

Identity Services Engine - Méfiance d'urgence des autorités de certification racine et intermédiaire eMudhra

Table des matières

Objectif

Vous trouverez ci-dessous les conseils sur Identity Services Engine et ISE PIC (Passive Identity Connector) pour la méfiance d'urgence des autorités de certification racine et intermédiaire eMudhra. La configuration du moteur Identity Service Engine n'inclut pas les autorités de certification racine et intermédiaire eMudhra affectées par défaut dans le magasin de confiance, mais la configuration ISE doit être examinée pour s'assurer qu'elles ne sont pas utilisées via la configuration post-installation.

***EXCLUSION DE RESPONSABILITÉ ***

Cet article a pour seul but de vous aider à vérifier la configuration ISE afin de détecter la présence des autorités de certification concernées. Le moteur Identity Services Engine dans son ensemble est toujours en cours d'étude et peut nécessiter d'autres mises à jour logicielles ou de configuration à l'avenir. Cet article sera mis à jour avec l'avis de sécurité disponible à l'adresse <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>.

Certificats système

Accédez à Administration -> Système -> Certificats -> Certificats système, sélectionnez chaque certificat attribué aux noeuds 1 par 1 et sélectionnez Affichage. [1]



Certificate Hierarchy

Certificate Services Root CA - zer0k-ise1

Certificate Services Node CA - zer0k-ise1

Certificate Services Endpoint Sub CA - zer0k-ise1

zer0k-ise1.zer0k.org



zer0k-ise1.zer0k.org

Issued By : Certificate Services Endpoint Sub CA - zer0k-ise1

Expires : Mon, 4 Aug 2031 10:52:08 EDT

Certificate status is good

Details

Issued To

Common Name (CN) zer0k-ise1.zer0k.org

Assurez-vous que l'autorité de certification concernée ou les certificats émetteurs ne figurent pas dans la hiérarchie de certificats. S'ils sont en cours d'utilisation, commencez à prendre des mesures pour migrer ce service vers une nouvelle autorité de certification.

Certificats approuvés

Accédez à Administration -> Système -> Certificats -> Certificats de confiance et vérifiez la liste des certificats racines et intermédiaires installés. Si vous trouvez une ou plusieurs autorités de certification concernées dans la liste Approuvées, notez la colonne « Approuvées pour » et effectuez l'action suivante pour chaque type [2] :

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From
		Endpoints				
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016
☐	Cisco Root CA M1	Infrastructure Cisco Services Endpoints AdminAuth NativeIPSec	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 20...

- Services Cisco - Cisco n'utilise pas eMudhra pour les services, s'il s'agit de la seule entrée, le certificat peut être supprimé.
- Infrastructure : vérifiez que le rôle Endpoints et/ou AdminAuth n'est pas requis, vérifiez qu'aucun certificat de l'autorité de certification ou des émetteurs n'est utilisé sous Certificats système
- Terminaux : vérifiez si les terminaux sont en cours d'authentification et nécessitent la chaîne compromise. Si vous ne savez pas si les terminaux utilisent l'autorité de certification ou les émetteurs, désactivez l'option « Approuver pour l'authentification client et Syslog » et surveillez les journaux en direct et les rapports pour les échecs d'authentification client.
- AdminAuth - Émettez de nouveaux certificats à vos administrateurs, car une option rapide L'authentification Admin peut être rétablie à la connexion par mot de passe pendant l'émission de nouveaux certificats.
- Native IPSec : si vous utilisez la fonctionnalité Native IPSec, migrez les clients IPSec vers une nouvelle autorité de certification

Autres services

Les configurations de service suivantes doivent être vérifiées afin de s'assurer que la suppression des certificats de confiance affectés n'aura pas d'impact sur le fonctionnement du système. S'ils sont utilisés, ces services doivent être reconfigurés pour utiliser de nouveaux certificats avant la suppression des certificats de confiance.

LDAP

Accédez à Administration -> Gestion des identités -> Sources d'identités externes -> LDAP. Sous chaque entrée LDAP, cliquez sur l'onglet Connexion. Si l'authentification sécurisée est activée, vérifiez la chaîne des paramètres « Autorité de certification racine du serveur LDAP » et « Autorité de certification émettrice des certificats ISE ». [3]

LDAP Server Root CA VeriSign Class 3 Public Pri... ⓘ

LDAP Server Root CA VeriSign Class 3 Public Pri... ⓘ

Issuer CA of ISE Certificates DigiCert Global Root CA ▼ ⓘ

Issuer CA of ISE Certificates Select if required (optional) ▼ ⓘ

SYSLOG

Accédez à Administration -> System -> Logging -> Remote Logging Targets, affichez chaque serveur SYSLOG sécurisé configuré pour le certificat racine de confiance configuré, si l'un des certificats d'autorité de certification concernés est en cours d'utilisation, vérifiez la chaîne sur le serveur SYSLOG et réexécutez et approuvez une nouvelle racine si nécessaire. [4]

Select CA Certificate

Cisco Root CA M1



Note: The CA certificates should be imported into the Certificate Store, enabled, and trusted for client authentication prior to configuring Secure Syslog. Ensure that a local certificate signed by the selected CA exists on the primary and secondary nodes.

If a local certificate signed by the selected CA does not exist, the self-signed local certificate will be used.

Ignore Server Certificate validation

☐

RADIUS DTLS

Il est possible de définir en option l'« Autorité de certification émettrice des certificats ISE pour CoA » sous chaque périphérique réseau sous Administration -> Ressources réseau -> Périphériques réseau. Ce paramètre est uniquement utilisé pour sélectionner le certificat client qu'ISE utilisera pour émettre une CoA à un périphérique réseau configuré pour DTLS. Le certificat s'affiche sur la page System Certificates dans ISE pour le nœud. Par conséquent, ce paramètre ne doit être vérifié pour chaque périphérique réseau configuré que si un certificat émis par l'un des certificats eMudhra est émis vers un nœud ISE.

[1] [Gestion des certificats dans ISE](#)

[2] [Paramètres du certificat de confiance ISE](#)

[3] [Configuration LDAP sécurisée ISE](#)

[4] [Configurer la cible de journalisation à distance Syslog sécurisée](#)

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.