

Zertifikatverlängerungen auf ISE konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Selbstsignierte ISE-Zertifikate anzeigen](#)

[Bestimmen, wann das Zertifikat geändert werden soll](#)

[Zertifikatsignierungsanfrage generieren](#)

[Zertifikat installieren](#)

[Alarmsystem konfigurieren](#)

[Überprüfung](#)

[Warnsystem verifizieren](#)

[Zertifikatsänderung verifizieren](#)

[Zertifikat verifizieren](#)

[Fehlerbehebung](#)

[Schlussfolgerung](#)

Einleitung

Dieses Dokument beschreibt die Best Practices und proaktiven Verfahren zur Verlängerung von Zertifikaten auf der Cisco Identity Services Engine (ISE). Außerdem wird erläutert, wie Sie Alarme und Benachrichtigungen einrichten, um Administratoren vor drohenden Ereignissen wie dem Ablauf eines Zertifikats zu warnen.

Anmerkung: Dieses Dokument ist nicht als Diagnosehandbuch für Zertifikate gedacht.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- X509-Zertifikate
- Konfiguration einer Cisco ISE mit Zertifikaten

Verwendete Komponenten

"Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen."

- Cisco ISE-Version 3.0.0.458
- Appliance oder VMware

Hintergrundinformationen

Als ISE-Administrator werden Sie feststellen, dass ISE-Zertifikate ablaufen. Wenn Ihr ISE-Server über ein abgelaufenes Zertifikat verfügt, können schwerwiegende Probleme auftreten, es sei denn, Sie ersetzen das abgelaufene Zertifikat durch ein neues, gültiges Zertifikat.

Anmerkung: Wenn das für das Extensible Authentication Protocol (EAP) verwendete Zertifikat abläuft, können alle Authentifizierungen fehlschlagen, da die Clients dem ISE-Zertifikat nicht mehr vertrauen. Wenn das ISE-Administratorzertifikat abläuft, ist das Risiko noch größer: kann sich ein Administrator nicht mehr bei der ISE anmelden, und die verteilte Bereitstellung kann nicht mehr funktionieren und sich nicht mehr replizieren.

Der ISE-Administrator muss ein neues, gültiges Zertifikat auf der ISE installieren, bevor das alte Zertifikat abläuft. Dieser proaktive Ansatz verhindert oder minimiert Ausfallzeiten und vermeidet Auswirkungen auf Ihre Endbenutzer. Sobald der Zeitraum für das neu installierte Zertifikat beginnt, können Sie EAP/Admin oder eine andere Rolle für das neue Zertifikat aktivieren.

Sie können die ISE so konfigurieren, dass sie Alarme generiert und den Administrator benachrichtigt, neue Zertifikate zu installieren, bevor die alten Zertifikate ablaufen.

Anmerkung: In diesem Dokument wird das ISE-Administratorzertifikat als selbstsigniertes Zertifikat verwendet, um die Auswirkungen der Zertifikatverlängerung darzustellen. Für Produktionssysteme wird dieser Ansatz jedoch nicht empfohlen. Es ist besser, ein Zertifizierungsstellenzertifikat sowohl für die EAP- als auch für die Admin-Rolle zu verwenden.

Konfigurieren

Selbstsignierte ISE-Zertifikate anzeigen

Wenn die ISE installiert wird, generiert sie ein selbstsigniertes Zertifikat. Das selbstsignierte Zertifikat wird für den administrativen Zugriff und die Kommunikation innerhalb der verteilten Bereitstellung (HTTPS) sowie für die Benutzerauthentifizierung (EAP) verwendet. Verwenden Sie in einem Live-System ein CA-Zertifikat anstelle eines selbstsignierten Zertifikats.

Tipp: Weitere Informationen finden Sie im [Hardware-Installationsleitfaden für die Cisco Identity Services Engine, Version 3.0](#) im Abschnitt zum [Zertifikatsmanagement in Cisco ISE](#).

Das Format für ein ISE-Zertifikat muss Privacy Enhanced Mail (PEM) oder Distinguished Encoding Rules (DER) sein.

Um das erste selbstsignierte Zertifikat anzuzeigen, navigieren Sie in der ISE-GUI zu **Administration > System > Certificates > System Certificates** (Administration > System > Zertifikate > Systemzertifikate), wie in der Abbildung dargestellt.

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 saml 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	●		

Wenn Sie ein Serverzertifikat über eine Zertifikatsignierungsanfrage (CSR, Certificate Signing Request) auf der ISE installieren und das Zertifikat für das Admin- oder EAP-Protokoll ändern, ist das selbstsignierte Serverzertifikat weiterhin vorhanden, befindet sich jedoch im Status „Not in use“ (Nicht verwendet).

Vorsicht: Bei Änderungen am Admin-Protokoll ist ein Neustart der ISE-Services erforderlich, wodurch einige Minuten Ausfallzeit entstehen. EAP-Protokolländerungen lösen keinen Neustart der ISE-Services aus und verursachen keine Ausfallzeiten.

Bestimmen, wann das Zertifikat geändert werden soll

Angenommen, das installierte Zertifikat läuft bald ab. Ist es besser, das Zertifikat ablaufen zu lassen, bevor Sie es verlängern, oder das Zertifikat vor Ablauf zu wechseln? Sie müssen das Zertifikat vor Ablauf ändern, damit Sie Zeit haben, den Austausch des Zertifikats zu planen und die durch den Austausch verursachten Ausfallzeiten zu bewältigen.

Wann müssen Sie das Zertifikat ändern? Rufen Sie ein neues Zertifikat mit einem Startdatum ab, das vor dem Ablaufdatum des alten Zertifikats liegt. Der Zeitraum zwischen diesen beiden Daten ist das Änderungszeitfenster.

Vorsicht: Wenn Sie Admin aktivieren, führt dies zu einem Neustart des Services auf dem ISE-Server, und es treten einige Minuten Ausfallzeit auf.

Die folgende Abbildung zeigt die Informationen für ein Zertifikat, das bald abläuft:

<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	⚠
--------------------------	--	--	----------------------------------	-------------------------	-------------------------	-----------------	-----------------	---

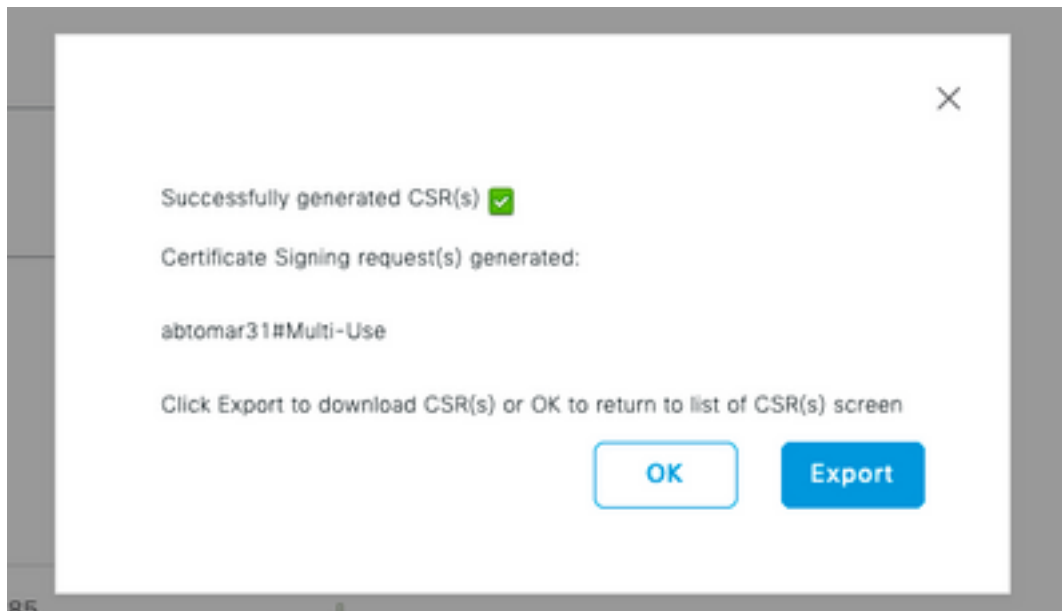
Zertifikatsignierungsanfrage generieren

Dieses Verfahren beschreibt, wie das Zertifikat über eine CSR verlängert wird:

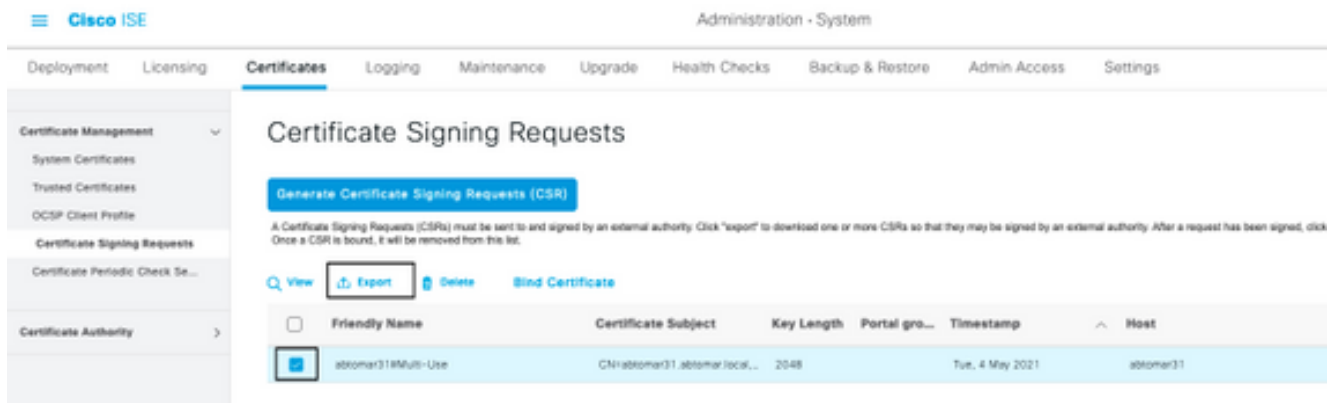
1. Navigieren Sie in der ISE-Konsole zu **Administration > System > Certificates > Certificate Signing Requests** (Administration > System > Zertifikate > Zertifikatsignierungsanfragen) und klicken Sie auf **Generate Certificate Signing Request (Zertifikatsignierungsanfrage erstellen)**:
2. Die Mindestinformationen, die Sie in das Textfeld **Certificate Subject** (Zertifikatsbetreff) eingeben müssen, sind CN = *ISEfqdn*, wobei *ISEfqdn* der Fully Qualified Domain Name (FQDN) der ISE ist. Fügen Sie zusätzliche Felder wie O (Organisation), OU (Organizational Unit [Organisationseinheit]) oder C (Country [Land]) im Zertifikatsbetreff mit Kommata hinzu:

The screenshot shows the Cisco ISE Administration console interface. The page title is "Administration - System". The navigation menu includes "Deployment", "Learning", "Certificates", "Logging", "Maintenance", "Upgrade", "Health Checks", "Backup & Restore", "Admin Access", and "Settings". The "Certificates" section is active, showing a table of certificates and a "Generate" button. The "Certificate Subject" field is highlighted with a red box, containing the text "CN=10.138.129.85, O=adidasnet1.adidasnet.local". Other fields include "Key Size", "Key Length", "Key Algorithm", and "Certificate Format". A "Generate" button is highlighted with a red box at the bottom right of the form.

3. Eine der SAN-Textfeldzeilen (**Subject Alternative Name**) muss den FQDN der ISE wiederholen. Sie können ein zweites SAN-Feld hinzufügen, wenn Sie alternative Namen oder ein Platzhalterzertifikat verwenden möchten.
4. Klicken Sie auf **Generate** (Generieren). In einem Popup-Fenster wird angezeigt, ob die CSR-Felder korrekt ausgefüllt sind:



- Um die CSR zu exportieren, klicken Sie im linken Bereich auf **Certificate Signing Requests** (Zertifikatsignierungsanfragen), wählen Sie Ihre CSR aus und klicken Sie auf **Export**:



- Der CSR wird auf Ihrem Computer gespeichert. Senden Sie sie zur Signatur an Ihre CA.

Zertifikat installieren

Sobald Sie das endgültige Zertifikat von Ihrer CA erhalten haben, müssen Sie es zur ISE hinzufügen:

- Navigieren Sie in der ISE-Konsole zu **Administration > System > Certificates > Certificate Signing Requests** (Administration > System > Zertifikate > Zertifikatsignierungsanfragen), aktivieren Sie dann das Kontrollkästchen bei CRS und klicken Sie auf **Bind Certificate** (Zertifikat binden):

Cisco ISE Administration - System

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

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Request (CSR) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, it will be removed from this list.

View Export Delete Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	abtomar31InMulti-Use	CN=abtomar31.abtomar.local...	2048		Tue, 4 May 2021	abtomar31

2. Geben Sie eine einfache, eindeutige Beschreibung des Zertifikats in das Textfeld **Friendly Name** (Anzeigename) ein und klicken Sie auf „Submit“ (Senden).

Anmerkung: Aktivieren Sie zu diesem Zeitpunkt nicht das EAP- oder Admin-Protokoll.

3. Unter „System Certificate“ (Systemzertifikat) sehen Sie ein neues Zertifikat mit dem Status „Not in use“ (Nicht verwendet), wie hier dargestellt:

<input type="checkbox"/>	AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNBS4PH-CA	Tue, 4 May 2021	Thu, 4 May 2023
<input type="checkbox"/>						

4. Da das neue Zertifikat installiert wird, bevor das alte abläuft, wird ein Fehler angezeigt, der einen Datumsbereich in der Zukunft meldet:



5. Klicken Sie auf **Yes** (Ja), um fortzufahren. Das Zertifikat ist jetzt installiert, wird aber nicht verwendet, wie in grün hervorgehoben.

<input type="checkbox"/>	AdminISE	Not in use	abtomar31.abtomar.local	abtomar-WIN-231PNBS4PH-CA	Tue, 4 May 2021	Thu, 4 May 2023
<input type="checkbox"/>						
<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

Anmerkung: Wenn Sie selbstsignierte Zertifikate in einer verteilten Bereitstellung verwenden, muss das primäre selbstsignierte Zertifikat im vertrauenswürdigen Zertifikatsspeicher des sekundären ISE-Servers installiert werden. Ebenso muss das sekundäre selbstsignierte Zertifikat im vertrauenswürdigen Zertifikatsspeicher des primären ISE-Servers installiert werden. Dadurch können sich die ISE-Server gegenseitig authentifizieren. Andernfalls kann die Bereitstellung unterbrochen werden. Wenn Sie Zertifikate von einer Drittanbieter-CA verlängern, überprüfen Sie, ob sich die

Stammzertifikatskette geändert hat, und aktualisieren Sie den vertrauenswürdigen Zertifikatsspeicher in ISE entsprechend. Stellen Sie in beiden Szenarien sicher, dass die ISE-Knoten, Endpunktsteuerungssysteme und Supplicants die Stammzertifikatskette validieren können.

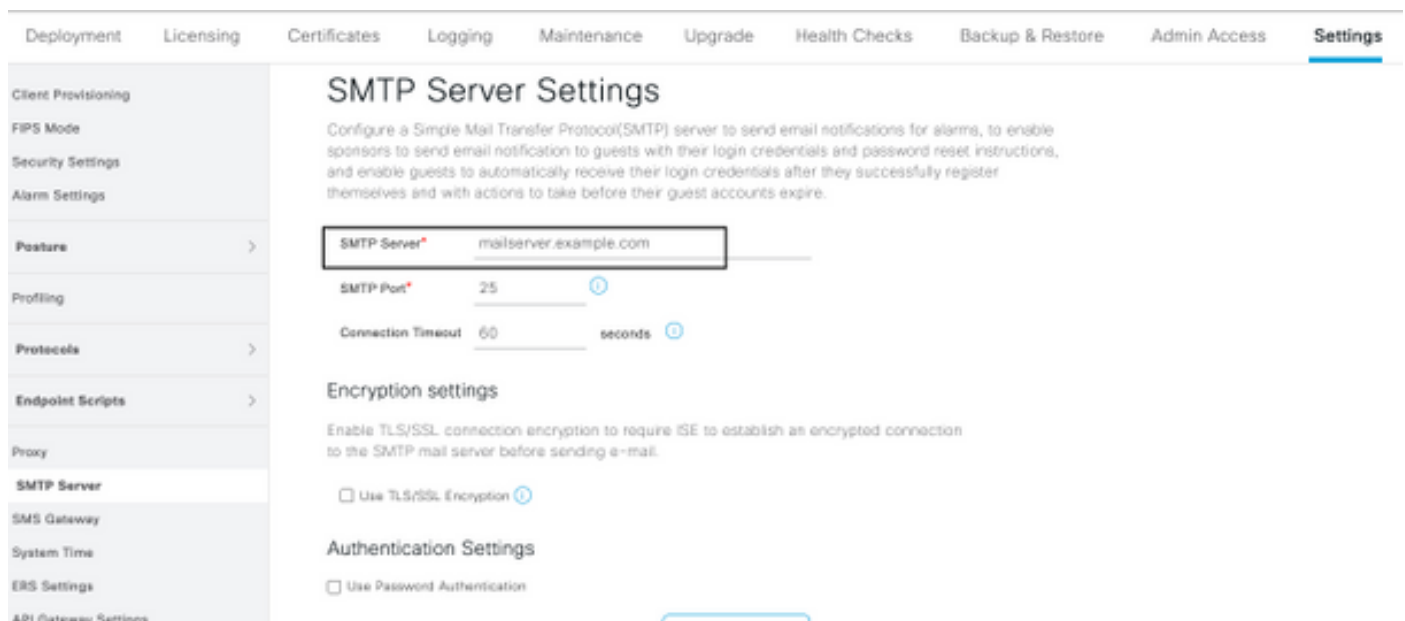
Alarmsystem konfigurieren

Die Cisco ISE benachrichtigt Sie, wenn das Ablaufdatum eines lokalen Zertifikats innerhalb von 90 Tagen liegt. Eine solche Vorabbenachrichtigung hilft Ihnen, abgelaufene Zertifikate zu vermeiden, die Zertifikatsänderung zu planen und Ausfallzeiten zu verhindern oder zu minimieren.

Die Benachrichtigung wird auf verschiedene Weise angezeigt:

- Auf der Seite „Local Certificates“ (Lokale Zertifikate) werden farbige Ablaufstatussymbole angezeigt.
- Ablaufnachrichten werden im Cisco ISE-Systemdiagnosebericht angezeigt.
- Ablaufalarme werden 90 Tage und 60 Tage vorher generiert, dann täglich in den letzten 30 Tagen vor dem Ablauf.

Konfigurieren Sie die ISE für die E-Mail-Benachrichtigung bei Ablaufalarmen. Navigieren Sie in der ISE-Konsole zu **Administration > System > Settings > SMTP Server** (Administration > System > Einstellungen > SMTP-Server), identifizieren Sie den SMTP-Server (Simple Mail Transfer Protocol) und definieren Sie die anderen Servereinstellungen, sodass E-Mail-Benachrichtigungen für die Alarme gesendet werden:



The screenshot displays the 'SMTP Server Settings' page in the Cisco ISE administration console. The page is divided into a left-hand navigation menu and a main content area. The navigation menu includes options like 'Client Provisioning', 'FIPS Mode', 'Security Settings', 'Alarm Settings', 'Posture', 'Profiling', 'Protocols', 'Endpoint Scripts', 'Proxy', 'SMTP Server', 'SMS Gateway', 'System Time', 'ERS Settings', and 'API Gateway Settings'. The main content area is titled 'SMTP Server Settings' and contains the following information:

- SMTP Server:** mailserver.example.com (highlighted with a red box)
- SMTP Port:** 25
- Connection Timeout:** 60 seconds
- Encryption settings:** A checkbox for 'Use TLS/SSL Encryption' is present and unchecked.
- Authentication Settings:** A checkbox for 'Use Password Authentication' is present and unchecked.

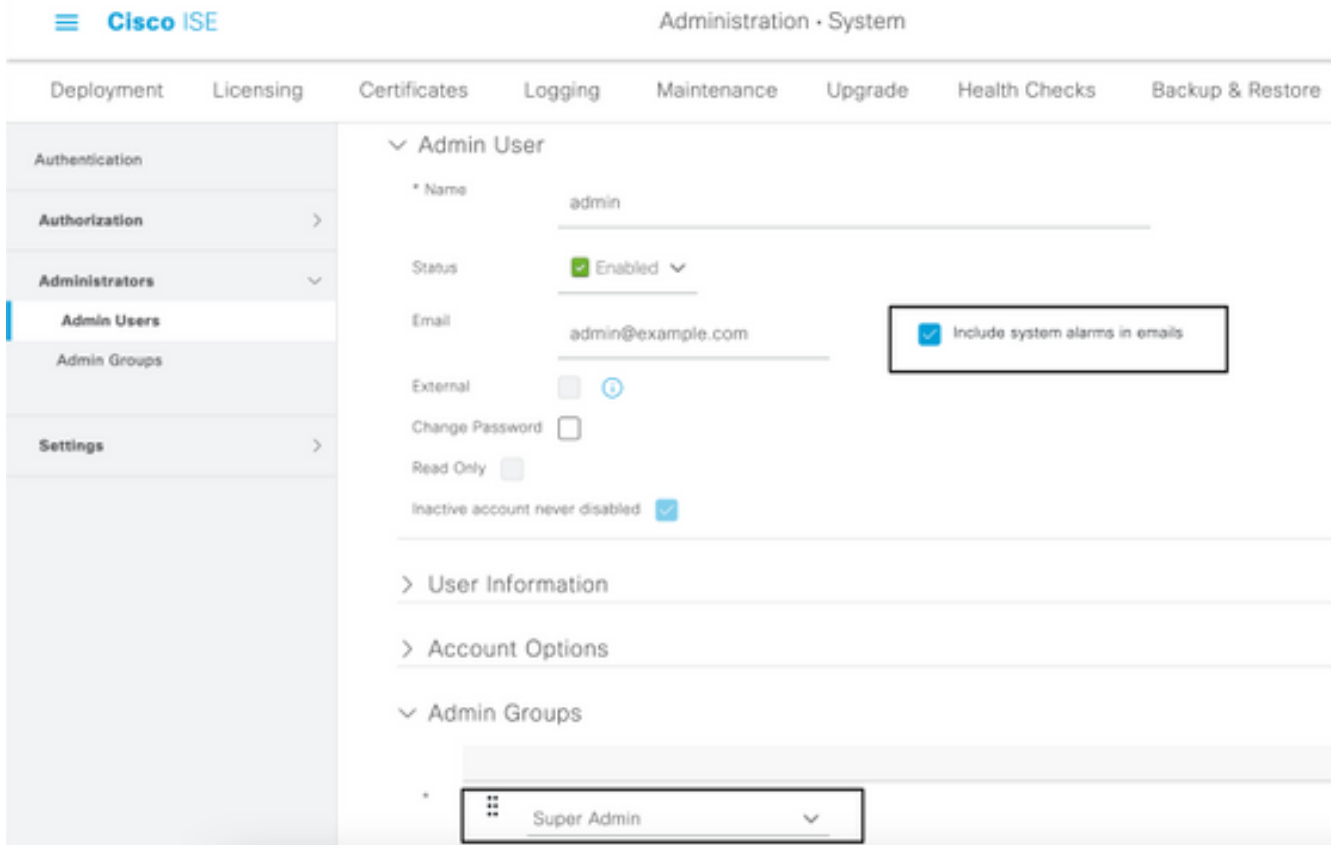
Es gibt zwei Möglichkeiten, Benachrichtigungen einzurichten:

- Verwenden Sie den Admin-Zugriff, um Administratoren zu benachrichtigen:

Navigieren Sie zu **Administration > System > Admin Access > Administrators > Admin Users**

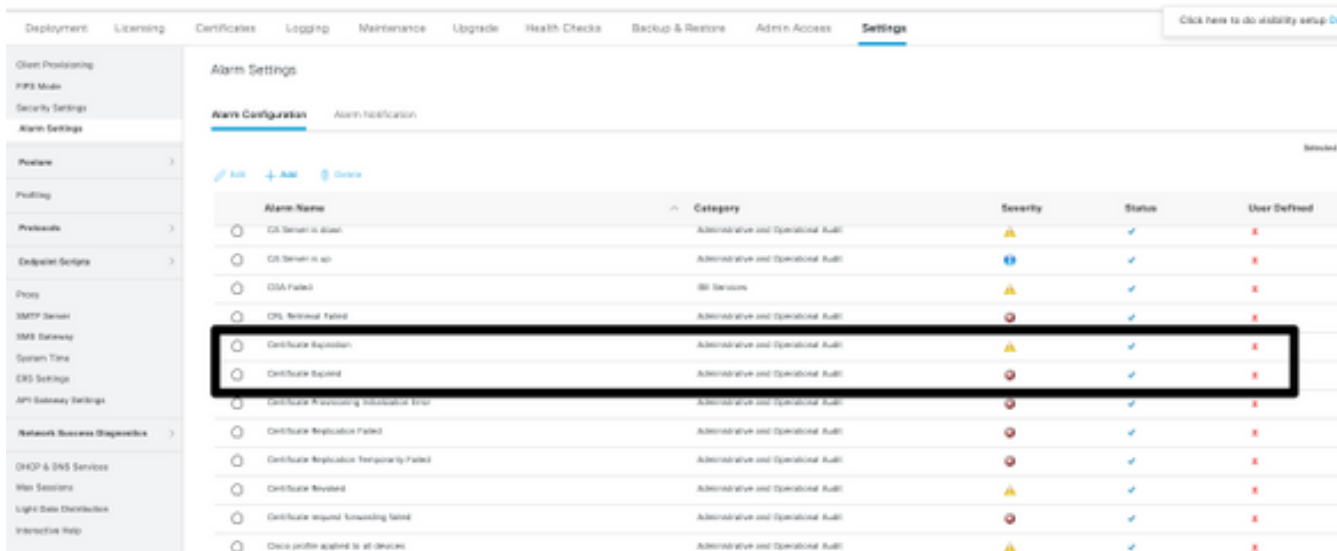
(Administration > System > Admin-Zugriff > Administratoren > Admin-Benutzer).

Aktivieren Sie das Kontrollkästchen **Include system alarms in emails** (Systemalarme in E-Mails einbeziehen) für Admin-Benutzer, die Alarmbenachrichtigungen erhalten sollen. Die E-Mail-Adresse des Absenders der Alarmbenachrichtigungen ist `ise@hostname` und kann nicht geändert werden.



- Konfigurieren Sie die ISE-Alarmeinstellungen, um Benutzer zu benachrichtigen:

Navigieren Sie zu **Administration > System > Settings > Alarm Settings > Alarm Configuration** (Administration > System > Einstellungen > Alarmeinstellungen > Alarmkonfiguration), wie in dieser Abbildung dargestellt.



Anmerkung: Deaktivieren Sie den Status für eine Kategorie, wenn Sie Alarme aus dieser Kategorie verhindern möchten. Wählen Sie „Certificate Expiration“ (Zertifikatsablauf) aus, klicken Sie dann auf **Alarm Notification** (Alarmbenachrichtigung), geben Sie die E-Mail-Adressen der Benutzer ein, die benachrichtigt werden sollen, und speichern Sie die Konfigurationsänderung. Änderungen können bis zu 15 Minuten dauern, bevor sie aktiv sind.

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

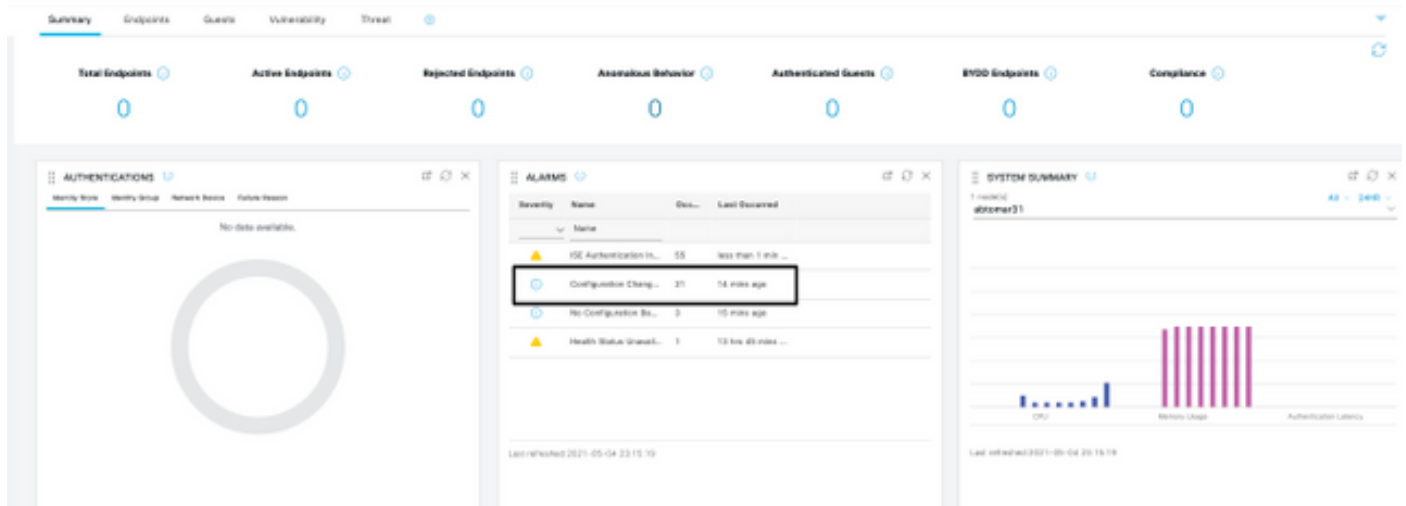
Notes in Email (0 to 4000 characters)

Überprüfung

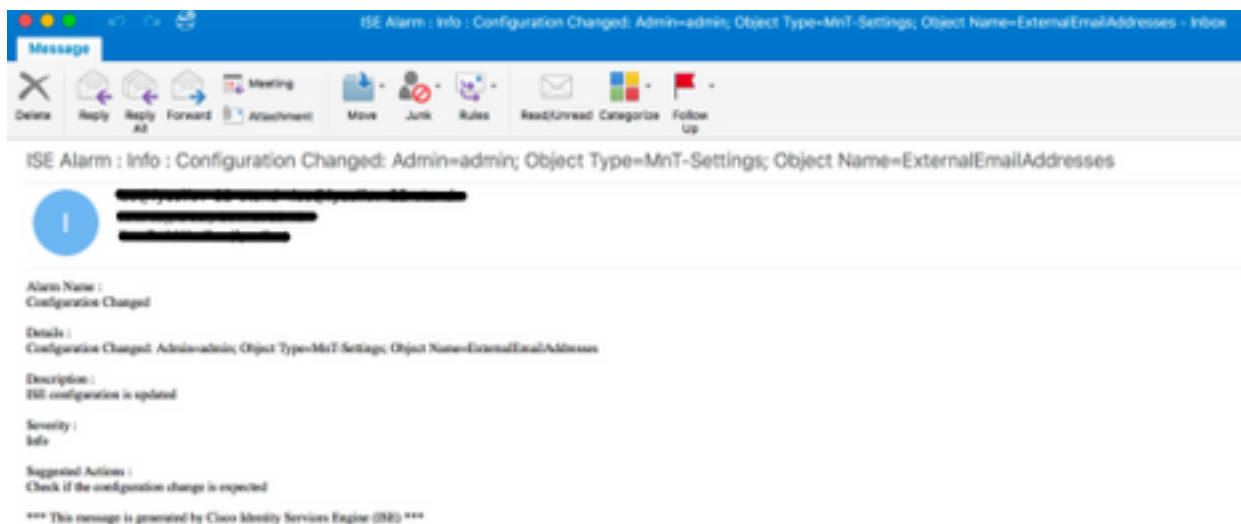
Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Warnsystem verifizieren

Überprüfen Sie, ob das Warnsystem ordnungsgemäß funktioniert. In diesem Beispiel generiert eine Konfigurationsänderung eine Warnung mit dem Schweregrad „Information“. (Ein Informationsalarm ist der niedrigste Schweregrad, während ein Zertifikatsablauf eine Warnung mit einem höheren Schweregrad generiert.)



Hier ein Beispiel für den E-Mail-Alarm, der von der ISE gesendet wird:



Zertifikatsänderung verifizieren

In diesem Verfahren wird beschrieben, wie Sie überprüfen, ob das Zertifikat richtig installiert ist, und wie Sie die EAP- und/oder Admin-Rollen ändern:

1. Navigieren Sie in der ISE-Konsole zu **Administration > Certificates > System Certificates** (Administration > Zertifikate > Systemzertifikate) und wählen Sie das neue Zertifikat aus, um die Details anzuzeigen.

Vorsicht: Wenn Sie „Admin Usage“ (Admin-Nutzung) aktivieren, wird der ISE-Service neu gestartet, was zu Serverausfällen führt.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration - System'. The main menu has 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', and 'Upgrade'. The 'Certificates' section is active, showing 'Certificate Management' and 'Certificate Authority' options. The 'Issuer' details for 'AdminISE' are displayed, including fields for 'Friendly Name', 'Description', 'Subject', 'Subject Alternative Name (SAN)', 'Issuer', 'Valid From', 'Valid To (Expiration)', 'Serial Number', 'Signature Algorithm', 'Key Length', and 'Certificate Policies'. A 'Usage' section at the bottom lists various services with checkboxes, where 'Admin' is checked.

2. Um den Zertifikatsstatus auf dem ISE-Server zu überprüfen, geben Sie folgenden Befehl in die CLI ein:

```
CLI:> show application status ise
```

3. Sobald alle Services aktiv sind, versuchen Sie, sich als Administrator anzumelden.

4. Für ein verteiltes Bereitstellungsszenario navigieren Sie zu **Administration > System > Deployment**. Überprüfen Sie, ob der Knoten über ein grünes Symbol verfügt. Platzieren Sie den Cursor über das Symbol, um zu überprüfen, ob die Legende "Verbunden" anzeigt.

5. Überprüfen Sie, ob die Endbenutzerauthentifizierung erfolgreich ist. Navigieren Sie dazu zu **Operations > RADIUS > Livelogs (Vorgänge > RADIUS > Livelogs)**. Sie können einen bestimmten Authentifizierungsversuch finden und überprüfen, ob diese Versuche erfolgreich authentifiziert wurden.

Zertifikat verifizieren

Wenn Sie das Zertifikat extern überprüfen möchten, können Sie die eingebetteten Microsoft Windows-Tools oder das OpenSSL-Toolkit verwenden.

OpenSSL ist eine Open-Source-Implementierung des SSL-Protokolls (Secure Sockets Layer). Wenn die Zertifikate Ihre eigene private CA verwenden, müssen Sie Ihr Root-CA-Zertifikat auf einem lokalen Computer ablegen und die OpenSSL-Option `-CApath` verwenden. Wenn Sie über eine Zwischenzertifizierungsstelle verfügen, müssen Sie diese ebenfalls im selben Verzeichnis

ablegen.

Um allgemeine Informationen zum Zertifikat abzurufen und zu verifizieren, verwenden Sie:

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

Es kann auch nützlich sein, die Zertifikate mit dem OpenSSL-Toolkit zu konvertieren:

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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Diagnoseinformationen verfügbar.

Schlussfolgerung

Da Sie ein neues Zertifikat auf der ISE installieren können, bevor es aktiv ist, empfiehlt Cisco, das neue Zertifikat zu installieren, bevor das alte Zertifikat abläuft. Dieser Überschneidungszeitraum zwischen dem Ablaufdatum des alten Zertifikats und dem Startdatum des neuen Zertifikats gibt Ihnen Zeit, Zertifikate zu verlängern und ihre Installation ohne oder mit nur geringen Ausfallzeiten zu planen. Sobald das neue Zertifikat seinen gültigen Datumsbereich erreicht hat, aktivieren Sie EAP und/oder Admin. Denken Sie daran: Wenn Sie die Admin-Nutzung aktivieren, wird der Service neu gestartet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.