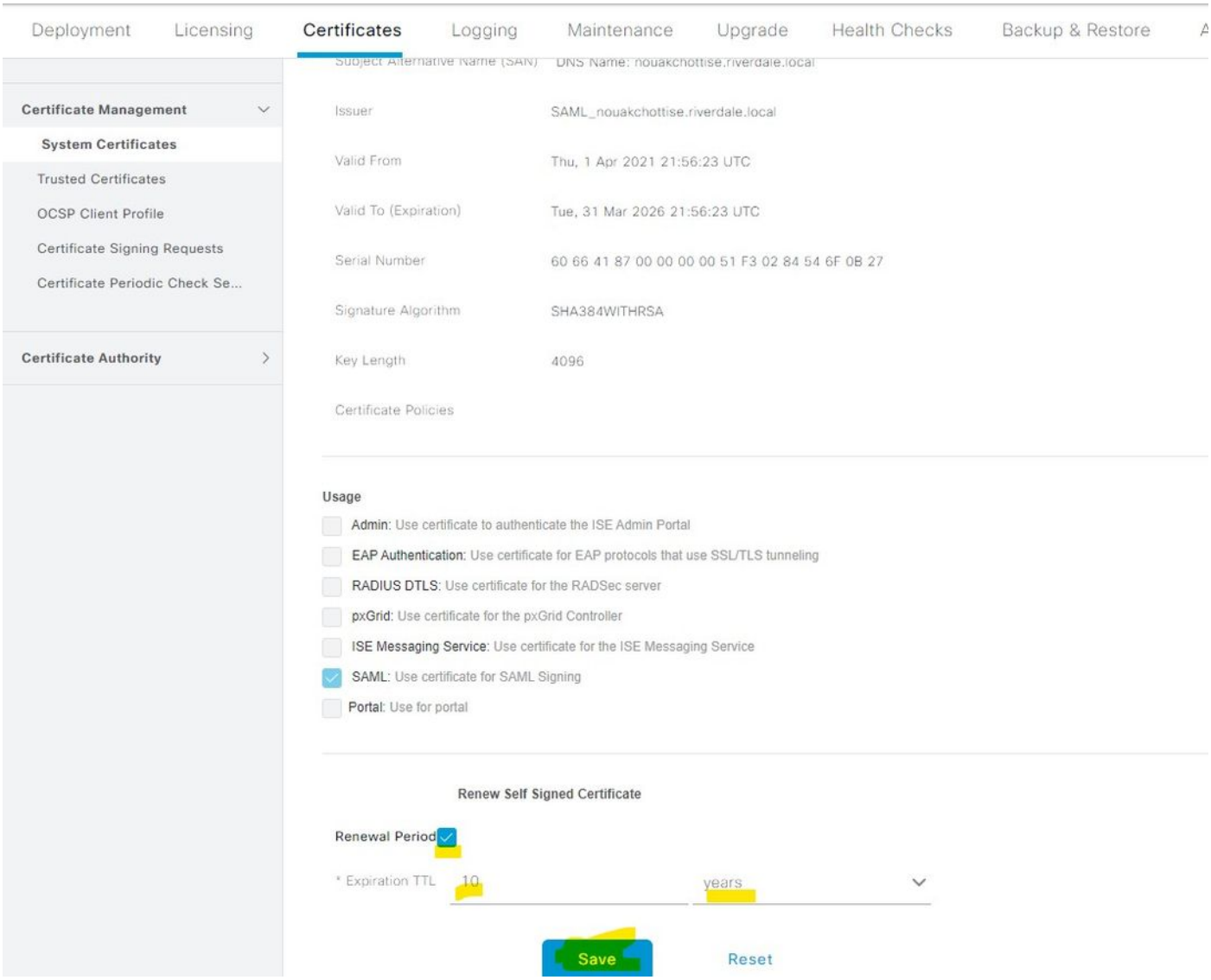
Un problème courant auquel les utilisateurs sont confrontés est que leurs certificats SAML finiront par expirer et ISE les avertit par ce message :

```
Alarm Name :
Certificate Expiration

Details :
Trust certificate 'Default self-signed server certificate' will expire in 60 days :
Server=Kolkata-ISE-001

Description :
This certificate will expire soon. When it expires, ISE may fail when attempting to establish
secure communications with clients. Inter-node communication may also be affected

Severity :
Warning

Suggested Actions :
Replace the certificate. For a trust certificate, contact the issuing Certificate Authority
(CA). For a CA-signed local certificate, generate a CSR and have the CA create a new
certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can
just delete the certificate if it is no longer used.
```

Pour les certificats de serveur auto-signés, il est possible de renouveler le certificat juste pour cocher la période de renouvellement de case et mettre 5-10 ans comme indiqué sur l'image.







En fait, tout certificat auto-signé qui n'est pas actif et utilisé par vos noeuds de déploiement ISE peut simplement être renouvelé pour une période de 10 ans ; cela garantit que vous ne recevez aucun avis d'expiration pour les certificats pour les services que vous n'utilisez pas. 10 ans est la

durée de vie maximale autorisée pour les certificats ISE auto-signés, et devrait généralement être suffisante. La mise à jour de certificats système sur ISE ne déclenche pas un redémarrage des services tant qu'il n'est pas désigné pour l'utilisation 'Admin'.

Conclusion

Pour tout certificat système ISE expiré (autosigné et signé par l'autorité de certification) non utilisé, il est recommandé de le remplacer, de le supprimer ou de le renouveler, et il est recommandé de ne pas conserver de certificats périmés (système ou approuvé) sur ISE avant d'effectuer une mise à niveau ISE.

Informations connexes

- ISE 3.0 Gestion des certificats : Guide de l'administrateur de Cisco Identity Services Engine, version 3.0 - Configuration de base [Cisco Identity Services Engine] - Cisco
- Certificats SSL dans ISE : Certificats TLS/SSL dans ISE - Cisco
- Support et documentation techniques - Cisco Systems