

# Identity Services Engine - Noodsituatie wantrouwen van Mudhra Root en Intermediate Certificate Autoriteiten

## Inhoud

---

## Doel

Hieronder vindt u de richtlijnen over Identity Services Engine en ISE PIC (Passive Identity Connector) voor het wantrouwen in noodgevallen van Mudhra Root en Intermediate Certificate Authorities. De configuratie van de identiteitsservice-engine omvat niet standaard de betrokken eMudhra Root- en Intermediate Certificate Authorities in de vertrouwde winkel, maar de ISE-configuratie moet worden gecontroleerd om te controleren of deze niet worden gebruikt via de configuratie na installatie.

### \*\*\*DISCLAIMER\*\*\*

Dit artikel is alleen bedoeld om te helpen bij het beoordelen van de ISE-configuratie op aanwezigheid van de betrokken certificeringsautoriteiten. Identity Services Engine als geheel wordt nog onderzocht en kan in de toekomst verdere configuratie- of software-updates vereisen. Dit artikel zal worden bijgewerkt samen met de Security Advisory op <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-emudhra-info-ScS22A1r>.

## Systeemcertificaten

Blader naar Beheer -> Systeem -> Certificaten -> Systeemcertificaten, selecteer elk certificaat dat is toegewezen aan de knooppunten 1 voor 1 en selecteer Weergave. [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

Zorg ervoor dat de betrokken certificeringsinstantie of certificaten van afgifte niet in de certificaathierarchie staan. Als ze in gebruik zijn, begin dan met het nemen van stappen om die service naar een nieuwe certificeringsinstantie te migreren.

## Vertrouwde certificaten

Blader naar Beheer -> Systeem -> Certificaten -> Vertrouwde certificaten en bekijk de lijst met geïnstalleerde basiscertificaten en tussentijdse certificaten. Als u een of meer van de getroffen CA's in de lijst Vertrouwd vindt, noteert u de kolom Vertrouwd voor en onderneemt u de volgende actie voor elk type [2]:

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

- Cisco Services - Cisco gebruikt eMudhra niet voor enige service, als dit de enige vermelding is, kan het certificaat worden verwijderd.
- Infrastructuur - Controleer of de rol Eindpunten en/of AdminAuth niet vereist is, controleer of er geen certificaten van de CA of Emittenten worden gebruikt onder Systeemcertificaten
- Eindpunten - Controleer of eindpunten worden geverifieerd waarvoor de gecompromitteerde keten vereist is, als u niet zeker weet of eindpunten de CA of Emittenten gebruiken, schakel de optie "Vertrouwen voor clientverificatie en Syslog" uit en bewaak live logs en rapporten voor clientverificatiefouten.
- AdminAuth - Geef nieuwe certificaten uit aan uw beheerders, omdat een snelle optie Admin Authentication kan worden teruggezet naar een wachtwoord gebaseerde login terwijl nieuwe certificaten worden uitgegeven.
- NativeIPSec - Als u de Native IPSec-functie gebruikt, migreert u de IPSec-clients naar een nieuwe CA

## Overige diensten

De volgende serviceconfiguraties moeten worden gecontroleerd om te garanderen dat het verwijderen van getroffen vertrouwde certificaten geen invloed heeft op de functie van het systeem. Als deze services worden gebruikt, moeten de services opnieuw worden geconfigureerd om nieuwe certificaten te gebruiken voordat de vertrouwde certificaten worden verwijderd.

### LDAP

Blader naar Beheer -> Identiteitsbeheer -> Externe identiteitsbronnen -> LDAP. Klik onder elk LDAP-item op het tabblad Verbinding als Secure Authentication is ingeschakeld en controleer de keten voor de instellingen "LDAP Server Root CA" en "Issuer CA of ISE Certificates". [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

Blader naar Beheer -> Systeem -> Logboekregistratie -> Doelstellingen voor externe logboekregistratie, bekijk elke geconfigureerde Secure SYSLOG Server voor het geconfigureerde Trusted Root-certificaat, als een van de betrokken CA-certificaten in gebruik is, verifieer de keten op de SYSLOG-server en geef indien nodig een nieuwe root opnieuw uit en vertrouw deze. [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

Het is mogelijk om optioneel de "Issuer CA of ISE Certificates for CoA" in te stellen onder elk netwerkkapparaat onder Beheer -> Netwerkbronnen -> Netwerkkapparaten. Deze instelling wordt alleen gebruikt om het clientcertificaat te selecteren dat ISE zal gebruiken om een CoA uit te geven aan een netwerkkapparaat dat is geconfigureerd voor DTLS. Het certificaat wordt weergegeven op de pagina Systeemcertificaten in ISE voor het knooppunt, dus deze instelling hoeft alleen voor elk geconfigureerd netwerkkapparaat te worden geverifieerd als een certificaatafgifte van een van de eMudra-certificaten wordt afgegeven aan een ISE-knooppunt.

[1] [Certificaatbeheer in ISE](#)

[2] [Instellingen vertrouwde certificaten van ISE](#)

[3] [ISE Secure LDAP-configuratie](#)

[4] [Beveiligd doel voor externe logboekregistratie van Syslog configureren](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.