

Certificaat-renewals configureren op ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[ISE-zelfondertekende certificaten bekijken](#)

[Bepalen wanneer het certificaat moet worden gewijzigd](#)

[Aanvraag voor certificaatondertekening genereren](#)

[Installatiecertificaat](#)

[Alarmsysteem configureren](#)

[Verifiëren](#)

[Controleer het waarschuwingssysteem](#)

[Controleer de certificaatwijziging](#)

[Certificaat controleren](#)

[Problemen oplossen](#)

[Conclusie](#)

Inleiding

In dit document worden de best practices en proactieve procedures beschreven om certificaten te verlengen in de Cisco Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- X509-certificaten
- Configuratie van een Cisco ISE-lijnkaart met certificaten

Gebruikte componenten

"De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt."

- Cisco ISE-software release 3.0.0458
- Applicatie voor VMware

Achtergrondinformatie

Opmerking: Dit document is niet bedoeld als diagnostische gids voor certificaten.

In dit document worden de best practices en proactieve procedures beschreven om certificaten te verlengen in de Cisco Identity Services Engine (ISE). Het bekijkt ook hoe alarmen en meldingen op te zetten, zodat beheerders worden gewaarschuwd voor aanstaande gebeurtenissen zoals het verlopen van certificaten.

Als ISE-beheerder kom je uiteindelijk het feit tegen dat ISE-certificaten verlopen. Als uw ISE-server een verlopen certificaat heeft, kunnen er ernstige problemen ontstaan, tenzij u het verlopen certificaat vervangt door een nieuw, geldig certificaat.

Opmerking: als het certificaat dat wordt gebruikt voor het EAP (Extensible Authentication Protocol) verloopt, kunnen alle verificaties mislukken omdat clients niet meer op het ISE-certificaat vertrouwen. Als het ISE-beheercertificaat verloopt, is het risico nog groter: een beheerder kan niet meer inloggen op de ISE en de gedistribueerde implementatie kan ophouden te functioneren en repliceren.

De ISE-beheerder moet een nieuw, geldig certificaat op de ISE installeren voordat het oude certificaat verloopt. Deze proactieve benadering voorkomt of minimaliseert downtime en vermijdt gevolgen voor uw eindgebruikers. Zodra de tijdsperiode van het nieuwe certificaat begint, kunt u EAP/Admin of een andere rol op het nieuwe certificaat inschakelen.

U kunt de ISE configureren zodat er alarmen worden gegenereerd en de beheerder wordt gewaarschuwd om nieuwe certificaten te installeren voordat de oude certificaten verlopen.

Opmerking: in dit document wordt het ISE Admin-certificaat gebruikt als een zelfondertekend certificaat om het effect van de verlenging van het certificaat aan te tonen, maar deze aanpak wordt niet aanbevolen voor een productiesysteem. Het is beter om een CA-certificaat te gebruiken voor zowel de EAP- als de Admin-rollen.

Configureren

ISE-zelfondertekende certificaten bekijken

Wanneer de ISE is geïnstalleerd, wordt er een zelfondertekend certificaat gegenereerd. Het zelfondertekende certificaat wordt gebruikt voor administratieve toegang en voor communicatie binnen de gedistribueerde implementatie (HTTPS) en voor gebruikersverificatie (EAP). Gebruik in een bewegend systeem een CA-certificaat in plaats van een zelfondertekend certificaat.

Tip: raadpleeg het [certificaatbeheer in Cisco ISE](#)-gedeelte van de [hardwaregids voor de hardware-installatie van Cisco Identity Services Engine, release 3.0](#) voor meer informatie.

Het formaat voor een ISE-certificaat moet Privacy Enhanced Mail (PEM) of Distinguished Encoding Rules (DER) zijn.

Om het eerste zelfondertekende certificaat te bekijken, navigeer je naar **Beheer > Systeem > Certificaten > Systeemcertificaten** in de ISE GUI, zoals in deze afbeelding wordt getoond.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Certificate Management									
System Certificates									
Trusted Certificates									
OCSP Client Profile									
Certificate Signing Requests									
Certificate Periodic Check Se...									
Certificate Authority									
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date			
abtomar31									
OU=ISE Messaging Service, CN=abtomar31.abtomar.local#Certificate Services Endpoint Sub CA - abtomar31#00001	ISE Messaging Service		abtomar31.abtomar.local	Certificate Services Endpoint Sub CA - abtomar31	Mon, 3 May 2021	Mon, 4 May 2026	●		
OU=Certificate Services System Certificate, CN=abtomar31.abtomar.local#Certificate Services Endpoint Sub CA - abtomar31#00002	pxGrid		abtomar31.abtomar.local	Certificate Services Endpoint Sub CA - abtomar31	Mon, 3 May 2021	Mon, 4 May 2026	●		
Default self-signed server certificate - CN=SAML_abtomar31.abtomar.local	SAML		SAML_abtomar31.abtomar.local	SAML_abtomar31.abtomar.local	Tue, 4 May 2021	Sun, 3 May 2026	●		
Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	abtomar31.abtomar.local	abtomar31.abtomar.local	Tue, 4 May 2021	Thu, 4 May 2023	●		

Als u een servercertificaat installeert op de ISE via een certificaatondertekeningsaanvraag (CSR) en het certificaat wijzigt voor de Admin of EAP-protocol, is het zelfondertekende servercertificaat nog steeds aanwezig, maar is het niet in gebruik.

Waarschuwing: voor wijzigingen in het beheerprotocol is een herstart van de ISE-services vereist, waardoor een paar minuten downtime wordt gecreëerd. EAP-protocolwijzigingen leiden niet tot een herstart van de ISE-diensten en veroorzaken geen downtime.

Bepalen wanneer het certificaat moet worden gewijzigd

Veronderstel dat het geïnstalleerde certificaat spoedig verloopt. Is het beter om het certificaat te laten verlopen voordat u het verlengt of om het certificaat te wijzigen vóór het verloopdatum? U moet het certificaat voor afloop wijzigen, zodat u tijd hebt om de certificaatruil te plannen en om eventuele downtime te beheren die door de ruil wordt veroorzaakt.

Wanneer moet je het certificaat wijzigen? Ontvang een nieuw certificaat met een begindatum die voorafgaat aan de verloopdatum van het oude certificaat. De tijdsperiode tussen deze twee data is het wijzigingsvenster.

Waarschuwing: als u Admin inschakelt, wordt de service opnieuw gestart op de ISE-server en ervaart u een paar minuten downtime.

In deze afbeelding wordt de informatie weergegeven voor een certificaat dat binnenkort verloopt:

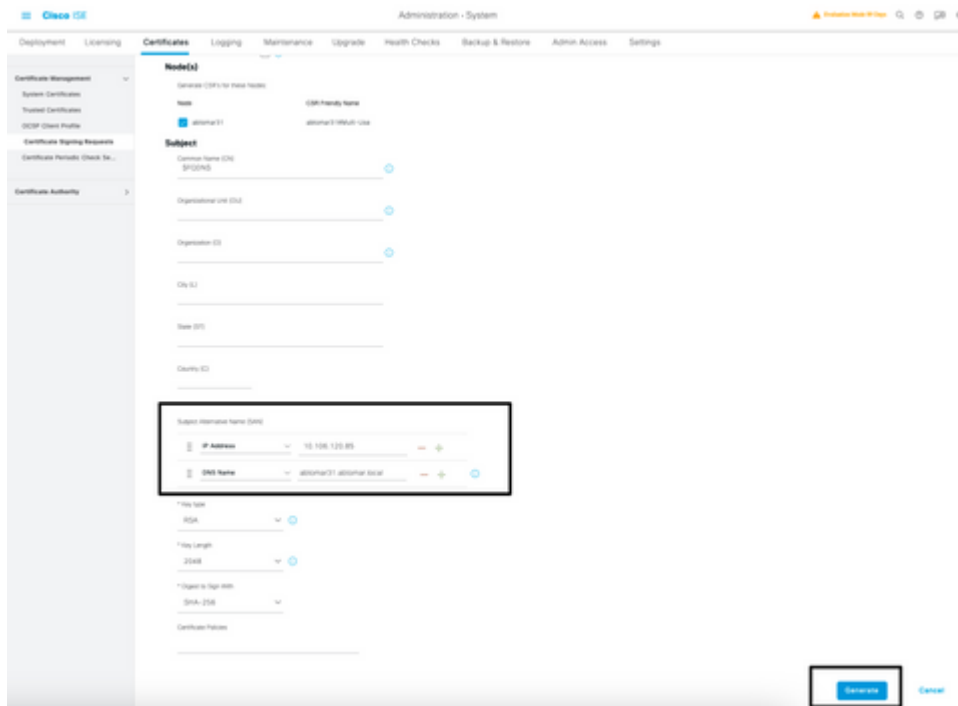
<input type="checkbox"/>	Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group ⓘ	abtomar31.abtomar.local	abtomar31.abtomar.local	Tue, 4 May 2021	Wed, 5 May 2021 ⚠
--------------------------	--	--	------------------------------------	-------------------------	-------------------------	-----------------	-------------------

Aanvraag voor certificaatondertekening genereren

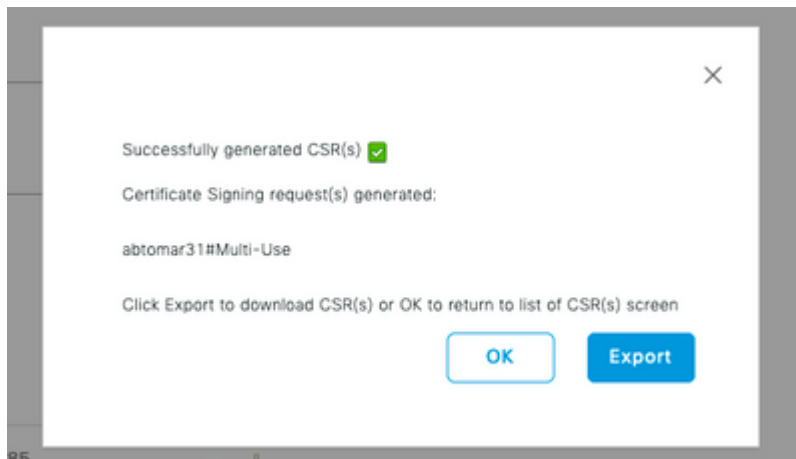
In deze procedure wordt beschreven hoe het certificaat via een MVO kan worden verlengd:

1. Navigeer in de ISE-console naar **Beheer > Systeem > Certificaten > Aanvragen voor certificaatondertekening** en klik op **Generate Certificate Signing request**:

2. De minimuminformatie die u in het tekstveld **Certificaat onderwerp** moet invoeren is **CN=ISEfqdn**, waar *ISEfqdn* de Volledig gekwalificeerde domeinnaam (FQDN) van de ISE is. Voeg extra velden toe zoals O (Organisatie), OU (Organisatorische eenheid) of C (Land) in het Certificaat Onderwerp met behulp van komma's:



3. In een van de tekstveldlijnen **Onderwerp Alternatieve Naam (SAN)** moet de ISE-FQDN worden herhaald. U kunt een tweede SAN-veld toevoegen als u alternatieve namen of een wildcard-certificaat wilt gebruiken.
4. Klik op **Generate**, een pop-upvenster geeft aan of de CSR-velden al dan niet correct zijn ingevuld:



5. Klik op **certificaatondertekeningaanvragen** in het linkerdeelvenster om de **CSR** te exporteren, selecteer uw CSR en klik op **Exporteren**:

The screenshot shows the Cisco ISE Administration console. The left sidebar has 'Certificate Management' expanded to 'Certificate Signing Requests'. The main area is titled 'Certificate Signing Requests' and contains a table with one entry:

Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
abtomar31Multi-Use	CN=abtomar31.abtomar.local...	2048		Tue, 4 May 2021	abtomar31

6. De MVO wordt opgeslagen op uw computer. Leg het ter ondertekening voor aan uw CA.

Installatiecertificaat

Zodra u het definitieve certificaat van uw CA ontvangt, moet u het certificaat aan de ISE toevoegen:

1. Navigeer in de ISE-console naar **Beheer > System > Certificaten > Certificaatondertekeningaanvragen**, vink vervolgens het aanvinkvakje op CRS aan en klik op **Bindcertificaat**:

This screenshot is identical to the one above, showing the 'Certificate Signing Requests' table with the 'Bind Certificate' button highlighted.

2. Voer in het tekstveld **Vriendelijke naam** een eenvoudige, duidelijke beschrijving van het certificaat in en druk op Verzenden.

Opmerking: Schakel EAP- of Admin-protocol momenteel niet in.

3. Onder Systeemcertificaat, hebt u een nieuw certificaat dat niet in gebruik is zoals hier getoond:

The screenshot shows a table with certificate entries. One entry is highlighted:

AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNB56PH-CA	Tue, 4 May 2021	Thu, 4 May 2023
<input type="checkbox"/>					

4. Omdat het nieuwe certificaat wordt geïnstalleerd voordat het oude verloopt, ziet u een fout die een datumbereik in de toekomst rapporteert:

The dialog box contains the following text:

The certificate you are importing has a date range in the future - it is not yet valid. Are you sure you want to continue?

Buttons: Yes, No

5. Klik op **Ja** om verder te gaan. Het certificaat is nu geïnstalleerd, maar niet in gebruik, zoals in groen gemarkeerd.

<input type="checkbox"/>	AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNBS-4IPH-CA	Tue, 4 May 2021	Thu, 4 May 2023	●	
<input type="checkbox"/>	Default self-signed server certificate	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group	abtomar31.abtomar.local	abtomar31.abtomar.local	Tue, 4 May 2021	Wed, 5 May 2021	▼

Opmerking: als u zelfondertekende certificaten gebruikt in een gedistribueerde implementatie, moet het primaire zelfondertekende certificaat worden geïnstalleerd in het vertrouwde certificaatarchief van de secundaire ISE-server. Op dezelfde manier moet het secundaire zelfondertekende certificaat worden geïnstalleerd in het vertrouwde certificaatarchief van de primaire ISE-server. Hierdoor kunnen de ISE-servers elkaar wederzijds authenticeren. Zonder dit kan de inzet breken. Als u certificaten van een derde CA verlengt, controleert u of de basiscertificaatketen is gewijzigd en werkt u het vertrouwde certificaatarchief in de ISE dienovereenkomstig bij. Zorg er in beide scenario's voor dat de ISE-knooppunten, endpointcontrolesystemen en applicaties de root certificate chain kunnen valideren.

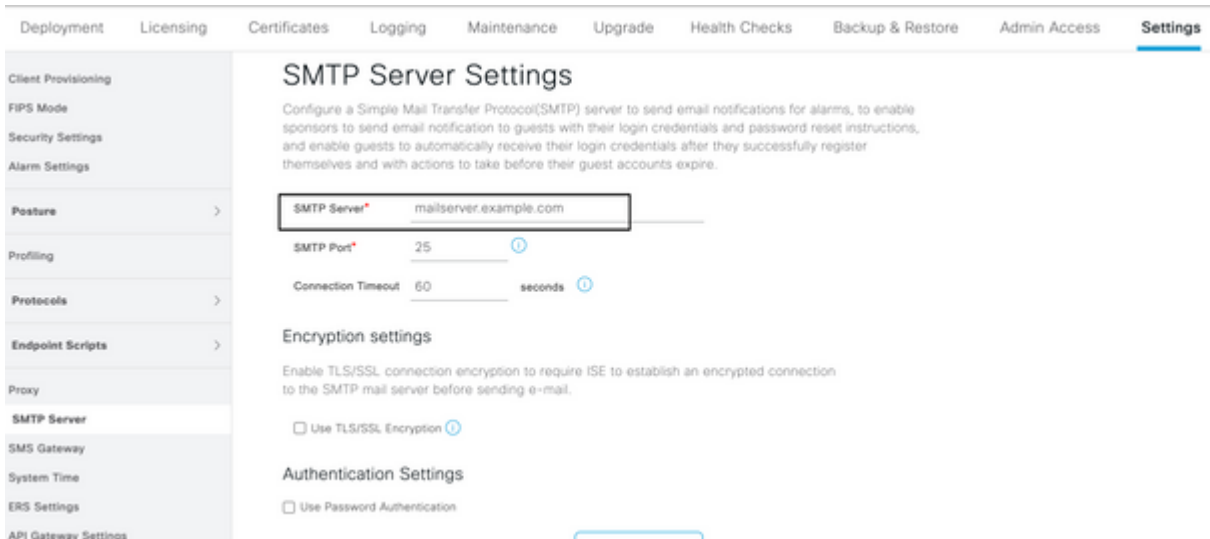
Alarmsysteem configureren

Cisco ISE waarschuwt u wanneer de verloopdatum van een lokaal certificaat binnen 90 dagen valt. Dergelijke voorafgaande kennisgeving helpt u verlopen certificaten te vermijden, de certificaatwijziging te plannen en downtime te voorkomen of te minimaliseren.

Het bericht verschijnt op verschillende manieren:

- De pictogrammen voor de verloopstatus van de kleur worden weergegeven op de pagina Lokale certificaten.
- Verloopberichten worden weergegeven in het diagnostische rapport van Cisco ISE-systeem.
- De alarmen worden gegenereerd op 90 dagen en 60 dagen, dan dagelijks in de laatste 30 dagen voor het verstrijken.

Configureer de ISE voor e-mailmeldingen van verloopalarmen. Ga in de ISE-console naar **Beheer > Systeem > Instellingen > SMTP-server**, identificeer de Simple Mail Transfer Protocol (SMTP)-server en definieer de andere serverinstellingen zodat e-mailmeldingen voor de alarmen worden verstuurd:

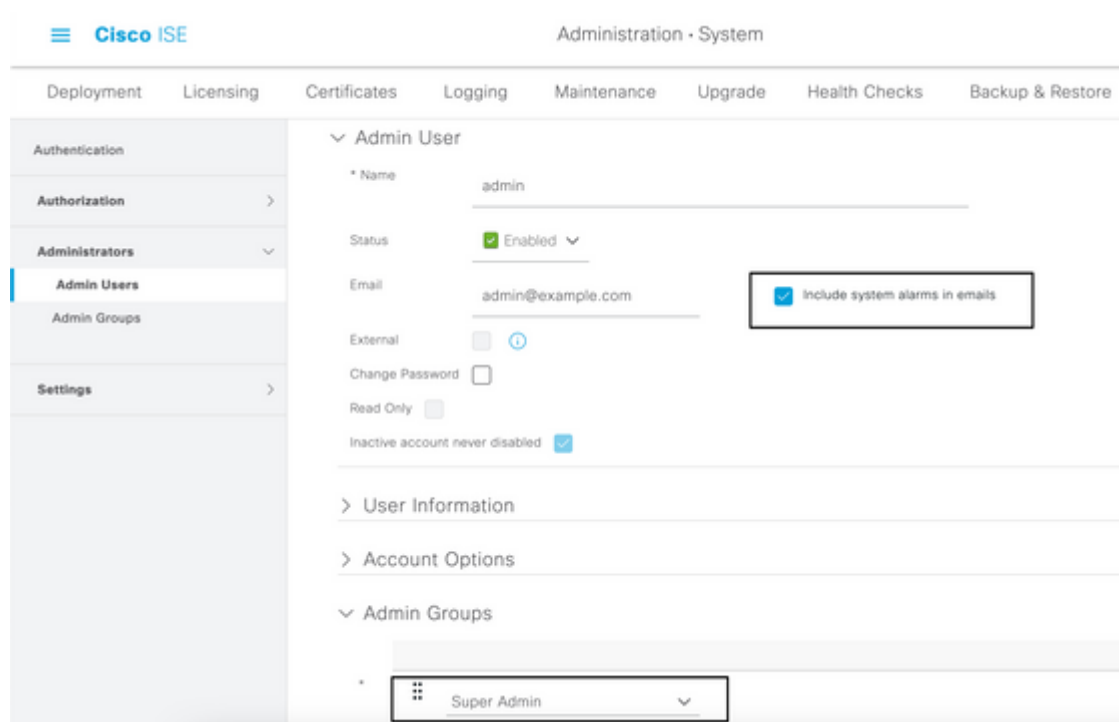


Er zijn twee manieren waarop u meldingen kunt instellen:

- Gebruik Admin Access om beheerders te informeren:

1. Ga naar **Beheer > System > Admin Access > Beheerders > Beheerders.**

- **Schakel het selectievakje Systemalarms opnemen in e-mails in voor de Admin-gebruikers die alarmmeldingen moeten ontvangen. Het e-mailadres voor de verzender van de alarmmeldingen is hardcoded als `ise@hostname`.**



- **Configureer de ISE-alarminstellingen om gebruikers te waarschuwen:**

1. Navigeer naar **Beheer > System > Instellingen > Alarminstellingen > Alarmconfiguratie**, zoals in deze afbeelding wordt weergegeven.

Alarm Name	Category	Severity	Status	User Defined
CA Server is down	Administrative and Operational Audit	Warning	Enabled	Yes
CA Server is up	Administrative and Operational Audit	Info	Enabled	Yes
CCA Failed	ISE Services	Warning	Enabled	Yes
CRS Removal Failed	Administrative and Operational Audit	Error	Enabled	Yes
Certificate Expiration	Administrative and Operational Audit	Warning	Enabled	Yes
Certificate Expired	Administrative and Operational Audit	Error	Enabled	Yes
Certificate Processing Information Error	Administrative and Operational Audit	Error	Enabled	Yes
Certificate Replication Failed	Administrative and Operational Audit	Error	Enabled	Yes
Certificate Replication Temporarily Failed	Administrative and Operational Audit	Error	Enabled	Yes
Certificate Revoked	Administrative and Operational Audit	Warning	Enabled	Yes
Certificate request forwarding failed	Administrative and Operational Audit	Error	Enabled	Yes
Class profile applied to all devices	Administrative and Operational Audit	Warning	Enabled	Yes

Opmerking: Schakel de status van een categorie uit als u alarmen uit die categorie wilt voorkomen.

2. Selecteer Certificaatverloop en klik vervolgens op Alarmmelding, voer de e-mailadressen in van de gebruikers die op de hoogte moeten worden gebracht en sla de configuratiewijziging op. Veranderingen kunnen tot 15 minuten duren voordat ze actief zijn.

Alarm Settings

Alarm Configuration Alarm Notification

Alarm Name: Certificate Expiration

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

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

Status: Enable

Severity: WARNING

Send Syslog Message:

Enter multiple e-mails separated with comma: admin@abtomar.com

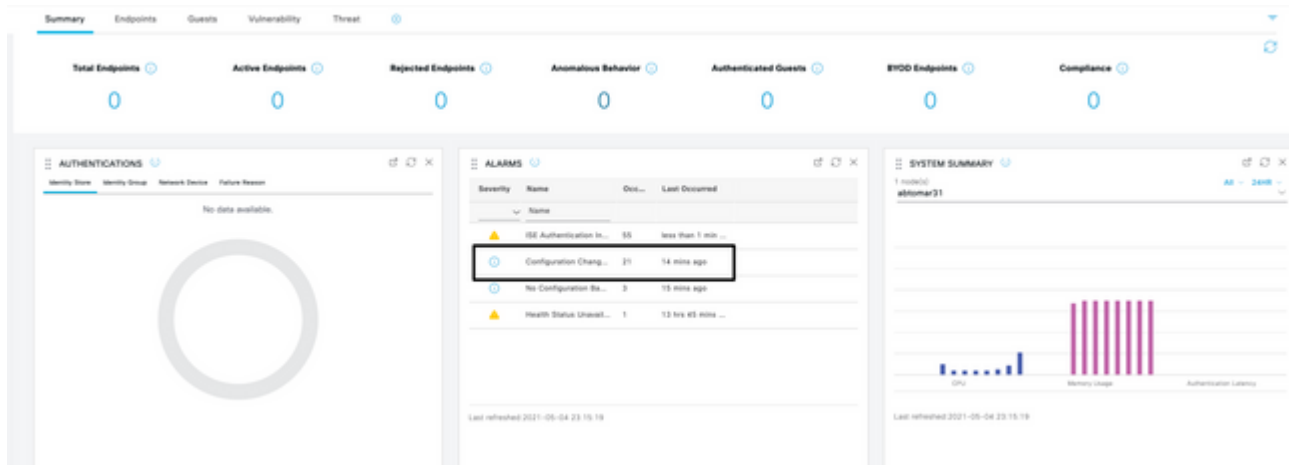
Notes in Email (0 to 4000 characters)

Verifiëren

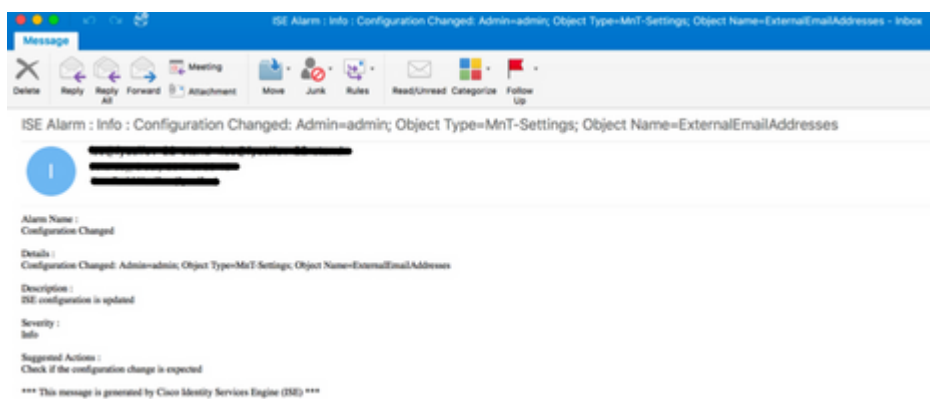
Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Controleer het waarschuwingssysteem

Controleer of het waarschuwingssysteem correct werkt. In dit voorbeeld genereert een configuratiewijziging een waarschuwing met een informatieniveau voor de ernst. (Een alarm van de Informatie is de laagste strengheid, terwijl de certificaatverloopdatums een hoger strengheidsniveau van Waarschuwing genereren).



Dit is een voorbeeld van het e-mailalarm dat wordt verzonden door de ISE:



Controleer de certificaatwijziging

In deze procedure wordt beschreven hoe u kunt controleren of het certificaat correct is geïnstalleerd en hoe u EAP- en/of Admin-rollen kunt wijzigen:

- Navigeer op de ISE-console naar **Beheer > Certificaten > Systemcertificaten** en selecteer het nieuwe certificaat om de details te bekijken.

Waarschuwing: als u het gebruik van de beheerder inschakelt, wordt de ISE-service opnieuw gestart, waardoor serverdowntime wordt veroorzaakt.

The screenshot shows the Cisco ISE Administration console. A warning dialog box is displayed in the foreground, stating: "Warning: Enabling Admin role for this certificate will cause an application server restart on the selected node." The dialog has "OK" and "Cancel" buttons. In the background, the "Certificates" section is visible, showing details for an issuer named "AdminISE". The details include: Friendly Name: AdminISE, Description: (empty), Subject: CN=abtomar31.abtomar.local,OU=cisco, Subject Alternative Name (SAN): IP Address: 10.106.120.85, DNS Name: abtomar31.abtomar.local, Issuer: abtomar-WIN-231PNBS4IPH-CA, Valid From: Tue, 4 May 2021 21:00:34 IST, Valid To (Expiration): Thu, 4 May 2023 21:00:34 IST, Serial Number: 22 00 00 00 11 D8 BC 40 BD 11 C0 68 3E 00 00 00 00 11, Signature Algorithm: SHA256WITHRSA, Key Length: 2048, and Certificate Policies: (empty). The Usage section is also visible with several checkboxes: Admin (checked), EAP Authentication, RADIUS DTLS, pxGrid, ISE Messaging Service, and SAN.

- Om de certificaatstatus op de ISE-server te verifiëren, voert u deze opdracht in de CLI in:

```
<#root>
```

```
CLI:>
```

```
show application status ise
```

- Wanneer alle services actief zijn, probeert u in te loggen als beheerder.
- Voor een gedistribueerd implementatiescenario, navigeren naar **Beheer > Systeem > Implementatie**. Controleer of het knooppunt een groen pictogram heeft. Plaats de cursor over het pictogram om te controleren of de legende "Verbonden" toont.
- Controleer of de verificatie van de eindgebruiker is geslaagd. Hiervoor navigeer je naar **Operations > RADIUS > Livelogs**. U kunt een specifieke verificatiepoging vinden en controleren of deze pogingen zijn geverifieerd.

Certificaat controleren

Als u het certificaat extern wilt controleren, kunt u de ingesloten Microsoft Windows-tools of de OpenSSL-toolkit gebruiken.

OpenSSL is een opensource-implementatie van het Secure Sockets Layer (SSL)-protocol. Als de certificaten uw eigen privé CA gebruiken, moet u uw wortel CA certificaat op een lokale machine

plaatsen en de OpenSSL optie *-CApath* gebruiken. Als je een tussenliggende CA hebt, moet je deze ook in dezelfde directory plaatsen.

Gebruik om algemene informatie over het certificaat te verkrijgen en te verifiëren:

```
<#root>
```

```
openssl x509 -in certificate.pem -noout -text  
openssl verify certificate.pem
```

Het kan ook handig zijn om de certificaten te converteren met de OpenSSL toolkit:

```
<#root>
```

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Problemen oplossen

Er is momenteel geen specifieke diagnostische informatie beschikbaar voor deze configuratie.

Conclusie

Aangezien u een nieuw certificaat kunt installeren op de ISE voordat deze actief is, raadt Cisco u aan het nieuwe certificaat te installeren voordat het oude certificaat verloopt. Deze overlappende periode tussen de oude verloopdatum van het certificaat en de nieuwe begindatum van het certificaat geeft u tijd om certificaten te vernieuwen en hun installatie te plannen met weinig of geen downtime. Zodra het nieuwe certificaat zijn geldige datumbereik heeft, schakelt u de EAP en/of Admin in. Vergeet niet dat als u het gebruik van Admin inschakelt, er een herstart van de service is.

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.